eHealth
elektronické zdravotníctvo

eSO1
eHealth služby občanom

TVORÍME VEDOMOSTNÚ SPOLOČNOSŤ

CP CA NZIS

Elektronické služby zdravotníctva

kód ITMS projektu: **2110120009**

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

Obsah

1. ÚVOD

Tento dokument definuje certifikačný poriadok certifikačnej autority Národného centra zdravotníckych informácií (ďalej aj „CA NZIS“) pre použitie na vydávanie certifikátov zdravotníckym profesionálom určených na používanie v rámci Národného zdravotného informačného systému (NZIS).

Tento CP obsahuje pravidlá pre vydávanie a používanie certifikátov tým osobám, ktoré sú oprávnené využívať NZSI. Štruktúra CP 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.

Bezpečnostné mechanizmy poskytované v rámci NZIS sú určené na použitie v kombinácii s jedným alebo viacerými ďalšími bezpečnostnými opatreniami na dostatočné zabezpečenie ochrany citlivých informácií.

1.1. Prehľad

Pri odvolávaní sa na tento dokument môžu byť použité pojmy "CP", "poriadok" alebo CP CA NZIS. CP CA NZIS je určený na manažovanie a využívanie certifikátov, ktoré obsahujú verejné kľúče slúžiace na identifikáciu, autentizáciu, elektronické podpisovanie, prístup do registrov zdravotného poistenia, šifrovanie citlivých informácií v rámci NZIS.

CP je určený na použitie v určitých situáciách a identifikuje špecifické úlohy a zodpovednosti pre:

- CA NZIS pri vydávaní certifikátov pre potreby NZIS,
- registračné autority (RA),
- držiteľov certifikátov a
- spoliehajúce sa strany,

pričom všetky tieto špecifické povinnosti sú v ňom popísané.

Certifikačná autorita musí byť zviazaná a používať jeden alebo viac koreňových certifikátov a musí vydávať príslušný počet zoznamov zrušených certifikátom (CRL). Používané certifikáty CA NZIS musia byť k dispozícii držiteľom certifikátov.

Použitie šifrovacích kľúčov je vhodné pre utajenie / šifrovanie určených informácií.

Akékoľvek spory týkajúce sa kľúčov alebo manažmentu certifikátov podľa tejto politiky, pokiaľ nie sú vyriešené dotknutými stranami pomocou k tomu určených mechanizmov (rokovanie, mediácia, rozhodcovské konanie) môžu byť predložené na riešenie príslušnému súdu a riadia sa platnými zákonmi Slovenskej republiky.

Certifikačná autorita NCZI:

- zruší platnosť certifikátu len v prípadoch, ktoré sú uvedené v tomto CP,
- je povinná viesť záznamy alebo logy spôsobom popísaným v tomto CP,

- musí zabezpečiť oddelenie kritických funkcií CA medzi najmenej tri osoby priradené do rôznych dôveryhodných rolí.

Len oprávnený držiteľ môže vlastniť súkromný kľúč určený na operácie v prostredí NZIS. Kľúče a k nim vydané certifikáty môžu mať dobu platnosti, ako je uvedené v tomto poriadku.

Žiadne údaje poskytnuté držiteľom pre potreby CA NZIS nesmú byť zverejnené bez jeho súhlasu, ak to nevyžaduje zákon alebo súdny príkaz.

CA činnosti podliehajú kontrole vykonávanej Policy Management Authority (PMA) alebo jej zástupcom podľa uváženia PMA.

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) CP CA NZIS (1)

Tento poriadok bola navrhnutý pre použitie v určitých situáciách a identifikuje konkrétne úlohy pre ich vykonanie. Certifikačná autorita (CA), registračné autority (RA), osoby zodpovedná za úložisko, držitelia certifikátov a spoliehajúce sa strany majú špecifické povinnosti, ktoré sú uvedené v tomto poriadku.

1.3. Účastníci PKI

Tento CP bol pripravený tak, aby spĺňal všeobecné požiadavky na certifikát verejného kľúča v zmysle Zákona č. 215/2002 Z. z. o elektronickom podpise v aktuálnom znení a požiadavky RFC 3647.

CA NZIS môže postúpiť povinnosti a iné zodpovednosti ustanovené v tomto poriadku na tretiu osobu, ktorá súhlasí s tým, že bude viazaná týmto poriadkom. CA NZIS zostáva zodpovedná za výkon postúpených povinností a zodpovedností treťou stranou v súlade s touto politikou v plnom rozsahu.

1.3.1. Autorita na správu politík

Autorita na správu politík (Policy Management Authority - PMA) je zložka ustanovená za účelom:

- dohľadu na vytváranie a aktualizáciu certifikačných politík (CP, CPS) a iných dokumentov, vrátane vyhodnocovania zmien a plánov na implementovanie prijatých zmien tak, aby sa zaručilo, že prax CA NZIS vyhovuje príslušnému CP,
- revízie výsledkov auditov zhody, aby sa určilo, či CA NZIS adekvátne dodržuje ustanovenia schválených politík,
- dávania odporúčaní pre CA NZIS týkajúcich sa nápravných opatrení a iných vhodných akcií,
- dávania odporúčaní ohľadne vhodnosti certifikátov asociovaných s daným CP pre špecifické aplikácie riadenia a usmerňovania činnosti certifikačnej autority a registračných autorít,
- výkladu ustanovení CPS a svojich pokynov pre RA a CA,
- vykonávania auditu CA NZIS,
- zabezpečenia, že prijatý a schválený certifikačný poriadok (CP) a pravidlá na výkon certifikačných činnosti (CPS) sú riadne a náležite realizované.

PMA predstavuje vrcholovú zložku, ktorá rozhoduje s konečnou platnosťou vo všetkých záležitostiach a aspektoch týkajúcich sa CA NZIS a jej činnosti.

1.3.2. Certifikačná autorita (CA)

CA, ktorá vydáva certifikáty v súlade s touto politikou:

- vytvorí, podpíše, distribuuje a ruší certifikáty zaväzujúce X.500 Distinguished Name žiadateľa (držiteľa) s ich verejným kľúčom a tým aj ich podpisovým kľúčom (súkromný kľúč),
- poskytuje informáciu o stave certifikátov prostredníctvom zoznamy zrušených certifikátov (CRL) a prípadne cez Online Certificate Status Protocol (OCSP),
- má pripravené, implementované a prevádzkuje postupy pri poskytovaní certifikačných služieb tak, aby boli adekvátne dosiahnuté požiadavky tohto poriadku.

Konkrétne praktiky a postupy CA NZIS, ktorými sa vykonávajú požiadavky tohto CP musia byť stanovené v pravidlách na výkon certifikačných činností (CPS) alebo z iných verejne dostupných dokumentoch.

1.3.3. Registračné autority (RA)

RA prevádzkovaná v zmysle tohto certifikačného poriadku je zodpovedná za všetky povinnosti, ktoré na ňu kladené zo strany vydávajúcej CA NZIS.

1.3.4. Personalizačné pracovisko

Zabezpečuje potlač čipových kariet, ich inicializáciu a sprostredkovanie vydania certifikátov na čipové karty, ako aj dohľad nad kartami.

1.3.5. Držitelia

Držiteľmi certifikátu vydávaného CA NZIS môžu byť fyzické osoby, ktoré ich budú využívať na autentifikáciu resp. elektronický podpis v rámci NZIS alebo ako technologické certifikáty v rámci NZIS.

Certifikát pre potreby NZIS môže byť vydaný len na základe predloženej žiadosti a následnej autorizácie zo strany zodpovednej osoby.

Vhodnosť vydania certifikátu je na zvážení CA NZIS. CA NZIS môže spravovať akýkoľvek počet držiteľov certifikátov.

1.3.6. Spoliehajúce sa strany

Spoliehajúce sa strany sú používatelia NZIS.

Akceptovaním certifikátu vydaného v súlade s ustanoveniami tohto poriadku, vrátane a nie len na základe požiadaviek uvedených v časti 2.1.4 a jej podkapitol, spoliehajúca sa strana súhlasí s tým, že bude viazaná ustanoveniami tohto poriadku.

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 alebo ako technologické certifikáty 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 CP

Za správu (vypracovanie, udržiavanie, aktualizáciu) tohto CP 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 CP 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)
DN	-	Rozlišujúce meno (Distinguished name)
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
ETSI	-	Európsky telekomunikačný štandardizačný úrad (European Telecommunications Standards Institute)
ePZP	-	Elektronický preukaz zdravotníckeho pracovníka

2. Zverejňovanie informácií a úložisko

2.1. Úložisko

Úložisko CA NZIS je prevádzkovaný 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

Vydávajúca CA NZIS musí:

- uvádzať v každom vydanom certifikáte URL webovej stránky ňou vedenej resp. vedenej v jej mene,
- zabezpečiť zverejnenie tohto CP a k nemu patriacich CPS, na webových stránkach, vedených CA NZIS alebo v mene CA NZIS, pričom umiestnenie stránky musí byť v súlade s požiadavkami uvedenými v časti 8,
- zabezpečiť, priamo alebo prostredníctvom zmluvy, že operačný systém resp. systém kontroly prístupu bude nakonfigurovaný tak, aby len oprávnené osoby mohli prepísať resp. modifikovať takto publikovaný CP resp. CPS,
- poskytujú plnú textovú verziu svojich CPS ak je to potrebné pre účely akéhokoľvek auditu, kontroly alebo akreditácie,
- poskytuje verejnosti konečné prehlásenie z akéhokoľvek auditu vykonaného k zabezpečeniu súladu s požiadavkami na audit zo strany PMA.

2.3. Čas a frekvencia zverejňovania informácií

Všetky informácie musia byť zverejnené v úložisku ihneď ako je taká informácia k dispozícii CA NZIS. Certifikáty vydané certifikačnou autoritou, ktoré odkazujú na tento poriadok budú zverejnené ihneď po ich vydaní.

2.4. Kontroly prístupu k úložisku

CA NZIS musí chrániť 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 boli vykonané logické a bezpečnostné opatrenia, aby zabránili neautorizovanému prístupu osobám, ktoré by mohli akýmkoľvek spôsobom zmeniť, poškodiť, pridať resp. vymazať údaje uložené v repozitári.

3. Identifikácia a autentizácia

V tejto časti sú popísané postupy, ktoré CA NZIS používa na overenie identity a/alebo iných atribútov žiadateľa o vydanie certifikátu buď priamo na CA resp. na príslušných RA.

Tiež popisuje, ako sú overované strany pokiaľ požadujú opakované vydanie certifikátu resp. zrušenie certifikátu. Táto časť rieši aj postupy týkajúce sa používaných mien, vrátane uznávania práv k ochrannej známke v niektorých menách.

3.1. Pomenovanie

3.1.1. Typy mien

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

3.1.2. Potreba zmysluplnosti mien

Obsah poľa obsahujúci meno držiteľa resp. názov vydavateľa certifikátu musí mať spojitosť s identifikovateľným menom osoby resp. inej entity. V prípade fyzických osôb to môže byť výhradne kombinácia mena a priezviska držiteľa.

3.1.3. Anonymita alebo pseudonymita držiteľov

Používanie pseudonymov, prezývok, krycích mien, aliasov a podobne (tzv. nicknames) v certifikátoch nie je dovolené.

3.1.4. Pravidlá pre interpretáciu rôznych foriem mien

Nie sú definované žiadne podmienky.

3.1.5. Jedinečnosť mien

Nie je požadovaná jedinečnosť mien v rámci komunity držiteľov certifikátov, avšak je 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.

3.2. Prvotné overenie identity

3.2.1. Spôsob preukazovania vlastníctvo súkromného kľúča

Vzhľadom k tomu, že generovanie súkromného kľúča uskutoční vydávajúca CA NZIS priamo na čipovú kartu, nie je potrebné zo strany žiadateľa preukazovanie jeho vlastníctva.

3.2.2. Overenie identity organizácie

Certifikáty pre organizácie nebudú vydávané.

3.2.3. Overenie identity fyzickej osoby

Overenie identity fyzickej osoby prebehne na základe vzájomnej kontroly elektronickej a papierovej formy dokumentov žiadosti o vydanie certifikátu, ktorá bude okrem iného obsahovať aj osobné údaje žiadateľa požadované CA NZIS.

3.2.4. Neoverované údaje o žiadateľovi

Nie sú definované žiadne podmienky.

3.2.5. Overovanie právomocí

V rámci overovania právomocí pracovník CA NZIS resp. RA vykoná formálnu kontrolu, či žiadateľ o certifikát má oprávnenie pristupovať do NZIS (pracovník overuje údaje zo žiadosti voči autoritatívnemu zdroju dát (JRÚZ).

3.2.6. Kritériá pre interoperabilitu

Nie sú definované žiadne podmienky.

3.3. Identifikácia a autentizácia pri obnove certifikátu

Obnova certifikátu znamená rutinnú výmenu kryptografických kľúčov pred exspiráciou certifikátu alebo výmenu kľúčov po zrušení platného certifikátu.

3.3.1. Obnova certifikátu

Vzhľadom na totožnú dobu platnosti čipovej karty a certifikátov, ktoré sú na nej uložené, sa obnova certifikátov (vydávanie následných certifikátov) pri ich prirodzenej exspirácií nevykonáva.

3.3.2. Obnova certifikátu po jeho zrušení

Ak sa informácie obsiahnuté v certifikáte zmenili alebo je známe alebo existuje podozrenie kompromitácie súkromného kľúča, musí CA NCZI pred obnovou certifikátu overiť identitu žiadateľa rovnakým spôsobom, ako pri prvotnej registrácii. CA NCZI alebo RA oprávnená konať v jej mene musia overiť akúkoľvek zmenu informácií obsiahnutých v žiadosti ešte pred jeho vydaním..

3.3.3. Identifikácia a autentifikácia žiadosti o zrušenie certifikátu

V situáciách, ktoré nepredstavujú riziko zneužitia karty inou osobou ako je jej držiteľ bude zrušenie platnosti neaktuálnych kariet vrátane certifikátov realizované technickým spôsobom (CMS). V tomto prípade o zrušenie platnosti certifikátov držiteľ karty nežiada.

V situáciách, ktoré predstavujú riziko zneužitia karty inou osobou ako je jej držiteľ bude zrušenie platnosti neaktuálnych kariet vrátane certifikátov realizované bezodkladne jedným z nasledovných spôsobov:

- kontaktovaním registračnej autority,
- kontaktovaním certifikačnej autority,

Všetky žiadosti o zrušenie certifikátu musia byť zaznamenané.

.

4. Prevádzkové požiadavky

4.1. Žiadanie o certifikát

CA NZIS musí zabezpečiť, že všetky postupy a požiadavky kladené na žiadosť o vydanie certifikátu sú popísané v CPS alebo inom verejne dostupnom dokumente.

4.1.1. Žiadatelia o certifikát

Žiadateľom o certifikát môže byť fyzická osoba, ktorá je oprávnená využívať NZIS, a ktorá splnila požiadavky dané týmto CP a súvisiacim CPS.

4.1.2. Postup žiadania a zodpovednosti

Žiadateľ o certifikát vyplní žiadosť o certifikát vo forme žiadosti o elektronický preukaz zdravotníckeho pracovníka (ePZP) a túto doručí vopred certifikačnej autorite NCZI alebo vyplní žiadosť o technologický certifikát. Podrobnosti vytvorenia žiadosti a spôsob zasielania bude stanovený v príslušnom CPS.

CA NZIS musí zabezpečiť, že každá doručená žiadosť bude sprevádzaná:

- overením súladu údajov na zaslanej žiadosti s údajmi v systéme CA NZIS
- overením existencie záznamu v JRUZ a
- overením splnenia náležitostí týkajúcich sa overenia identity a autenticity žiadateľa (pozri časť 4.2.1)

Zaslaním žiadosti nevzniká CA NZCI automatická povinnosť na vydanie certifikátu.

4.2. Spracovanie žiadosti o certifikát

4.2.1. Spôsob overenia identity a autenticity žiadateľa

Overenie identity a autenticity žiadateľa vykoná CA NZIS resp. RA vystupujúca v jej mene na základe zaslanej žiadosti o ePZP, ktorá bude obsahovať údaje preukazujúci identitu a autenticitu žiadateľa). CA NZIS resp. RA vykoná formálnu kontrolu súladu elektronickej žiadosti s predloženým dokumentom.

4.2.2. Schválenie alebo zamietnutie žiadosti

Pokiaľ overenie identity a autenticity vykonané CA NZIS resp. RA bude úspešné a všetky ostatné náležitosti žiadosti v poriadku bude žiadosť postúpená CA NZIS na vydanie certifikátu. Pokiaľ pri overenie identity a autenticity preukáže nezrovnalosti v predložených údajoch resp. žiadosti, vydanie certifikátu bude CA NZIS zamietnuté. CA NZIS nebude vydávať certifikát bez existencie žiadosti zo strany potenciálneho držiteľa.

4.2.3. Spracovanie žiadosti o vydanie certifikátu

Po postúpení žiadosti certifikačnej autorite NCZI táto pristúpi k procedúre vydania bez zbytočného zdržania.

4.3. Vydanie certifikátu

4.3.1. Činnosť CA NZIS pri vydaní certifikátu

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

4.4. Prevzatie certifikátu

4.4.1. Spôsob prevzatia certifikátu

CA NZIS odovzdá ePZP s vygenerovanými kľúčmi a vydaným certifikátom dôveryhodným spôsobom žiadateľovi na pracovisku CA/RA.

4.4.2. Notifikácia o vydaní certifikátu iným entitám

Nie sú definované žiadne podmienky.

4.5. Kľúčový pár a používanie certifikátu

4.5.1. Súkromný kľúč držiteľa a používanie certifikátu

Držiteľ certifikátu je povinný používať svoj súkromný kľúč a certifikát len v systéme NZIS na svoju autentifikáciu resp. podpisovanie elektronických dokumentov v zmysle podmienok ich používania dohodnutých v zmluve. Na autentifikáciu a podpisovanie môže používať len k tomu účelu určené aplikácie. Používanie súkromného kľúča zo strany je možné len v prípade, že tento akceptoval naň vydaný certifikát. V prípade, že bol certifikát zrušený resp. skončila doba jeho platnosti je používanie jemu zodpovedajúceho súkromného kľúča zakázané.

4.5.2. Používanie certifikátu a verejného kľúča spoliehajúcou sa stranou

Spoliehajúca strana sa môže spoliehať na podpísaný elektronický dokument obsahujúci certifikát držiteľa len v prípade, že sa tento nachádza v systéme NZIS resp. bol získaný z tohto systému a bola plne overená jeho platnosť buď prostredníctvom zoznamu zrušených certifikátov (CRL) alebo služby OCSP. Spoliehajúca sa strana musí dodržiavať všetky podmienky, ktoré sú stanovené pre prácu v systéme NZIS.

4.6. Obnova certifikátu na pôvodné kľúče – tzv. recovery

Obnova certifikátu bez zmeny žiadateľovho/držiteľovho verejného kľúča nie je možná.

4.7. Obnova certifikátu na nové kľúče – tzv. renewal

Pod obnovou certifikátu sa rozumie jeho vydanie na novo vygenerované kľúče za podmienok, že nedôjde k zmene údajov v predmetnej časti v porovnaní s pôvodným certifikátom.

4.7.1. Okolnosti obnovy certifikátu na nové kľúče

Obnova certifikátu s vygenerovaním nového kľúčového páru sa uskutoční v prípade:

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

4.7.2. Kto môže žiadať o obnovu certifikátu na nové kľúče

O obnovu certifikátu na nové kľúče môže požiadať len oprávnený držiteľ pôvodného certifikátu.

4.7.3. Postup žiadania o obnovu certifikátu

Obnova certifikátu po jeho zrušení z akéhokoľvek dôvodu resp. po jeho exspirácii je možná len rovnakým spôsobom ako bolo vykonané prvotné vydanie certifikátu.

4.7.4. Spôsob prevzatia obnoveného certifikátu

Prevzatie obnoveného certifikátu sa vykoná rovnakým spôsobom ako pri jeho prvotnom vydaní.

4.7.5. Zverejnenie obnoveného certifikátu

Vykoná sa rovnakým spôsobom ako pri jeho prvotnom vydaní.

4.7.6. Notifikácia o vydaní obnoveného certifikátu spoliehajúcim sa stranám

Vykoná sa rovnakým spôsobom ako u prvotného vydania.

4.8. 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 novo platnými údajmi. Vydanie nového certifikátu sa vykoná rovnako ako v prípade vydanie pôvodného certifikátu (pozri časť 4.).

4.9. Zrušenie certifikátu

4.9.1. Okolnosti zrušenia certifikátu

Certifikát je možné zrušiť v nasledovných prípadoch:

- držiteľ certifikátu alebo iná oprávnená strana požiada o zrušenie certifikátu,
- je podozrenie, že bol kompromitovaný súkromný kľúč (zodpovedajúci verejnému kľúču v certifikáte), alebo certifikát bol iným spôsobom zneužitý,
- ukázalo sa, že držiteľ certifikátu nedodržuje svoje povinnosti držiteľa certifikátu, ktoré ho zmluvne viažu,
- identifikačné informácie alebo pričlenené prvky ľubovoľných mien v certifikáte sa stanú neplatnými,
- je podozrenie, že certifikát nebol vydaný v súlade s týmto CP resp. zodpovedajúcimi CPS,
- zistilo sa, že niektorá z informácií uvedených v certifikáte je chybná alebo nesprávna,
- CA NZIS ukončí z akéhokoľvek dôvodu svoju činnosť a zmluvne nezaisti u inej CA, aby poskytovala informácie o zrušených certifikátoch v mene CA NZIS,
- skončili okolnosti, ktoré vyžadovali vydanie certifikátu (testovanie, overovanie aplikácií ap.),
- došlo ku strate súkromného kľúča,
- technické parametre alebo formát certifikátu by mohli viesť k neakceptovateľnému riziku z pohľadu dodávateľov softvéru alebo spoliehajúcich sa strán (zmena kryptografických algoritmov na podpisovanie, dĺžka kryptografických kľúčov ap.),
- smrť držiteľa certifikátu,
- došlo ku kompromitácii súkromného kľúča vydávajúcej CA NZIS,

4.9.2. Kto môže žiadať o zrušenie certifikátu

Držiteľ certifikátu (alebo ním poverená fyzická alebo právnická osoba) môže kedykoľvek požiadať o zrušenie svojho vlastného certifikátu.

O zrušenie certifikátu môže tiež požiadať:

- pracovník CA NZIS alebo RA konajúcej v jej mene, pričom daný pracovník je povinný písomne zdokumentovať túto skutočnosť vrátane dôvodu svojho konania,
- Člen PMA ak sa zistí závažnú skutočnosť na zrušenie certifikátu (pozri časť 4.9.1.)

4.9.3. Procedúra žiadosti o zrušenie certifikátu

Žiadosť o zrušenie certifikátu možno podať:

- osobne v sídle CA NZIS resp. v sídle RA konajúcej v jej mene,
- telefonicky na telefónnom čísle patriacom CA NZIS resp. RA konajúcej v jej mene.

4.9.4. 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.

4.9.5. Čas na zrušenie certifikátu

CA NZIS je povinná 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 zrušenia certifikátu.

4.9.6. Povinnosti overovania stavu certifikátu zo strany spoliehajúcich sa strán

Spoliehajúce sa strany sú povinné pred tým ako sa spoľahnú na elektronický podpis resp. inú skutočnosť zviazanú s vydaným certifikátom overiť jeho platnosť buď použitím aktuálneho vydaného zoznamu zrušených certifikátov (CRL) alebo využitím službu potvrdzovania existencie a platnosti certifikátu (OCSP).

4.9.7. Frekvencia zverejňovania CRL

Zoznam zrušených certifikátov (CRL) je vydávaný s frekvenciou minimálne 1 krát za 24 hodín.

4.9.8. Čas zverejnenia vydaného CRL

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

4.9.9. Overovanie stavu certifikátu prostredníctvom OCSP

Spoliehajúce sa strany majú k dispozícii možnosť overenia aktuálneho stavu certifikátu prostredníctvom služby potvrdzovania existencie a platnosti certifikátu OCSP. Služba OCSP je dostupná na URL adrese uvedenej v predmetnom certifikáte.

4.9.10. Požiadavky na overenie stavu certifikátu prostredníctvom OCSP

Pri overovaní stavu certifikátu prostredníctvom protokolu OCSP musí žiadosť o zistenie stavu zodpovedať požiadavkám RFC 2560. Za odoslanie korektnej žiadosti sú zodpovedné spoliehajúce sa strany.

4.9.11. Pozastavenie platnosti certifikátu

Pozastavenie certifikátu nie je zo strany CA NZIS podporované.

4.10. Služby overovania stavu certifikátu

4.10.1. Charakteristika služby

CA NZIS poskytuje službu overovania stavu certifikátu buď prostredníctvom zverejňovania zoznamu zrušených certifikátov alebo prostredníctvom služby potvrdenia existencie a platnosti certifikátu (OCSP).

4.10.2. Dostupnosť služby

Aktuálny zoznam je dostupný na URL uvedenom v predmetnom certifikáte.

4.11. Ukončenie zmluvného vzťahu

Zmluva o vydaní certifikátu pre potreby identifikácie a autentifikácie v NZIS je uzatváraná na dobu 5 rokov. Zmluva sa automaticky nepredlžuje a po skončení jej platnosti musí žiadateľ o certifikát uzatvoriť novú zmluvu. Platnosť zmluvy sa automaticky ukončí v prípade, že certifikát, ktorý bol na základe nej vydaný, je zrušený. Takéto zrušenie si vyžaduje okamžité zrušenie certifikátu zo strany CA NZIS, ktorý bol na základe danej zmluvy vydaný.

4.12. Obnova kľúčov z depozitu alebo zálohy

CA NZIS nepodporuje uchovávanie súkromných kľúčov držiteľov certifikátov.

5. Manažérske, prevádzkové a fyzické bezpečnostné opatrenia

5.1. Fyzické bezpečnostné opatrenia

5.1.1. Umiestnenie, priestory a prístup

Umiestnenie infraštruktúry CA NZIS musí zabezpečiť že:

- priestory CA sú nepretržite fyzicky alebo elektronický monitorované proti neoprávnenému vniknutiu,
- samostatný prístup k serverom CA budú mať len osoby nachádzajúce sa na zozname oprávnených osôb s právom prístupu,
- osoby, ktoré nie sú na zozname oprávnených osôb na vstup budú vstupovať do priestorov CA len pod dohľadom oprávnenej osoby,
- záznamy o vstupe do priestorov sú udržiavané a kontrolované pravidelne,
- všetky vymeniteľné médiá a dokumenty obsahujúce citlivé informácie sú uložené v zabezpečených kontajneroch.

Všetky pracoviská RA resp. RA pracovné stanice používané pre on-line komunikáciu s CA NZIS musí byť umiestnená v priestoroch, ktoré spĺňajú nasledujúce požiadavky:

- nepretržitý fyzický alebo elektronický monitoring proti neoprávnenému vniknutiu,
- prístup bez sprievodu zodpovednej osoby je možný len osobám na zozname oprávnených osôb,
- prístup osobám, ktorý nie sú na zozname oprávnených osôb je umožnený len v sprievode a pod dohľadom oprávnenej osoby,
- všetky vymeniteľné médiá a dokumenty obsahujúce citlivé informácie sú uložené v zabezpečených kontajneroch.

CA NZIS zabezpečí prevádzku RA tak, že zaistí primeranú bezpečnosť kryptografickému modulu s podpisovými kľúčmi CA a systémovému softvéru.

Držitelia by nemali ponechať svoje pracovné stanice bez dozoru, pokiaľ sú kryptografické kľúče používané t.j. keď PIN alebo heslo už boli zadané. Pracovné stanice, ktoré majú uložený súkromný kľúč na pevnom disku musia byť fyzicky zabezpečené alebo chránené vhodným produktom riadenie prístupu.

Certifikáty pracovníkov RA, ktoré sú umiestnené na bezpečnom hardvérovom zariadení musia byť chránené fyzicky. To môže byť vykonané napríklad tým, že je zariadenie je prechovávané u jeho držiteľa.

5.1.2. Dodávka energie a klimatizácia

NCZI musí zabezpečiť že zdroj elektrickej energie a klimatizácia bude postačujúca k bezproblémovému chodu systému CA.

5.1.3. Ohrozenie vodou

NCZI musí zabezpečiť, že CA systém je chránený pred ohrozením vodou.

5.1.4. Protipožiarna ochrana

NCZI musí zabezpečiť, že CA systém je chránený protipožiarnym systémom.

5.1.5. Uchovávanie médií

CA NZIS musí zabezpečiť, že uchovávané média používané v systéme CA sú chránené pred nepriaznivými účinkami okolitého prostredia ako sú teplota, vlhkosť a elektromagnetické žiarenie. Záložné kópie musia byť uchovávané v oddelených priestoroch chránených pred zničením požiarom resp. vodou.

5.1.6. Nakladanie s odpadom

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

5.1.7. Záložné pracovisko

CA NZIS musí zabezpečiť, že záložné pracovisko, ak existuje, musí mať rovnakú úroveň bezpečnosti ako primárne pracovisko CA.

5.2. Procedurálne bezpečnostné opatrenia

5.2.1. Dôveryhodné roly

5.2.1.1. Dôveryhodné roly CA

CA NZIS musí zabezpečiť rozdelenie povinností pre kritické funkcie CA, aby sa zabránilo, že jedna osoba môže zneužiť systém CA bez možnosti zistenia. Každý prístup užívateľa do systému by mal byť prístup obmedzený len na tie akcie, ktoré sú potrebné na vykonanie pri plnení ich povinností.

CA NZIS musí mať minimálne tieto odlišné roly v rámci PKI, ktoré oddelia každodennú správu systému CA, manažment a auditu tejto správy a manažment podstatných zmien v požiadavkách na systém, vrátane politiky, poriadkov, postupov a personálu.

Rozdelenie zodpovednosti medzi týmito tromi rolami je nasledujúci, pričom sú uvedené len príklady najčastejšie vykonávaných činnosti:

Systémový administrátor:

- konfigurácia a údržba hardvéru a softvéry systému CA,
- spúšťanie a ukončovanie služieb CA.

Bezpečnostný správca zabezpečuje najmä:

- celkovú systémovú a sieťovú bezpečnosť infraštruktúry CA NZIS,
- analýzu auditovacích logov,
- pravidelné a nepravidelné kontroly:

- o výkonu činností všetkých pracovníkov CA NZIS v zmysle definovaných smerníc,
- o fyzickej bezpečnosti a objektovej bezpečnosti,
- o zabezpečenia infraštruktúry CA NZIS.

Audítor systému:

- overovanie auditných záznamov,
- overovanie dodržiavania súladu CP a CPS,

Člen PMA

- správa CA bezpečnostnej politiky,
- správa CP a CPS
- revízie výsledkov auditov zhody
- Alternatívne rozdelenie povinností, ktoré poskytuje rovnaký stupeň odolnosti k útokom z vnútra môže byť prijateľné.

Iba osoby zodpovedné za vyššie uvedené povinností majú povolený prístup k softvéru, ktorý riadi prevádzku CA NZIS.

5.2.1.2. Dôveryhodné roly RA

CA NZIS musí zabezpečiť, aby pracovníci RA pochopili svoju zodpovednosť za identifikáciu a overovanie žiadateľov a vykonávanie nasledovných funkcií:

- prijatie žiadosti, zmena certifikátu, rušenie certifikátu,
- overenie identity a autenticity žiadateľa,
- prenos informácie o žiadateľovi k CA,
- overovanie všetkých ostatných informácií súvisiacich s vydaním certifikátu

5.2.2. Počet osôb potrebný na výkon úloh

Generovanie kľúčov CA NZIS si vyžaduje prítomnosť najmenej troch rolí CA NZIS. Pracovníci môžu samostatne vykonávať všetky prevádzkové povinnosti spojené s ich rolou v CA NZIS.

CA NZIS musí zabezpečiť, že ktorýkoľvek zavedený overovací proces poskytne celkový prehľad všetkých aktivít vykonaný pracovníkmi v dôveryhodných rolách.

5.2.3. Identifikácia a autentizácia jednotlivých rolí

Všetky CA alebo RA zamestnanci sa musia podrobiť overeniu identity a oprávnení pred tým, ako:

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

Každý z týchto certifikátov a účtov (s výnimkou podpisových certifikátov CA NZIS):

- musí byť priamo priradený fyzickej osobe,
- nemôže byť zdieľaný,
- musí mať obmedzený rozsah oprávnení na oprávnenia danej roly v CA softvéri, operačnom systéme a riadení procesov.

CA operácie musia byť, pri prístupe cez zdieľanú sieť, zabezpečené použitím mechanizmov, akými sú silná autentifikácia a šifrovanie s využitím hardvérových tokenov.

5.3. Personálne opatrenia

NCZI musí zabezpečiť, že všetci zamestnanci vykonávajúci povinnosti v súvislosti s prevádzkou CA alebo RA musia:

- byť písomne menovaní,
- byť viazaný zmluvou alebo štatútom k podmienkam a pravidlám pre danú pozíciu, ktoré musia plniť,
- absolvovať komplexné školenie s ohľadom na povinnosti, ktoré majú plniť,
- byť viazaný zákonom alebo zmluvou k mlčanlivosti o citlivých skutočnostiach týkajúcich sa CA NZIS alebo držiteľov certifikátov,

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

5.3.1. Vzdelanie, kvalifikácia, skúsenosti a vôľové požiadavky

NCZI musí formulovať a dodržiavať personálnu a manažérsku politiku dostatočnú na to aby poskytla primeranú istotu o dôveryhodnosti a kompetentnosti svojich zamestnancov a viedla k uspokojivému plneniu ich povinností v súlade s týmto CP.

5.3.2. Postupy overovania

NCZI vykoná zodpovedajúce preskúmanie všetkých pracovníkov, ktorí sú zaradení v dôveryhodných rolách (pred ich zamestnaním a potom v pravidelných intervaloch podľa potreby) na overenie ich dôveryhodnosti a kompetencie v súlade s požiadavkami tohto poriadku a postupov personálnej práce CA alebo ekvivalentných požiadaviek. Všetci pracovníci, ktorí neuspejú v rámci počiatočného alebo pravidelného preskúmavania nesmú ďalej pôsobiť, alebo pokračovať v pôsobení v dôveryhodnej role. PMA môže stanoviť dodatočné požiadavky v súlade s národnou legislatívou.

5.3.3. Požiadavky na školenie

CA NZIS musí zabezpečiť, že všetci zamestnanci plniaci si povinnosti v súvislosti s prevádzkou CA alebo RA musia dostať komplexné školenie v oblasti:

- bezpečnostných pravidiel a mechanizmov platných pre CA alebo 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 musí dostať primeraný školenie, aby mohli plniť svoje povinnosti a následne musia byť pravidelne preškoľovaní na zabezpečenie aktuálnosti ich vedomostí.

5.3.4. Frekvencia preškoľovania a požiadavky

Požiadavky podľa odseku 5.3.3 musí byť aktuálne v závislosti od zmien v systéme CA. Preškoľovanie musí byť vykonávané podľa potreby a CA musí preskúmať tieto požiadavky najmenej raz za rok.

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, môže CA pozastaviť jeho/jej prístup k systému CA.

5.3.7. Zamestnanci na zmluvu

CA NZIS musí zabezpečiť, že prístup do CA zamestnancov na zmluvu bude v súlade s požiadavkou článku 5.1.1.

5.3.8. Dokumentácia poskytovaná zamestnancom

CA NZIS musí sprístupniť všetkým pracovníkom CA NZIS certifikačný poriadok, pravidlá na výkon certifikačných činností a ostatné špecifické nariadenia, politiky alebo zmluvy týkajúce sa ich pozície.

5.4. Postupy zaznamenávania auditných logov

5.4.1. Typy zaznamenávaných udalostí

CA NZIS by mal zaznamenať 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, by mal obsahovať dátum a čas udalosti, a totožnosť subjektu, ktorý udalosť spôsobil.

CA NZIS môže tiež zbierať a konsolidovať, a to buď elektronicky alebo manuálne, 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.

CA musí zabezpečiť, že v CPS uvádza, aké informácie sú zaznamenávané.

Pre uľahčenie rozhodovania, by mali byť všetky zmluvy a korešpondencia vzťahujúce sa k službám CA uchovávané a konsolidované na jednom mieste, a to buď elektronicky, alebo manuálne.

5.4.2. Frekvencia spracovávania auditných log záznamov

CA NZIS musí zabezpečiť, že pracovníci CA preskúmavajú svoje audit log záznamy minimálne raz týždenne a všetky významné udalosti sú 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 musia byť dokumentované.

5.4.3. Doba uchovávanie auditných log záznamov

CA musí zachovať svoju auditné log záznamy k dispozícii najmenej dva mesiace a následne archivovať.

5.4.4. Ochrana auditných log záznamov

Systém zaznamenávanie auditných log záznamov musí zahŕňať mechanizmy na ochranu log súborov proti neoprávnenému prezeraniu, úprave a vymazaniu. Manuálne log záznamy musia byť chránené pred neoprávneným prezeraním, úpravou a zničením.

5.4.5. Postup zálohovania auditných log záznamov

Auditné log záznamy a súhrnné reporty musia byť zálohované alebo kopírované manuálne.

5.4.6. Systém získavania auditných záznamov

CA NZIS musí identifikovať spôsob získavania auditných záznamov v svojom CPS.

5.4.7. Upozornenie pôvodcu na udalosť

Pokiaľ je zaznamenaná udalosť systémom zaznamenávania auditných logov nemusí dôjsť k upozorneniu jedinca, organizácie, zariadenia alebo aplikácie, ktorá ju zapríčinila.

5.4.8. Zraniteľnosti

V rámci zaznamenávania auditných logov sú tieto zaznamenávané aj z dôvodu monitorovania zraniteľnosti systému. NCZI musí zabezpečiť, aby bolo vykonávané hodnotenie zraniteľnosti, ich preskúmavanie a revízia, po ich dôkladnej analýze

5.5. Uchovávanie záznamov

5.5.1. Typy uchovávaných záznamov

Nasledujúce dáta a súbory musia byť archivované CA alebo v jej mene:

- 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,
- osobné údaje držiteľa certifikátu,
- dokumentácia o odovzdaní a prijatí certifikátu,
- dokumentácia o prijatí tokenov,
- všetky vydané a/alebo zverejnenie certifikáty,
- zmena kľúčov CA,
- všetky ARL a CRL vydané a / alebo zverejnené,
- všetky auditné log záznamy,
- ostatné údaje alebo aplikácie na overenie obsahu archívu,
- dokumentácia vyžadovaná audítormi,
- konečné stanovisko vyplývajúce z vykonaného auditu zhody.

5.5.2. Doba uchovávanie archívnych záznamov

Archív kľúčov a informácie o certifikáte sa musia uchovávať po dobu najmenej 10 rokov. Archív auditných log záznamov musí byť uchovávaný po dobu najmenej troch (3) mesiacov.

Každý podpísaný dokument môže podliehať požiadavkám na uchovávanie, ktoré musia byť splnené.

5.5.3. Ochrana archívnych záznamov

Archívne médiá musí byť chránené len fyzickými bezpečnostnými opatreniami alebo kombináciou fyzických bezpečnostných opatrení a kryptografickej ochrany. Táto ochrana musí spĺňať alebo prekračovať legislatívne požiadavky SR na uchovávanie takýchto materiálov.

5.5.4. Archívny systém

Nie sú stanovené žiadne požiadavky.

5.6. Zmena kľúčov

Držiteľ môže požiadať o obnovu jeho/jej kľúčového páru v priebehu 30 dní pred exspiráciou kľúčov, ak predchádzajúci certifikát nebol zrušený. Proces obnovy môže začať držiteľ, CA alebo RA. CA musí zabezpečiť, že podrobnosti tohto procesu sú uvedené v jeho CPS.

Držitelia bez platného certifikátu musia byť znovu overení CA alebo RA rovnakým spôsobom ako pri prvej registrácii.

V prípade, že držiteľov certifikát bol zrušený v dôsledku nedodržania jeho povinností, musí CA overiť, že všetky dôvody pre nedodržania povinností boli odstránené k jej spokojnosti ešte pred obnovou certifikátu.

5.7. Kompromitácia a obnova po havárii

5.7.1. Postupy dokumentovania a riadenia incidentov a kompromitácií

NCZI musí prijať postupy dokumentovania a riadenia incidentov a kompromitácií v zmysle ktorých bude vykonávaná obnova jej činnosti.

5.7.2. Poškodený hardvér, softvér, a/alebo údaje

NCZI musí prijať postupy obnovy s definovanými krokmi pre prípad, že dôjde k poškodeniu alebo strate hardvéru, softvéru a/alebo údajov. V prípade, že úložisko nie je pod kontrolou CA, musí CA zaistiť súhlas s poskytovateľom úložiska, aby postupy obnovy boli prijaté a dokumentované poskytovateľom.

5.7.3. Kompromitácia súkromného kľúča CA

CA NZIS musí mať zavedený vhodný plán pre prípad kompromitácie kľúčov, ktorý rieši postupy, ktoré budú nasledovať v prípade kompromitácie súkromného podpisového kľúča používaného na podpisovanie CA NZIS vydávaných certifikátov pre koncových používateľov alebo kľúčov používaných akoukoľvek CA na vyššej úrovni. Takýto plán musí obsahovať postupy na zrušenie všetkých dotknutých certifikátov a postupu na bezodkladné informovanie všetkých držiteľov týchto certifikátov a spoliehajúcich sa strán.

V prípade potreby zrušenia podpisového certifikátu CA NZIS musí CA bezodkladne o tom informovať držiteľa certifikátu.

CA NZIS musí tiež zverejniť sériové číslo zrušeného certifikátu vo vhodnom CRL.

5.8. Ukončenie činnosti CA

V prípade, že CA NZIS ukončí prevádzku, musí to okamžite oznámiť držiteľom platných certifikátov a spolu s PMA zabezpečiť ďalšie uchovávanie kľúčov CA a ďalších potrebných informácií.

V prípade, že CA NZIS ukončí prevádzku budú o tejto skutočnosti urýchlene informovaní všetci držitelia, RA a spoliehajúce sa strany

Všetky platné certifikáty vydané CA NZIS v zmysle tohto CP budú zrušené skôr ako dôjde k ukončeniu činnosti. Všetky aktuálne a archivované dokumenty CA musia byť odovzdané PMA (alebo inej určenej osobe) počas 48 hodín po ukončení činnosti CA a v súlade s týmto CP. Žiadne úložisko s možnosťou obnovy kľúčov nesmie byť súčasťou odovzdaných údajov.

6. Technické bezpečnostné opatrenia

6.1. Generovanie kľúčového páru a jeho inštalácia

6.1.1. Generovanie kľúčov

Generovanie kľúčových párov pre koncového užívateľa sa uskutoční v priebehu personalizácie karty na personalizačnom pracovisku NCZI priamo na čipovej karte prostredníctvom PMA schváleného algoritmu. V prípade technologických certifikátov si kľúčový pár generuje žiadateľ.

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 musí zabezpečiť, že kľúčová páry pre všetky subjekty v rámci PKI NCZI budú mať dĺžku najmenej 2048 bit RSA.

6.1.5. Parametre generovania kľúčov a kontrola kvality

Žiadne požiadavky.

6.1.6. Účel použitia kľúčov

Kryptografické kľúče koncových používateľov uložené na čipovej karte sú určené na:

- autentifikáciu držiteľa,
- vytváranie elektronického podpisu a
- end-2-end šifrovanie údajov.

Polia určujúce možnosti použitia certifikátu musia byť použité v súlade s požiadavkami RFC 5280 „Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile“ V certifikáte koncového používateľa musia byť prítomné nasledovné rozšírenia pre použitie kľúčov:

Digital Signature, Non-Repudiation, Key Encipherment.

Podpisové kľúče CA NZIS sú jediné kľúče určené na podpisovanie vydávaných certifikátov a CRL. V podpisovom certifikáte CA NZIS musia byť prítomné nasledovné hodnoty „Key Certifikát Sign a CRL Sign“.

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

Vydávajúca CA NCZI musí uchovávať svoje kryptografické kľúče určené na podpisovanie certifikátov koncových používateľov v kryptografickom bezpečnostnom module (HSM).

6.2.1. Štandardné požiadavky na HSM

CA NZIS použitý kryptografický modul musí spĺňať požiadavky bezpečnosti na úrovni FIPS 140-2 Level 3. Modul musí byť uložený v bezpečných priestoroch bez prístupu neoprávnených osôb. HSM modul musí spĺňať ochranu pred odchytávaním elektromagnetického vyžarovania , podporovať funkciu self test, poskytovať funkciu key recovery.

HSM musí podporovať minimálne podpisové algoritmy RSA s SHA-1, SHA-224, SHA-256, SHA-384 a SHA-512.

6.2.2. Práca so súkromných kľúčom

Súkromný kľúč certifikačnej autority musí byť generovaný a obnovovaný pod kontrolou viacerých osôb podľa princípu *n* z *m*, pričom minimálne 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

Súkromný kľúč CA NZIS je zálohovaný pri vytváraní pravidelných záloh servera certifikačnej autority, nakoľko sa v zašifrovanej podobe nachádza na pevnom disku servera CA s pripojeným HSM modulom. Obnova kľúča je možná len v jednom konkrétnom prostredí HSM (Security world) a s použitím príslušného počtu operátorských kariet (princíp *n* z *m*). Bezpečnostné opatrenia týkajúce sa zálohovania sú popísané v príslušných smerniciach (pozri).

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*).

6.2.7. Uchovávanie súkromného kľúča v HSM module

Súkromný kľúč v HSM module je uložený vo forme plain textu. Mimo HSM modulu je uložený v zašifrovanej podobe a chránený príslušným počtom operátorských kariet (princíp n z m) t. j. heslo na dešifrovanie je možné získať len použitím predpísaného počtu operátorských kariet.

6.2.8. Spôsob aktivácie súkromného kľúča

Oprávnené osoby musia byť overené kryptografickým modulom pred aktiváciou súkromného kľúča. Toto overenie môže byť vo forme hesla. Pri reaktivácii, musí byť súkromný kľúč uchovávaný iba v šifrovanej podobe.

6.2.9. Spôsob deaktivácia súkromného kľúča

Pri deaktivácii musí byť kľúč vymazaný z pamäte HSM modulu. Každý priestor na disku, v ktorom boli uložené kľúče musí byť prepísaný pokiaľ sa uvoľní na použitie pre operačný systém. Kryptografický modul musí automaticky vypnúť súkromný kľúč po uplynutí prednastavenej doby nečinnosti.

6.2.10. Spôsob zničenia súkromného kľúča

Po ukončení používania súkromného kľúča, všetky kópie súkromného kľúča v pamäti počítača a na zdieľanom diskovom priestore musia byť bezpečne zlikvidované jeho prepísaním. Spôsob prepísania musí byť schválený PMA. Spôsob ničenia súkromného kľúča musí byť popísané v CPS alebo inom verejne dostupnom dokumente.

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. 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 musia byť jedinečné a nepredvídateľné. Aktivačné údaje, v spojení s niektorým iným overovaním prístupu, musia mať primeranú úroveň sily v závislosti na kľúčoch alebo údajoch, ktoré majú byť chránené. Tam, kde sa používajú heslá, musí mať subjekt možnosť zmeniť jeho heslo kedykoľvek.

6.4.2. Ochrana aktivačných údajov

Údaje použité pre inicializáciu entity musia byť chránené pred neoprávneným použitím kombinácie mechanizmov kryptografického a fyzického riadenia prístupu.

Súkromné kľúče subjektov musia byť chránené pred neoprávneným použitím kombinácie mechanizmov kryptografického a fyzického riadenia prístupu. Úroveň ochrany musí byť dostatočná, tak aby odradila motivovaného útočníka s dostatočnými prostriedkami. Ak je možné používať heslo opakovane, mechanizmus by mal zahŕňať možnosť dočasne zablokovať účet po vopred určenom počte pokusov o prihlásenie.

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 musí umožňovať nasledovnú funkcionalitu:

- riadenie prístupu k službám CA a PKI rolám,
- vynucovať 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,
- dôveryhodnú cestu k identifikácii PKI rolí a súvisiacich identít,
- mechanizmus obnovy kľúčov a systému CA.

Táto funkcia môže byť poskytovaná operačným systémom, alebo v kombinácii operačného systému, PKI CA softvéru a fyzickej ochrany.

6.5.2. Hodnotenie počítačovej bezpečnosti

Žiadne požiadavky.

6.6. Životný cyklus riadenia bezpečnosti

6.6.1. Riadenie vývoja systému

CA musí používať softvér, ktorý bol navrhnutý a vyvinutý v zmysle formálnej metodiky a je podporovaný nástrojmi pre riadenie konfigurácie. CA softvér musí mať overenie súladu procesov zhody od nezávislej tretej strany.

6.6.2. Riadenie manažmentu bezpečnosti

Na inštaláciu a následnú údržbu systému CA musí byť použitá oficiálna metodika na manažment konfigurácií. Softvér CA, pri spustení, musí poskytnúť možnosť pre CA na overenie, že softvér systéme:

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

CA NZIS musí poskytnúť mechanizmus pre pravidelné overovanie integrity používaného softvéru. CA NZIS musí mať tiež mechanizmy a implementované pravidlá na riadenie a sledovanie konfigurácie systému CA. Po inštalácie a aspoň raz týždenne musí byť overovaná integrita systému CA.

6.7. Riadenie sieťovej bezpečnosti

Servery CA NZIS musia byť chránené pred napadnutím z ľubovoľnej otvorenej alebo internej siete, do ktorej sú pripojené. Táto ochrana musí byť riešená prostredníctvom inštalácie zariadení nakonfigurovaný tak, že budú prístupné len protokoly a príkazy potrebné pre prevádzku CA. CA musí zabezpečiť, aby jej CPS definovala tieto protokoly a príkazy potrebné pre prevádzku CA.

7. Profily certifikátov a CRL

7.1. Profily certifikátov

7.1.1. 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“.

7.1.2. Použite rozšírenia v certifikátoch

Softvér CA NZIS musí podporovať všetky základné X.509 definované položky:

Podpis (Certificate Signature)	Podpis CA na autentifikáciu certifikátu
Algoritmus podpisu (Certificate Signature Algorithm)	Použitý algoritmus podpisu
Vydavateľ (Issuer)	Meno CA
Platnosť (Validity)	Dátum začiatku a konca platnosti
Subjekt (Subject)	Rozlišovacie meno držiteľa
Informácie o verejnom kľúči subjektu (Subject Public Key Information)	ID algoritmu, kľúč
Verzia (Certificate Version)	Verzia X.509 certifikátu, verzia 3
Sériové číslo (Serial NUmber)	Jedinečné sériové číslo certifikátu

Žiadne rozšírenie nesmie modifikovať alebo podkopať dôveru použitia týchto základných položiek.

CPS musí definovať použitie akýchkoľvek rozšírení podporovaný CA, jeho RA a koncovými používateľmi.

7.1.3. Identifikácia kryptografických algoritmov

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

- RSA 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]

7.1.4. Menná konvencia

Žiadne požiadavky.

7.1.5. Obmedzenia týkajúce sa mena

DN subjektu a vydavateľa musí byť prítomné v každom certifikáte a musí spĺňať požiadavky RFC 5280.

7.1.6. Aplikované OID certifikačného poriadku

CA NZIS musí zabezpečiť, že OID certifikačného poriadku je zahrnutý v certifikátoch, ktoré vydáva.

7.1.7. Použitie rozšírenia „policy constraints“

Žiadne požiadavky.

7.1.8. Sémantika spracovanie kritických rozšírení CP

Kritické rozšírenia musia byť interpretované spôsobom definovaným v RFC 5280.

7.2. Profil CRL

7.2.1. Podporovaná verzia

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

7.2.2. CRL a CRL rozšírenia

Každý softvér používaný účastníkmi NZIS musí správne spracovať všetky rozšírenie CRL definované v RFC 5280. CPS musí vymedziť použitie akýchkoľvek rozšírenie podporovaných CA, jeho RA a koncových držiteľov certifikátov.

7.3. OCSP profil

7.3.1. Používaná verzia

CA NZIS poskytuje službu OCSP v súlade s RFC 2560.

7.3.2. **Rozšírenia OCSP**

Žiadne požiadavky.

8. AUDIT súladu a iné posudzovanie

Audit súladu určuje, či poskytovanie služieb CA NZIS spĺňa štandardy stanovené v jeho CPS a spĺňa požiadavky tohto CP.

Autorita zodpovedná za správu certifikačného poriadku musí vymedziť špecifické požiadavky pre audit súladu. Tieto požiadavky budú zodpovedať všetkým zákonným a regulačným požiadavkám legislatívy Slovenskej republiky.

8.1. Frekvencia auditu alebo iného hodnotenia

Audit súladu CA NZIS musí byť vykonaný minimálne 1 krát ročne a vždy pokiaľ tak rozhodne PMA ako následok potenciálneho resp. aktuálneho porušenia bezpečnosti.

8.2. Rozsah auditu a použité metódy

Audit CA NZIS bude zameraný na splnenie požiadaviek Zákona č. 215/2002 Z. z. o elektronickom podpise a požiadaviek ETSI definovaných v aktuálnej verzii dokumentu ETSI TS 102 042 „Electronic Signatures and Infrastructures (ESI), Policy requirements for certification authorities issuing public key certificates“.

8.3. Vzťah audítora a hodnoteného subjektu

Audítor musí byť nezávislý od CA NZIS.

8.4. Možné opatrenia prijaté na základe výsledkov auditu

Výsledky auditu musia byť predložené PMA. Ak sa zistia nezrovnalosti, musí CA predložiť správu PMA aké nápravné opatrenia uskutoční CA ako reakciu na správu o audite.

8.5. Výsledok auditu a jeho zverejnenie

CA NZIS musí poskytnúť PMA kópiou výsledkov auditu zhody. Tieto úplné výsledky nebudú zverejnené, pokiaľ to nevyžaduje zákon.

9. 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 IS 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 do 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 NCZI 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 NCZI 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.

10.Ostatné obchodné a legislatívne otázky

10.1. Poplatky

10.1.1. Poplatok za vydanie a obnovu certifikátu

CA NZIS poskytuje svoje služby bezodplatne.

10.2. Finančná zodpovednosť

CA NZIS nenesie žiadnu finančnú zodpovednosť za škody spôsobené používaním ním vydaných certifikátov ich držiteľom a spoliehajúcim sa stranám resp. za škody spôsobené poskytovaním súvisiacich certifikačných služieb v zmysle požiadaviek legislatívy Slovenskej republiky.

10.3. Ochrana osobných údajov

10.3.1. Požiadavky na ochranu osobných údajov

CZ NCZI a jeho RA musia pri spracovávaní osobných údajov žiadateľov resp. držiteľov certifikátov dodržiavať požiadavky zákona č. 428/2002 Z. z. o ochrane osobných údajov v aktuálnom znení.

10.3.2. Informácie, ktoré nie sú považované za osobné

Za osobné údaje v rámci PKI NCZI nie sú považované vydané certifikáty verejného kľúča a certifikáty vydávajúcej CA NZIS. Rovnako publikované zoznamy zrušených certifikátov.

10.3.3. 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).

10.3.4. Súhlas so spracovaním osobných údajov

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

10.3.5. Podmienky zverejnenia osobných údajov

CA NZIS nezverejní žiadne informácie týkajúce sa žiadateľa o certifikát alebo držiteľa certifikátu žiadnej tretej strane.

CA NZIS nesmie poskytnúť osobné údaje žiadnej tretej strane s výnimkou subjektov, ktoré zo zákona majú právo kontrolovať činnosť CA a kompetentných štátnych orgánov ako sú polícia, súdy, prokuratúra.

10.4. Právo duševného vlastníctva

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

Tento CP a jeho OID sú majetkom NCZI a môžu byť použité len CA NZIS v súlade s ustanoveniami uvedenými v tomto CP. Akékoľvek iné použitie tohto CP a jeho OID bez výslovného písomného súhlasu CA NZIS je výslovne zakázané.

10.5. Vyhlásenia a záruky

10.5.1. Záruky CA

Všetky informácie uvedené v certifikáte musia byť presné a správne do takej miery ako sú poskytnuté žiadateľom o certifikát v procese jeho identifikácie a autentifikácie. CA NZIS neposkytuje držiteľovi certifikátov žiadne záruky.

10.6. Odmietnutie záruky

Žiadne požiadavky.

10.7. Obmedzenie zodpovednosti

Žiadne požiadavky.

10.8. Náhrady

Žiadne požiadavky

10.9. Doba platnosti a jej ukončenie

10.9.1. Doba platnosti

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

10.9.2. Následky ukončenia platnosti

CA NZIS je povinná uchovávať jeden exemplár z každej platnej verzie CP resp. CPS pre archívne účely a to buď v tlačenej alebo elektronickej forme. Pokiaľ sú dokumenty uchovávané v elektronickej forme, musí byť zachovaná ich integrita.

10.10. Notifikácia a komunikácia s držiteľmi

CZ NCZI musí definovať spôsob komunikácie s držiteľmi ňou vydaných certifikátov resp. inými subjektmi využívajúcimi NZIS. Spôsob komunikácie môže zahŕňať využívanie-mailových správ, listovú komunikáciu, priamu komunikáciu na k tomu určených miestach.

10.11. Zmeny a prílohy CP a CPS

10.11.1. Postup zmeny dokumentácie

PMA má právo posúdiť a prípadne revidovať tento CP. Chyby, požiadavky na aktualizáciu alebo navrhované zmeny tohto CP sa majú oznámiť kontaktu uvedenému v časti 1.5. Takáto komunikácia musí obsahovať popis zmeny, zdôvodnenie zmeny a kontaktné údaje osoby, ktorá zmenu požaduje.

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

Za revíziu týchto dokumentov je zodpovedná Autorita pre správu CP (PMA) – pozri 1.3.1.1.

10.11.2. Notifikácia o zmene dokumentácie

Všetky zmeny CP motivované PMA majú byť dané na vedomie subjektom, ktorých sa týkajú v perióde aspoň jedného mesiaca. Elektronická verzia tohto CP musí byť dostupná na verejnej web stránke CA

10.11.3. Okolnosti, za ktorých sa musí OID byť menené

V prípade, že prípadné zmeny v CP výrazne ovplyvnia jeho obsah v porovnaní s pôvodnou verziou môže PMA rozhodnúť o pridelení nového OID pre takto zmenený CP.

10.12. Riešenie sporov

Pre potreby interpretácie CP, CPS a zmluvy alebo riešenia sporov sa možno obrátiť na PMA. PMA rozhoduje s konečnou platnosťou v prípade akýchkoľvek sporov o interpretácii alebo použiteľnosti tohto CP, CPS a zmluvy.

Žiadnym rozhodnutím PMA nie je dotknuté právo sťažovateľa postúpiť sťažnosť nezávislému súdu.

10.13. Uplatňované právne predpisy

Pri rozhodovaní v súdnych sporoch sa uplatňuje právo Slovenskej republiky.

10.14. 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.

10.15. Rôzne ustanovenia

10.15.1. 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.

10.15.2. 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.

10.15.3. Výnimky

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

10.15.4. Vyššia moc

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

10.16. Ostatné dojednania

Žiadne požiadavky