OS - 404
Certifikačný poriadok poskytovateľa dôveryhodných služieb

(reg. číslo: NCZI-01410-2025-7300, Z006558-2025)

Účel: Týmto certifikačným poriadkom vedenie Národného centra zdravotníckych informácií ako poskytovateľ dôveryhodných služieb stanovuje pravidlá pre manažovanie certifikátov.

Určené pre: Tento certifikačný poriadok je určený pre všetky organizačné útvary a zamestnancov, ktorí prichádzajú do kontaktu s certifikátmi NCZI, pre všetky spoliehajúce sa strany ako aj pre všetkých používateľov certifikátov NCZI.

Dokument je účinný od: 22.09.2025	
Vypracoval: Meno a priezvisko: **Mária Frigová MSc.** Funkcia: procesný špecialista ePZP Podpis: Mária Frigová MSc. v. r.	Schválil: Meno a priezvisko: **Mgr. Pavol Vršanský** Funkcia: riaditeľ NCZI Dátum: 06.09.2025 Podpis: Mgr. Pavol Vršanský v. r.
Gestor dokumentu: Meno a priezvisko: **Mgr. Zuzana Lališová** Funkcia: riaditeľka sekcie prevádzky IT Podpis: Mgr. Zuzana Lališová v. r.	

Aktuálne vydanie tohto dokumentu je v elektronickej forme. Ak je dokument v papierovej forme, pred použitím skontrolujte aktuálnosť tohto dokumentu s elektronickou formou, uverejnenou na intranete.

História revízií:

Dátum revízie	**Popis zmeny**	**Zmeny označené**
28.05.2024	Prvá verzia dokumentu	Čierne písmo
10.09.2025	Aktualizácia (zapracovanie formálnych zmien na základe zmeny OŠ k 1.6.2025 a k 1.9.2025) CP PDS (reg. číslo: NCZI-00888-2024-4320-001) na v. 02 (reg. číslo: NCZI-01410-2025-7300, Z006558-2025)	Červené písmo

Schválenie:

Tento dokument bol schválený:

Číslo a názov materiálu predloženého na poradu riaditeľa NCZI	**Dátum schválenia**
Formálne úpravy bez predloženia na poradu štatutárneho orgánu, schválené priamo štatutárnym orgánom NCZI v zmysle podkapitoly 3.1 ods. 1 OS – 110 Riadenie dokumentov	16. 09. 2025

Distribúcia:

Tento dokument bol elektronicky distribuovaný:

Prostredníctvom	**Komu**
Intranet, oznamujúci mail, webové sídlo NCZI	Zamestnanci NCZI, web NCZI www.nczisk.sk

OBSAH

1 POJMY A POUŽITÉ SKRATKY 9
2 ÚVOD 10
2.1 Prehľad 10
2.2 Identifikácia 11
2.3 Účastníci PKI 11
2.3.1 Autorita na správu politík 12
2.3.2 Poskytovateľ dôveryhodných služieb (PDS) 12
2.3.3 Špecialista personalizácie dôveryhodnej služby 12
2.3.4 Personalizačné pracovisko 12
2.3.5 Držitelia 12
2.3.6 Spoliehajúce sa strany 13
2.4 Používanie certifikátu 13
2.4.1 Povolené používanie 13
2.5 Správa politík 13
2.5.1 Organizácia zodpovedná za správu CP 13
2.5.2 Kontakt 13
3 ZVEREJŇOVANIE INFORMÁCIÍ A ÚLOŽISKO 13
3.1 Úložisko 13
3.2 Publikovanie informácií 13
3.3 Čas a frekvencia aktualizovania a dostupnosti informácií 14
3.4 Kontroly prístupu k úložisku 14
4 IDENTIFIKÁCIA, AUTENTIZÁCIA 14
4.1 Pomenovanie 14
4.1.1 Typy mien 14
4.1.2 Potreba zmysluplnosti mien 14
4.2 Prvotné overenie identity 15
4.2.1 Overenie identity žiadateľa 15
4.2.2 Overenie organizácie 15
4.2.3 Spôsob preukazovania vlastníctva nosiča súkromného kľúča 15
4.2.4 Overovanie právomocí 15
4.3 Identifikácia a autentizácia pri obnove certifikátu 15
4.3.1 Obnova certifikátu po uplynutí platnosti certifikátu 15
4.3.2 Obnova certifikátu po jeho znefunkčnení pred uplynutím platnosti certifikátu 15
4.3.3 Identifikácia a autentifikácia žiadosti o znefunkčnenie certifikátu 16

5 PREVÁDZKOVÉ POŽIADAVKY 16
5.1 Žiadanie o certifikát 16
5.1.1 Žiadatelia o certifikát 16
5.1.2 Postup žiadania a zodpovednosti 16
5.2 Spracovanie žiadosti o vydanie certifikátu 17
5.2.1 Spôsob overenia identity a autenticity žiadateľa 17
5.2.2 Overenie identity a autenticity 17
5.2.3 Overenie splnenia podmienok pre vydanie certifikátu 17
5.3 Vydanie certifikátu 17
5.3.1 Činnosť PDS pri vydaní certifikátu 17
5.4 Prevzatie certifikátu 18
5.4.1 Spôsob prevzatia certifikátu 18
5.4.2 Notifikácia o vydaní certifikátu iným entitám ako žiadateľ 18
5.5 Kľúčový pár a používanie certifikátu 18
5.5.1 Súkromný kľúč držiteľa a používanie certifikátu 18
5.5.2 Používanie certifikátu a verejného kľúča spoliehajúcou sa stranou 18
5.6 Vydanie nového certifikátu pri jeho obnove na pôvodné kľúče – tzv. recovery 18
5.7 Vydanie nového certifikátu pri jeho obnove na nové kľúče – tzv. renewal 19
5.7.1 Kto môže žiadať o obnovu certifikátu na nové kľúče / automatizované obnovenie 19
5.7.2 Postup žiadania o obnovu certifikátu 19
5.7.3 Spôsob prevzatia obnoveného certifikátu 19
5.7.4 Zverejnenie obnoveného certifikátu 19
5.7.5 Notifikácia o vydaní obnoveného certifikátu spoliehajúcim sa stranám 19
5.8 Zmena kľúčov 19
5.9 Zmena údajov v certifikáte 19
5.10 Znefunkčnenie certifikátu 20
5.10.1 Dôvody znefunkčnenia certifikátu 20
5.10.2 Kto môže žiadať o znefunkčnenie certifikátu 20
5.10.3 Miesto podania žiadosti o znefunkčnenie certifikátu 20
5.10.4 Lehota na podanie žiadosti o znefunkčnenie certifikátu 21
5.10.5 Vybavenie žiadosti na znefunkčnenie certifikátu 21
5.10.6 Povinnosti overovania stavu certifikátu zo strany spoliehajúcich sa strán 21
5.10.7 Frekvencia aktualizácie CRL 21
5.10.8 Čas zverejnenia vydaného CRL 21
5.10.9 Overovanie stavu certifikátu prostredníctvom OCSP 21
5.10.10 Požiadavky na overenie stavu certifikátu prostredníctvom OCSP 21

5.10.11 Pozastavenie platnosti certifikátu 21
5.11 Služby overovania stavu certifikátu 21
5.11.1 Charakteristika služby 21
5.11.2 Dostupnosť služby 21
5.12 Obnova kľúčov z depozitu alebo zálohy 22
6 MANAŽÉRSKE, PREVÁDZKOVÉ A FYZICKÉ BEZPEČNOSTNÉ OPATRENIA 22
6.1 Fyzické bezpečnostné opatrenia 22
6.1.1 Umiestnenie, priestory a prístup 22
6.1.2 Dodávka energie a teplota 23
6.1.3 Ohrozenie vodou 23
6.1.4 Protipožiarna ochrana 23
6.1.5 Uchovávanie médií 23
6.1.6 Nakladanie s odpadom 23
6.1.7 Záložné pracovisko 23
6.2 Procedurálne bezpečnostné opatrenia 23
6.2.1 Dôveryhodné role PDS 23
6.2.2 Počet rolí potrebný na výkon úloh 25
6.2.3 Identifikácia a autentizácia jednotlivých rolí 25
6.3 Personálne opatrenia 25
6.3.1 Vzdelanie, kvalifikácia, skúsenosti a vôľové požiadavky 26
6.3.2 Postupy overovania 26
6.3.3 Požiadavky na školenie a personálna bezpečnosť 26
6.3.4 Frekvencia preškoľovania a požiadavky 26
6.3.5 Obmena pozícií 26
6.3.6 Postup pri neoprávnenom zásahu 27
6.3.7 Dokumentácia poskytovaná zamestnancom 27
6.4 Postupy zaznamenávania auditných logov 27
6.4.1 Typy zaznamenávaných udalostí 27
6.4.2 Frekvencia spracovávania auditných log záznamov 28
6.4.3 Doba uchovávanie auditných log záznamov 28
6.4.4 Ochrana auditných log záznamov 28
6.4.5 Postup zálohovania auditných log záznamov 28
6.4.6 Systém získavania auditných záznamov 28
6.4.7 Upozornenie pôvodcu na udalosť 28
6.4.8 Zraniteľnosti 28
6.5 Uchovávanie záznamov 28

6.5.1 Typy uchovávaných záznamov 28
6.5.2 Doba uchovávanie archívnych záznamov 29
6.5.3 Ochrana archívnych záznamov 29
6.5.4 Archívny systém 29
6.6 Kompromitácia a obnova po havárii 29
6.6.1 Postupy dokumentovania a riadenia incidentov a kompromitácií 29
6.6.2 Poškodený hardvér, softvér a/alebo údaje 29
6.6.3 Kompromitácia súkromného kľúča PDS 29
6.7 Ukončenie činnosti PDS 30
7 TECHNICKÉ BEZPEČNOSTNÉ OPATRENIA 30
7.1 Generovanie kľúčového páru a jeho inštalácia 30
7.1.1 Generovanie kľúčov 30
7.1.2 Doručenie privátneho kľúča držiteľovi 30
7.1.3 Doručenie verejného kľúča na PDS 30
7.1.4 Veľkosť kľúčov 30
7.1.5 Parametre generovania kľúčov a kontrola kvality 30
7.1.6 Účel použitia kľúčov 31
7.2 Ochrana súkromného kľúča a využívanie kryptografických hardvérových modulov (HSM) . 31
7.2.1 Štandardné požiadavky na HSM 31
7.2.2 Práca so súkromným kľúčom 31
7.2.3 Obnova súkromných kľúčov z depozitu 31
7.2.4 Zálohovanie súkromných kľúčov 32
7.2.5 Archivácia súkromných kľúčov 32
7.2.6 Prenos súkromného kľúča do alebo z kryptografického modulu HSM 32
7.2.7 Uchovávanie súkromného kľúča v HSM module 32
7.2.8 Spôsob aktivácie súkromného kľúča 32
7.2.9 Spôsob deaktivácie súkromného kľúča 32
7.2.10 Spôsob zničenia súkromného kľúča 32
7.2.11 Charakteristika HSM modulu 32
7.3 Ďalšie aspekty manažmentu kľúčového páru 32
7.3.1 Doba platnosti certifikátov a použiteľnosti kľúčového páru 32
7.4 Aktivačné údaje 33
7.4.1 Generovanie aktivačných údajov a ich inštalácia 33
7.4.2 Ochrana aktivačných údajov 33
7.4.3 Ďalšie aspekty aktivačných údajov 33
7.5 Počítačové bezpečnostné opatrenia 33

7.5.1 Špecifické technické požiadavky z oblasti počítačovej bezpečnosti 33
7.5.2 Hodnotenie počítačovej bezpečnosti 33
7.6 Životný cyklus riadenia bezpečnosti 34
7.6.1 Riadenie vývoja systému 34
7.6.2 Riadenie manažmentu bezpečnosti 34
7.7 Riadenie sieťovej bezpečnosti 34
8 PROFILY CERTIFIKÁTOV A CRL 34
8.1 Profily certifikátov 34
8.1.1 Podporovaná verzia 34
8.1.2 Použite rozšírenia v certifikátoch 34
8.1.3 Identifikácia kryptografických algoritmov 35
8.1.4 Menná konvencia 35
8.1.5 Obmedzenia týkajúce sa mena 35
8.1.6 Aplikované OID certifikačného poriadku 35
8.1.7 Použitie rozšírenia „policy constraints“ 35
8.1.8 Sémantika spracovanie kritických rozšírení CP 35
8.2 Profil CRL 35
8.2.1 Podporovaná verzia 35
8.2.2 CRL a CRL rozšírenia 36
8.3 OCSP profil 36
8.3.1 Používaná verzia 36
8.3.2 Rozšírenia OCSP 36
9 AUDIT SÚLADU A INÉ POSUDZOVANIE 36
9.1 Frekvencia auditu alebo iného hodnotenia 36
9.2 Rozsah auditu a použité metódy 36
9.3 Vzťah audítora a hodnoteného subjektu 36
9.4 Možné opatrenia prijaté na základe výsledkov auditu 36
9.5 Výsledok auditu a jeho zverejnenie 36
10 BEZPEČNOSTNÁ KAPITOLA PDS 37
11 OSTATNÉ OBCHODNÉ A LEGISLATÍVNE OTÁZKY 38
11.1 Poplatky 38
11.1.1 Poplatok za vydanie a obnovu certifikátu 38
11.2 Finančná zodpovednosť 38
11.3 Ochrana osobných údajov 38
11.3.1 Požiadavky na ochranu osobných údajov 38

11.3.2 Informácie, ktoré nie sú považované za osobné 38
11.3.3 Zodpovednosť za ochranu osobných údajov 38
11.3.4 Právny základ na spracúvanie osobných údajov 38
11.3.5 Podmienky zverejnenia osobných údajov 38
11.4 Právo duševného vlastníctva 38
11.5 Vyhlásenia a záruky, zodpovednosť za škodu 39
11.5.1 Záruky PDS 39
11.6 Odmietnutie záruky 39
11.7 Obmedzenie zodpovednosti 39
11.8 Zodpovednosť za škodu 39
11.9 Doba platnosti a jej ukončenie 40
11.9.1 Doba platnosti 40
11.9.2 Následky ukončenia platnosti 40
11.10 Notifikácia a komunikácia s držiteľmi 40
11.11 Zmeny a prílohy CP 40
11.11.1 Postup zmeny dokumentácie 40
11.11.2 Notifikácia o zmene dokumentácie 40
11.11.3 Okolnosti za ktorých sa musí OID meniť 40
11.12 Riešenie sporov 40
11.13 Uplatňované právne predpisy 41
11.14 Súlad s platnými zákonmi 41
11.15 Rôzne ustanovenia 41
11.15.1 Zmluva 41
11.15.2 Ostatné dojednania 41
11.15.3 Postúpenie práv a povinností 41
12 ZÁVEREČNÉ USTANOVENIA 41
13 PRÍLOHY 42

1 POJMY A POUŽITÉ SKRATKY

ADMIN Správca, najmä informačných systémov a databáz.
ARL Zoznam revokovaných autorít (Authority Revocation List)
CMS Systém čipových kariet (Card Management System)
CP Certifikačný poriadok
CP PDS Certifikačný poriadok Poskytovateľa dôveryhodných služieb
CRL Zoznam zrušených certifikátov (Certificate Revocation List)
CSIRT Označenie jednotky pre riešenie počítačových bezpečnostných incidentov (Computer Security Incident Response Team)
DN Rozlišujúce meno (Distinguished name)
ePZP Elektronický preukaz zdravotníckeho pracovníka
ETSI Európsky inštitút pre telekomunikačné normy (European Telecommunications Standards Institute)

EÚ Európska únia (European Union)
FIPS USA štandard z oblasti informačnej bezpečnosti (Federal Information Processing Standards)
FO Fyzická osoba
GDPR Nariadenie Európskeho parlamentu a Rady (EÚ) 2016/679 z 27. apríla 2016 o ochrane fyzických osôb pri spracúvaní osobných údajov a o voľnom pohybe takýchto údajov, ktorým sa zrušuje smernica 95/46/ES (všeobecné nariadenie o ochrane údajov)
HSM Hardvérový bezpečnostný modul (hardware Security Module)
IS Informačný systém
ISO Medzinárodná štandardizačná organizácia (International Standard Organization)
JRÚZ Jednotná referenčná údajová základňa pozostávajúca z číselníkov, zoznamov a registrov pre potreby NZIS, do ktorej údaje sa získavajú zapracovaním číselníkov, integráciou údajov z referenčných zdrojov ako napr. zo ŠÚ SR a MV SR alebo spracúvaním dávok s údajmi od povinných osôb dotknutých zoznamov a registrov ako napr. od povoľovacích orgánov, ÚDZS, stavovských organizácií v zdravotníctve (komôr), zdravotných poisťovní, MZ SR, ŠÚKL atď.
KOMORA Stavovská organizácia v zdravotníctve
MV SR Ministerstvo vnútra Slovenskej republiky
MZ SR Ministerstvo zdravotníctva Slovenskej republiky
NCZI Národné centrum zdravotníckych informácií
NZIS Národný zdravotnícky informačný systém
OCSP Služba okamžitého poskytovania informácie o stave certifikátu (Online Certificate Status Protocol)
OID Objektový identifikátor (Object Identifier)
PDS Poskytovateľ dôveryhodných služieb, ktorým je Národné centrum zdravotníckych informácií
PIN Osobné identifikačné číslo (Personal Identification Number)
PKCS Kryptografické štandardy pre PKI (Public Key Cryptography Standards)
PKI Infraštruktúra verejného kľúča (Public Key Infrastructure)
PMA Autorita na správu politík (Policy Management Authority), ktorou je štatutárny orgán NCZI
PO Právnická osoba
PPVZ Pracovník pracujúci v zdravotníctve
PZS Poskytovateľ zdravotnej starostlivosti
RFC Request for Comment
RFO Register fyzických osôb
RSA Kryptografický algoritmus pomenovaný podľa tvorcov (Rivest, Shamir, Adleman)
SHA Kryptografická funkcia na vytváranie odtlačkov (hash) elektronických informácií (Secure Hash Algorithm)

ŠÚKL Štátny ústav pre kontrolu liečiv
ŠÚ SR Štatistický úrad Slovenskej republiky
ÚDZS Úrad pre dohľad nad zdravotnou starostlivosťou
URL Uniform Resource Locator
VPN SD Virtuálna privátna sieť Servis Desk IBM
ZPr Zdravotnícky pracovník
Zákon o NZIS - Zákon č. 153/2013 Z. z. o národnom zdravotníckom informačnom systéme a o zmene a doplnení niektorých zákonov v znení neskorších predpisov
Zákon o ochrane osobných údajov – Zákon č. 18/2018 Z. z. o ochrane osobných údajov a o zmene a doplnení niektorých zákonov v znení neskorších predpisov
ZNCZI Zamestnanci Národného centra zdravotníckych informácií zabezpečujúci podporu fungovania národného zdravotníckeho informačného systému.

2 ÚVOD

(1) Tento CP definuje pravidlá poskytovateľa dôveryhodných služieb, ktorým je Národné centrum zdravotníckych informácií, určené na vydávanie certifikátov zdravotníckym pracovníkom a iným pracovníkom v zdravotníctve v osobitných prípadoch, určených na používanie v rámci NZIS, a to pravidlá pre vydávanie certifikátov a výkonu servisu pre ZNCZI.

(2) Tento CP obsahuje pravidlá pre vydávanie a používanie certifikátov tým osobám, ktoré sú oprávnené využívať NZIS a vendorom dodávajúcim IS. Štruktúra CP je plne v súlade s požiadavkami RFC 3647 „ Internet X.509 v3 Public Key Infrastructure Certificate Policy and Certification Practices Framework“.

(3) Držitelia certifikátov, spoliehajúce strany, ako aj iné osoby, ktorým to vyplýva z toho CP, zmluvy (ak je uzavretá) a/alebo iných dokumentov (napr. osobitné podmienky používania certifikátov vydaných PDS, interné predpisy PDS) sú povinné dodržiavať ustanovenia tohto CP.

(4) V dokumente sú používané technické pojmy spojené s technológiou PKI. V dokumente sú používané technické pojmy spojené s technológiou PKI. Za účelom plného porozumenia dokumentu, vrátane jeho terminológie je potrebné pred čítaním ďalších častí dokumentu sa oboznámiť s vysvetleniami pojmov a skratiek uvedených v kapitole "POJMY A POUŽITÉ SKRATKY".

(5) 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.

2.1 Prehľad

(1) CP je určený na manažovanie a využívanie certifikátov, ktoré obsahujú verejné kľúče slúžiace na identifikáciu, autentizáciu, elektronické podpisovanie a šifrovanie citlivých informácií.

(2) CP identifikuje špecifické úlohy, upravuje procesy a zodpovednosti pre:

a) PDS pri vydávaní certifikátov,

b) špecialistov personalizácie PDS, ZNCZI,

c) držiteľov certifikátov a

d) spoliehajúce sa strany, pričom všetky tieto špecifické povinnosti sú v ňom popísané.

(3) PDS je viazaný legislatívou SR a EÚ, používa jeden alebo viac koreňových certifikátov a vydáva príslušný zoznam zrušených certifikátov (CRL). Používané certifikáty PDS sú k dispozícii držiteľom certifikátov.

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

(5) PDS manažuje:

a) poskytovanie dôveryhodných služieb formou certifikátov, pričom nosičmi certifikátov sú ePZP, ADMIN karty, PPVZ, HSM,

b) distribúciu certifikátov,

c) znefunkčnenie certifikátov len v prípadoch, ktoré sú uvedené v tomto CP,

d) zabezpečenie kritických funkcií PDS medzi najmenej tri osoby priradené do rôznych dôveryhodných rolí a

e) ďalšie povinnosti PDS.

(6) 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 no nie dlhšiu ako stanovuje platná legislatíva SR.

(7) Žiadne údaje poskytnuté držiteľom pre potreby PDS nesmú byť zverejnené bez jeho súhlasu, ak to nevyžaduje zákon alebo rozhodnutie príslušného orgánu verejnej moci.

(8) Činnosti PDS podliehajú kontrole vykonávanej Policy Management Authority (PMA) alebo jej zástupcom podľa uváženia PMA.

2.2 Identifikácia

(1) OID tohto CP je registrovaný pod ISO a je {ISO assigned OIDs (1) ISO Identified Organization (3).

(2) Identifikačné číslo organizácie (IČO) Národné centrum zdravotníckych informácií (00165387) PDS NCZI (1) CP PDS NCZI (1).

(3) Tento CP identifikuje konkrétne úlohy pri manažovaní poskytovaní dôveryhodných služieb pre ich vykonanie a definuje kompetentné pracovné role. CP identifikuje osoby zodpovedné za úložisko, držiteľov certifikátov a spoliehajúce sa strany, ktoré majú špecifické povinnosti a ktoré sú uvedené v tomto poriadku.

2.3 Účastníci PKI

(1) Technické, programové vybavenie a personálne obsadenie na zaistenie služieb a na vydávanie a správu certifikátov.

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

2.3.1 Autorita na správu politík

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

a) dohľadu na vytváranie a aktualizáciu certifikačných politík a iných dokumentov, vrátane vyhodnocovania zmien a plánov na implementovanie prijatých zmien tak, aby sa zaručilo, že prax PDS vyhovuje príslušnému CP,

b) revízie výsledkov auditov zhody, aby sa určilo, či PDS adekvátne dodržuje ustanovenia schválených politík,

c) rozhodovania o vhodnosti certifikátov asociovaných s daným CP pre špecifické aplikácie riadenia a usmerňovania činnosti certifikačnej autority a registračných autorít,

d) vykonávania auditu PDS,

e) zabezpečenia, že prijatý a schválený certifikačný poriadok (CP) sú riadne a náležite realizované.

(2) PMA predstavuje vrcholovú zložku, ktorá rozhoduje s konečnou platnosťou vo všetkých záležitostiach a aspektoch týkajúcich sa PDS a jej činnosti.

2.3.2 Poskytovateľ dôveryhodných služieb (PDS)

PDS, ktorý vydáva certifikáty v súlade s touto politikou:

a) vytvorí, podpíše, distribuuje a znefunkční certifikáty zaväzujúce X.500 Distinguished Name žiadateľa (držiteľa) s ich verejným kľúčom a tým aj ich podpisovým kľúčom (súkromný kľúč),

b) poskytuje informáciu o stave certifikátov prostredníctvom zoznamov znefunkčnených certifikátov (CRL) a prípadne cez Online Certificate Status Protocol (OCSP),

c) má pripravené, implementované a prevádzkuje postupy pri poskytovaní certifikačných služieb tak, aby boli adekvátne dosiahnuté požiadavky tohto poriadku.

2.3.3 Špecialista personalizácie dôveryhodnej služby

Špecialista personalizácie PDS (ePZP) v zmysle tohto CP je zodpovedný za povinnosti a postupy, ktoré sú kladené zo strany vydávajúcej PDS v rozsahu svojich pracovných povinností.

2.3.4 Personalizačné pracovisko

Je režimové pracovisko s materiálnym a technickým vybavením, kde špecialista personalizácie zabezpečuje potlač čipových kariet, ich inicializáciu a sprostredkovanie vydania certifikátov na čipové karty, ako aj dohľad nad kartami.

2.3.5 Držitelia

(1) Držiteľmi certifikátu vydávaného PDS môžu byť fyzické osoby, ktoré ich budú využívať v súlade so Zákonom o NZIS na identifikáciu, autentifikáciu a elektronický podpis v rámci NZIS a ZNCZI, ktorí vykonávajú činnosti PDS.

(2) Certifikát môže byť vydaný len na základe predloženej žiadosti a následnej autorizácie zo strany zodpovednej osoby personalizačného pracoviska (špecialistom personalizácie ePZP).

(3) Vhodnosť vydania certifikátu je na zvážení PDS, ak táto povinnosť nevzniká zo zákona o NZIS. PDS môže spravovať akýkoľvek počet držiteľov certifikátov.

2.3.6 Spoliehajúce sa strany

(1) Za spoliehajúce sa strany sa primárne považujú ZPr pristupujúci do NZIS, primárne vendori využívajúci VPN SD a ZNCZI.

(2) Akceptovaním certifikátu vydaného v súlade s ustanoveniami tohto CP, zmluvou (ak je uzavretá) a/alebo osobitnými podmienkami používania certifikátov spoliehajúca sa strana súhlasí s tým, že bude viazaná ustanoveniami tohto CP.

2.4 Používanie certifikátu

2.4.1 Povolené používanie

Certifikáty vydávané PDS je možné používať na prístup zdravotníckych pracovníkov a iných pracovníkov v zdravotníctve v osobitných prípadoch k informáciám v NZIS a k podpisovaniu odosielaných resp. ukladaných informácií v rámci NZIS alebo ako technologické certifikáty NZIS, pre servis zdravotníckych služieb a na poskytnutie podpory pre príslušných používateľov NZIS.

2.5 Správa politík

2.5.1 Organizácia zodpovedná za správu CP

Za správu (vypracovanie, udržiavanie, aktualizáciu) tohto CP je zodpovedné:

Národné centrum zdravotníckych informácií

Lazaretská 26 811 09 Bratislava 1

e-mail: nczisk@nczisk.sk

tel. číslo: +421 2 57 269 111

2.5.2 Kontakt

e-mail: Sprava_ePZP@nczisk.sk, tel. číslo: +421 2/32 35 30 30.

3 ZVEREJŇOVANIE INFORMÁCIÍ A ÚLOŽISKO

3.1 Úložisko

Úložisko PDS tvorí webová stránka dostupná na adrese http://www.nczisk.sk.

3.2 Publikovanie informácií

PDS zabezpečí:

a) uvádzanie v každom vydanom certifikáte URL webovej stránky ním vedenej resp. vedenej v jeho mene,

b) zverejnenie tohto CP, na webových stránkach vedených PDS,

c) 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,

d) poskytovanie verejnosti konečné prehlásenie z akéhokoľvek auditu vykonaného k zabezpečeniu súladu s požiadavkami na audit zo strany PMA.

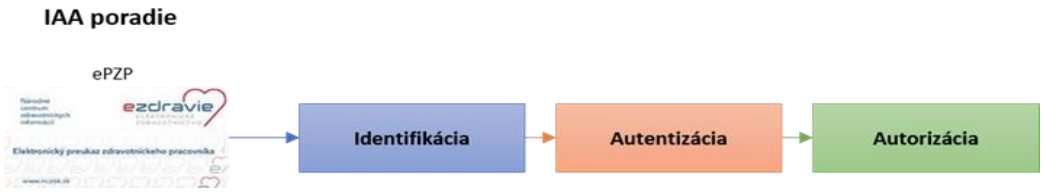
3.3 Čas a frekvencia aktualizovania a dostupnosti informácií

Všetky informácie musia byť aktualizované a dostupné v úložisku ihneď, ako je taká informácia k dispozícii PDS. Certifikáty vydané poskytovateľom dôveryhodných služieb, ktoré odkazujú na tento poriadok, budú aktualizované a dostupné ihneď po ich vydaní.

3.4 Kontroly prístupu k úložisku

PDS musí chrániť ľubovoľnú informáciu uloženú v úložisku, ktorá nie je určená na verejné rozširovanie. PDS vynaloží maximálne úsilie na to, aby zaistila integritu, dôvernosť a dostupnosť dát vyplývajúcich z poskytovania 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.

4 IDENTIFIKÁCIA, AUTENTIZÁCIA



(1) V tejto časti sú popísané postupy, ktoré PDS používa na overenie identity a autenticity alebo iných atribútov žiadateľa o vydanie certifikátu.

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

4.1 Pomenovanie

4.1.1 Typy mien

PDS je schopný 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.

4.1.2 Potreba zmysluplnosti mien

(1) 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.

(2) **Anonymita alebo pseudonymita držiteľov**

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

(3) **Pravidlá pre interpretáciu rôznych foriem mien**

Nie sú definované žiadne podmienky.

(4) **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.

4.2 Prvotné overenie identity

4.2.1 Overenie identity žiadateľa

Overenie identity žiadateľa alebo osoby oprávnenej konať za žiadateľa, ak ide o PO bude vykonané na základe vzájomnej kontroly elektronickej a papierovej formy dokumentov žiadosti o vydanie certifikátu, ktorá bude okrem iného obsahovať aj identifikačné údaje žiadateľa.

4.2.2 Overenie organizácie

Certifikáty pre organizácie nebudú vydávané.

4.2.3 Spôsob preukazovania vlastníctva nosiča súkromného kľúča

Nevyžaduje sa.

4.2.4 Overovanie právomocí

V rámci overovania právomocí pracovník PDS resp. špecialista personalizácie PDS vykoná formálnu kontrolu údajov v JRÚZ, ktorých zdrojom je RFO a príslušná komora, či žiadateľ o certifikát má oprávnenie pristupovať do NZIS (pracovník overuje údaje zo žiadosti voči autoritatívnemu zdroju dát (JRÚZ). Overenie právomocí pre vydanie certifikátov Admin, overí voči žiadosti o certifikát, v ktorej sú definované právomoci žiadateľa jeho priamym nadriadeným v PDS.

4.3 Identifikácia a autentizácia pri obnove certifikátu

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

4.3.1 Obnova certifikátu po uplynutí platnosti certifikátu

(1) Platnosť certifikátov vydaných PDS je päť rokov a vydávanie nových certifikátov na kartových nosičoch je vykonaná automaticky pred ich exspiráciou, bez opakovaného overenia identity žiadateľa, pokiaľ u žiadateľa nedošlo k zmene identifikačných údajov (zmena mena / priezviska).

(2) Pri certifikátoch uložených na nosičoch HSM je obnova certifikátu pri ich exspirácii vykonaná na základe novej žiadosti.

4.3.2 Obnova certifikátu po jeho znefunkčnení pred uplynutím platnosti certifikátu

(1) Ak dôjde k znefunkčneniu certifikátu pred uplynutím jeho platnosti jeho exspiráciou z dôvodu, ktoré vymedzuje Zákon o NZIS, zmluva (ak bola uzavretá), z dôvodov uvedených v iných dokumentoch (napr. v osobitných podmienkach používania certifikátov vydaných PDS) alebo na základe žiadosti o znefunkčnenie certifikátu, musí PDS pred obnovou certifikátu overiť identitu žiadateľa primeraným spôsobom, aby bolo obmedzené riziko zneužitia.

(2) PDS alebo autorizujúci vyškolený pracovník PDS oprávnený konať v jej mene musí overiť akúkoľvek zmenu informácií obsiahnutých v žiadosti ešte pred jeho vydaním.

4.3.3 Identifikácia a autentifikácia žiadosti o znefunkčnenie certifikátu

(1) V situáciách, ktoré nepredstavujú riziko zneužitia karty bude znefunkčnenie platnosti neaktuálnych kariet vrátane certifikátov realizované technickým spôsobom (CMS). V tomto prípade o znefunkčnenie platnosti certifikátov držiteľ karty nežiada.

(2) V situáciách, ktoré predstavujú riziko zneužitia karty bude znefunkčnenie platnosti neaktuálnych kariet vrátane certifikátov realizované bezodkladne jedným z nasledovných spôsobov:

a) kontaktovaním PDS,

b) kontaktovaním certifikačnej autority.

(3) Všetky žiadosti o revokáciu certifikátu musia byť zaznamenané.

(4) V situáciách, ktoré predstavujú riziko zneužitia karty inou osobou ako je jej držiteľ bude znefunkčnenie platnosti aktuálnych kariet vrátane certifikátov realizované technickým spôsobom (CMS). V tomto prípade o znefunkčnenie platnosti certifikátov držiteľ karty požiada PDS.

(5) V situáciách, ktoré predstavujú udalosť ako strata, krádež karty a udalosť je eskalovaná ku zneužitiu karty inou osobou ako je jej držiteľ, zo strany PDS je nutné kontaktovať CSIRT na zníženie incidentu a znefunkčnenie platnosti kariet vrátane certifikátov realizované CSIRT jednotkou.

5 PREVÁDZKOVÉ POŽIADAVKY

5.1 Žiadanie o certifikát

(1) PDS musí zabezpečiť, aby všetky postupy a požiadavky kladené na žiadosť o vydanie certifikátu boli popísané v tomto CP alebo inom verejne dostupnom dokumente a rešpektovali príslušnú legislatívu v platnom znení.

(2) Súčasťou preukazov v zmysle Zákona o NZIS je elektronický čip, ktorého súčasťou sú certifikáty. Preto pre potreby CP PDS sa na žiadosť o preukaz pozerá ako na žiadosť o certifikát.

5.1.1 Žiadatelia o certifikát

Žiadateľom o certifikát môžu byť osoby, pri ktorých to ustanovuje Zákon o NZIS, a ZNCZI.

5.1.2 Postup žiadania a zodpovednosti

(1) Žiadateľ o certifikát vyplní žiadosť o vydanie preukazu podľa Zákona o NZIS alebo inú žiadosť o vydanie certifikátu stanovenú a sprístupnenú od PDS.

(2) PDS zabezpečuje, aby každá doručená žiadosť bola overená v nasledovnom rozsahu:

a) overením súladu údajov na zaslanej žiadosti s údajmi v systéme PDS,

b) overením existencie záznamu v JRÚZ a/alebo iných záznamov vedených PDS (napr. pracovnoprávne vzťahy),

c) overením splnenia náležitostí týkajúcich sa overenia identity a autenticity žiadateľa (pozri kapitolu 5.2.1).

(3) Ak na základe podanej žiadosti o vydanie certifikátu nie sú splnené podmienky pre vydanie príslušného certifikátu ani do 12 mesiacov od podania žiadosti, PDS na podanú žiadosť ďalej neprihliada a vymaže osobné údaje uvedené v žiadosti v súlade so zásadou správnosti spracúvania osobných údajov podľa čl. 5 ods. 1 písm. d) GDPR a v súlade so zásadou minimalizácie uchovávania osobných údajov podľa čl. 5 ods. 1 písm. e) GDPR.

5.2 Spracovanie žiadosti o vydanie certifikátu

5.2.1 Spôsob overenia identity a autenticity žiadateľa

(1) Overenie identity a autenticity žiadateľa, alebo osoby oprávnenej konať za žiadateľa, ak ide o PO, vykoná špecialista personalizácie PDS na základe doručenej žiadosti o certifikát, ktorá obsahuje údaje preukazujúce identitu a autenticitu žiadateľa alebo osoby oprávnenej konať za žiadateľa, ako aj ďalšie údaje o žiadateľovi nevyhnutné k vydaniu certifikátov.

(2) Špecialista personalizácie PDS vykoná formálnu kontrolu súladu žiadosti s relevantnými dokumentmi predloženými žiadateľom alebo nachádzajúcimi sa u PDS (napr. občiansky preukaz, splnomocnenie, pracovná zmluva, zápis o pracovno-právnych vzťahoch žiadateľa a PZS v IS PDS a pod.).

5.2.2 Overenie identity a autenticity

(1) Pokiaľ overenie identity a autenticity bude úspešné a aj ostatné náležitosti žiadosti v poriadku, bude žiadosť postúpená v procese na ďalšie spracovanie.

(2) Pokiaľ sa pri overovaní identity a autenticity preukážu nezrovnalosti v predložených údajoch resp. žiadosti o vydanie certifikátu, vyžiada PDS doplnenie alebo opravu príslušných údajov, ak Zákon o NZIS neustanovuje inak. Pre overenie identity a autenticity sa považujú dokumenty - platný cestovný pas, občiansky preukaz alebo vodičský preukaz.

(3) Ak nepríde k náprave nezrovnalostí údajov, v žiadosti o vydanie certifikátu, tak po uplynutí roka nasledujúceho po roku, v ktorom bola žiadosť podaná (doručená PDS) ju PDS vymaže/odstráni v súlade so zásadou správnosti spracúvania osobných údajov podľa čl. 5 ods. 1 písm. d) GDPR a v súlade so zásadou minimalizácie uchovávania osobných údajov podľa čl. 5 ods. 1 písm. e) GDPR.

5.2.3 Overenie splnenia podmienok pre vydanie certifikátu

Ak došlo k úspešnému overeniu identity podľa kapitol 5.2.1 a 5.2.2, PDS pristúpi k procedúre overenia žiadateľa voči tým istým údajom v JRÚZ, ktorých zdrojom je RFO a príslušná komora. V prípade HSM aj k overeniu PZS a pracovno-právnych vzťahov ZPr s PZS, v prípade Admin preukazu voči žiadosti o vydanie certifikátu (Admin) a po overení zhody voči požadovaným údajom vydá certifikáty bez zbytočného zdržania.

5.3 Vydanie certifikátu

5.3.1 Činnosť PDS pri vydaní certifikátu

Po úspešnom overení podľa kapitoly 5.2 tohto CP pracovník PDS iniciuje proces samotného vygenerovania kryptografických kľúčov, on-line vydanie certifikátov a ich uloženie na príslušný nosič certifikátov. Po tomto procese sú certifikáty aktívne.

5.4 Prevzatie certifikátu

5.4.1 Spôsob prevzatia certifikátu

PDS odovzdá alebo odošle príslušný preukaz obsahujúci certifikáty určenej FO, alebo zabezpečí doručenie certifikátu bezpečnou cestou. Pri certifikátoch ukladaných na HSM, zašle PDS žiadateľovi certifikát zabezpečený heslom prostredníctvom e-mailu, a to na základe vygenerovanej technologickej žiadosti žiadateľa.

5.4.2 Notifikácia o vydaní certifikátu iným entitám ako žiadateľ

Nevykonáva sa.

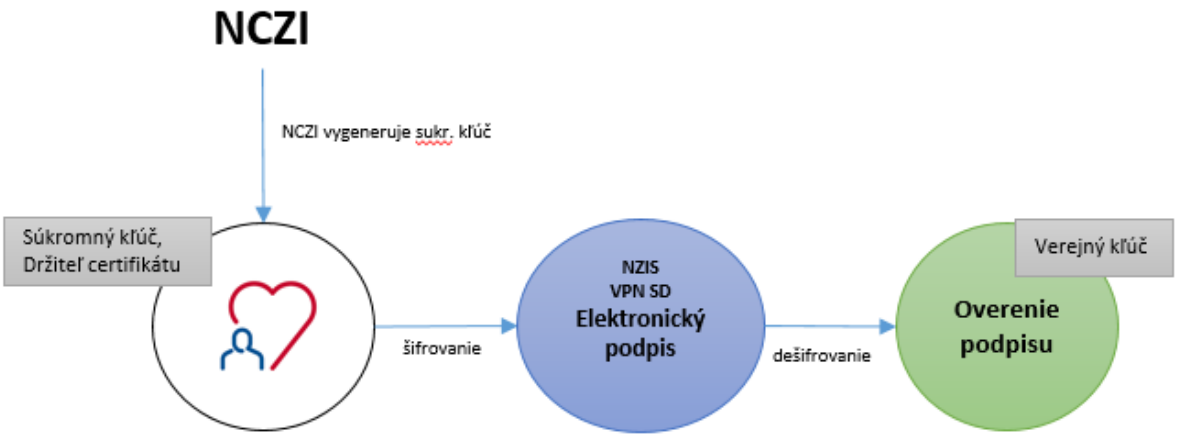
5.5 Kľúčový pár a používanie certifikátu

5.5.1 Súkromný kľúč držiteľa a používanie certifikátu

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

5.5.2 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 a VPN SD.



5.6 Vydanie nového certifikátu pri jeho obnove na pôvodné kľúče – tzv. recovery

Vydanie nového certifikátu pri obnove certifikátu bez zmeny žiadateľovho/držiteľovho verejného kľúča PDS nevykonáva.

5.7 Vydanie nového certifikátu pri jeho obnove na nové kľúče – tzv. renewal

Vydanie nového certifikátu je vždy spojené aj so zmenou verejného kľúča.

5.7.1 Kto môže žiadať o obnovu certifikátu na nové kľúče / automatizované obnovenie

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

(2) V prípade exspirácie platnosti certifikátu držiteľ pôvodného certifikátu nežiada o obnovu certifikátu (je to automatizované z informačného systému PDS, nevykonáva ani opakovaná identifikácia žiadateľa), okrem certifikátov uložených na HSM, pri ktorých sa vyžaduje podanie novej žiadosti.

5.7.2 Postup žiadania o obnovu certifikátu

Pre podanie žiadosti platia obdobne ustanovenia kapitoly 5.1 tohto CP.

5.7.3 Spôsob prevzatia obnoveného certifikátu

Platia ustanovenia kapitoly 5.4 CP.

5.7.4 Zverejnenie obnoveného certifikátu

Vykoná sa rovnakým spôsobom ako pri jeho prvotnom vydaní.

5.7.5 Notifikácia o vydaní obnoveného certifikátu spoliehajúcim sa stranám

Platí ustanovenie 5.4.2 tohto CP.

5.8 Zmena kľúčov

(1) Držiteľ môže požiadať o obnovu jeho/jej kľúčového páru v priebehu 30 dní pred exspiráciou kľúčov. Proces obnovy môže začať držiteľ alebo PDS.

(2) Držitelia bez platného certifikátu musia byť znovu overení PDS obdobným spôsobom ako pri prvej registrácii.

(3) V prípade, že držiteľov certifikát bol znefunkčnený v dôsledku nedodržania jeho povinností, musí PDS overiť, že všetky dôvody pre nedodržania povinností boli odstránené k jeho spokojnosti ešte pred obnovou certifikátu.

5.9 Zmena údajov v certifikáte

(1) 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 kapitolu 5.).

(2) So zmenou alebo obnovou certifikátov je spojená aj zmena nosiča certifikátu (preukazu), s výnimkou certifikátov ukladaných na HSM. Z praktického hľadiska je totiž neaplikovateľné meniť, rušiť, alebo obnovovať certifikáty na rovnakom preukaze.

5.10 Znefunkčnenie certifikátu

5.10.1 Dôvody znefunkčnenia certifikátu

(1) Dôvody znefunkčnenia certifikátu ustanovuje Zákon o NZIS alebo iné právne predpisy, interné predpisy PDS (napr. tento CP), osobitné podmienky používania certifikátov a/alebo zmluva (ak je uzavretá).

(2) Certifikát sa znefunkčňuje napr. v nasledovných prípadoch:

a) držiteľ certifikátu zomrel alebo bol vyhlásený za mŕtveho,

b) držiteľ certifikátu stratil ePZP alebo ak mu bol odcudzený a táto skutočnosť bola ohlásená PDS,

c) certifikát (nosič certifikátu) bol zničený alebo poškodený,

d) držiteľ certifikátu prestal vykonávať príslušné povolanie,

e) držiteľ certifikátu alebo iná oprávnená osoba požiada o znefunkčnenie certifikátu,

f) existuje podozrenie zverejnenia, sprístupnenia, straty, kompromitovania a/alebo iného zneužitia certifikátu alebo došlo k niektorej z uvedených skutočností ukázalo sa, že držiteľ certifikátu nedodržuje svoje povinnosti držiteľa certifikátu,

g) identifikačné informácie alebo pričlenené prvky ľubovoľných mien v certifikáte sa stanú neplatnými,

h) certifikát nebol vydaný v súlade s týmto CP,

i) zistilo sa, že niektorá z informácií uvedených v certifikáte je chybná alebo nesprávna,

j) skončili okolnosti, ktoré vyžadovali vydanie certifikátu (testovanie, overovanie aplikácií ap.),

k) 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 apod.),

l) došlo ku kompromitácii súkromného kľúča PDS.

(3) Znefunkčnenie certifikátu vykoná PDS na základe žiadosti alebo skutočností zistených z vlastnej činnosti.

5.10.2 Kto môže žiadať o znefunkčnenie certifikátu

(1) Držiteľ certifikátu (alebo ním poverená FO alebo PO) môže kedykoľvek požiadať o znefunkčnenie certifikátu.

(2) O znefunkčnenie certifikátu môže požiadať aj akákoľvek iná osoba, ak zistí skutočnosť odôvodňujúcu znefunkčnenie certifikátu.

5.10.3 Miesto podania žiadosti o znefunkčnenie certifikátu

(1) Žiadosť o znefunkčnenie certifikátu možno podať:

a) osobne v sídle PDS resp. na pracoviskách PDS,

b) písomne.

(2) PDS môže na svojom webovom sídle zverejniť vzor tlačiva za účelom podania žiadosti o znefunkčnenie certifikátu.

5.10.4 Lehota na podanie žiadosti o znefunkčnenie certifikátu

Držiteľ certifikátu alebo iná povinná osoba (napr. pracovník PDS) podľa Zákona o NZIS, tohto CP, interných predpisov, iných dokumentov PDS (napr. osobitné podmienky pre používanie certifikátov) je povinný požiadať o znefunkčnenie certifikátu bezodkladne ako nastane niektorá zo skutočnosti odôvodňujúcich znefunkčnenie certifikátu.

5.10.5 Vybavenie žiadosti na znefunkčnenie certifikátu

PDS je povinný znefunkčniť certifikát bezodkladne po tom, čo zistil skutočnosti odôvodňujúce znefunkčnenie certifikátu.

5.10.6 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).

5.10.7 Frekvencia aktualizácie CRL

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

5.10.8 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.

5.10.9 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.

5.10.10 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.

5.10.11 Pozastavenie platnosti certifikátu

Pozastavenie certifikátu nie je zo strany PDS podporované.

5.11 Služby overovania stavu certifikátu

5.11.1 Charakteristika služby

PDS poskytuje službu overovania stavu certifikátu prostredníctvom služby potvrdenia existencie a platnosti certifikátu (OCSP).

5.11.2 Dostupnosť služby

Aktuálny zoznam je dostupný na URL uvedenom v predmetnom certifikáte.

5.12 Obnova kľúčov z depozitu alebo zálohy

PDS nepodporuje uchovávanie súkromných kľúčov držiteľov certifikátov.

6 MANAŽÉRSKE, PREVÁDZKOVÉ A FYZICKÉ BEZPEČNOSTNÉ OPATRENIA

6.1 Fyzické bezpečnostné opatrenia

6.1.1 Umiestnenie, priestory a prístup

(1) PDS musí zabezpečiť že:

a) priestory PDS sú nepretržite fyzicky alebo elektronicky monitorované pred neoprávneným vniknutím,

b) samostatný prístup k serverom PDS budú mať len osoby nachádzajúce sa na zozname oprávnených osôb s právom prístupu,

c) osoby, ktoré nie sú na zozname oprávnených osôb na vstup budú vstupovať do priestorov PDS len pod dohľadom oprávnenej osoby,

d) záznamy o vstupe do priestorov sú udržiavané a kontrolované pravidelne,

e) všetky vymeniteľné médiá a dokumenty obsahujúce citlivé informácie sú uložené v zabezpečených kontajneroch.

(2) Všetky pracoviská PDS ako aj pracovné stanice používané pre on-line komunikáciu PDS zabezpečujúce výrobu, distribúciu, evidenciu certifikátov musia byť umiestnené v priestoroch, ktoré spĺňajú nasledujúce požiadavky:

a) nepretržitý fyzický alebo elektronický monitoring proti neoprávnenému vniknutiu,

b) prístup bez sprievodu zodpovednej osoby je možný len osobám na zozname oprávnených osôb,

c) prístup osobám, ktorý nie sú na zozname oprávnených osôb je umožnený len v sprievode a pod dohľadom oprávnenej osoby,

d) všetky vymeniteľné médiá a dokumenty obsahujúce citlivé informácie sú uložené v zabezpečených kontajneroch.

(3) PDS zabezpečí prevádzku špecialistovi personalizácie PDS tak, že zaistí primeranú bezpečnosť kryptografickému modulu s podpisovými kľúčmi PDS a systémovému softvéru.

(4) Špecialisti personalizácie PDS nesmú 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.

(5) Certifikáty PDS, ktoré sú umiestnené na bezpečnom hardvérovom zariadení musia byť chránené fyzicky. To môže byť vykonané napríklad tým, že je zariadenie prechovávané u pracovníka PDS.

6.1.2 Dodávka energie a teplota

NCZI musí zabezpečiť že zdroj elektrickej energie a teplota bude postačujúca k bezproblémovému chodu systému PDS.

6.1.3 Ohrozenie vodou

PDS musí zabezpečiť, že systém výroby a distribúcie certifikátov je chránený pred ohrozením vodou.

6.1.4 Protipožiarna ochrana

PDS musí zabezpečiť, že systém výroby a distribúcie certifikátov je chránený protipožiarnym systémom.

6.1.5 Uchovávanie médií

PDS musí zabezpečiť, že uchovávané média používané v systéme PDS 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.

6.1.6 Nakladanie s odpadom

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

6.1.7 Záložné pracovisko

PDS musí zabezpečiť, aby záložné pracovisko, ak existuje, malo rovnakú úroveň bezpečnosti ako primárne pracovisko PDS. Záložným voči pracovisku NCZI v Bratislave je pracovisko NCZI vo Zvolene a naopak.

6.2 Procedurálne bezpečnostné opatrenia

6.2.1 Dôveryhodné role PDS

(1) PDS zabezpečuje dôveryhodné roly jednotlivých zamestnancov na základe vytvorenia písomnej formy žiadosti prístupového oprávnenia, podľa štandardného postupu vyplnením a odsúhlasením žiadosti v súlade so smernicou NCZI. (*Smernica **OS - 504 Stratégia a politika informačnej a kybernetickej bezpečnosti***). NCZI rešpektuje kybernetickú a informačnú bezpečnosť ako komplexný proces, definuje jednotlivé organizačné zložky, roly a funkcie, ktoré sú potrebné na spoľahlivé a efektívne fungovanie. Z pohľadu bezpečnosti ePZP má prístup k tým funkcionalitám, údajom a službám, ktoré sú nevyhnutné na plnenie zverených úloh používateľa a používateľské role si ePZP eviduje v matici riadenia prístupov.

(2) PDS musí zabezpečiť rozdelenie povinností pre kritické funkcie PDS, tak aby jedna osoba nemohla zneužiť systém PDS bez možnosti zistenia a identifikovania tejto osoby. Každý prístup užívateľa do systému musí byť obmedzený len na tie akcie, ktoré sú potrebné na vykonanie pri plnení ich povinností.

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

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

a. Systémový administrátor:

1. konfigurácia a údržba hardvéru a softvérov systému PDS,
2. spúšťanie a ukončovanie služieb PDS.

b. Bezpečnostný správca:

1. celková systémová a sieťová bezpečnosť infraštruktúry PDS,
2. analýza auditovacích logov,
3. pravidelné a nepravidelné kontroly:

3.a pri výkone činností všetkých pracovníkov PDS v zmysle definovaných smerníc,

3.b fyzickej bezpečnosti a objektovej bezpečnosti,

3.c o zabezpečení infraštruktúry PDS.

c. Audítor systému:

1. overovanie auditných záznamov,
2. overovanie dodržiavania súladu CP,
3. člen PMA,
4. správa PDS bezpečnostnej politiky,
5. správa CP,
6. revízie výsledkov auditov zhody.

(5) Alternatívne rozdelenie povinností a rolí, ktoré poskytuje rovnaký stupeň odolnosti k útokom z vnútra je prijateľné pokiaľ je zachovaná úroveň bezpečnosti z pozície rozdelenia povinností a rolí v procese vydávania certifikátov.

(6) Iba osoby zodpovedné za vyššie uvedené povinností majú povolený prístup k softvéru, ktorý riadi prevádzku PDS.

(7) **Dôveryhodné roly zabezpečujúce výrobu a distribúciu certifikátov PDS:**

a) PDS musí personálne a technologicky zabezpečiť, aby pracovné roly PDS boli od seba nezávislé a aby nebolo možné spájanie výkonu činností rolí, ktoré by mohli kompromitovať dôveryhodnosť certifikátov:

1. rola prevzatia žiadostí ich overenia a vygenerovania certifikátov,
2. rola generovania, doručenia PIN kódov a nosičov certifikátov, pokiaľ je nosičom certifikátu preukaz,

b) zároveň, aby špecialisti personalizácie PDS pochopili svoju zodpovednosť za identifikáciu a overovanie žiadateľov a vykonávanie nasledovných funkcií:

1. prijatie žiadosti, zmena certifikátu, znefunkčnenie certifikátu,
2. overenie identity a autenticity žiadateľa,
3. prenos informácie o žiadateľovi k PDS,
4. overovanie všetkých ostatných informácií súvisiacich s vydaním certifikátu.

6.2.2 Počet rolí potrebný na výkon úloh

(1) Generovanie kľúčov PDS si vyžaduje prítomnosť najmenej troch rolí PDS:

a) **Rola špecialistu personalizácie** – zabezpečuje prevzatie žiadostí, výrobu a doručenie certifikátov.

b) **Rola administrátora aplikácii II** – zabezpečuje správu certifikátov koreňovej certifikačnej autority a podriadených certifikačných autorít (napríklad: Auth CA, Tech CA, Protection CA, B2B CA). Kontrola CRL, správa PIN.

c) **Rola manažéra informačnej a kybernetickej bezpečnosti** – zabezpečuje kontrolu a vyhodnocovanie bezpečnosti infraštruktúry a SW bezpečnosti PDS pri práci s certifikátmi.

(2) Pod správou certifikátov sa rozumie vydávanie (podpisovanie žiadosti o certifikát danou certifikačnou autoritou) revokovanie nepotrebných certifikátov, distribúciu vydaných certifikátov.

(3) PDS musí zabezpečiť, že ktorýkoľvek zavedený overovací proces poskytne celkový prehľad všetkých aktivít vykonaný pracovníkmi v dôveryhodných rolách.

6.2.3 Identifikácia a autentizácia jednotlivých rolí

(1) Všetci zamestnanci PDS vykonávajúci jednotlivé role sa musia podrobiť overeniu identity a oprávnení pred tým, ako:

a) sú priradení na zoznam s oprávnením prístupu do priestorov PDS,

b) sú priradení na zozname s oprávnením fyzického prístupu k systému PDS,

c) im je pridelený certifikát na výkon roly v rámci PDS,

d) im je pridelený účet v systéme PDS.

(2) Každý z týchto certifikátov a účtov (s výnimkou podpisových certifikátov PDS):

a) musí byť priamo priradený fyzickej osobe,

b) nemôže byť zdieľaný,

c) musí mať obmedzený rozsah oprávnení na oprávnenia danej roly v PDS softvéri, operačnom systéme a riadení procesov.

(3) PDS operácie musia byť, pri prístupe cez vzdialené pripojenie (vzdialený prístup), zabezpečené použitím mechanizmov, akými sú silná autentifikácia a šifrovanie s využitím hardvérových tokenov.

6.3 Personálne opatrenia

(1) PDS musí zabezpečiť, že všetci zamestnanci vykonávajúci povinnosti v súvislosti s prevádzkou PDS musia:

a) byť v pracovnoprávnom vzťahu k PDS a byť viazaný k mlčanlivosti o citlivých skutočnostiach, o ktorých sa v súvislosti s výkonom práce dozvedel,

b) mať písomné menovanie s presne vyšpecifikovanými kompetenciami, ktoré súvisia s prevádzkou PDS,

c) mať zadefinované činnosti súvisiace s prevádzkou PDS,

d) absolvovať komplexné školenia s ohľadom na povinnosti, ktoré majú plniť.

(2) Zamestnanci nesmú mať pridelené povinnosti, ktoré môžu vyvolať konflikt záujmov s ich PDS alebo povinnosťami špecialistu personalizácie PDS.

6.3.1 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.

6.3.2 Postupy overovania

(1) NCZI vykoná zodpovedajúce preskúmanie všetkých zamestnancov, 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 PDS alebo ekvivalentných požiadaviek.

(2) Všetci zamestnanci, ktorí neuspejú v rámci počiatočného alebo pravidelného preskúmavania, nesmú ďalej pôsobiť alebo pokračovať v pôsobení v dôveryhodnej role.

(3) Interval preskúmavania je stanovený v kapitole 6.3.4.

(4) PMA môže stanoviť dodatočné požiadavky v súlade s legislatívou.

6.3.3 Požiadavky na školenie a personálna bezpečnosť

(1) PDS musí zabezpečiť, že všetci zamestnanci plniaci si povinnosti v súvislosti s prevádzkou PDS musia dostať komplexné školenie v oblasti:

a) všeobecne záväzných právnych predpisov, bezpečnostných pravidiel a mechanizmov platných pre PDS,

b) GDPR – ochrana osobných údajov,

c) všetkých verzií PKI softvéru v systéme PDS,

d) všetkých povinnosti v rámci PKI,

e) postupov obnovy po havárii a postupov obnovy činnosti (business continuity).

(2) Všetci zamestnanci PDS musia dostať primerané školenie, aby mohli plniť svoje povinnosti a následne musia byť pravidelne preškoľovaní na zabezpečenie aktuálnosti ich vedomostí a pravidelného zvyšovania rozvoja a vzdelávania ich bezpečnostného povedomia počas trvania pracovnoprávneho vzťahu.

(3) ePZP vo všetkom intenzívne spolupracuje s organizačnými útvarmi NCZI, ako aj špecialistami a správcami CMS, s odbornou špecializáciou a kvalifikáciou.

6.3.4 Frekvencia preškoľovania a požiadavky

Požiadavky podľa kapitoly 6.3.3 musia byť aktuálne v závislosti od zmien v systéme PDS. Preškoľovanie musí byť vykonávané podľa potreby a PDS musí preskúmať tieto požiadavky najmenej raz za 2 roky u všetkých pracovníkov PDS.

6.3.5 Obmena pozícií

Žiadne požiadavky.

6.3.6 Postup pri neoprávnenom zásahu

V prípade výkonu neoprávneného zásahu osobou vykonávajúcou povinnosti v súvislosti s prevádzkou PDS alebo podozrenia z takéhoto neoprávneného zásahu PDS pozastaví jeho/jej prístup k systému PDS, a to až do času objasnenia udalosti.

6.3.7 Dokumentácia poskytovaná zamestnancom

PDS musí sprístupniť všetkým pracovníkom PDS tento CP a ostatné dokumenty (nariadenia, politiky, zmluvy a iné) týkajúce sa ich pozície.

6.4 Postupy zaznamenávania auditných logov

6.4.1 Typy zaznamenávaných udalostí

(1) PDS by mal zaznamenať do auditných log súborov všetky udalosti týkajúce sa bezpečnosti systému PDS. Do tohto patria také udalosti, ako je:

a) spustenie a vypnutie systému,

b) spustenie PDS aplikácie a jej vypnutie,

c) pokusy o vytvorenie, vymazanie, nastavenie hesla alebo zmenu systémových nastavení všetkých rolí v rámci PKI NCZI, ktoré majú prístup k systému PDS,

d) zmeny nastavení PDS a / alebo kryptografických kľúčov,

e) zmena pravidiel vytvárania certifikátov napr. zmena doby platnosti,

f) pokusy o prihlásenie sa a odhlásenia sa,

g) neoprávnené pokusy o prístup po sieti do systému PDS,

h) neoprávnené pokusy o prístup k systémovým súborom,

i) generovania vlastných alebo podriadených kľúčov,

j) vydávanie a znefunkčnenie certifikátov,

k) chybná operácia pri čítaní resp. zápise certifikátu alebo a CRL adresára.

(2) Všetky záznamy, či už elektronické alebo na papierovom nosiči, by mali obsahovať dátum a čas udalosti a totožnosť subjektu, ktorý udalosť spôsobil.

(3) PDS môže tiež zbierať a konsolidovať, a to buď elektronicky alebo na papierovom nosiči bezpečnostné informácie, ktoré nie sú generované priamo systémom PDS, ako sú:

a) záznamy o fyzickom prístupe,

b) zmeny konfigurácie systému a jeho údržba,

c) personálne zmeny,

d) záznamy o odchýlkach a kompromitáciách,

e) záznamy o zničení médií obsahujúce kryptografické kľúče, aktivačné údaje alebo osobné údaje držiteľov.

(4) Pre uľahčenie rozhodovania, by mali byť všetky zmluvy a korešpondencia vzťahujúce sa k službám PDS uchovávané a konsolidované na jednom mieste a to buď elektronicky alebo na papierovom nosiči.

6.4.2 Frekvencia spracovávania auditných log záznamov

(1) PDS musí zabezpečiť, že zamestnanci PDS preskúmavajú svoje audit log záznamy minimálne raz týždenne a všetky významné udalosti sú vysvetlené v súhrnom zázname s preskúmavania.

(2) 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.

(3) Podporné elektronické alebo papierové nosiče log záznamov PDS by mali byť porovnávané pokiaľ sa nejaký zásah javí ako podozrivý.

(4) Všetky prijaté opatrenia prijaté na základe týchto hodnotení musia byť dokumentované.

6.4.3 Doba uchovávanie auditných log záznamov

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

6.4.4 Ochrana auditných log záznamov

(1) Systém zaznamenávanie auditných log záznamov musí zahŕňať mechanizmy na ochranu log súborov proti neoprávnenému prezeraniu, úprave a vymazaniu.

(2) Papierové nosiče log záznamov musia byť chránené pred neoprávneným prezeraním, úpravou a zničením.

6.4.5 Postup zálohovania auditných log záznamov

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

6.4.6 Systém získavania auditných záznamov

PDS musí identifikovať spôsob získavania auditných záznamov.

6.4.7 Upozornenie pôvodcu na udalosť

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

6.4.8 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.

6.5 Uchovávanie záznamov

6.5.1 Typy uchovávaných záznamov

Nasledujúce dáta a súbory musia byť archivované PDS:

a) konfigurácia systémov a zariadení,

b) zmeny a aktualizácia systému alebo jeho konfigurácie,

c) žiadosti o vydanie certifikátu,

d) žiadosti o znefunkčnenie certifikátu,

e) osobné údaje držiteľa certifikátu,

f) dokumentácia o odovzdaní a prijatí certifikátu,

g) dokumentácia o prijatí tokenov,

h) všetky vydané a/alebo zverejnené certifikáty,

i) zmena kľúčov PDS,

j) všetky ARL a CRL vydané a/alebo zverejnené,

k) všetky auditné log záznamy,

l) ostatné údaje alebo aplikácie na overenie obsahu archívu,

m) dokumentácia vyžadovaná audítormi,

n) konečné stanovisko vyplývajúce z vykonaného auditu zhody.

6.5.2 Doba uchovávanie archívnych záznamov

(1) Doba uchovávania archívu kľúčov a informácie o certifikáte je 10 rokov.

(2) Doba uchovávania archívu auditných log záznamov sú 3 mesiace.

6.5.3 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.

6.5.4 Archívny systém

Nie sú stanovené žiadne požiadavky.

6.6 Kompromitácia a obnova po havárii

6.6.1 Postupy dokumentovania a riadenia incidentov a kompromitácií

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

6.6.2 Poškodený hardvér, softvér a/alebo údaje

PDS 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 PDS, musí PDS zaistiť súhlas s poskytovateľom úložiska, aby postupy obnovy boli prijaté a dokumentované poskytovateľom.

6.6.3 Kompromitácia súkromného kľúča PDS

(1) PDS musí mať zavedené postupy, ktoré budú nasledovať v prípade kompromitácie súkromného podpisového kľúča používaného na podpisovanie PDS vydávaných certifikátov pre koncových používateľov alebo kľúčov používaných akoukoľvek PDS na vyššej úrovni. Musí obsahovať postupy na znefunkčnenie všetkých dotknutých certifikátov a postupu na bezodkladné informovanie všetkých držiteľov týchto certifikátov a spoliehajúcich sa strán.

(2) V prípade potreby zrušenia podpisového certifikátu PDS musí PDS bezodkladne o tom informovať držiteľa certifikátu.

(3) PDS musí tiež zverejniť sériové číslo zrušeného certifikátu vo vhodnom CRL.

6.7 Ukončenie činnosti PDS

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

(2) V prípade, že PDS ukončí prevádzku budú o tejto skutočnosti urýchlene informovaní všetci držitelia, špecialisti personalizácie PDS a spoliehajúce sa strany.

(3) Všetky platné certifikáty vydané PDS v zmysle tohto CP budú zrušené skôr, ako dôjde k ukončeniu činnosti.

(4) Všetky aktuálne a archivované dokumenty PDS musia byť odovzdané PMA (alebo inej určenej osobe) počas 48 hodín po ukončení činnosti PDS a v súlade s týmto CP.

(5) Žiadne úložisko s možnosťou obnovy kľúčov nesmie byť súčasťou odovzdaných údajov.

7 TECHNICKÉ BEZPEČNOSTNÉ OPATRENIA

7.1 Generovanie kľúčového páru a jeho inštalácia

7.1.1 Generovanie kľúčov

(1) Generovanie kľúčových párov pre koncového užívateľa sa uskutoční v priebehu personalizácie karty na personalizačnom pracovisku NCZI priamo na čipovej karte prostredníctvom PMA schváleného algoritmu.

(2) V prípade technologických certifikátov – Admin NZIS karty, SD karty si kľúčový pár generuje žiadateľ. Pri generovaní kľúčov pre použitie v HSM si žiadateľ o certifikát vygeneruje technologickú žiadosť o certifikát na zariadení, ktorého súčasťou je HSM (pritom vzniká privátny kľuč). V žiadosti je uvedený Crypto provider (napr: nCipher Enhanced RSA and AES Cryptographic Provider), ktorý určuje, že privátny kľuč bude šifrovaný HSM. Vygenerovanú žiadosť pošle systémovému administrátorovi (správcovi PDS), ktorý ju podpíše adekvátnym certifikátom. Správca pošle späť žiadateľovi verejnú časť certifikátu. Žiadateľ naimportuje verejnú časť napríklad do úložiska certifikátov na zariadení, kde vygeneroval žiadosť a tým sa sparuje verejná a súkromná časť a certifikát je pripravený na použitie.

7.1.2 Doručenie privátneho kľúča držiteľovi

Súkromné kľúče budú odovzdané držiteľovi bezpečným spôsobom, a to buď prostredníctvom Slovenskej pošty do vlastných rúk alebo osobne do vlastných rúk. V prípade HSM podľa kapitoly 7.1.1.

7.1.3 Doručenie verejného kľúča na PDS

Žiadne požiadavky.

7.1.4 Veľkosť kľúčov

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

7.1.5 Parametre generovania kľúčov a kontrola kvality

Žiadne požiadavky.

7.1.6 Účel použitia kľúčov

(1) Kryptografické kľúče koncových používateľov uložené na čipovej karte sú určené na:

a) autentifikáciu držiteľa,

b) vytváranie elektronického podpisu a

c) end-2-end šifrovanie údajov.

(2) 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“.

(3) V certifikáte koncového používateľa musia byť prítomné nasledovné rozšírenia pre použitie kľúčov:

a) Digital Signature,

b) Non-Repudiation,

c) Key Encipherment.

(4) Podpisové kľúče PDS NCZI sú jediné kľúče určené na podpisovanie vydávaných certifikátov a CRL.

(5) V podpisovom certifikáte PDS NCZI musia byť prítomné nasledovné hodnoty „Key Certifikát Sign a CRL Sign“.

7.2 Ochrana súkromného kľúča a využívanie kryptografických hardvérových modulov (HSM)

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

7.2.1 Štandardné požiadavky na HSM

(1) PDS použitý kryptografický modul musí spĺňať požiadavky bezpečnosti na úrovni FIPS 140-2 Level 3.

(2) Modul musí byť uložený v bezpečných priestoroch bez prístupu neoprávnených osôb.

(3) HSM modul musí spĺňať ochranu pred odchytávaním elektromagnetického vyžarovania, podporovať funkciu self test, poskytovať funkciu key recovery.

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

7.2.2 Práca so súkromným kľúčom

Súkromný kľúč PDS musí byť generovaný a obnovovaný pod kontrolou viacerých osôb podľa princípu n z m, pričom minimálne je n=4 a m=7.

7.2.3 Obnova súkromných kľúčov z depozitu

Súkromný kľúč PDS nie je uložený v depozite u tretej osoby.

7.2.4 Zálohovanie súkromných kľúčov

(1) Súkromný kľúč PDS je zálohovaný pri vytváraní pravidelných záloh servera certifikačnej autority, nakoľko sa v zašifrovanej podobe nachádza na pevnom disku servera PDS s pripojeným HSM modulom.

(2) Obnova kľúča je možná len v jednom konkrétnom prostredí HSM (Security world) a s použitím príslušného počtu operátorských kariet (princíp n z m).

(3) Bezpečnostné opatrenia týkajúce sa zálohovania sú popísané v dokumente *„Základy administrácie HSM“*.

7.2.5 Archivácia súkromných kľúčov

Pozri kapitolu 7.2.4.

7.2.6 Prenos súkromného kľúča do alebo z kryptografického modulu HSM

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).

7.2.7 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.

7.2.8 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.

7.2.9 Spôsob deaktivácie súkromného kľúča

(1) Pri deaktivácii musí byť kľúč vymazaný z pamäte HSM modulu.

(2) Každý priestor na disku, v ktorom boli uložené kľúče musí byť prepísaný, pokiaľ sa uvoľní na použitie pre operačný systém.

(3) Kryptografický modul musí automaticky vypnúť súkromný kľúč po uplynutí prednastavenej doby nečinnosti.

7.2.10 Spôsob zničenia súkromného kľúča

(1) Po ukončení používania súkromného kľúča, všetky kópie súkromného kľúča v pamäti počítača a na zdieľanom diskovom priestore musia byť bezpečne zlikvidované jeho prepísaním.

(2) Spôsob prepísania musí byť schválený PMA.

7.2.11 Charakteristika HSM modulu

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

7.3 Ďalšie aspekty manažmentu kľúčového páru

7.3.1 Doba platnosti certifikátov a použiteľnosti kľúčového páru

(1) Doba platnosti certifikátov vydaných na kľúče s veľkosťou 2048 bit je maximálne 5 rokov.

(2) Kľúčový pár je použiteľný len po dobu platnosti naň vydaného certifikátu.

7.4 Aktivačné údaje

7.4.1 Generovanie aktivačných údajov a ich inštalácia

(1) Všetky aktivačné údaje musia byť jedinečné a nepredvídateľné.

(2) Aktivačné údaje, v spojení s niektorým iným overovaním prístupu, musia mať primeranú úroveň sily v závislosti na kľúčoch alebo údajoch, ktoré majú byť chránené.

(3) Tam, kde sa používajú heslá, musí mať subjekt možnosť zmeniť jeho heslo kedykoľvek.

7.4.2 Ochrana aktivačných údajov

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

(2) 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.

7.4.3 Ďalšie aspekty aktivačných údajov

Žiadne požiadavky.

7.5 Počítačové bezpečnostné opatrenia

7.5.1 Špecifické technické požiadavky z oblasti počítačovej bezpečnosti

(1) Každý server PDS musí umožňovať nasledovnú funkcionalitu:

a) riadenie prístupu k službám PDS a PKI rolám,

b) vynucovať zodpovedností pre PKI roly,

c) identifikáciu a autentizáciu PKI rolí a s nimi súvisiace identity,

d) použitie kryptografie pri komunikácii v rámci session a zabezpečenie databázy,

e) archiváciu histórie PDS a koncových používateľov a auditných údajov,

f) audit udalostí súvisiacich s bezpečnosťou,

g) dôveryhodnú cestu k identifikácii PKI rolí a súvisiacich identít,

h) mechanizmus obnovy kľúčov a systému PDS.

(2) Táto funkcia môže byť poskytovaná operačným systémom, alebo v kombinácii operačného systému, PKI PDS softvéru a fyzickej ochrany.

7.5.2 Hodnotenie počítačovej bezpečnosti

Žiadne požiadavky.

7.6 Životný cyklus riadenia bezpečnosti

7.6.1 Riadenie vývoja systému

(1) PDS musí používať softvér, ktorý bol navrhnutý a vyvinutý v zmysle formálnej metodiky a je podporovaný nástrojmi pre riadenie konfigurácie.

(2) PDS softvér musí mať overenie súladu procesov zhody od nezávislej tretej strany.

(3) PDS software musí byť získaný legálnym spôsobom z dôveryhodných zdrojov, musí byť počas celého životného cyklu podporovaný výrobcom.

7.6.2 Riadenie manažmentu bezpečnosti

(1) Na inštaláciu a následnú údržbu systému PDS musí byť použitá oficiálna metodika (návod) na manažment konfigurácií.

(2) Softvér PDS, pri spustení, musí poskytnúť možnosť pre PDS na overenie, že softvér:

a) pochádza od tvorcu softvéru (z dôveryhodného zdroja),

b) nedošlo k žiadnym zmenám pred samotnou inštaláciou,

c) nainštalovaná verzia softvéru je určená pre reálne použitie v produkčnom prostredí.

(3) PDS musí poskytnúť mechanizmus pre pravidelné overovanie integrity používaného softvéru. V intervaloch minimálne raz týždenne musí byť overovaná integrita systému PDS.

(4) PDS musí mať tiež mechanizmy a implementované pravidlá na riadenie a sledovanie konfigurácie systému PDS.

(5) PDS musí upozorniť na exspiráciu certifikátu, upozorniť na blížiaci sa koniec platnosti certifikátu spoliehajúcej sa strany.

(6) PDS musí poskytovať službu overovania stavu certifikátu (overenie CRL) pre spoliehajúce sa strany.

7.7 Riadenie sieťovej bezpečnosti

(1) Servery PDS musia byť chránené pred napadnutím z ľubovoľnej otvorenej (externej) alebo internej siete, do ktorej sú pripojené. Táto ochrana musí byť riešená prostredníctvom inštalácie zariadení, ktoré sú nakonfigurované tak, že budú prístupné len protokoly a príkazy potrebné pre prevádzku PDS. PDS musí zabezpečiť, aby definovala len tieto protokoly a príkazy potrebné pre prevádzku PDS.

(2) Pred nasadením softvéru do prevádzky PDS musia byť vykonané penetračné testovanie.

8 PROFILY CERTIFIKÁTOV A CRL

8.1 Profily certifikátov

8.1.1 Podporovaná verzia

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

8.1.2 Použite rozšírenia v certifikátoch

(1) Softvér PDS musí podporovať všetky základné X.509 definované položky:

Podpis (Certifikate Signature)	**Podpis PDS na autentifikáciu certifikátu**
Algoritmus podpisu (Certificate Signature Algorithm)	Použitý algoritmus podpisu
Vydavateľ (Issuer)	Meno PDS
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

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

8.1.3 Identifikácia kryptografických algoritmov

PDS a používatelia certifikátov musia podporovať na podpisovanie a overovanie nasledovné algoritmy:

a) RSA 2048 v súlade s PKCS#1

b) SHA-2 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].

8.1.4 Menná konvencia

Žiadne požiadavky.

8.1.5 Obmedzenia týkajúce sa mena

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

8.1.6 Aplikované OID certifikačného poriadku

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

8.1.7 Použitie rozšírenia „policy constraints“

Žiadne požiadavky.

8.1.8 Sémantika spracovanie kritických rozšírení CP

Kritické rozšírenia musia byť interpretované spôsobom definovaným v RFC 5280.

8.2 Profil CRL

8.2.1 Podporovaná verzia

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

8.2.2 CRL a CRL rozšírenia

Každý softvér používaný účastníkmi NZIS musí správne spracovať všetky rozšírenie CRL definované v RFC 5280.

8.3 OCSP profil

8.3.1 Používaná verzia

PDS poskytuje službu OCSP v súlade s RFC 2560.

8.3.2 Rozšírenia OCSP

Žiadne požiadavky.

9 AUDIT SÚLADU A INÉ POSUDZOVANIE

(1) Audit súladu určuje, či poskytovanie služieb PDS spĺňa štandardy stanovené v jeho interných smerniciach a spĺňa požiadavky tohto CP.

(2) Autorita zodpovedná za správu CP musí vymedziť špecifické požiadavky pre audit súladu. Tieto požiadavky budú zodpovedať všetkým zákonným a regulačným požiadavkám legislatívy Slovenskej republiky.

9.1 Frekvencia auditu alebo iného hodnotenia

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

9.2 Rozsah auditu a použité metódy

Audit PDS bude zameraný na splnenie požiadaviek zákona č. 272/2016 Z. z. o dôveryhodných službách pre elektronické transakcie na vnútornom trhu 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“.

9.3 Vzťah audítora a hodnoteného subjektu

Audítor musí byť nezávislý od PDS.

9.4 Možné opatrenia prijaté na základe výsledkov auditu

Výsledky auditu musia byť predložené PMA. Ak sa zistia nezrovnalosti, musí PDS predložiť správu PMA o nápravných opatreniach, ktoré budú prijaté na elimináciu nezrovnalostí uvedených v správe z auditu.

9.5 Výsledok auditu a jeho zverejnenie

PDS musí poskytnúť PMA kópiu výsledkov auditu zhody. Tieto úplné výsledky nebudú zverejnené, pokiaľ to nevyžaduje zákon.

10 BEZPEČNOSTNÁ KAPITOLA PDS

(1) Pre potreby PKI infraštruktúry NZIS bol vypracovaný tento dokument „Certifikačný poriadok poskytovateľa dôveryhodných služieb“.

(2) Organizácia bezpečnosti informácií sa riadi internými predpismi PDS.

(3) Infraštruktúra (jednotlivé komponenty) PDS predstavuje kritické prvky.

(4) Bezpečnosť ľudských zdrojov definuje role a základné zodpovednosti – iba vybraní zamestnanci majú umožnený prístup k infraštruktúre výroby a distribúcie certifikátov.

(5) Infraštruktúra PDS je chránená bezpečnostným parametrom pozostávajúceho z mechanických zábranných prostriedkov a technických zabezpečovacích prostriedkov, ktoré zabraňujú neautorizovanému prístupu.

(6) Riadenie prístupu k infraštruktúre PDS 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

(7) Vývojové a produkčné prostredia sú fyzicky oddelené.

(8) Na ochranu citlivých informačných aktív (kryptografický materiál) sú použité špeciálne kryptografické prostriedky (HSM moduly).

(9) Zálohovanie, archivácia a prenos súkromného kľúča PDS musí byť prostredníctvom HSM modulu.

(10) Infraštruktúra PDS 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 PDS sú nasadené technológie zabezpečujúce dostupnosť a synchronizáciu presného času.

(14) V rámci infraštruktúry PDS sú nasadené technológie zabezpečujúce online poskytovanie informácií o stave a platnosti certifikátov.

(15) V rámci infraštruktúry PDS sú nasadené technológie zabezpečujúce priradenie presného času k definovaným udalostiam.

(16) V rámci infraštruktúry PDS sú nasadené technológie zabezpečujúce vytváranie a zber auditných záznamov.

(17) V rámci infraštruktúry PDS sú nasadené technológie zabezpečujúce ochranu pred neautorizovanou inštaláciou softvéru.

11 OSTATNÉ OBCHODNÉ A LEGISLATÍVNE OTÁZKY

11.1 Poplatky

11.1.1 Poplatok za vydanie a obnovu certifikátu

PDS poskytuje svoje služby bezodplatne.

11.2 Finančná zodpovednosť

PDS 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.

11.3 Ochrana osobných údajov

11.3.1 Požiadavky na ochranu osobných údajov

PDS pri spracúvaní osobných údajov žiadateľov resp. držiteľov certifikátov dodržiava požiadavky platnej a účinnej legislatívy v oblasti ochrany osobných údajov (GDPR, Zákon o ochrane osobných údajov).

11.3.2 Informácie, ktoré nie sú považované za osobné

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

11.3.3 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).

11.3.4 Právny základ na spracúvanie osobných údajov

(1) PDS nemusí mať k dispozícii písomný súhlas žiadateľa/držiteľa certifikátu so spracovaním jeho osobných údajov v systéme PDS.

(2) Informácie o spracúvaní osobných údajov zo strany poskytovateľa sú dostupné na webovej stránke poskytovateľa, v sekcii Ochrana osobných údajov: https://www.nczisk.sk/O-nas/Ochrana-osobnych-udajov/Pages/default.aspx

11.3.5 Podmienky zverejnenia osobných údajov

(1) PDS nezverejní žiadne informácie týkajúce sa žiadateľa o certifikát alebo držiteľa certifikátu žiadnej tretej strane.

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

11.4 Právo duševného vlastníctva

(1) Na nakladanie so súkromným kľúčom je oprávnený výlučne oprávnený držiteľ súkromného kľúča.

(2) Tento CP je majetkom NCZI a jeho použitie je možné len pre potreby PDS a potreby spoliehajúcich sa strán v súlade s ustanoveniami uvedenými v tomto CP. Akékoľvek iné použitie tohto CP bez výslovného písomného súhlasu PDS je výslovne zakázané.

11.5 Vyhlásenia a záruky, zodpovednosť za škodu

11.5.1 Záruky PDS

(1) 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. PDS neposkytuje držiteľovi certifikátov žiadne záruky.

(2) Za škodu spôsobenú porušením povinností zodpovedá PDS podľa všeobecne záväzných platných právnych predpisov. PDS nezodpovedá za škodu, ktorá má povahu zmareného zisku.

11.6 Odmietnutie záruky

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

11.7 Obmedzenie zodpovednosti

(1) PDS nezodpovedá sa škody spôsobené držiteľom certifikátov, spoliehajúcim sa stranám, ani akýmkoľvek iným tretím stranám (ďalej spolu len „**tretie strany**“) v prípadoch, keď nedodržali ustanovenia tohto CP, zmluvy (ak je uzavretá), osobitných podmienok používania certifikátov alebo ustanovenia uvedené v iných dokumentoch, s ktorými boli oboznámené.

(2) PDS rovnako nezodpovedá za škodu, ktorá vznikla tretej strane z dôvodu:

a) porušenia povinností treťou stranou uvedených vo všeobecne záväzných právnych predpisov,

b) znemožnenia inštalovania alebo použitia certifikátov pre nekompatibilitu použitých hardvérových alebo softvérových prostriedkov v PZS,

c) spočívajúcom v technických vlastnostiach, parametroch a/alebo funkčnosti použitých hardvérových alebo softvérových prostriedkov tretej strany,

d) spoliehania sa na certifikát, ktorého platnosť skončila, alebo ktorý bol znefunkčnený,

e) uvedenia nesprávnych údajov pre PDS,

f) zneužitia certifikátu,

g) neposkytnutia potrebnej súčinnosti tretej strany,

h) neposkytnutia niektorej zo služieb PDS alebo jej nedostupnosti v priebehu plánovanej údržby alebo výpadku,

i) pôsobenia vyššej moci.

11.8 Zodpovednosť za škodu

Kto poruší svoju povinnosť alebo akýkoľvek záväzok, vyplývajúci z tohto CP, zmluvy (ak je uzavretá), osobitných podmienok používania certifikátov alebo uvedený v iných dokumentoch

PDS, s ktorými bol oboznámený, zodpovedá za škodu podľa všeobecne záväzných platných právnych predpisov.

11.9 Doba platnosti a jej ukončenie

11.9.1 Doba platnosti

CP zostáva v platnosti, pokiaľ nie je nahradený novšou verziou. Podrobnosti o histórii zmien tohto CP sú uvedené na začiatku dokumentu v časti „História revízií“. Účinnosť CP je obsiahnutá v príslušnej verzii CP.

11.9.2 Následky ukončenia platnosti

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

11.10 Notifikácia a komunikácia s držiteľmi

PDS 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.

11.11 Zmeny a prílohy CP

11.11.1 Postup zmeny dokumentácie

(1) PMA má právo posúdiť a prípadne revidovať tento CP. Chyby, požiadavky na aktualizáciu alebo navrhované zmeny tohto CP sa majú oznámiť kontaktu uvedenému v kapitole 2.5. Takáto komunikácia musí obsahovať popis zmeny, zdôvodnenie zmeny a kontaktné údaje osoby, ktorá zmenu požaduje.

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

(3) Za revíziu týchto dokumentov je zodpovedná Autorita pre správu CP (PMA) – pozri 2.3.1.

11.11.2 Notifikácia o zmene dokumentácie

Všetky zmeny CP motivované PMA majú byť dané na vedomie subjektom, ktorých sa týkajú. Elektronická verzia tohto CP musí byť dostupná na verejnej web stránke PDS.

11.11.3 Okolnosti za ktorých sa musí OID meniť

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.

11.12 Riešenie sporov

(1) Pre potreby interpretácie CP, iných dokumentov, podmienok PDS a/alebo zmluvy (ak je uzavretá) alebo riešenia sporov sa možno obrátiť na PMA. PMA rozhoduje s konečnou platnosťou v prípade akýchkoľvek sporov o interpretáciu.

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

(3) Ak je alebo sa stane niektoré ustanovenie tohto CP celkom alebo sčasti neplatným alebo nezákonným alebo neuplatniteľným, nemá táto skutočnosť vplyv na platnosť a uplatniteľnosť ostatných ustanovení CP. CP sa v takomto prípade vykladá tak, ako keby neplatné ustanovenia vôbec neobsahoval a PDS vykoná aktualizáciu CP a nahradí dotknuté ustanovenie novými ustanoveniami, ktoré v čo najväčšej miere zodpovedajú sledovanému účelu.

11.13 Uplatňované právne predpisy

Pri rozhodovaní v súdnych sporoch sa uplatňuje právo Slovenskej republiky.

11.14 Súlad s platnými zákonmi

Všetky zúčastnené strany sú povinné dodržiavať pri poskytovaní a využívaní služieb PDS požiadavky zákona č. 272/2016 Z. z. o dôveryhodných službách pre elektronické transakcie na vnútornom trhu, zákona č. 153/2013 Z. z. o národnom zdravotnom informačnom systéme a o zmene a doplnení niektorých zákonov v znení neskorších predpisov, ako aj ostatných všeobecne záväzných právnych predpisov.

11.15 Rôzne ustanovenia

11.15.1 Zmluva

Ak nie je v tomto CP uvedené alebo PDS neurčí inak, PDS vydáva certifikáty bez uzatvorenia osobitnej zmluvy.

11.15.2 Ostatné dojednania

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.

11.15.3 Postúpenie práv a povinností

Tretie strany nie sú oprávnené postúpiť akékoľvek práva a/alebo povinnosti vyplývajúce z tohto CP, zmluvy (ak je uzavretá), osobitných podmienok používania certifikátov alebo z iných dokumentov, s ktorými boli oboznámené, na iný subjekt bez predchádzajúceho písomného súhlasu PDS. Akýkoľvek súhlas PDS v zmysle predchádzajúcej vety je platný iba v prípade, ak naň bol udelený predchádzajúci písomný súhlas Ministerstva zdravotníctva Slovenskej republiky.

12 ZÁVEREČNÉ USTANOVENIA

(1) Tento CP PDS nahrádza CP PDS, reg. číslo: NCZI-00888-2024-4320-001, verzia 01.

(2) Tento CP PDS nadobúda platnosť dňom jej schválenia štatutárnym orgánom a účinnosť dňa 22.09.2025.

13 PRÍLOHY

Tento CP obsahuje 6 príloh:

Príloha č. 1: F-OS-404_01 CP PDS Prezenčná listina školenie – vzor
Príloha č. 2: F-OS-404_02 CP PDS Prezenčná listina preškolenie – vzor
Príloha č. 3: F-OS-404_03 Kniha CP
Príloha č. 4: F-OS-404_04 Zoznam oprávnených osôb
Príloha č. 5: F-OS-404_05 Zoznam zodpovedných osôb
Príloha č. 6: F-OS-404_06 Matica prístupov