eHealth
elektronické zdravotníctvo

eSO1
eHealth služby občanom

TVORÍME VEDOMOSTNÚ SPOLOČNOSŤ

CPS - pravidlá pre výkon certifikačných činností

Elektronické služby zdravotníctva

kód ITMS projektu: **2110120009**

Projekt je spolufinancovaný Európskou úniou
Európsky fond regionálneho rozvoja
www.informatizacia.sk
www.opis.gov.sk

Contents

1. ÚVOD

Tento dokument definuje pravidlá na výkon certifikačných činností certifikačnej autority Národného zdravotníckeho informačného systému (ďalej aj „CA NZIS“) pre použitie na vydávanie certifikátov zdravotníckym profesionálom určených na používanie v rámci Národného zdravotníckeho informačného systému (NZIS). Pravidlá na výkon certifikačných činností (ďalej aj „CPS“) vychádzajú z ustanovení platného certifikačného poriadku CA NZIS.

Tieto CPS obsahujú postupy vykonávania certifikačných služieb zo strany CA NZIS pri vydávaní certifikátov oprávneným osobám. Štruktúra CPS je plne v súlade s požiadavkami RFC 3647 „Internet X.509 Public Key Infrastructure Certificate Policy and Certification Practices Framework“.

V dokumente sú používané technické pojmy spojené s technológiou PKI. Ak sa chcete oboznámiť s použitou terminológiu, dôrazne odporúčame, aby ste si prečítali časti dokumentu, kde sú vysvetlené skratky a uvedené potrebné definície, skôr ako budete pokračovať v čítaní dokumentu.

1.1. Prehľad

Pri odvolávaní sa na tento dokument môžu byť použité pojmy "CPS", "Pravidlá" alebo „CPS CA NZIS“.

CPS sú určené na použitie v určitých situáciách a identifikujú konkrétne úlohy a zodpovednosti pre:

- CA NZIS pri poskytovaní certifikačných služieb,
- registračné autority (RA),
- personalizačné pracovisko,
- držiteľov certifikátov a
- spoliehajúce sa strany,

pričom všetky povinnosti sú v ňom popísané.

1.2. Identifikácia

OID tohto poriadku je registrovaný pod ISO a je {ISO assigned OIDs (1) ISO Identified Organization (3) Identification number of economic subject (IČO) (158) Národné centrum zdravotníckych informácií (00165387) CA NZIS (1) CPS CA NZIS (2)

Tieto Pravidlá identifikujú konkrétne úlohy pre CA NZIS, registračné autority, osoby zodpovedná za úložisko, držiteľov certifikátov a spoliehajúce sa strany.

1.3. Účastníci PKI

Tieto CPS sú pripravené tak, aby spĺňali všeobecné požiadavky na certifikát verejného kľúča v zmysle Zákona č. 215/2002 Z. z. o elektronickom podpise v aktuálnom znení a požiadavky RFC 3647.

Prehľad účastníkov PKI, ktorý je súčasťou NZIS je podrobne popísaný v časti 1.3. CP CA NZIS.

1.4. Používanie certifikátu

1.4.1. Povolené používanie

Certifikáty vydávané CA NZIS je možné používať len na prístup účastníkov k informáciám v NZIS a k podpisovaniu odosielaných resp. ukladaných informácií v rámci NZIS, pre technologické zariadenia NZIS a prístup obsluhy NZIS.

1.4.2. Obmedzenie používania

Certifikáty nie je možné používať na iné účely mimo NZIS.

1.5. Správa politík

1.5.1. Organizácia zodpovedná za správu CPS

Za správu (vypracovanie, udržiavanie, aktualizáciu) týchto Pravidiel je zodpovedný:

Národné centrum zdravotníckych informácií

Lazaretská 26

811 09 Bratislava 1

e-mail: nczisk@nczisk.sk

tel. číslo: 02 57 269 111

1.5.2. Kontaktná osoba

Kontaktnou osobou zodpovednou za obsah, udržiavanie a aktualizáciu CPS CA NZIS je:

Roman Tarina

e-mail: roman.tarina@nczisk.sk

tel.číslo: 02 57 269 111

1.6. Definície a skratky

CA	-	Certifikačná autorita (Certificate Authority)
NCZI	-	Národné centrum zdravotníckych informácií
NZIS	-	Národný zdravotný informačný systém
CP	-	Certifikačný poriadok
RFC	-	Request for Comment
PKI	-	Infraštruktúra verejného kľúča (Public Key Infrastructure!)
RA	-	Registračná autorita (Registration Authority)
PMA	-	Autorita na správu politík (Policy Management Authority)
OID	-	Objektový identifikátor (Object Identifier)
ISO	-	Medzinárodná štandardizačná organizácie (International Standard Organization)
CPS	-	Pravidlá na výkon certifikačných činností (Certificate Practice Statement)
OCSP	-	Služba okamžitého poskytovania informácie o stave certifikátu (Online Certificate Status Protocol)
CN	-	Meno subjektu (Common Name)
CRL	-	Zoznam zrušených certifikátov (Certificate Revocation List)
PIN	-	Osobné identifikačné číslo (Personal Identification Number)
ARL	-	Zoznam revokovaných autorít (Authority Revocation List)
RSA	-	Kryptografický algoritmus pomenovaný podľa tvorcov (Rivest, Shamir, Adleman)
FIPS	-	USA štandard z oblasti informačnej bezpečnosti (Federal Information Processing Standards)

SHA	-	Kryptografická funkcia na vytváranie odtlačkov (hash) elektronických informácií (Secure Hash Algorithm)
HSM	-	Hardvérový bezpečnostný modul (hardware Security Module)
PKCS	-	Kryptografické štandardy pre PKI (Public Key Cryptography Standards)
URL	-	Uniform Resource Locator
ePZP	-	Elektronický preukaz zdravotníckeho pracovníka
CMS	-	Systém manažovania kariet (Card Management System)
JRÚZ		Jednotná referenčná údajová základňa

2. Zverejňovanie informácií a úložisko

2.1. Úložisko

Úložisko CA NZIS je prevádzkované Národným centrom zdravotníckych informácií (pozri časť 1.5.1) a tvorí ho webová stránka dostupná na adrese http://www.nczisk.sk – Certifikačná autorita NZIS.

2.2. Publikovanie informácií o certifikátoch

Vydávajúca CA NZIS:

- uvádza v každom vydanom certifikáte URL webovej stránky ňou vedenej resp. vedenej v jej mene,
- publikuje aktuálny zoznam zrušených certifikátov (CRL) pre všetky vydávajúce CA (koreňová CA, podriadené CA) na URL adrese, ktorá je uvedená v každom vydanom certifikáte,
- poskytne plnú textovú verziu CPS ak je to potrebné pre účely akéhokoľvek auditu, kontroly alebo akreditácie,

2.3. Čas a frekvencia zverejňovania informácií

Všetky informácie sú zverejnené v úložisku ihneď ako je taká informácia k dispozícii CA NZIS.

2.4. Kontroly prístupu k úložisku

CA NZIS zodpovedajúcimi prostriedkami chráni ľubovoľnú informáciu uloženú v úložisku, ktorá nie je určená na verejné rozširovanie. CA NZIS vynaloží maximálne úsilie na to, aby zaistila integritu, dôvernosť a dostupnosť dát vyplývajúcich s poskytovaním certifikačných služieb. Taktiež sú vykonané

logické a bezpečnostné opatrenia, ktoré zabránia neautorizovanému prístupu osobám, ktoré by mohli akýmkoľvek spôsobom zmeniť, poškodiť, pridať resp. vymazať údaje uložené v repozitári.

3. Identifikácia a autentizácia

V tejto časti Pravidiel sú podrobnejšie popísané postupy, ktoré CA NZIS používa na overenie identity a/alebo iných atribútov žiadateľa o vydanie certifikátu.

Tiež popisuje, ako sú overované strany pokiaľ požadujú opakované vydanie certifikátu resp. zrušenie certifikátu.

3.1. Pomenovanie

3.1.1. Typy mien

CA NZIS vytvára certifikáty, ktoré obsahujú rozlišovacie mená v zmysle *X.500* (*X.500 Distinguished Name*, ďalej ako „rozlišovacie meno“). Každý držiteľ, pre ktorého je vydávaný certifikát, má jasne rozoznateľný a jedinečný X.501 rozlišujúce názov (DN) v poli *Subject Name*. DN je vo formáte *X.501 printable String* a nesmie to byť prázdny reťazec.

3.1.2. Potreba zmysluplnosti mien

Obsah poľa obsahujúci meno držiteľa (CN) pozostáva v prípade fyzických osôb výhradne z kombinácia mena a priezviska držiteľa.

3.1.3. Jedinečnosť mien

V prípade vydávania certifikátov pre potreby NZIS nie je garantovaná jedinečnosť mien v rámci komunity držiteľov certifikátov v položke CN. Je však garantované jedinečnosť sériového čísla (Serial number) každého vydaného certifikátu, tzn. je garantované, že neexistujú a nikdy nebudú existovať žiadne dva vydané certifikáty, ktoré by mali rovnaké sériové číslo a rovnako ďalšie položky v DN ako sú registračné číslo zdravotníckeho pracovníka a sériové číslo elektronického preukazu zdravotníckeho pracovníka.

3.2. Prvotné overenie identity

3.2.1. Spôsob preukazovania vlastníctvo súkromného kľúča

Vzhľadom k tomu, že generovanie súkromného kľúča je vykonávané CA NZIS priamo na čipovú kartu v procese jej personalizácie, žiadateľa nepreukazuje jeho vlastníctvo.

3.2.2. Overenie identity organizácie

Certifikáty pre organizácie nebudú vydávané.

3.2.3. Overenie identity fyzickej osoby

Identita fyzickej osoby sa overuje prostredníctvom zaslanej vyplnenej žiadosti o vydanie certifikátu v listinnej podobe, ktorá obsahuje všetky potrebné osobné údaje žiadateľa. Žiadosť obsahuje klauzulu o úplnosti a správnosti údajov a žiadosť je vlastnoručne podpísaná žiadateľom.

3.2.4. Overovanie právomocí

V rámci overovania právomocí pracovník RA NCZI vykoná formálnu kontrolu, či existujú záznamy o žiadateľovi v Registri zdravotníckych pracovníkov v JRUZ.

3.2.5. Kritériá pre interoperabilitu

Nie sú definované žiadne podmienky.

3.3. Identifikácia a autentizácia pri obnove certifikátu

Vzhľadom na totožnú dobu platnosti čipovej karty a certifikátov, ktoré sú na nej uložené, nie je nevyhnutné zabezpečiť vydávanie následných certifikátov (bez výmeny čipovej karty).

Získanie následnej čipovej karty, bude po procesnej stránke rovnaké ako úvodné získanie čipovej karty. Rozdiel spočíva v skutočnosti, že existujúci držitelia čipových kariet, ktorých platnosť sa blíži ku koncu, budú na túto skutočnosť vopred upozornení.

3.3.1. Obnova certifikátu

Obnova certifikátu po jeho exspirácii znamená vydanie novej čipovej karty s novými kľúčmi a novým certifikátom a postup je totožný s postupom zavedeným pre prvotné vydanie certifikátu.

3.3.2. Obnova certifikátu po jeho zrušení

Obnova certifikátu po jeho zrušení znamená vydanie novej čipovej karty s novými kľúčmi a novým certifikátom a postup je totožný s postupom zavedeným pre prvotné vydanie certifikátu.

3.3.3. Identifikácia a autentifikácia žiadosti o zrušenie certifikátu

Držiteľ čipovej karty alebo certifikátu je povinný zrušiť platnosť karty a certifikátov vo viacerých situáciách. V závislosti od potenciálneho rizika zneužitia karty alebo certifikátu inou osobou ich možno rozdeliť na rizikové a bezpečné.

Identifikácia držiteľa žiadajúceho o zrušenie certifikátu sa vykonáva:

- Osobne na registračnej autorite predložením občianskeho preukazu
- Držiteľ certifikátu (telefonicky) kontaktuje pracovníka registračnej autority CA NZIS a požiada o zrušenie platnosti karty. Pracovník RA CA NZIS preverí základné údaje o žiadateľovi spojené so zodpovedaním bezpečnostných otázok zadaných žiadateľom pri aktivácii karty.

4. Prevádzkové požiadavky

4.1. Žiadanie o certifikát

V procese žiadania o certifikát vystupujú nasledovný účastníci: žiadateľ, pracovníci certifikačnej autority.

4.1.1. Žiadatelia o certifikát

Žiadateľom o kartu a certifikáty môže byť fyzická osoba, ktorá je evidovaná ako zdravotnícky pracovník v JRÚZ. Žiadateľom o technologické certifikáty môže byť fyzická osoba, ktorá je evidovaná ako pracovník NCZI. Žiadateľom o certifikáty obsluhy NZIS môže byť fyzická osoba, ktorá je evidovaná ako pracovník NCZI, alebo pracovník zmluvne pracujúci pre NCZI.

4.1.2. Postup žiadania a zodpovednosti

4.1.2.1. Vyplnenie žiadosti

Žiadateľ vyplní žiadosť prostredníctvom aplikácie ISZI. Súčasťou žiadosti sú minimálne:

Identifikačné údaje:

meno a priezvisko a rodné priezvisko zdravotníckeho pracovníka,

dátum narodenia,

rodné číslo,

príslušnosť ku komore a registračné číslo komore prislúchajúce k zdravotníckemu povolaniu.

Kontaktné údaje:

telefónne číslo,

adresa trvalého pobytu,

adresa na doručenie písomností

adresa elektronickej pošty.

Vyplnením žiadosti sa zároveň vygenerujú dokumenty ZMLUVA s prílohami ŽIADOSŤ, PREBERACÍ-PROTOKOL a ZOZNAM CERTFIKÁTOV.

Po obdržaní vygenerovanej žiadosti je žiadateľ povinný potvrdiť úplnosť a správnosť údajov svojim podpisom.

4.1.2.2. Vyplnenie žiadosti o technologický certifikát

Žiadateľ vygeneruje kryptografické kľúče a CSR vo formáte PKCS#10, tiež vyplní žiadosť o technologický certifikát NZIS v súlade so schváleným procesom v dizajne diela.

Žiadosť o technologický certifikát schváli vedúci odboru správy aplikácií NCZI alebo vedúci odboru informačnej bezpečnosti NCZI v závislosti od citlivosti certifikátu.

So schválenou žiadosťou žiadateľ požiada bezpečnostného správcu technologickej certifikačnej autority NCZI v roli RA-PKI-TC o vydanie technologického certifikátu.

4.2. Spracovanie žiadosti o certifikát

4.2.1. Overenie žiadosti

Pracovník registračnej autority v roli RA-ZIADOSTI z doručenej žiadosti v listinnej podobe prostredníctvom webového rozhrania CMS_ADMIN skontroluje, či údaje v žiadosti korešpondujú s údajmi v CMS.

Rovnako overí, či je žiadateľ držiteľom už existujúceho platného ePZP.

Ak žiadateľ už platným ePZP disponuje, musí uviesť dôvod, prečo žiada o nové ePZP. Žiadateľ smie získať najviac jeden ePZP za deň (pre jedno povolanie).

Pri prvotnom vydaní sú vzniknuté situácie riešené nasledovne:

- Ak žiadateľ nie je evidovaný v JRÚZ v roli zdravotníckeho pracovníka, žiadosť sa zamieta; žiadateľ musí požiadať komoru o zaradenie do jej registra zdravotníckych pracovníkov, ktorý sa následne prenáša do JRÚZ.
- Ak je žiadateľ evidovaný v JRUZ, ale neexistuje k nemu MIZPr (z akýchkoľvek dôvodov) žiadosť sa zamieta a žiadateľ musí požiadať o priradenie MIZPr v zmysle procesov platných pre spracovanie údajov JRÚZ.
- Ak žiadosť obsahuje údaje v rozpore s JRÚZ databázou, musí žiadateľ požiadať o úpravu údajov v zmysle procesov platných pre spracovanie údajov JRÚZ. Žiadosť sa zamieta.
- Ak sa údaje na žiadosti zhodujú s údajmi v JRÚZ, pracovník v roli RA-ZIADOSTI eviduje požiadavku na personalizáciu karty prostredníctvom webového rozhrania CMS_ADMIN.
- V prípade zamietnutia žiadosti pracovník RA informuje žiadateľa o zamietnutí žiadosti. Rovnako informuje o tejto skutočnosti príslušnú profesnú komoru.

4.2.1.1. Overenie žiadosti o technologický certifikát

Vedúci odboru správy aplikácií NCZI alebo vedúci odboru informačnej bezpečnosti NCZI v závislosti od citlivosti certifikátu overí identitu žiadateľa a jeho oprávnenie žiadať o technologický certifikát.

4.2.2. Spôsob overenia identity a autenticity žiadateľa

Vyššie uvedené overenie žiadosti o certifikát sa z pohľadu CA NZIS považuje za overenie identity a autenticity budúceho držiteľa certifikátu.

4.2.3. Schválenie alebo zamietnutie žiadosti

Pokiaľ je overenie žiadosti uvedené v časti 4.2.1 úspešné bude žiadosť postúpená na personalizačné pracovisko, ktoré zabezpečí vydanie certifikátu zo strany CA NZIS.

4.2.4. Spracovanie žiadosti o vydanie certifikátu

Pracovník CA v roli RA-ŽIADOSTI po pozitívnom overení vytlačí dokumenty ZMLUVA s prílohami ŽIADOSŤ, PREBERACÍ-PROTOKOL a zažiada o vydanie ePZP.

Pracovník CA v roli RA-KARTY pomocou tučného CMS klienta a CMS_ADMIN personalizuje ePZP.

Výstupom procesu personalizácie je dávka ktorá obsahuje:

Fyzicky personalizované (potlačené) čipové karty. Karta obsahuje X.509 certifikáty a prislúchajúce kryptografické kľúče. Po personalizácii je karta zablokovaná a na jej aktiváciu je nevyhnutný prístup k CMS a aktivačný kód.

4.2.4.1. Spracovanie žiadosti o vydanie technologického certifikátu

Žiadateľ uloží žiadosť do chráneného úložiska datového centra vo formáte PKCS#10 a iniciuje prostredníctvom elektronickej pošty na adresu prodtechca@nczisk.sk proces vydania TC.

Pracovník RA-PKI-TC skontroluje CSR. V prípade písomnej žiadosti skontroluje podpis na žiadosti a overí identitu žiadateľa voči údajom na žiadosti.

Ak sa jedná o špeciálny TC alebo žiadosť obsahuje CSR, pracovník v roli RA-PKI-TC skontroluje, že CSR uvedené v žiadosti sa zhoduje s CSR.

Systém skontroluje platnosť CSR po technickej stránke (súlad s PKCS#10) a vypíše jednotlivé časti mena v žiadosti o certifikát.

Pracovník CA v roli RA-PKI-TC overí platnosť mena (súlad so žiadosťou) a prípadne opraví komponenty mena (CN alebo Serial Number) tak, aby boli v súlade so žiadosťou.

4.3. Vydanie certifikátu

4.3.1. Činnosť CA NZIS pri vydaní certifikátu

Po úspešnom overení žiadosti pracovník personalizačného pracoviska iniciuje proces personalizácie ePZP. Súčasťou personalizácie ePZP je aj samotné vygenerovanie kryptografických kľúčov a on-line vydanie certifikátov certifikačnou autoritou CA NZIS a ich uloženie na ePZP. Po personalizácii je ePZP zablokovaná a na jej aktiváciu je nevyhnutný prístup k CMS a aktivačný kód.

4.3.1.1. Činnosť TechCA NZIS pri vydaní certifikátu

Ak v predošlom kroku neprišlo k nezhode (tzn. meno: DN v CSR je totožné s menom na žiadosti a CSR je validné), pracovník RA-PKI-TC vydá TC.

4.4. Prevzatie certifikátu

4.4.1. Spôsob prevzatia certifikátu

Držiteľ prevezme certifikáty na karte osobne v priestoroch RA/CA NZIS. Pracovník v roli RA-AKTIV overí identitu žiadateľa voči preukazu totožnosti a žiadosti. Ak je výsledok kontroly pozitívny, RA-AKTIV vytlačí ZOZNAM CERTIFIKÁTOV a odovzdá ePZP žiadateľovi. Následne si žiadateľ prostredníctvom NB-AKTIVÁCIA za podpory pracovníka v roli RA-AKTIV zaktivuje ePZP a skontroluje a podpíše ZOZNAM CERTIFIKÁTOV. Pracovník v roli RA-AKTIV zároveň poučí žiadateľa o základných

povinnostiach pri práci s ePZP. Žiadateľ zároveň podpíše ZMLUVU, ŽIADOSŤ a PREBERACÍ PROTOKOL.

4.4.1.1. Spôsob prevzatia technologického certifikátu

Pracovník CA v roli RA-PKI-TC uloží vydaný TC do chráneného úložiska v datovom centre.

4.4.2. Publikovanie certifikátu

Certifikáty nie sú publikované.

4.4.3. Kľúčový pár a používanie certifikátu

Pozri časť 4.5.1 aktuálneho CP CA NZIS.

4.5. Obnova certifikátu na pôvodné kľúče

Obnovu certifikátu na pôvodný kľúč CA NZIS nepodporuje.

4.6. Obnova certifikátu na nové kľúče

CA NZIS nevykonáva obnovu certifikátov na čipovej karte vzhľadom k skutočnosti, že platnosť vydaného certifikátu a aj samotnej čipovej karty sú rovnaké. Obnova certifikátu pre oprávneného držiteľa je vykonávaná spôsobom, ktorý je totožný zo získaním pôvodného (pozri časť 4).

4.6.1. Okolnosti obnovy certifikátu na nové kľúče

Obnova certifikátu s vygenerovaním nového kľúčového páru uskutočňuje RA CA NZIS v prípade:

- jeho exspirácie,
- jeho zrušenia na základe kompromitácie súkromného kľúča resp. iných okolností vedúcich k jeho zrušeniu.

4.6.2. Kto môže žiadať o obnovu certifikátu na nové kľúče

Pozri časť 4.7.2 CP CA NZIS.

4.7. Zmena údajov v certifikáte

V prípade, že u držiteľa dôjde z akéhokoľvek dôvodu k zmene údajov, ktoré sú uvedené v certifikáte (napr. zmena priezviska pri vydaji) a tieto sa týmto stanú neaktuálne, je potrebné požiadať o vydanie certifikátu s platnými údajmi. Vydanie nového certifikátu sa vykoná rovnako, ako v prípade vydanie pôvodného certifikátu (pozri časť 4.).

4.8. Zrušenie certifikátu

4.8.1. Okolnosti zrušenia certifikátu

Okolnosti zrušenia certifikátu, oprávnené osoby, ktoré môžu žiadať o zrušenie a možné spôsoby zrušenia sú popísané v časti 4.9. CP CA NZIS.

4.8.2. Procedúra žiadosti o zrušenie certifikátu

4.8.2.1. Zrušenie platnosti certifikátu iniciované držiteľom karty offline

Pod offline spôsobom sa rozumie kontakt držiteľa certifikátu s RA bez možnosti využitia CMS. Držiteľ certifikátu telefonicky kontaktuje pracovníka RA CA NZIS v roli HelpDesk a požiada o zrušenie platnosti certifikátu, pričom sa musí identifikovať prostredníctvom jedného z nasledovných údajov:

- JRÚZ identifikátor ZPr,
- priezvisko, rodné priezvisko a dátum narodenia
- rodné číslo,
- MIZPr,
- sériové číslo ePZP.

Pracovník RA autentifikuje zdravotníckeho pracovníka prostredníctvom sekundárneho mechanizmu (bezpečnostné otázky) a ak je autentifikácia úspešná, iniciuje zrušenie certifikátu zo strany CA NZIS. CA NZIS o zrušení certifikátu informuje žiadateľa notifikačným e-mailom na adresu, ktorá bola držiteľom zadaná v procese žiadosti. Po zrušení certifikátu je okamžite vydaný zo strany CA NZIS nový zoznam zrušených certifikátov (CRL).

4.8.2.2. Zrušenie platnosti certifikátu iniciované držiteľom karty osobne na CA/RA

Držiteľ certifikátu osobne navštívi pracovisko registračnej autority CA NZIS a požiada o zrušenie platnosti certifikátu, pričom sa musí identifikovať prostredníctvom identifikačného dokladu (občiansky preukaz, pas). Pracovník RA autentifikuje zdravotníckeho pracovníka na základe predloženého identifikačného dokladu a zároveň vykoná overenie existencie držiteľa voči údajom nachádzajúcim sa v JRÚZ. V prípade zhody požiada CA NZIS o zrušenie certifikátu. Držiteľ zároveň vyplní žiadosť o zrušenie, ktorá sa archivuje v archíve NCZI.

CA NZIS o zrušení certifikátu informuje žiadateľa notifikačným e-mailom na adresu, ktorá bola držiteľom zadaná v procese registrácie. Po zrušení certifikátu je okamžite vydaný zo strany CA NZIS nový zoznam zrušených certifikátov (CRL).

4.8.2.3. **Zrušenie platnosti technologického certifikátu**

K zrušeniu platnosti TC dochádza inicializovaním cez adresu prodtechca@nczisk.sk v prípade:

- vydania nového certifikátu,
- zmeny v údajoch certikátu,
- inciovania pracovníkom RA CA NZIS alebo pracovníkom v zmluvnom vzťahu s NCZI.

4.8.3. Lehota na zaslanie žiadosti o zrušenie certifikátu

Držiteľ certifikátu musí požiadať o jeho zrušenie okamžite, ako nastane niektorá zo skutočnosti uvedená v časti 4.9.1 CP CA NZIS.

4.8.4. Čas na zrušenie certifikátu

CA NZIS zrušiť certifikát čo najskôr po prevzatí žiadosti o jeho zrušenie za podmienky, že boli splnené zo strany držiteľa resp. inej oprávnenej osoby všetky náležitosti týkajúce sa žiadosti o zrušenie certifikátu..

4.8.5. Povinnosti overovania stavu certifikátu zo strany spoliehajúcich sa strán

Žiadne ustanovenia.

4.8.6. Frekvencia zverejňovania CRL

CA NZIS publikuje zoznam zrušených certifikátov (CRL) minimálne 1 krát za 24 hodín aj v prípade, že nebol v tomto čase zrušený žiadny certifikát. CRL je publikovaný prostredníctvom úložiska (pozri čas. 2.1).

4.8.7. Čas zverejnenia vydaného CRL

Vydaný zoznam zrušených certifikátov je publikovaný v úložisku bezodkladne, pričom čas od vydania CRL do jeho publikovania v úložisku neprekročí 120 sekúnd.

4.8.8. Overovanie stavu certifikátu prostredníctvom OCSP

Po zrušení certifikátu je okamžite zaznamenaná zmena jeho stavu v repozitári slúžiacom pre potreby overenia aktuálneho stavu certifikátu prostredníctvom služby potvrdzovania existencie a platnosti certifikátu OCSP.

4.8.9. Požiadavky na overenie stavu certifikátu prostredníctvom OCSP

Žiadne ustanovenia.

4.8.10. Pozastavenie platnosti certifikátu

Žiadne ustanovenia.

4.9. Služby overovania stavu certifikátu

Pozri časť 4.10. CP CA NZIS.

4.10. Ukončenie zmluvného vzťahu

Žiadne ustanovenia

4.11. Obnova kľúčov z depozitu alebo zálohy

CA NZIS neuchováva súkromné kľúče držiteľov certifikátov.

5. Manažérske, prevádzkové a fyzické bezpečnostné opatrenia

5.1. Fyzické bezpečnostné opatrenia

5.1.1. Umiestnenie, priestory a prístup

Infraštruktúra CA NZIS je umiestnená v priestoroch, ktoré sú nepretržite fyzicky a elektronický monitorované proti neoprávnenému vniknutiu.

Samostatný prístup k vyhradeným priestorom CA (miestnosť serverov) majú len osoby, ktoré sú uvedené na zozname oprávnených osôb s právom prístupu.

Ostatné osoby môžu vstupovať do vyhradených priestorov len pod dozorom oprávnenej osoby. O každom vstupe do vyhradených priestorov sú vykonávané záznamy, ktoré sú pravidelne kontrolované zo strany bezpečnostného správcu.

Pracovisko RA a personalizačné pracovisko, ktoré on-line komunikujú s CA NZIS sú umiestnené v priestoroch:

- ktoré sú nepretržite fyzický alebo elektronicky monitorované proti neoprávnenému vniknutiu,
- kde je umožnený prístup len osobám na zozname oprávnených osôb,
- kde prístup iných osôb je umožnený len v sprievode v sprievode a pod dohľadom oprávnenej osoby,
- kde všetky vymeniteľné médiá a dokumenty obsahujúce citlivé informácie sú uložené v priestore zabezpečenom podľa FOB NCZI.

Certifikáty pracovníkov RA umožňujúce komunikáciu s CA NZCI, sú umiestnené na bezpečnom hardvérovom zariadení a sú fyzicky chránené samotnými držiteľmi, pracovníkmi RA.

5.1.2. Dodávka energie a klimatizácia

CA NZIS ma zabezpečený zdroj elektrickej energie a klimatizáciu priestorov s infraštruktúrou CA, ktorá je postačujúca k bezproblémovému chodu celého systému CA.

5.1.3. Ohrozenie vodou

Infraštruktúra CA NZIS je chránená pred ohrozením vodou.

5.1.4. Protipožiarna ochrana

Infraštruktúra CA NZIS je chránená protipožiarnym systémom.

5.1.5. Uchovávanie médií

CA NZIS uchováva média používané v systéme CA tak, že sú chránené pred nepriaznivými účinkami okolitého prostredia ako sú teplota, vlhkosť a elektromagnetické žiarenie. Záložné kópie sú uchovávané v oddelených priestoroch chránených pred zničením požiarom resp. vodou, ktoré sa nachádzajú dátovom centre.

5.1.6. Nakladanie s odpadom

Všetky média používané na uchovávanie informácií ako sú kľúče, aktivačné údaje alebo súbory CA sú pred vyhodením do odpadu odstránené a/alebo fyzicky zničené.

5.1.7. Záložné pracovisko

CA NZIS neprevádzkuje záložné pracovisko.

5.2. Procedurálne bezpečnostné opatrenia

5.2.1. Dôveryhodné roly

5.2.1.1. Dôveryhodné roly CA

CA NZIS má definované nasledovné roly v rámci PKI:

Systémový administrátor:

Vykonáva najmä konfiguráciu a údržbu hardvéru a softvéru systému CA vrátane ich inštalovania, spúšťanie a ukončovanie služieb CA, update a upgrade OS a aplikácií, riadi zálohovanie používaných OS a ich aktuálnych konfiguračných súborov, prezerá záznamy (logy) vytvárané systémom. Všetky povinnosti systémového administrátora sú podrobne popísané v jeho menovacom dekréte.

Bezpečnostný správca:

Je zodpovedný najmä za celkovú systémovú a sieťovú bezpečnosť infraštruktúry CA NZIS, analýzu auditovacích logov, pravidelné a nepravidelné kontroly výkonu činností všetkých pracovníkov CA NZIS v zmysle definovaných smerníc, fyzickej bezpečnosti a objektovej bezpečnosti, zabezpečenia infraštruktúry CA NZIS. Dohliada na činnosť systémových administrátorov z hľadiska kontroly logov a hlásení o detekcii možných útokov a zraniteľností. Všetky povinnosti bezpečnostného správcu sú podrobne popísané v jeho menovacom dekréte.

Rola **Bezpečnostný správca** (pracovník registračnej autority) bude v rámci prevádzky IAM subsystému ďalej rozdelená nasledovne:

- **RA-ZIADOSTI**

  Typ: Prevádzková rola – registračná autorita

  Opis: Osoba zodpovedná za kontrolu a zadávanie žiadostí o ePZP. Medzi hlavné činnosti patrí: registrácia žiadosti o ePZP.

  Miesto vykonávania práce: NCZI / Personalizačné centrum

- **RA-KARTY**

  Typ: Prevádzková rola – registračná autorita

  Opis: Osoba zodpovedná za personalizáciu ePZP a rušenie platnosti ePZP.

  Miesto vykonávania práce: NCZI / Personalizačné centrum

- **RA-AKTIV**

  Typ: Prevádzková rola – registračná autorita

  Opis: Osoba zodpovedná za priamu komunikáciu s ZPr / držiteľom ePZP. Medzi hlavné činnosti patrí: overenie identity ZPr v procese odovzdania karty, asistencia pri aktivácii kariet ePZP, asistencia pri odblokovaní kariet ePZP, asistencia pri zrušení platnosti kariet ePZP.

  Miesto vykonávania práce: Výdajňa kariet

- **RA-CC**

  Typ: Prevádzková rola – registračná autorita

  Opis: Osoba zodpovedná za komunikáciu s ZPr / držiteľom ePZP prostredníctvom telefónu alebo elektronickou poštou. Medzi hlavné činnosti patrí: evidencia odblokovania ePZP / reset hesla v Active Directory a zadanie a schválenie žiadosti o zrušenie platnosti ePZP, notifikácia držiteľov ePZP o blížiacej sa exspirácii ePZP.

  Predpokladané miesto vykonávanie práce NCZI / HelpDesk

- **RA-PKI-TC**

  Typ: Prevádzková rola – registračná autorita

  Opis: Osoba zodpovedná za správu životného cyklu technologických certifikátov.

  Miesto vykonávanie práce: NCZI / prevádzka

Audítor systému:

Vykonáva najmä pravidelnú a náhodnú kontrolu činnosti všetkých pracovníkov CA NZIS v zmysle definovaných smerníc a postupov, overovanie auditných záznamov, overovanie dodržiavania súladu CP a CPS, komunikáciu zistených skutočností smerom k PMA. Všetky povinnosti interného audítora sú podrobne popísané v jeho menovacom dekréte.

Člen PMA:

Je zodpovedný najmä za správu bezpečnostnej politiky CA, správu CP a CPS, revízie výsledkov auditov zhody. Všetky povinnosti PMA sú podrobne popísané v jeho menovacom dekréte.

5.2.1.2. Dôveryhodné roly RA

CA NZIS prehlasuje, že pracovníci RA a personalizačného centra pochopili svoju zodpovednosť za identifikáciu a overovanie žiadateľov a vykonávanie nasledovných funkcií:

- prijatie žiadosti na vydanie certifikátu resp. jeho zrušenie,
- overenie identity a autenticity žiadateľa v zmysle časti 4.2,
- prenos informácie od žiadateľa do personalizačného centra a na vydanie certifikátu CA NZIS,
- odoslanie vydaného certifikátu jeho držiteľovi,
- overovanie všetkých ostatných informácií súvisiacich s vydaním certifikátu

5.2.2. Počet osôb potrebný na výkon úloh

Generovanie kľúčov CA NZIS je vykonávané za prítomnosti najmenej troch rolí CA NZIS zaradených v dôveryhodných rolách. Pracovníci môžu samostatne vykonávať všetky prevádzkové povinnosti spojené s ich rolou v CA NZIS.

CA NZIS má zavedený overovací proces, ktorý poskytne celkový prehľad všetkých aktivít vykonaných pracovníkmi v dôveryhodných rolách.

5.2.3. Identifikácia a autentizácia jednotlivých rolí

Všetky CA zamestnanci boli podrobení overeniu identity a oprávnení pred tým, ako:

- boli priradení na zoznam s oprávnením prístupu do priestorov CA,
- boli priradení na zozname s oprávnením fyzického prístupu k systému CA,
- im bol pridelený certifikát na výkon roly v rámci CA
- im bol zriadený účet v systéme CA NZIS.

Všetky účty a certifikáty (s výnimkou technologických certifikátov):

- sú priamo priradené konkrétnej fyzickej osobe,
- nie sú zdieľané,
- majú obmedzený rozsah oprávnení len na oprávnenia danej roly CA.

Všetky CA operácie sú pri prístupe cez zdieľanú sieť zabezpečené použitím silných autentifikačných mechanizmov a šifrovania s využitím hardvérových tokenov.

5.3. Personálne opatrenia

Všetci zamestnanci vykonávajúci povinnosti v súvislosti s prevádzkou CA alebo RA:

- sú písomne menovaní,
- sú viazaní zmluvou alebo štatútom k podmienkam a pravidlám pre danú pozíciu, ktoré musia plniť,
- absolvovali komplexné školenie s ohľadom na povinnosti, ktoré plnia,

- sú viazaní zákonom alebo zmluvou k mlčanlivosti o citlivých skutočnostiach týkajúcich sa CA NZIS alebo držiteľov certifikátov,

Zamestnanci nemajú pridelené povinnosti, ktoré môžu vyvolať konflikt záujmov s ich CA alebo RA povinnosťami.

5.3.1. Vzdelanie, kvalifikácia, skúsenosti a vôľové požiadavky

NCZI má definovanú personálnu a manažérsku politiku, ktorá poskytuje primeranú istotu o dôveryhodnosti a kompetentnosti svojich zamestnancov a vedie k uspokojivému plneniu ich povinností v súlade s CP a týmito CPS.

5.3.2. Postupy overovania

NCZI vykonala pred zaradením preskúmanie všetkých pracovníkov, pri ich zaradení do dôveryhodných rolí. Po zaradení je v pravidelných intervaloch overovaná ich dôveryhodnosť a kompetencia v súlade s požiadavkami CP a týchto Pravidiel, postupov personálnej práce CA alebo ekvivalentných požiadaviek.

5.3.3. Požiadavky na školenie

CA NZIS prehlasuje, že všetci zamestnanci plniaci si povinnosti v súvislosti s prevádzkou CA alebo RA absolvovali komplexné školenie v oblasti:

- bezpečnostných pravidiel a mechanizmov platných pre CA / RA,
- všetkých verzií PKI softvéru v systéme CA,
- všetkých povinnosti v rámci PKI, ktorých plnenie sa očakáva,
- postupov obnovy po havárii a postupov obnovy činnosti (business continuity).

Všetci zamestnanci CA NZIS sa následne zúčastňujú pravidelného preškoľovania na zabezpečenie aktuálnosti ich vedomostí.

5.3.4. Frekvencia preškoľovania a požiadavky

Preškoľovanie pracovníkov CA NZIS sa vykonáva podľa potreby a CA preskúmava požiadavky na preškolenie minimálne jeden krát ročne.

5.3.5. Obmena pozícií

Žiadne požiadavky

5.3.6. Sankcie za neoprávnené zásahy

V prípade reálneho alebo údajného výkonu neoprávneného zásahu osobou vykonávajúcou povinnosti v súvislosti s prevádzkou CA alebo RA, CA okamžite pozastaví jeho/jej prístup k systému CA.

5.3.7. Zamestnanci na zmluvu

Žiadne požiadavky.

5.3.8. Dokumentácia poskytovaná zamestnancom

CA NZIS sprístupnila všetkým pracovníkom CA NZIS certifikačný poriadok, pravidlá na výkon certifikačných činností a ostatné špecifické nariadenia, politiky alebo zmluvy týkajúce sa ich pozície na http://www.nczisk.sk/ – Certifikačná autorita NZIS.

5.4. Postupy zaznamenávania auditných logov

5.4.1. Typy zaznamenávaných udalostí

CA NZIS zaznamenáva do auditných log súborov všetky udalosti týkajúce sa bezpečnosti systému CA. Do tohto patria také udalosti ako:

- spustenie a vypnutie systému,
- spustenie CA aplikácie a jej vypnutie,
- pokusy o vytvorenie, vymazanie, nastavenie hesla alebo zmenu systémových nastavení všetkých rolí v rámci PKI NCZI, ktoré majú prístup k systému CA,
- zmeny nastavení CA a / alebo kryptografických kľúčov,
- zmena pravidiel vytvárania certifikátov napr. zmena doby platnosti,
- pokusy o prihlásiť a odhlásenia,
- neoprávnené pokusy o prístup po sieti do systému CA,
- neoprávnené pokusy o prístup k systémovým súborom,
- generovania vlastných alebo podriadených kľúčov,
- vydávanie a zrušenie platnosti certifikátov,
- chybná operácia pri čítaní resp. zápise certifikátu alebo a CRL adresára.

Všetky záznamy, či už elektronické alebo manuálne, obsahujú dátum a čas udalosti, a totožnosť subjektu, ktorý udalosť spôsobil.

CA NZIS ďalej zbiera a konsoliduje v elektronickej forme resp. manuálne (písomné záznamy), bezpečnostné informácie, ktoré nie sú generované priamo systémom CA, ako sú:

- záznamy o fyzickom prístupe,
- zmeny konfigurácie systému a jeho údržba,
- personálne zmeny,
- záznamy o odchýlkach a kompromitáciách,
- záznamy o zničenie médií obsahujúcich kryptografické kľúče, aktivačných údajoch alebo osobné údajov držiteľov.

Všetky zmluvy a korešpondencia vzťahujúce sa k službám CA sú uchovávané v archíve NCZI.

5.4.2. Frekvencia spracovávania auditných log záznamov

Pracovníci CA NZIS preskúmavajú audit log záznamy, ktoré patria do ich kompetencie na dennej báze a minimálne raz týždenne sú všetky významné udalosti vysvetlené v súhrnom zázname s preskúmavania. Postup hodnotenia zahŕňa overovanie, či nedošlo k manipulácii so záznamami, krátkeho prezretia všetkých položiek log záznamov s dôkladnejším preskúmaním akýchkoľvek upozornení alebo nepravidelností v záznamoch. Podporné manuálne alebo elektronické log záznamy CA resp. RA by mali byť porovnávané pokiaľ sa nejaký zásah javí ako podozrivý. Všetky prijaté opatrenia prijaté na základe týchto hodnotení sú dokumentované.

5.4.3. Doba uchovávanie auditných log záznamov

CA uchováva svoje auditné log záznamy k dispozícii dva mesiace od ich zaznamenania a následne ich archivuje v zmysle časti 5.5.

5.4.4. Ochrana auditných log záznamov

Systém zaznamenávanie auditných log záznamov chráni súbory proti neoprávnenému prezeraniu, úprave a vymazaniu.

5.4.5. Postup zálohovania auditných log záznamov

Auditné log záznamy a súhrnné reporty sú zálohované v zmysle postupu, ktorý je popísaný v dokumente Vysokúrovňový dizajn bezpečnosti NZIS.

5.4.6. Systém získavania auditných záznamov

Auditné záznamy sú vytvárané a uchovávané automaticky systémom.

5.4.7. Zraniteľnosti

CA NZIS preskúmava log súbory aj s dôrazom na hodnotenie zraniteľnosti systému CA a podrobuje ich dôkladnej analýze za účelom zaistenia maximálnej bezpečnosti.

5.5. Uchovávanie záznamov

5.5.1. Typy uchovávaných záznamov

CA NZIS archivuje nasledovné údaje a súbory:

- Certifikačný poriadok (CP),
- Pravidlá na výkon certifikačných činností (CPS),
- zmluvné záväzky,
- konfigurácia systémov a zariadení,
- zmeny a aktualizácia systému alebo jeho konfigurácie,
- žiadosti o certifikát,
- žiadosti o zrušenie certifikátu,

- dokumentácia o odovzdaní a prijatí certifikátu,
- zmena kľúčov CA,
- všetky ARL a CRL vydané a / alebo zverejnené,
- všetky auditné log záznamy,
- dokumentácia vyžadovaná audítormi,
- konečné stanovisko vyplývajúce z vykonaného auditu zhody.

Druhé kópie všetkých uchovávaných alebo zálohovaných materiálov, sú uložené na inom mieste, ako je umiestnenie CA infraštruktúry a sú chránené buď opatreniami fyzickej bezpečnosti. Miesto uloženia kópií poskytuje primeranú ochranu pred environmentálnymi hrozbami ako je teplota, vlhkosť a magnetizmus. CA overuje integritu záloh raz za šesť mesiacov. Materiál uložený off-site je pravidelne overovaný na zachovanie integrity údajov o čom sú vytvárané písomné záznamy.

5.5.2. Doba uchovávanie archívnych záznamov

Archív kľúčov a informácie o certifikáte sa uchovávajú po dobu 10 rokov. Archív auditných log záznamov je uchovávaný po dobu troch mesiacov (3) mesiacov.

5.5.3. Ochrana archívnych záznamov

Archívne médiá sú chránené fyzickými bezpečnostnými opatreniami. Ochrana archívnych médií spĺňa legislatívne požiadavky SR na uchovávanie takýchto materiálov.

5.6. Zmena kľúčov

Poskytnutie nového verejného kľúča CA NZIS po obnove kľúčov certifikačnej autority sa uskutoční rovnakým spôsobom ako u pôvodného verejného kľúča, jeho publikovaním na verejnej web stránke CA NZIS.

5.7. Kompromitácia a obnova po havárii

5.7.1. Postupy dokumentovania a riadenia incidentov a kompromitácií

Postupy dokumentovania a riadenia incidentov a kompromitácií CA NZIS sú popísané podľa plánov obnovy (DRP) a uložené v elektronickom systéme LDRPS. Obnova činnosti CA NZIS sa vykonáva v zmysle uvedeného.

5.7.2. Poškodený hardvér, softvér, a/alebo údaje

CA NZIS má stanovené postupy obnovy s definovanými krokmi pre prípad, že dôjde k poškodeniu alebo strate hardvéru, softvéru a/alebo údajov.

5.7.3. Kompromitácia súkromného kľúča CA

CA NZIS nemá zavedený plán pre prípad kompromitácie kľúčov,

V prípade potreby zrušenia podpisového certifikátu CA NZIS bezodkladne informuje:

- PMA,
- všetky jeho RA,
- všetkých držiteľov platných certifikátov,
- všetky osoby a organizácie, ktoré sú zodpovedné za certifikáty vydané pre nimi používané zariadenia alebo aplikácie.

CA NZIS zároveň:

- zverejní sériové číslo zrušeného certifikátu vo vhodnom ARL,

Po vyriešení skutočností, ktoré viedli k zrušeniu, CA NZIS:

- vygeneruje nový kľúčový pár CA,
- obnoví certifikáty všetkým subjektom, ktorým boli tieto z dôvodu kompromitácie súkromného kľúča, zrušené
- zabezpečí podpísanie všetkých zoznamov CRL a ARL prostredníctvom nových kľúčov.

5.7.4. Pokračovanie v poskytovaní služieb po havárii

CA NZIS zabezpečí v prípade havárie spôsobenej prírodnou alebo inou katastrofou vydávanie CRL. Pokračovanie poskytovania služieb bude k dispozícii na mieste obnovy.

NCZI má postup, ktorý zahŕňa ochranu priestorov a zariadení v čase po výskyte prírodnej alebo inej katastrofy pred samotnou obnovou činnosti v pôvodných priestoroch, aby nedošlo k odcudzeniu citlivých informácií.

5.8. Ukončenie činnosti CA

V prípade, že CA NZIS ukončí prevádzku, oznámi túto skutočnosť okamžite všetkým držiteľom platných certifikátov, RA a spoliehajúcim sa stranám a spolu s PMA zabezpečí uchovávanie kľúčov CA a ďalších potrebných informácií.

Všetky platné certifikáty vydané CA NZIS budú zrušené skôr ako dôjde k ukončeniu činnosti. Všetky aktuálne a archivované dokumenty CA budú odovzdané PMA počas 48 hodín po ukončení činnosti CA a v súlade s CP a CPS. Žiadne úložisko s možnosťou obnovy kľúčov nebude súčasťou odovzdaných údajov.

Archívy CA NZIS budú aj naďalej udržiavané spôsobom a počas doby ako je stanovená v časti 5.5.

6. Technické bezpečnostné opatrenia

6.1. Generovanie kľúčového páru a jeho inštalácia

6.1.1. Generovanie kľúčov

Generovanie kľúčových párov pre koncového užívateľa je vykonávané v priebehu personalizácie karty na personalizačnom pracovisku NCZI priamo na čipovej karte prostredníctvom PMA schváleného algoritmu.

6.1.2. Doručenie privátneho kľúča držiteľovi

Súkromné kľúče budú odovzdané držiteľovi bezpečným spôsobom v priestoroch RA alebo CA.

6.1.3. Doručenie verejného kľúča na CA NZIS

Doručenie verejného kľúča na CA NZIS sa uskutoční on-line cez zabezpečený kanál po vygenerovaní kľúčového páru na čipovej karte.

6.1.4. Veľkosť kľúčov

CA NZIS vydáva certifikáty len na verejný kľúč s veľkosťou najmenej 2048 bit RSA.

6.1.5. Parametre generovania kľúčov a kontrola kvality

Žiadne požiadavky.

6.1.6. Účel použitia kľúčov

Pozri časť 6.1.6 aktuálneho CP CA NZIS.

6.2. Ochrana súkromného kľúča a využívanie kryptografických hardvérových modulov (HSM)

Vydávajúca CZ NCZI uchovávať svoje kryptografické kľúče určené na podpisovanie certifikátov koncových používateľov v kryptografickom bezpečnostnom module (HSM) nShield e500 F3

6.2.1. Štandardné požiadavky na HSM

CA NZIS použitý kryptografický modul spĺňa požiadavky bezpečnosti na úrovni FIPS 140-2 Level 3. Modul je uložený v bezpečných priestoroch bez prístupu neoprávnených osôb. HSM modul spĺňa ochranu pred odchytávaním elektromagnetického vyžarovania, podporuje funkciu self test a poskytuje funkciu key recovery.

HSM podporuje nasledovné podpisové algoritmy:

- RSA s SHA-1,
- RSA s SHA-224,

- RSA s SHA-256,
- RSA s SHA-384, RSA s SHA-512

6.2.2. Práca so súkromných kľúčom

Súkromný kľúč certifikačnej autority je generovaný a obnovovaný pod kontrolou viacerých osôb podľa princípu *n* z *m*, pričom je n=4 a m=7.

6.2.3. Obnova súkromných kľúčov z depozitu

Súkromný kľúč CA NZIS nie je uložený v depozite u tretej osoby.

6.2.4. Zálohovanie súkromných kľúčov

Pozri časť 6.2.4 aktuálneho CP CA NZIS

6.2.5. Archivácia súkromných kľúčov

Pozri časť 6.2.4.

6.2.6. Prenos súkromného kľúča do alebo z kryptografického modulu

Súkromný kľúč je štandardne uložený v zašifrovanej podobne na pevnom disku počítača, ku ktorému je pripojený HSM modul. Do HSM modulu sa prenáša pri spustení operácia aktivácie kľúčov za použitia príslušného počtu operátorských kariet (princíp n z m). Aktiváciu vykonáva systémový administrátor za prítomnosti ďalších osôb vlastniacich požadovaný počet operátorských kariet príslušného z príslušnej série operátorských kariet, ktoré chránia daný súkromný kľúč.

6.2.7. Uchovávanie súkromného kľúča v HSM module

Pozri časť 6.2.7 aktuálny CP CA NZIS..

6.2.8. Spôsob aktivácie súkromného kľúča

Oprávnené osoby sa musia pri aktivácii súkromného kľúča v kryptografickom module identifikovať a autentifikovať príslušnou operátorskou kartou a heslom. Po vypnutí resp. reštartovaní HSM modulu je súkromný kľúč automaticky deaktivovaný a v HSM module sa nenachádza. Je uložený len v šifrovanej podobe na pevnom disku počítača, ku ktorému je pripojený HSM modul.

6.2.9. Spôsob deaktivácia súkromného kľúča

Pri deaktivácii (vypnutie modulu, ukončenie služby) je súkromný kľúč vymazaný z pamäte HSM modulu.

6.2.10. Spôsob zničenia súkromného kľúča

Po ukončení používania súkromného kľúča CA NZIS znemožnení jeho opätovné použitie tak, že sa vykoná vymazaním obsahu všetkých operátorských kariet patriacich k operátorskej sérii kariet (OCS), ktoré chránia daný súkromný kľúč. Vymazaním OCS sa zabezpečí, že už v žiadnom prípade nie je možné použiť príslušný súkromný kľúč uložený v zašifrovanej podobe mimo HSM. V prípade, že je daný kľúč chránený v Security world, ktorý neobsahuje žiadne iné kľúče, vykoná sa vymazanie obsahu

všetkých kariet patriacich k administrátorskej sérii kariet (ACS) a zároveň vymazanie daného Security worldu z HSM modulu.

O všetkých aktivitách súvisiacich so znemožnením opätovného použitia podpisového kľúča sa vypracuje podrobný záznam. Ak je dôvodom ukončenia činnosti CA NZIS nejaký dôvod bez vzťahu k bezpečnosti, potom ani certifikát CA NZIS, ktorá končí činnosť, ani certifikáty podpísané touto CA nemusia zrušiť.

6.2.11. Charakteristika HSM modulu

Použitý HSM modul spĺňa bezpečnostné požiadavky na úrovni FIPS 140-2 Level 3.

6.3. Ďalšie aspekty manažmentu kľúčového páru

6.3.1. Archivácia verejného kľúča

Pozri časť 4.6

6.3.2. Doba platnosti certifikátov a použiteľnosti kľúčového páru

Doba platnosti certifikátov vydaných na kľúče s veľkosťou 2048 bit je maximálne 5 rokov. Kľúčový pár je použiteľný len po dobu platnosti naň vydaného certifikátu.

6.4. Aktivačné údaje

6.4.1. Generovanie aktivačných údajov a ich inštalácia

Všetky aktivačný údaje sú jedinečné a nepredvídateľné. Aktivačné údaje, v spojení s niektorým iným overovaním prístupu, majú primeranú úroveň sily v závislosti na kľúčoch alebo údajoch, ktoré sú nimi chránené. Každý držiteľ si počas aktivácie karty určuje vlastné prístupové heslá (PIN) a má prostredníctvom softvérových nástrojov možnosť si hesle kedykoľvek zmeniť.

6.4.2. Ochrana aktivačných údajov

Súkromné kľúče subjektov na čipovej karte sú pred jej doručením držiteľovi po vydaní certifikátu chránené pred neoprávneným použitím blokovaní. Na možnosť použitia daného súkromného kľúča musí mať oprávnený držiteľ k dispozícii samotnú čipovú kartu a aktivačný kód. Keďže čipová karta a aktivačný kód sú zasielané držiteľovi dvomi rozdielnymi spôsobmi považuje sa takáto ochrana aktivačných údajov za dostatočnú. Čipová karta sa automaticky zablokuje po treťom nesprávnom zadaní PIN-u.

6.4.3. Ďalšie aspekty aktivačných údajov

Žiadne požiadavky.

6.5. Počítačové bezpečnostné opatrenia

6.5.1. Špecifické technické požiadavky z oblasti počítačovej bezpečnosti

Každý server certifikačnej autority umožňuje nasledovnú funkcionalitu:

- riadenie prístupu k službám CA a PKI rolám,
- oddelenie zodpovedností pre PKI roly,
- identifikáciu a autentizáciu PKI rolí a s nimi súvisiace identity,
- použitie kryptografie pri komunikácii v rámci session a zabezpečenie databázy,
- archiváciu histórie CA a koncových používateľov a auditných údajov,
- audit udalostí súvisiacich s bezpečnosťou,
- self-test CA služieb vzťahujúcich sa k bezpečnosti,
- dôveryhodnú cestu k identifikácii PKI rolí a súvisiacich identít,
- mechanizmus obnovy kľúčov a systému CA.

6.5.2. Hodnotenie počítačovej bezpečnosti

Žiadne požiadavky.

6.6. Životný cyklus riadenia bezpečnosti

6.6.1. Riadenie vývoja systému

CA NZIS používa softvér, ktorý bol navrhnutý a vyvinutý v zmysle formálnej metodiky a je podporovaný nástrojmi pre riadenie konfigurácie.

6.6.2. Riadenie manažmentu bezpečnosti

Použitý softvér CA NZIS, pri spustení, poskytuje CA možnosť na overenie, že:

- pochádza od tvorcu softvéru,
- nedošlo k žiadnym zmenám pred samotnou inštaláciou,
- ide o verziu určenú pre reálne použitie.

CA NZIS používa softvér schopný pri každom spustení overovať svoju integritu. Všetky zmeny konfigurácie systému CA NZIS musia byť vopred schválené PMA a o ich aplikácii je vykonaný písomný záznam.

6.7. Riadenie sieťovej bezpečnosti

Servery CA NZIS sú chránené pred napadnutím z ľubovoľnej otvorenej alebo internej siete, do ktorej sú pripojené. Ochrana je riešená prostredníctvom inštalácie zariadení nakonfigurovaný tak, že sú prístupné len protokoly a príkazy potrebné pre prevádzku CA. Profily certifikátov a CRL

6.8. Profily certifikátov

6.8.1. Podporovaná verzia

CA NZIS vydáva X.509 verzie 3 certifikáty v zmysle RFC 5280 „Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile“.

6.8.2. Certifikát koreňovej CA NZIS

Algoritmy a dĺžky kľúčov uplatňované v koreňovom certifikáte CA NZIS:

Algoritmus podpisu (Signature Algorithm)
sha256RSA

Verejný kľúč
RSA, dĺžka 4 096 bitov

Doba platnosti certifikátu CA
maximálne 20 rokov

Tabuľka č. 1: Obsah položiek v certifikáte koreňovej certifikačnej autority CA Disig

Skratka názvu	OID	Názov	Hodnota
C	2.5.4.6	countryName	SK
O	2.5.4.10	organizationName	NCZI
CN	2.5.4.3	commonName	NCZI Root CA 1

Tabuľka č. 2: Použité rozšírenia (certificate extensions) v certifikáte koreňovej CA NZIS

Rozšírenie / OID Typ rozšírenia	Hodnota
basicConstraints / 2.5.29.19 kritické rozšírenie	CA:TRUE
keyUsage / 2.5.29.15 kritické rozšírenie	Certificate Signing, Off-line CRL Signing, CRL Signing (06)
subjectKeyIdentifier / 2.5.29.14 nekritické rozšírenie	vygenerovaný systémom
subjectAltName / 2.5.29.17 nekritické rozšírenie	RFC822 Name= URL=
crlDistributionPoints / 2.5.29.31 nekritické rozšírenie	Distribution Point Name: Full Name: URL=

6.8.3. Podriadené certifikačné autority CA NZIS

6.8.3.1. Podriadené certifikačné autority CA NZIS – užívateľské certifikáty

Algoritmy a dĺžky kľúčov uplatňované v certifikáte podriadenej CA NZIS:

Algoritmus podpisu (Signature Algorithm)
sha256RSA

Verejný kľúč
RSA, dĺžka 2 048 bitov

Doba platnosti certifikátu CA
maximálne 10 rokov

Tabuľka č. 3: Obsah položiek v certifikáte podriadenej certifikačnej autority CA NZIS

Skratka názvu	OID	Názov	Hodnota
C	2.5.4.6	countryName	SK
O	2.5.4.10	organizationName	NCZI
CN	2.5.4.3	commonName	NCZI Protection CA RA-1

Tabuľka č. 4: Použité rozšírenia (certificate extensions) v certifikáte podriadených CA NZIS

Rozšírenie / OID Typ rozšírenia	Hodnota
authorityInfoAccess / 1.3.6.1.5.5.7.1.1	[1]Authority Info Access Access Method=Certification Authority Issuer (1.3.6.1.5.5.7.48.2) Alternative Name: URL= http://pki.infra.npz.sk/rootca/cert/nczi_rootca-1.der
basicConstraints / 2.5.29.19 kritické rozšírenie	CA:TRUE Path Length Constraint=0
keyUsage / 2.5.29.15 kritické rozšírenie	Certificate Signing, Off-line CRL Signing, CRL Signing (06)
subjectKeyIdentifier / 2.5.29.14 nekritické rozšírenie	vygenerovaný systémom
crlDistributionPoints / 2.5.29.31 nekritické rozšírenie	[1]CRL Distribution Point Distribution Point Name: Full Name: URL= http://pki.infra.npz.sk/rootca/crl/nczi_rootca-1.crl
Authority Key Identifier / 2.5.29.35 nekritické rozšírenie	KeyID= Hodnota je automaticky pridávaná certifikačnou autoritou CA NZIS
certificatePolicies / 2.5.29.32* nekritické rozšírenie	Policy Identifier=1.3.158.165387.100.90.10.20.10.10.1 [1,1]Policy Qualifier Info: Policy Qualifier Id=CPS Qualifier: http://pki.infra.npz.sk/cps/

	Notice text = Tento certifikat bol vydany pre ucely NCZI.

6.8.3.2. Podriadené certifikačné autority CA NZIS – technologické certifikáty

Algoritmy a dĺžky kľúčov uplatňované v certifikáte podriadenej CA NZIS:

Algoritmus podpisu (Signature Algorithm)
sha256RSA

Verejný kľúč
RSA, dĺžka 2 048 bitov

Doba platnosti certifikátu CA
maximálne 10 rokov

Tabuľka č. 5: Obsah položiek v certifikáte podriadenej certifikačnej autority CA NZIS

Skratka názvu	OID	Názov	Hodnota
C	2.5.4.6	countryName	**SK**
O	2.5.4.10	organizationName	**NCZI**
CN	**2.5.4.3**	**commonName**	**NCZI HPROTech CA RA-1**

Tabuľka č. 6: Použité rozšírenia (certificate extensions) v certifikáte podriadených CA NZIS

Rozšírenie / OID Typ rozšírenia	Hodnota
authorityInfoAccess / 1.3.6.1.5.5.7.1.1	**[1]Authority Info Access Access Method=Certification Authority Issuer (1.3.6.1.5.5.7.48.2) Alternative Name: URL= http://pki.infra.npz.sk/rootca/cert/nczi_rootca-1.der**
basicConstraints / 2.5.29.19 kritické rozšírenie	**CA:TRUE Path Length Constraint=0**
keyUsage / 2.5.29.15 kritické rozšírenie	**Certificate Signing, Off-line CRL Signing, CRL Signing (06)**
subjectKeyIdentifier / 2.5.29.14 nekritické rozšírenie	vygenerovaný systémom
crlDistributionPoints / 2.5.29.31 nekritické rozšírenie	**[1]CRL Distribution Point Distribution Point Name: Full Name: URL= http://pki.infra.npz.sk/rootca/crl/nczi_rootca-1.crl**
Authority Key Identifier / 2.5.29.35 nekritické rozšírenie	**KeyID= Hodnota je automaticky pridávaná certifikačnou autoritou CA NZIS**
certificatePolicies / 2.5.29.32* nekritické rozšírenie	**Policy Identifier=1.3.158.165387.100.90.10.20.10.20.1 [1,1]Policy Qualifier Info: Policy Qualifier Id=CPS Qualifier: http:// pki.infra.npz.sk/cps/**

	Notice text = Tento certifikat bol vydany pre ucely NCZI.

6.8.4. Certifikáty na správu

6.8.4.1. Certifikát služby poskytovanie informácie o existencii a platnosti certifikátu (OCSP)

Algoritmy a dĺžky kľúčov uplatňované v certifikáte na poskytovanie služby o existencii a platnosti certifikátu (OCSP):

Algoritmus podpisu (Signature Algorithm)
sha256RSA

Verejný kľúč
RSA, dĺžka 2 048 bitov

Doba platnosti certifikátu CA
maximálne 2 roky

Tabuľka č. 7: Obsah položiek v certifikáte OCSP CA NZIS

Skratka názvu	OID	Názov	Hodnota
CN	**2.5.4.3**	**commonName**	**OCSP NCZI**

Tabuľka č. 8: Použité rozšírenia (certificate extensions) v certifikáte OCSP CA NZIS

Rozšírenie / OID Typ rozšírenia	Hodnota
authorityInfoAccess / 1.3.6.1.5.5.7.1.1	**[1]Authority Info Access Access Method=Certification Authority Issuer (1.3.6.1.5.5.7.48.2) Alternative Name: URL= http://pki.infra.npz.sk/techca/cert/nczi_techca-R1-1.der**
keyUsage / 2.5.29.15 kritické rozšírenie	**Digital Signature**
subjectKeyIdentifier / 2.5.29.14 nekritické rozšírenie	vygenerovaný systémom
crlDistributionPoints / 2.5.29.31 nekritické rozšírenie	**[1]CRL Distribution Point Distribution Point Name: Full Name: URL= http://pki.infra.npz.sk/techca/crl/nczi_techca-R1-1.crl**
Authority Key Identifier / 2.5.29.35 nekritické rozšírenie	**KeyID= Hodnota je automaticky pridávaná certifikačnou autoritou CA NZIS**
Extended Key Usage / 2.5.29.37 kritické	**OCSP Signing (1.3.6.1.5.5.7.3.9)**

certificatePolicies / 2.5.29.32* nekritické rozšírenie	**Policy Identifier=1.3.158.165387.100.90.10.20.10.20.1 [1,1]Policy Qualifier Info: Policy Qualifier Id=CPS Qualifier: http:// pki.infra.npz.sk/cps/ Notice text = UPOZORNENIE: Tato OCSP sluzba je poskytovana pre zakaznikov NCZI.**
subjectAltName / 2.5.29.17 nekritické rozšírenie	**E-mail adresa držiteľa certifikátu (rfc822Name)**

6.8.5. Certifikáty vydávané CA NZIS koncovým užívateľom

6.8.5.1. Osobný certifikát na podpisovanie

Algoritmy a dĺžky kľúčov uplatňované v osobnom certifikáte na podpisovanie vydávanom CA NZIS:

Algoritmus podpisu (Signature Algorithm)
sha256RSA

Verejný kľúč
RSA, dĺžka je minimálne 2 048 bitov

Doba platnosti osobného certifikátu
Maximálne 1825 dní t.j. 5 rokov

Tabuľka č. 9: Obsah štandardných položiek v osobnom certifikáte na podpisovanie

Skratka názvu	OID	Názov	Hodnota
C	2.5.4.6	countryName	**SK Údaj je povinný!!!**
O	2.5.4.10	organizationName	**Názov organizácie Údaj je povinný!!!**
OU	2.5.4.11	organizationUnitName	**Názov útvaru vo firme Údaj je povinný!!!**
OU	2.5.4.11	organizationUnitName	**Názov útvaru vo firme Údaj je povinný!!!**
CN	2.5.4.3	commonName	**Meno a priezvisko Údaj je povinný!!!**
SERIALNUMBER	2.5.4.5	SerialNumber	**JRÚZ identifikátor Údaj je povinný!!!**

Tabuľka č. 10: Základné rozšírenia (certificate extensions) v osobnom certifikáte na podpisovanie

Rozšírenie / OID Typ rozšírenia	Hodnota
authorityInfoAccess / 1.3.6.1.5.5.7.1.1	**[1]Authority Info Access Access Method=Certification Authority Issuer (1.3.6.1.5.5.7.48.2)**

	Alternative Name: **URL=** **http://pki.infra.npz.sk/protectionca/cert/nczi_protectionca-R1-1.der**
Subject Key Identifier / 2.5.29.14 **nekritické rozšírenie**	**Hodnota je automaticky vytváraná certifikačnou autoritou CA NZIS**
Authority Key Identifier / 2.5.29.35 **nekritické rozšírenie**	**KeyID= Hodnota je automaticky pridávaná certifikačnou autoritou CA NZIS**
Key Usage / 2.5.29.15 **kritické rozšírenie**	**Digital Signature, Non-Repudiation**
CRL Distribution Points / 2.5.29.31 **nekritické rozšírenie**	**[1]CRL Distribution Point** **Distribution Point Name:** **Full Name:** **URL=** **http://pki.infra.npz.sk/protectionca/crl/nczi_protectionca-R1-1.crl**
Extended Key Usage / 2.5.29.37 **nekritické rozšírenie**	**Signer of documents -- szOID_KP_DOCUMENT_SIGNING (1.3.6.1.4.1.311.10.3.12)**
Certificate Policies / 2.5.29.32 **nekritické rozšírenie**	**Policy Identifier=1.3.158.165387.100.90.10.20.10.10.1** **[1,1]Policy Qualifier Info:** **Policy Qualifier Id=CPS** **Qualifier:** **http:// pki.infra.npz.sk/cps/** **Notice text = UPOZORNENIE: Tento sluzba je poskytovana pre zakaznikov NCZI.**

6.8.6. **Osobný certifikát na šifrovanie**

Algoritmy a dĺžky kľúčov uplatňované v osobnom certifikáte na šifrovanie vydávanom CA NZIS:

Algoritmus podpisu (Signature Algorithm)
sha256RSA

Verejný kľúč
RSA, dĺžka je minimálne 2 048 bitov

Doba platnosti osobného certifikátu
Maximálne 1825 dní t.j. 5 rokov

Tabuľka č. 11: Obsah štandardných položiek v osobnom certifikáte na šifrovanie

Skratka názvu	OID	Názov	Hodnota
C	2.5.4.6	countryName	**SK** **Údaj je povinný!!!**
O	2.5.4.10	organizationName	**Názov organizácie** **Údaj je povinný!!!**

OU	2.5.4.11	organizationUnitName	**Názov útvaru vo firme** **Údaj je povinný!!!**
OU	2.5.4.11	organizationUnitName	**Názov útvaru vo firme** **Údaj je povinný!!!**
CN	2.5.4.3	commonName	**Meno a priezvisko** **Údaj je povinný!!!**
SERIALNUMBER	2.5.4.5	SerialNumber	**JRÚZ identifikátor** **Údaj je povinný!!!**

Tabuľka č. 12: Základné rozšírenia (certificate extensions) v osobnom certifikáte na šifrovanie

Rozšírenie / OID Typ rozšírenia	Hodnota
authorityInfoAccess / 1.3.6.1.5.5.7.1.1	[1]Authority Info Access Access Method=On-line Certificate Status Protocol (1.3.6.1.5.5.7.48.1) Alternative Name: URL= http://ocsp.infra.npz.sk/ocsp/protectionca-R1-1 [2]Authority Info Access Access Method=Certification Authority Issuer (1.3.6.1.5.5.7.48.2) Alternative Name: URL= http://pki.infra.npz.sk/protectionca/cert/nczi_protectionca-R1-1.der
Subject Key Identifier / 2.5.29.14 nekritické rozšírenie	Hodnota je automaticky vytváraná certifikačnou autoritou CA NZIS
Authority Key Identifier / 2.5.29.35 nekritické rozšírenie	KeyID= Hodnota je automaticky pridávaná certifikačnou autoritou CA NZIS
Key Usage / 2.5.29.15 kritické rozšírenie	keyEncipherment, dataEncipherment
CRL Distribution Points / 2.5.29.31 nekritické rozšírenie	[1]CRL Distribution Point Distribution Point Name: Full Name: URL= http://pki.infra.npz.sk/protectionca/crl/nczi_protectionca-R1-1.crl
Extended Key Usage / 2.5.29.37 nekritické rozšírenie	szOID_EFS_CRYPTO (1.3.6.1.4.1.311.10.3.4)
Certificate Policies / 2.5.29.32 nekritické rozšírenie	Policy Identifier=1.3.158.165387.100.90.10.20.10.10.1 [1,1]Policy Qualifier Info: Policy Qualifier Id=CPS Qualifier: http:// pki.infra.npz.sk/cps/ Notice text = UPOZORNENIE: Tento sluzba je poskytovana pre zakaznikov NCZI.

6.8.7. **Osobný certifikát na identifikáciu**

Algoritmy a dĺžky kľúčov uplatňované v osobnom certifikáte na identifikáciu CA NZIS:

Algoritmus podpisu (Signature Algorithm)
sha256RSA

Verejný kľúč
RSA, dĺžka je minimálne 2 048 bitov

Doba platnosti osobného certifikátu
Maximálne 1825 dní t.j. 5 rokov

Tabuľka č. 13: Obsah štandardných položiek v osobnom certifikáte na identifikáciu

Skratka názvu	OID	Názov	Hodnota
C	2.5.4.6	countryName	SK Údaj je povinný!!!
O	2.5.4.10	organizationName	Názov organizácie Údaj je povinný!!!
OU	2.5.4.11	organizationUnitName	Názov útvaru vo firme Údaj je povinný!!!
OU	2.5.4.11	organizationUnitName	Názov útvaru vo firme Údaj je povinný!!!
CN	2.5.4.3	commonName	Meno a priezvisko Údaj je povinný!!!
SERIALNUMBER	2.5.4.5	SerialNumber	JRÚZ identifikátor Údaj je povinný!!!

Tabuľka č. 14: Základné rozšírenia (certificate extensions) v osobnom certifikáte na identifikáciu

Rozšírenie / OID Typ rozšírenia	Hodnota
authorityInfoAccess / 1.3.6.1.5.5.7.1.1	[1]Authority Info Access Access Method=On-line Certificate Status Protocol (1.3.6.1.5.5.7.48.1) Alternative Name: URL= http://ocsp.infra.npz.sk/ocsp/authca-R1-1 [2]Authority Info Access Access Method=Certification Authority Issuer (1.3.6.1.5.5.7.48.2) Alternative Name: URL= http://pki.infra.npz.sk/authca/cert/nczi_authca-R1-1.der
Subject Key Identifier / 2.5.29.14 nekritické rozšírenie	Hodnota je automaticky vytváraná certifikačnou autoritou CA NZIS
Authority Key Identifier / 2.5.29.35 nekritické rozšírenie	KeyID= Hodnota je automaticky pridávaná certifikačnou autoritou CA NZIS
Key Usage / 2.5.29.15 kritické rozšírenie	Digital Signature, Key Encipherment
CRL Distribution Points / 2.5.29.31 nekritické rozšírenie	[1]CRL Distribution Point Distribution Point Name: Full Name: URL= http://pki.infra.npz.sk/authca/crl/nczi_authca-R1-1.crl
Extended Key Usage / 2.5.29.37 nekritické rozšírenie	Client Authentication (1.3.6.1.5.5.7.3.2)

Certificate Policies / 2.5.29.32 nekritické rozšírenie	**Policy Identifier=1.3.158.165387.100.90.10.20.10.10.1 [1,1]Policy Qualifier Info: Policy Qualifier Id=CPS Qualifier: http:// pki.infra.npz.sk/cps/ Notice text = UPOZORNENIE: Tento sluzba je poskytovana pre zakaznikov NCZI.**

6.8.8. Osobný certifikát administrátora IAM NZIS

Algoritmy a dĺžky kľúčov uplatňované v osobnom certifikáte na identifikáciu CA NZIS:

Algoritmus podpisu (Signature Algorithm)
sha256RSA

Verejný kľúč
RSA, dĺžka je minimálne 2 048 bitov

Doba platnosti osobného certifikátu
Maximálne 1825 dní t.j. 5 rokov

Tabuľka č. 15: Obsah štandardných položiek v osobnom certifikáte na identifikáciu

Skratka názvu	OID	Názov	Hodnota
C	2.5.4.6	countryName	**SK Údaj je nepovinný**
O	2.5.4.10	organizationName	**Názov organizácie Údaj je nepovinný**
OU	2.5.4.11	organizationUnitName	**Názov útvaru vo firme Údaj je nepovinný**
OU	2.5.4.11	organizationUnitName	**Názov útvaru vo firme Údaj je nepovinný**
CN	2.5.4.3	commonName	**Meno a priezvisko Údaj je povinný!!!**
SERIALNUMBER	2.5.4.5	SerialNumber	**Prihlasovacie meno v rámci ADr Údaj je povinný!!!**

Tabuľka č. 16: Základné rozšírenia (certificate extensions) v osobnom certifikáte na identifikáciu

Rozšírenie / OID Typ rozšírenia	Hodnota
authorityInfoAccess / 1.3.6.1.5.5.7.1.1	**[1]Authority Info Access Access Method=On-line Certificate Status Protocol (1.3.6.1.5.5.7.48.1) Alternative Name: URL= http://ocsp.infra.npz.sk/ocsp/techca-R1-1**

	[2]Authority Info Access Access Method=Certification Authority Issuer (1.3.6.1.5.5.7.48.2) Alternative Name: URL= http://pki.infra.npz.sk/techca/cert/nczi_techca-R1-1.der
Subject Key Identifier / 2.5.29.14 nekritické rozšírenie	Hodnota je automaticky vytváraná certifikačnou autoritou CA NZIS
Authority Key Identifier / 2.5.29.35 nekritické rozšírenie	KeyID= Hodnota je automaticky pridávaná certifikačnou autoritou CA NZIS
Key Usage / 2.5.29.15 kritické rozšírenie	Digital Signature, Key Encipherment
CRL Distribution Points / 2.5.29.31 nekritické rozšírenie	[1]CRL Distribution Point Distribution Point Name: Full Name: URL= http://pki.infra.npz.sk/techca/crl/nczi_techca-R1-1.crl
Extended Key Usage / 2.5.29.37 nekritické rozšírenie	Client Authentication (1.3.6.1.5.5.7.3.2) Smart card logon (1.3.6.1.4.1.311.20.2.2)
Certificate Policies / 2.5.29.32 nekritické rozšírenie	Policy Identifier=1.3.158.165387.100.90.10.20.10.20.1 [1,1]Policy Qualifier Info: Policy Qualifier Id=CPS Qualifier: http:// pki.infra.npz.sk/cps/ Notice text = UPOZORNENIE: Tento sluzba je poskytovana pre zakaznikov NCZI.

6.8.9. Technologický certifikát

6.8.9.1. Technologický certifikát pre zariadenia a webové služby

Algoritmy a dĺžky kľúčov uplatňované v certifikáte pre zariadenia a webové služby:

Algoritmus podpisu (Signature Algorithm)
Sha1

Verejný kľúč
RSA, dĺžka 2 048 bitov

Doba platnosti certifikátu CA
maximálne 2 roky

Tabuľka č. 17: Obsah položiek v certifikáte pre webové služby

Skratka názvu	OID	Názov	Hodnota
C	2.5.4.6	countryName	SK Údaj je nepovinný
O	2.5.4.10	organizationName	Názov organizácie Údaj je nepovinný
OU	2.5.4.11	organizationUnitName	Identifikácia služby Údaj je nepovinný

OU	2.5.4.11	organizationUnitName	**Identifikácia typu služby** **Údaj je nepovinný**
CN	2.5.4.3	commonName	**Názov služby** **Hodnota je povinná**
SERIALNUMBER	2.5.4.5	SerialNumber	**Identifikátor webovej služby** **Hodnota je nepovinná**

Tabuľka č. 18: Obsah položiek v certifikáte pre zariadenia a IAM certifikáty

Skratka názvu	OID	Názov	Hodnota
C	2.5.4.6	countryName	**SK** **Údaj je nepovinný**
O	2.5.4.10	organizationName	**Názov organizácie** **Údaj je nepovinný**
CN	**2.5.4.3**	**commonName**	**Názov služby / DNS meno** **Hodnota je povinná**

Tabuľka č. 19: Použité rozšírenia (certificate extensions) v certifikáte pre zariadenia a webové služby

Rozšírenie / OID Typ rozšírenia	Hodnota
authorityInfoAccess / 1.3.6.1.5.5.7.1.1	**[1]Authority Info Access** **Access Method=Certification Authority Issuer (1.3.6.1.5.5.7.48.2)** **Alternative Name:** **URL= http://pki.infra.npz.sk/techca/cert/nczi_techca-R1-1.der**
keyUsage / 2.5.29.15 **kritické rozšírenie**	**Digital Signature, Key encipherment**
subjectKeyIdentifier / 2.5.29.14 **nekritické rozšírenie**	vygenerovaný systémom
crlDistributionPoints / 2.5.29.31 **nekritické rozšírenie**	**[1]CRL Distribution Point** **Distribution Point Name:** **Full Name:** **URL= http://pki.infra.npz.sk/techca/crl/nczi_techca-R1-1.crl**
Authority Key Identifier / 2.5.29.35 **nekritické rozšírenie**	**KeyID= Hodnota je automaticky pridávaná certifikačnou autoritou CA NZIS**
Extended Key Usage / 2.5.29.37 **kritické**	**Server Authentication (1.3.6.1.5.5.7.3.1)** **Client Authentication (1.3.6.1.5.5.7.3.2)**
certificatePolicies / 2.5.29.32* **nekritické rozšírenie**	**Policy Identifier=1.3.158.165387.100.90.10.20.10.20.1** **[1,1]Policy Qualifier Info:** **Policy Qualifier Id=CPS** **Qualifier:** **http:// pki.infra.npz.sk/cps/** **Notice text = Tento certifikat bol vydany pre ucely NCZI.**

subjectAltName / 2.5.29.17 nekritické rozšírenie	**dnsHostName, v závislosti od potreby, ak bude extenzia vyplnená musí obsahovať DNS meno na ktorom klienti kontaktujú službu**

6.8.9.2. Technologický certifikát pre doménové radiče

Algoritmy a dĺžky kľúčov uplatňované v certifikáte pre zariadenia a webové služby:

Algoritmus podpisu (Signature Algorithm)
Sha1

Verejný kľúč
RSA, dĺžka 2 048 bitov

Doba platnosti certifikátu CA
maximálne 2 roky

Tabuľka č. 20: Obsah položiek v certifikáte pre doménové radiče

Skratka názvu	OID	Názov	Hodnota
C	2.5.4.6	countryName	**SK** **Údaj je nepovinný**
O	2.5.4.10	organizationName	**Názov organizácie** **Údaj je nepovinný**
OU	2.5.4.11	organizationUnitName	**Identifikácia služby** **Údaj je nepovinný**
OU	2.5.4.11	organizationUnitName	**Identifikácia typu služby** **Údaj je nepovinný**
CN	**2.5.4.3**	**commonName**	**FDQN DC** **Hodnota je povinná**

Tabuľka č. 21: Použité rozšírenia (certificate extensions) v certifikáte doménové radiče

Rozšírenie / OID Typ rozšírenia	Hodnota
authorityInfoAccess / 1.3.6.1.5.5.7.1.1	**[1]Authority Info Access Access Method=Certification Authority Issuer (1.3.6.1.5.5.7.48.2) Alternative Name: URL= http://pki.infra.npz.sk/techca/cert/nczi_techca-R1-1.der**
keyUsage / 2.5.29.15 kritické rozšírenie	**Digital Signature, Key encipherment**
subjectKeyIdentifier / 2.5.29.14 nekritické rozšírenie	vygenerovaný systémom
crlDistributionPoints / 2.5.29.31 nekritické rozšírenie	**[1]CRL Distribution Point Distribution Point Name: Full Name:**

	URL= http://pki.infra.npz.sk/techca/crl/nczi_techca-R1-1.crl
Authority Key Identifier / 2.5.29.35 nekritické rozšírenie	KeyID= Hodnota je automaticky pridávaná certifikačnou autoritou CA NZIS
Extended Key Usage / 2.5.29.37 kritické	Server Authentication (1.3.6.1.5.5.7.3.1) Client Authentication (1.3.6.1.5.5.7.3.2) Smart Card Logon (1.3.6.1.4.1.311.20.2.2)
certificatePolicies / 2.5.29.32* nekritické rozšírenie	Policy Identifier=1.3.158.165387.100.90.10.20.10.20.1 [1,1]Policy Qualifier Info: Policy Qualifier Id=CPS Qualifier: http:// pki.infra.npz.sk/cps/ Notice text Tento certifikat bol vydany pre ucely NCZI.
subjectAltName / 2.5.29.17 nekritické rozšírenie	dnsHostName, v závislosti od potreby, ak bude extenzia vyplnená musí obsahovať DNS meno na ktorom klienti kontaktujú službu

6.8.10. Identifikácia kryptografických algoritmov

CA NZIS a používatelia certifikátov musia podporovať na podpisovanie a overovanie nasledovné algoritmy:

- RSA 2048 v súlade s PKCSRSA 2048 v súlade s PKCS#1
- SHA-1 v súlade s FIPS PUB 180-4 a ANSI X9.30 (cast 2) – [ID sha1WithRSAEncryption, OID 1 2 840 113549 1 1 5, Issuing Authority RSADSI]

6.8.11. Menná konvencia

Žiadne požiadavky.

6.8.12. Obmedzenia týkajúce sa mena

DN subjektu a vydavateľa je prítomné v každom certifikáte a spĺňa požiadavky RFC 5280. V položke CN je uvedené meno a priezvisko držiteľa.

6.8.13. Aplikované OID certifikačného poriadku

Každý vydaný certifikát obsahuje OID certifikačného poriadku CA NZIS.

6.8.14. Použitie rozšírenia „policy constraints“

Žiadne požiadavky.

6.8.15. Sémantika spracovanie kritických rozšírení CP

Kritické rozšírenia sú interpretované spôsobom definovaným v RFC 5280.

6.9. Profil CRL

6.9.1. Podporovaná verzia

CA NZIS publikuje CRL vo verzii X.509 verzia 2 v súlade s požiadavkami RFC 5280.

6.10. OCSP profil

6.10.1. Používaná verzia

CA NZIS poskytuje službu OCSP v súlade s RFC 2560.

6.10.2. Rozšírenia OCSP

Žiadne požiadavky.

7. AUDIT súladu a iné posudzovanie

CA NZIS je podrobovaná minimálne jeden krát ročne nezávislému bezpečnostného auditu na výkon poskytovaných certifikačných služieb. Výber audítora zabezpečí manažment CA NZIS v súlade s požiadavkami časť 8 CP CA NZIS.

CA NZIS zverejňuje prehlásenie audítora o výsledku auditu zhody na svojej web stránke.

8. Bezpečnostná kapitola pre certifikačné autority v rámci NZIS

1. Pre potreby PKI infraštruktúry NZIS bol vypracovaný dokument „Certifikačný poriadok“, ktorého obsahová stránka zodpovedá požiadavkám legislatívy v zmysle zákona č. 215/2002 Z. z. o elektronickom podpise.
2. Pre potreby PKI infraštruktúry NZIS bol vypracovaný dokument „Pravidlá poskytovania certifikačných služieb“, ktorého obsahová stránka zodpovedá požiadavkám legislatívy v zmysle zákona č. 215/2002 Z. z. o elektronickom podpise.
3. Organizácia bezpečnosti informácií sa riadi internými predpismi NCZI.
4. Infraštruktúra (jednotlivé komponenty) certifikačných autorít NZIS predstavuje kritické prvky NZIS.
5. Bezpečnosť ľudských zdrojov definuje role a základné zodpovednosti – iba vybraní pracovníci majú umožnení prístup k infraštruktúre certifikačných autorít NZIS.
6. Infraštruktúra certifikačných autorít NZIS je chránená bezpečnostným perimetrom pozostávajúceho s mechanických zábranných prostriedkov a technických zabezpečovacích prostriedkov, ktoré zabraňujú neautorizovanému prístupu.
7. Riadenie prístupu k infraštruktúre certifikačných autorít NZIS je definovaný na viacerých úrovniach:
    a. Fyzický prístup so priestorov serverovne
    b. Logický prístup na úrovni serverov
    c. Logický prístup na úrovni aplikácie/kryptografických zariadení
8. Vývojové a produkčné prostredia sú fyzicky oddelené.

9. Na ochranu citlivých informačných aktív (kryptografický materiál) sú použité špeciálne kryptografické prostriedky (HSM moduly)
10. Infraštruktúra certifikačných autorít NZIS je navrhnutá redundantným spôsobom, pre potreby zabezpečenia požadovanej úrovne dostupnosti služieb.
11. Pre potreby riadenia kontinuity činnosti bola spracovaná detailná inštalačná a prevádzková dokumentácia umožňujúca prevádzkovateľovi zabezpečiť kontinuitu činnosti systému.
12. Parametre kryptografického materiálu využívaného v rámci infraštruktúry certifikačných autorít NZIS zodpovedajú odporúčaniam Best Practice (požiadavky na dĺžky kľúčov, požiadavky na algoritmy).
13. V rámci infraštruktúry certifikačných autorít NZIS sú nasadené technológie zabezpečujúce dostupnosť a synchronizáciu presného času.
14. V rámci infraštruktúry certifikačných autorít NZIS sú nasadené technológie zabezpečujúce online poskytovanie informácií o stave a platnosti certifikátov.
15. V rámci infraštruktúry certifikačných autorít NZIS sú nasadené technológie zabezpečujúce priradenie presného času k definovaným udalostiam.
16. V rámci infraštruktúry certifikačných autorít NZIS sú nasadené technológie zabezpečujúce vytváranie a zber auditných záznamov.
17. V rámci infraštruktúry certifikačných autorít NZIS sú nasadené technológie zabezpečujúce ochranu pred neautorizovanou inštaláciou softvéru.

9. Ostatné obchodné a legislatívne otázky

9.1. Poplatky

9.1.1. Poplatok za vydanie a obnovu certifikátu

Všetky certifikačné služby sú zo strany CA NZIS poskytované bezodplatne.

9.2. Ochrana osobných údajov

9.2.1. Požiadavky na ochranu osobných údajov

CZ NCZI a jeho RA má spracovanú dokumentáciu týkajúcu sa ochrany osobných údajov držiteľov certifikátov v zmysle požiadaviek zákona č. 428/2002 Z. z. o ochrane osobných údajov v aktuálnom znení.

9.2.2. Informácie, ktoré nie sú považované za osobné

Pozri časť 10.3.2 aktuálneho CP CA NZIS.

9.2.3. Zodpovednosť za ochranu osobných údajov

Všetci držitelia certifikátov musia v maximálne možnej miere zabezpečiť bezpečnosť svojich súkromných kľúčov a informácií, ktoré chránia ich použitie (PIN, heslá). Za ochranu osobných údajov

v rámci CA NZIS zodpovedá poverená osoba NCZI v zmysle § 19 zákona č. 428/2002 Z. z. o ochrane osobných údajov v aktuálnom znení.

9.2.4. Súhlas so spracovaním osobných údajov

CA NZIS má k dispozícii písomný súhlas žiadateľ/držiteľa certifikátu so spracovaním jeho osobných údajov v systéme CA.

9.2.5. Podmienky zverejnenia osobných údajov

Pozri časť 9.4.5 aktuálneho CP CA NZIS.

9.3. Právo duševného vlastníctva

Súkromný kľúč je považovaný za výslovný majetok oprávneného držiteľa zodpovedajúceho verejného kľúča identifikovaného v certifikáte.

Tieto Pravidlá a ich OID sú majetkom NCZI a môžu byť použité len CA NZIS v súlade s ustanoveniami uvedenými v CP CA NZIS. Akékoľvek iné použitie týchto CPS a ich OID bez výslovného písomného súhlasu CA NZIS je zakázané.

9.4. Vyhlásenia a záruky

9.4.1. Záruky CA

Všetky informácie uvedené v certifikáte sú presné a správne do takej miery ako sú poskytnuté žiadateľom o certifikát v procese jeho identifikácie a autentifikácie. Záruky poskytované zo strany CA NZIS sú uvedené v zmluve uzavretej s držiteľom certifikátu pri jeho vydaní.

9.4.2. Záruky RA

RA poskytujúca služby v mene CA NZIS poskytuje záruky v súlade s poskytovanými zárukami CA NZIS.

9.5. Odmietnutie záruky

Podmienky odmietnutia záruky sú uvedené v zmluve uzavretej s držiteľom certifikátu.

9.6. Obmedzenie zodpovednosti

Žiadne požiadavky.

9.7. Náhrady

Žiadne požiadavky

9.8. Doba platnosti a jej ukončenie

9.8.1. Doba platnosti

Všetky verzie CP a CPS zostáva v platnosti pokiaľ nie sú nahradené novšími verziami. Nové verzie týchto dokumentov v plnej miere nahrádzajú predchádzajúce verzie.

9.8.2. Ukončenie doby platnosti

Pozri časť 9.10.1.

9.8.3. Následky ukončenia platnosti

CA NZIS uchováva vždy jeden exemplár z každej platnej verzie CP resp. CPS pre archívne účely a to v elektronickej forme. Elektronická forma je zabezpečená hešovacím algoritmom SHA1, aby zostala zachovaná jej integrita.

9.9. Notifikácia a komunikácia s držiteľmi

CA NCZI prednostne komunikuje s klientmi prostredníctvom e-mailových správ na adresu, ktorú títo zadali spolu so žiadosťou o vydanie certifikátu. Ďalšími spôsobmi komunikácie sú telefonická, listovú alebo priama komunikáciu na k tomu určených miestach.

V prípade, že sú zo strany držiteľov zaslané požiadavky e-mailom, poštou resp. sú vznesené telefonicky RA resp. CA NZIS takéto požiadavky zaznamená a vybaví rovnakým spôsobom ako keby boli predložené osobne

9.10. Zmeny a prílohy CP a CPS

9.10.1. Postup zmeny dokumentácie

PMA má právo posúdiť a prípadne revidovať tieto CPS. Chyby, požiadavky na aktualizáciu alebo navrhované zmeny týchto CPS je potrebné oznámiť kontaktu uvedenému v časti 1.4. Oznámenie musí obsahovať popis zmeny, zdôvodnenie zmeny a kontaktné údaje osoby, ktorá zmenu požaduje.

Po uplynutí doby určenej na posúdenie môže PMA navrhovanú zmenu prijať, prijať s úpravou alebo odmietnuť.

Tieto CPS sú revidované v pravidelnom intervale minimálne 1x ročne, bez ohľadu na to, či v danom časovom období sú navrhované ich zmeny, alebo nie. Za revíziu týchto CPS je zodpovedná Autorita pre správu CP (PMA) – pozri 1.3.1.1.

9.10.2. Notifikácia o zmene dokumentácie

Všetky zmeny CPS sú dané na vedomie subjektom, ktorých sa týkajú v perióde aspoň jedného mesiaca. Elektronická verzia tohto CPS musí byť dostupná na verejnej web stránke NCZI.

9.10.3. Okolnosti, za ktorých sa musí OID byť menené

V prípade, že prípadné zmeny v týchto CPS výrazne ovplyvnia ich obsah v porovnaní s pôvodnou verziou, môže PMA rozhodnúť o pridelení nového OID pre takto zmenené CPS.

9.11. Riešenie sporov

Pozri časť 10.12 aktuálneho CP CA NZIS.

9.12. Uplatňované právne predpisy

Pri rozhodovaní v súdnych sporoch sa uplatňuje právo Slovenskej republiky.

9.13. Súlad s platnými zákonmi

Všetky zúčastnené strany sú povinné dodržiavať pri poskytovaní a využívaní služieb CA NZIS požiadavky Zákona č. 215/2002 Z. z. o elektronickom podpise, Zákona č. 153/2013 Z.z. o národnom zdravotnom informačnom systéme a vykonávacích vyhlášok NBÚ č. 131 až 136/2009 Z. z. v aktuálnom znení.

9.14. Rôzne ustanovenia

9.14.1. Platnosť zmluvy

Zmluva sa uzatvára na dobu určitú, ktorá je určená dobou platnosti karty a certifikátov vydaných na základe návrhu zmluvy.

Zmluva zaniká dohodou zmluvných strán alebo odstúpením ktoroukoľvek zo zmluvných strán v prípade podstatného porušenia zmluvnej alebo zákonnej povinnosti. Ukončenie a zánik zmluvy nemá vplyv na vyrovnanie všetkých záväzkov, ktoré medzi zmluvnými stranami vznikli počas jej platnosti.

9.14.2. Obmedzenia zmluvy

Žiadateľ udeľuje v zmysle ust. § 7 zákona č. 428/2002 Z. z. O ochrane osobných údajov v znení neskorších predpisov súhlas s tým, aby všetky osobné údaje Žiadateľa uvedené v Žiadosti na základe ktorej bola uzavretá zmluva, rovnako ako aj jeho osobné údaje uvedené v zmluve, boli spracovávané v informačnom systéme poskytovateľa. Osobné údaje Žiadateľa budú spracovávané len za účelom ich využitia pri vykonávaní a poskytovaní certifikačných služieb Poskytovateľa. Žiadateľ udeľuje tento súhlas na dobu, počas ktorej je Poskytovateľovi zákonom stanovená povinnosť uchovávať Žiadosti o vydanie certifikátov. Súhlas môže byť odvolaný písomne avšak najskôr len súčasne s ukončením tejto zmluvy.

9.14.3. Výnimky

Zmluvu je možné meniť len po vzájomnej dohode, písomne, formou očíslovaných dodatkov podpísaných oboma zmluvnými stranami.

9.14.4. **Vyššia moc**

Zmluvné strany sa dohodli, že v súlade s §262 Obchodného zákonníka sa táto zmluva spravuje ustanoveniami Obchodného zákonníka.

9.15. **Ostatné dojednania**

Žiadne požiadavky