POLITIKA

poskytovania dôveryhodnej služby vyhotovovania a overovania certifikátov na eID

Vypracoval	**Disig, a.s.**
Dátum platnosti	**29. 11. 2022**
Verzia	**1.8**
Typ	**POLITIKA**

Obsah

1. Úvod

Tento dokument obsahuje politiku (ďalej len „CP“) spoločnosti Disig, a.s., zápis v Obchodnom registri OS BA I, odd. Sa, vložka č. 3794/B, so sídlom Záhradnícka 151, 821 08 Bratislava, IČO: 35975946 ako poskytovateľa dôveryhodných služieb a kvalifikovaného poskytovateľa dôveryhodných služieb (ďalej len „Poskytovateľ“) vydávania a overovania certifikátov na elektronický občiansky preukaz (eID) resp. elektronický doklad o pobyte (eDoPP) (spolu ďalej len „eID“).

Pokiaľ sú v tomto dokumente uvádzané práva a povinnosti Poskytovateľa, tak právnym subjektom zodpovedným za ich vynucovanie resp. plnenie je spoločnosť Poskytovateľ.

1.1 Prehľad

Štruktúra tejto CP je plne v súlade s požiadavkami RFC 3647 „Internet X.509 Public Key Infrastructure Certificate Policy and Certification Practices Framework“.

Táto CP sa týka poskytovania dôveryhodných a kvalifikovaných dôveryhodných služieb vydávania a overovania týchto typov certifikátov na eID:

- kvalifikovaný certifikát pre elektronický podpis (ďalej len „KC“),
- certifikát pre elektronický podpis (ďalej len „certifikát na podpisovanie“),
- certifikát na šifrovanie.

Kvalifikovaná dôveryhodná služba vyhotovovania a overovania kvalifikovaného certifikátu pre elektronický podpis je poskytovaná týmito certifikačnými autoritami Poskytovateľa:

Názov	**Sériové číslo certifikátu**	**Vydavateľ**	**DigitalID v SK dôveryhodnom zozname**
SVK eID ACA	06DA	**KCA NBU SR 3**	**TLISK-09**
SVK eID ACA2	008e44f2a79a6aabf7	**self-signed**	**TLISK-126**

Dôveryhodná služba vyhotovovania a overovania certifikátu pre podpisovanie je poskytovaná touto certifikačnou autoritou Poskytovateľa:

Názov	**Sériové číslo certifikátu**	**Vydavateľ**	**Sériové číslo vydávajúcej SVK eID Root CA**
SVK eID PCA	01B41BF2206301122014	**SVK eID Root CA**	00DDBC6FEC11ECCB5A

Dôveryhodná služba vyhotovovania a overovania certifikátu pre šifrovanie je poskytovaná touto certifikačnou autoritou Poskytovateľa:

Názov	**Sériové číslo certifikátu**	**Vydavateľ**	**Sériové číslo vydávajúcej SVK eID Root CA**
SVK eID SCA	0173E1CADD8E01122015	**SVK eID Root CA**	00DDBC6FEC11ECCB5A

Všetky certifikáty sú vydávané v zmysle požiadaviek Nariadenia Európskeho parlamentu a Rady (EÚ) č. 910/2014 z 23. júla 2014 o elektronickej identifikácii a dôveryhodných službách pre elektronické transakcie na vnútornom trhu a o zrušení smernice 1999/93/ES (ďalej len „Nariadenie eIDAS“) [1], v zmysle požiadaviek zákona č. 272/2016 Z. z. o dôveryhodných službách pre elektronické transakcie na vnútornom trhu a o zmene a doplnení niektorých zákonov (zákon o dôveryhodných službách) (ďalej len „Zákon č. 272/2016 Z. z.“) [2] a zohľadnení ustanovení kapitoly 10 aktuálnej verzie dokumentu „Certifikačná politika pre koreňovú CA a dôveryhodnú službu vyhotovovania kvalifikovaných certifikátov, ktorej kvalifikovaný štatút udelil Národný bezpečnostný úrad“ (OID politiky: 1.3.158.36061701.0.0.0.1.2.2) [3].

Kvalifikovaný certifikát musí byť vydávaný Poskytovateľom, ktorý spĺňa požiadavky na kvalifikovaného poskytovateľa dôveryhodnej služby vyhotovovania a overovania kvalifikovaných certifikátov pre elektronický podpis v zmysle Nariadenia eIDAS.

Certifikát na šifrovanie a certifikát pre elektronický podpis musia byť vydávané Poskytovateľom, ktorý spĺňa požiadavky na poskytovateľa dôveryhodných služieb v zmysle Nariadenia eIDAS.

Ak sa v CP používa pojem CERTIFIKÁT alebo CERTIFIKÁTY (písané s veľkými písmenami) myslia sa tým všetky tri vydávané certifikáty – kvalifikovaný, certifikát na šifrovanie a certifikát na podpisovanie.

CP je využívaná pri implementácii infraštruktúry verejných kľúčov (ďalej len „PKI“), ktorá pozostáva z produktov a služieb, ktoré poskytujú a spravujú certifikáty podľa štandardu X.509 (Internet X.509 Public Key Infrastructure – Infraštruktúra verejných kľúčov).

1.2 Názov dokumentu a jeho identifikácia

Názov:	**POLITIKA poskytovania dôveryhodnej služby vyhotovovania a overovania certifikátov na eID**
Skratka názvu:	**CP SVK eID**
Verzia:	**1.8**
Schválené dňa:	**22. 11. 2022**
Platnosť od:	**29. 11. 2022**
Tomuto CP je priradený identifikátor objektu (OID):	**1.3.158.35975946.0.0.1.1.9**

Popis použitého identifikátora objektu (OID):

1. – ISO assigned OIDs

1.**3**. – ISO Identified Organization

1.3.**158**. – Identifikačné číslo subjektu (IČO)

1.3.158.**35975946**. – Disig

1.3.158.35975946.0.0.**1.** – vyhradené pre Disig (kvalifikované dôveryhodné služby)

1.3.158.35975946.0.0.1.**1.** – vyhradené pre Disig (dôveryhodné služby)

1.3.158.35975946.0.0.1.1.**9.** – CP SVK eID

Táto politika sa týka všetkých CERTIFIKÁTOV vydávaných na elektronickú identifikačnú kartu.

1.3 Účastníci PKI

1.3.1 Poskytovateľ

Poskytovateľ vydávajúci certifikáty v súlad s touto CP:

- je entita, ktorá poskytuje kvalifikované dôveryhodné služby vyhotovovania a overovania KC pre elektronický podpis používateľom (Zákazníci/Držitelia, Spoliehajúce sa strany),
- je entita, ktorá poskytuje dôveryhodné služby vyhotovovania certifikátov na podpisovanie a na šifrovanie používateľom (Zákazníci/Držitelia, Spoliehajúce sa strany),
- je uvádzaná vo vydanom KC resp. podpisovom certifikáte resp. certifikáte na šifrovanie ako vydavateľ certifikátu a jej súkromný kľúč je používaný na podpisovanie tohto certifikátu,
- musí poskytovať informáciu o stave CERTIFIKÁTOV prostredníctvom zoznamu zrušených certifikátov (CRL) a prípadne prostredníctvom služby na overovanie existencie a platnosti certifikátu (OCSP),
- musí mať pripravené, implementované a prevádzkované postupy pri poskytovaní kvalifikovaných dôveryhodných služieb a dôveryhodných služieb tak, aby boli adekvátne dosiahnuté požiadavky tejto politiky.

Konkrétne praktiky a postupy Poskytovateľa, ktorými sa vykonávajú požiadavky tejto CP musia byť stanovené v pravidlách poskytovania dôveryhodnej služby vyhotovovania a overovania certifikátov (CPS) alebo v iných verejne dostupných dokumentoch.

1.3.2 Registračná autorita

Registračná autorita (ďalej len „RA“) je entita, ktorá koná, na základe zmluvy, v mene Poskytovateľa, pričom vykonáva vybrané činnosti a sprostredkúva ich poskytovanie Zákazníkom/Držiteľom CERTIFIKÁTOV.

RA musí vykonávať svoje aktivity v súlade s CP a CPS v aktuálnom znení.

1.3.3 Koncové entity

1.3.3.1 Držiteľ

Držiteľ je držiteľ CERTIFIKÁTOV vydaných v zmysle tejto CP, uložených na eID, ktorého meno a priezvisko sa objaví v tele CERTIFIKÁTU. Držiteľom CERTIFIKÁTOV je občan Slovenskej republiky s trvalým pobytom v Slovenskej republike alebo s trvalým pobytom v zahraničí resp. cudzí štátny príslušník s trvalým pobytom v Slovenskej republike.

1.3.3.2 Zákazník

Zákazník je osoba, ktorej Poskytovateľ poskytuje Dôveryhodné služby a ktorá tieto služby uhrádza.

1.3.4 Spoliehajúce sa strany

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

1.3.5 Iní účastníci

Autorita pre správu politík (Policy Management Authority - ďalej len „PMA“) je zložka Poskytovateľa ustanovená za účelom:

- dohľadu na vytváranie a aktualizáciu politík a pravidiel Poskytovateľa, vrátane vyhodnocovania zmien a plánov na implementovanie ľubovoľných prijatých zmien,
- revízie politík a pravidiel poskytovania dôveryhodných služieb, aby sa zaručilo, že prax Poskytovateľa vyhovuje ustanoveniam príslušnému dokumentu (politika resp. pravidlá),
- revízie výsledkov auditov, aby sa určilo, či Poskytovateľ adekvátne dodržiava ustanovenia schválenej CP a CPS,
- vydávania odporúčaní pre Poskytovateľa ohľadom nápravných opatrení a iných vhodných opatrení,
- riadenia a usmerňovania činnosti vydávajúcej autority a registračných autorít,
- výkladu ustanovení CP a CPS a svojich pokynov pre RA a Poskytovateľa
- zverejňovanie aktuálnych dokumentov týkajúcich sa poskytovaných dôveryhodných služieb prostredníctvom k tomu určených repozitárov

Členov PMA menuje výkonný riaditeľ Poskytovateľa. Zložka PMA predstavuje vrcholovú zložku, ktorá rozhoduje s konečnou platnosťou vo všetkých záležitostiach a aspektoch týkajúcich sa Poskytovateľa a jeho činnosti a v plnej miere zodpovedá za to, že všetky aspekty CP a CPS sú správne a vhodne implementované.

O všetkých zásadných zmenách musí existovať záznam, ktorý preukáže ich formálne schválenie zo strany PMA.

1.4 Použiteľnosť CERTIFIKÁTOV na eID

1.4.1 Kvalifikovaný certifikát pre elektronický podpis

Kvalifikovaný certifikát pre elektronický podpis je certifikát fyzickej osoby definovaný v článku 3 bod 15 Nariadenia eIDAS a je vydávaný za účelom podpory kvalifikovaného elektronického podpisu v zmysle článku 3 bod 12 Nariadenia eIDAS pri komunikácii v rámci štátom poskytovaných služieb eGovernmentu, ako aj pri právnych úkonoch vykonávaným voči akýmkoľvek tretím osobám. V prípade, že sa v kvalifikovanom certifikáte neuvádza skutočnosť, že údaje na vyhotovenie elektronického podpisu súvisiace s údajmi na validáciu elektronického podpisu nachádzajú v kvalifikovanom zariadení na vyhotovenie elektronického podpisu, tak výsledkom použitia údajov na vyhotovenie elektronického podpisu je zdokonalený elektronický podpis v zmysle článku 3 bod 11 Nariadenia eIDAS.

1.4.2 Certifikát na šifrovanie

Certifikát na šifrovanie je určený na šifrovanie údajov pre jeho Držiteľa v rámci štátom poskytovaných služieb eGovernmentu.

1.4.3 Certifikát ma podpisovanie (autorizáciu)

Certifikát na podpisovanie je certifikát pre elektronický podpis definovaný v článku 3 bod 14 Nariadenia eIDAS a je vydávaný za účelom podpory zdokonaleného elektronického podpisu v zmysle článkov 26 a 27 nariadenia eIDAS pri komunikácii v rámci štátom poskytovaných služieb eGovernmentu.

1.5 Správa politiky

1.5.1 Organizácia zodpovedná za správu dokumentu

V tabuľke sú uvedené kontaktné údaje Poskytovateľa ktorý je zodpovedný za prípravu, vytvorenie a udržiavanie tohto dokumentu:

Poskytovateľ	
Spoločnosť:	**Disig, a.s.**
Adresa:	**Záhradnícka 151, 821 08 Bratislava 2**
IČO:	**359 75 946**
telefón	**+421 2 20850140**
e-mail:	**disig@disig.sk**
Webové sídlo:	https://www.disig.sk

1.5.2 Kontaktná osoba

Na účel tvorby politík má Poskytovateľ vytvorenú autoritu pre správu politík (PMA) (pozri kapitola 1.3.5), ktorá plne zodpovedá za jej obsah, a ktorá je pripravená odpovedať na všetky otázky týkajúce sa politík Poskytovateľa.

V tabuľke sú uvedené kontaktné údaje na zložku zodpovednú za prevádzku certifikačných autorít Poskytovateľa.

Certifikačná autorita: **SVK eID ACA, SVK eID ACA2, SVK eID Root CA, SVK eID PCA, SVKeID SCA**	
adresa:	**Záhradnícka 151, 821 08 Bratislava 2**
e-mail:	**spravaca@disig.sk**
telefón	**+421 2 20850140**
webové sídlo:	**https://eidas.disig.sk**

1.6 Použité skratky a pojmy

1.6.1 Skratky

BOK	-	Bezpečnostný osobný kód
CP	-	Politika poskytovania dôveryhodnej služby (Certification Policy)
CPS	-	Pravidlá poskytovania dôveryhodnej služby (Certificate Practice Statement)
CRL	-	Zoznam zrušených certifikátov (Certificate Revocation List)
eID	-	Elektronická identifikačná karta
HSM	-	Bezpečné zariadenie na vyhotovenie a uchovávanie elektronického podpisu; kryptografický modul, hardvérový bezpečnostný modul (Hardware Security Modul)
HW	-	Hardvér (Hardware)
KC	-	Kvalifikovaný certifikát pre elektronický podpis
NBÚ	-	Národný bezpečnostný úrad
OCSP	-	Protokol určený Spoliehajúcim sa stranám na potvrdenie existencie a platnosti certifikátu (OCSP – Online Certificate Status Protocol)
KEP PIN	-	Osobné identifikační číslo (Personal Identification Number), ktoré chráni prístup k súkromnému kľúču prostredníctvom, ktorého sa vyhotovuje kvalifikovaný elektronický podpis

PKCS	-	Séria štandardov určená pre kryptografiu verejných kľúčov (Public Key Cryptography Standard)
PKI	-	Infraštruktúra verejných kľúčov (Public Key Infrastructure)
PMA	-	Autorita na správu CP (Policy Management Authority)
KEP PUK	-	Kľúč na odblokovanie KEP PIN (PIN Unlock Key)
RA	-	Registračná autorita (Registration Authority)
RFC	-	Žiadosť o vyjadrenie (Request For Comment)
QSCD	-	Kvalifikované zariadenie na vyhotovenie elektronického podpisu
URL	-	Internetový ekvivalent pre web adresu (Uniform Resource Locator)
Z. z.	-	Zbierka zákonov Slovenskej republiky

1.6.2 Pojmy

Dôveryhodná služba - elektronická služba, ktorá sa spravidla poskytuje za odplatu a spočíva vo vyhotovovaní a overovaní Certifikátov;

Kvalifikovaný poskytovateľ dôveryhodných služieb - je poskytovateľ dôveryhodných služieb, ktorý poskytuje jednu alebo viacero kvalifikovaných dôveryhodných služieb a ktorému orgán dohľadu udelil kvalifikovaný štatút;

Certifikát – elektronický dokument, ktorým vydavateľ certifikátu (certifikačná autorita) potvrdzuje, že v certifikáte uvedený verejný kľúč patrí osobe, ktorej je certifikát vydaný;

Dokumentácia - je tvorená akýmkoľvek dokumentom v elektronickej alebo papierovej forme, ktorý obsahujú informáciu:

(i) na základe ktorej bol vydaný Certifikát, vrátane dokumentov, ktoré potvrdzujú identitu alebo špecifické atribúty fyzickej alebo právnickej osoby, ktorej sa Certifikát vydáva (najmä, nie však výlučne: žiadosti o vydanie Certifikátu, akékoľvek zmluvy týkajúce sa vydania a používania Certifikátu, plnomocenstvá, poverenia, výpisy z obchodného registra resp. iných verejných registrov, súhlasy s vydaním Certifikátu alebo iné dokumenty potvrdzujúce, že Držiteľ certifikátu je oprávnený konať za/v mene inej osoby, vykonávať určitú funkciu alebo činnosť, atď.),

(ii) týkajúcu sa vydania alebo zrušenia Certifikátu (najmä, nie však výlučne: potvrdenie o vydaní Certifikátu, žiadosť o zrušenie Certifikátu a pod.);

Držiteľ – entita identifikovaná v certifikáte ako Držiteľ súkromného kľúča prislúchajúceho k verejnému kľúču obsiahnutému v certifikáte;

Vlastník eID – fyzická osoba, ktorá vlastní eID;

Elektronický podpis – informácia v elektronickej forme, ktorá je pripojená alebo logicky inak spojená s elektronickým dokumentom, ktorá slúži ako metóda autentizácie tohto dokumentu;

Hashovacia funkcia (hash, message digest, fingerprint) – rýchlo spočítateľná funkcia, ktorá dostane na vstupe dokument ľubovoľnej dĺžky a zostrojí z neho pomerne krátku (napr. 256 bitov) charakteristiku, nazývanú hashovacia hodnota (tiež hašovacia hodnota, hash). Medzi v kryptografii najpoužívanejšie hašovacie funkcie v súčasnosti patria SHA1 a SHA2 (SHA224, SHA256, SHA384; SHA512);

Kvalifikovaný certifikát pre elektronický podpis – je certifikát pre elektronický podpis, ktorý vydáva kvalifikovaný poskytovateľ dôveryhodných služieb a ktorý spĺňa požiadavky stanovené v prílohe I Nariadenia eIDAS;

Poskytovateľ - súhrnné označenie pre spoločnosť Disig, a.s. poskytujúcu vybrané kvalifikované Dôveryhodné služby a Dôveryhodné služby;

Registračná autorita – Zákazník reprezentovaný jednotnými pracoviskami Ministerstva vnútra SR;

Spoliehajúca sa strana – entita, ktorá sa pri svojom konaní spolieha na Dôveryhodné služby Poskytovateľa;

Pravidlá na výkon certifikačných činností – postupy, ktoré Poskytovateľ používa pri vydávaní certifikátov;

RFC - Postup vytvárania štandardu na Internete a zároveň označenie takto vzniknutého štandardu;

Kvalifikované zariadenie na vyhotovenie elektronického podpisu (QSCD) - zariadenie na vyhotovenie elektronického podpisu, ktoré spĺňa požiadavky stanovené v prílohe II Nariadenia eIDAS;

Vlastná CA – časť infraštruktúry poskytovateľa dôveryhodných služieb (obsahujúca napr. HSM modul), ktorá spolu s registračnou autoritou vydáva certifikáty;

Kvalifikovaný elektronický podpis - je zdokonalený elektronický podpis vyhotovený s použitím kvalifikovaného zariadenia na vyhotovenie elektronického podpisu a založený na kvalifikovanom certifikáte pre elektronické podpisy;

Zdokonalený elektronický podpis – je elektronický podpis, ktorý spĺňa požiadavky stanovené v článku 26 Nariadenia eIDAS;

Zákazník – Ministerstvo vnútra Slovenskej republiky;

X.509 – medzinárodný štandard, ktorý okrem iného definuje aj formát certifikátu verejného kľúča;

2. Zverejňovanie informácií a úložiská

Poskytovateľ musí zverejňovať informácie o vlastných postupoch a procedúrach, vlastných certifikátoch a stave týchto certifikátov.

Poskytovateľ musí zverejňovať, v on-line režime, úložisko, ktoré je prístupné Zákazníkom, Držiteľom CERTIFIKÁTOV a Spoliehajúcim sa stranám, ktoré bude obsahovať minimálne tieto informácie:

- aktuálne CRL ako aj všetky CRL vydané od začiatku činnosti vydávania CERTIFIKÁTOV,
- vlastné certifikáty vydávajúcich certifikačných autorít Poskytovateľa, ktoré patria k jej verejným kľúčom, ktorých zodpovedajúcim súkromným kľúčom sú podpisované vydané KC a CRL

Zverejňovanie informácií musí zabezpečiť, že dostupné informácie budú aktuálne.

2.1.1 Frekvencia zverejňovania informácií

Zverejňované informácie, ktoré majú byť uložené v adresároch, musia byť publikované čo najskôr po ich vytvorení.

CRL sa publikuje, tak ako je špecifikované v ods. 4.9.7.

2.1.2 Kontroly prístupu

Poskytovateľ musí chrániť akúkoľvek informáciu uloženú v repozitári, ktorá nie je určená na verejné rozšírenie.

Poskytovateľ musí vynaložiť maximálne úsilie na to, aby zaistil integritu, dôvernosť a dostupnosť dát vyplývajúcich s poskytovania kvalifikovaných dôveryhodných služieb a dôveryhodných služieb. Taktiež musia byť vykonané logické a bezpečnostné opatrenia, aby zabránili neautorizovanému prístupu osobám, ktoré by mohli akýmkoľvek spôsobom zmeniť, poškodiť, pridať resp. vymazať údaje uložené v adresároch.

2.1.3 Adresáre

Adresáre musia byť lokalizované tak, aby boli prístupné Držiteľom CERTIFIKÁTOV a Spoliehajúcim sa stranám v súlade s celkovými bezpečnostnými požiadavkami.

3. Identifikácia a autentizácia

3.1 Prvotná registrácia

Žiadosť o vydanie KC musí vyhovovať štandardu PKCS #10.

3.1.1 Typy mien

CA musí vydávať CERTIFIKÁTY, ktoré obsahujú rozlišovacie mená v zmysle X.500 (X.500 Distinguished Name, ďalej ako „rozlišovacie meno“). Požiadavky na rozlišovacie mená sú uvedené nižšie.

3.1.2 Potreba zmysluplnosti mien

Pojem „zmysluplnosť“ znamená, že forma mena má bežne používaný tvar na určenie identity osoby.

Používané mená majú spoľahlivo identifikovať osoby, ktorým sú priradené. Dôraz sa pritom kladie na položku commonName (CN) resp. položky givenName (G) a Surname (SN), ktoré majú jednoznačne reprezentovať Držiteľa CERTIFIKÁTU spôsobom, ktorý je pre človeka ľahko pochopiteľný t. j. právoplatné meno a priezvisko v totožnej podobe, aká je uvedená v eID na ktorý sa CERTIFIKÁTY vydávajú.

CA má právo odmietnuť vydať CERTIFIKÁT, ktorý by obsahoval údaje porušujúce princíp zmysluplnosti mien, zvláštny dôraz sa pritom kladie na údaj v položkách commonName, givenName a Surname.

3.1.3 Jednoznačnosť mien

Poskytovateľ zodpovedá za jednoznačnosť mien v rámci celej komunity držiteľov CERTIFIKÁTOV.

3.1.4 Preukazovanie vlastníctva súkromného kľúča

Všetky žiadosti o CERTIFIKÁT musia byť vo formáte PKCS#10, čo znamená, že žiadosť o CERTIFIKÁT bude podpísaná s využitím súkromného kľúča patriaceho k verejnému kľúču nachádzajúcemu sa v danej žiadosti o CERTIFIKÁT.

Kľúčový pár, na ktorý sa má vydať CERTIFIKÁT sa musí generovať priamo v eID.

Žiadna zložka Poskytovateľa v nijakom prípade nesmie archivovať žiadne súkromné kľúče patriace Držiteľovi CERTIFIKÁTU, ktorý vydala.

3.1.5 Autentizácia identity fyzickej osoby

Poskytovateľ musí garantovať, že identita Držiteľa CERTIFIKÁTU a jeho verejný kľúč sú zodpovedajúco previazané.

Poskytovateľ špecifikuje vo vydanom CPS procedúry na autentizáciu identity Zákazníka/Držiteľa CERTIFIKÁTU. Dokumentácia o identifikácii musí minimálne obsahovať:

- Spôsob vykonania identifikácie,
- jednoznačnú identifikáciu osobných dokladov dokladujúcich identitu autentizovanej osoby,
- dátum vykonania identifikácie.

Fyzickou osobou, držiteľom CERTIFIKÁTU, môže byť len vlastník eID, na ktorý sa CERTIFIKÁTY vydávajú.

3.1.6 Predkladané doklady

Jediný doklad, ktorý sa vyžaduje pri vydaní CERTIFIKÁTOV je samotné eID, ktorý musí mať aktivovaný elektronický čip s údajmi o držiteľovi eID.

3.2 Vydanie následného CERTIFIKÁTU

Vydanie následného CETRIFIKÁTU znamená zmenu páru kľúčov – musí sa vytvoriť nový CERTIFIKÁT, ktorý môže mať zhodné rozlišovacie meno ako starý CERTIFIKÁT, ale nový CERTIFIKÁT musí mať odlišný verejný kľúč (zodpovedajúci novému, odlišnému súkromné kľúču), odlišné sériové číslo CERTIFIKÁTU (Serial Number) a môže mať zmenenú dĺžku platnosti.

3.3 Vydanie následného CERTIFIKÁTU po zrušení predchádzajúceho

Pre vydanie následného certifikátu po zrušení predchádzajúceho platia pravidlá stanovené v časti 3.2.

3.4 Žiadosť o zrušenie KC

Žiadosť o zrušenie CERTIFIKÁTU musí byť autentizovaná, pozri kapitola 4.9.

4. Požiadavky na životný cyklus certifikátu

4.1 Žiadosť o vydanie CERTIFIKÁTU

Účelom CP v tejto oblasti je:

- identifikovať minimálne požiadavky a procedúry, ktoré sú nevyhnutné na podporu dôvery v CERTIFIKÁT,
- minimalizovať špecifické požiadavky implementácie na CA, Zákazníkov/Držiteľov CERTIFIKÁTOV a Spoliehajúce sa strany.

Keď Zákazník požiada o vydanie CERTIFIKÁTU, musia byť vykonané nasledovné kroky:

- overenie identity fyzickej osoby, vlastníka eID (podľa ods. 3.1),
- zabezpečenie, že verejný kľúč tvorí pár kľúčov so súkromným kľúčom vlastneným Zákazníkom/Držiteľom o CERTIFIKÁT (podľa časti 3.1.4).

Komunikácia medzi jednotlivými systémami Poskytovateľa týkajúca sa elektronickej žiadosti o CERTIFIKÁT a procesu vydania CERTIFIKÁTU musí byť autentizovaná a chránená pred modifikáciou pomocou mechanizmov primeraných požiadavkám údajov. Ľubovoľný elektronický prenos spoločne delených tajomstiev musí byť uskutočnený šifrovane.

4.1.1 Kto môže žiadať o vydanie CERTIFIKÁTU

Poskytovateľa môže požiadať o vydanie CERTIFIKÁTU len fyzická osoba, ktorá je vlastníkom eID a predmetný eID má aktivovaný elektronický čip t. j. zvolený BOK.

4.1.2 Registračný proces a zodpovednosti

4.1.2.1 Príprava

Fyzická osoba, ktorý má záujem o vydanie CERIFIKÁTOV na eID ho musí mať k dispozícii počítač s nainštalovaným softvérom k eID karte (Aplikácia pre eID) a musí byť pripojený do siete internet.

Pred prvým vydaním CERTIFIKÁTOV sa musí oboznámiť s návodmi na ich získanie a musí si pripraviť potrebné hodnoty pre ochranné prvky (napr. KEP PIN a KEP PUK) pre ochranu kľúčov určených na vyhotovovanie kvalifikovaného/zdokonaleného elektronického podpisu.

4.1.2.2 Postup pre vydaním CERTIFIKÁTU

Pred vydaním certifikátu sa musí fyzická osoba oboznámiť so Všeobecnými podmienkach poskytovania a používania dôveryhodnej služby vydávania a overovania certifikátov na eID [4] (ďalej len „Všeobecné podmienky“), ktoré sú dostupné na webovom sídle https://www.slovensko.sk/sk/obciansky-preukaz-s-cipom/_obciansky-preukaz-s-cipom1.

4.1.3 Generovanie žiadosti

Všetky kryptografické kľúče pre vydávané CERTIFIKÁTY musia byť generované priamo v eID jeho vlastníka a z vygenerovaných kľúčov musí byť vytvorená elektronická žiadosť vo formáte PKCS#10.

4.2 Spracovanie žiadosti o vydanie CERTIFIKÁTU

Po vykonaní autentifikácie a identifikácie Držiteľa CERTIFIKÁTOV musí byť vykonané odoslanie žiadosti o CERTIFIKÁT do systému Poskytovateľa.

Komunikácia pracovnej stanice Zákazníka s Poskytovateľom musí prebehnúť cez zabezpečený kanál a musí byť umožnená len autentifikovaným Zákazníkom.

4.3 Vydania CERTIFIKÁTOV

Po odoslaní žiadosti na vydanie CERTIFIKÁTU do systému Poskytovateľa musí tento vykonať overenie prijatej žiadosti za účelom overenia, či:

- zodpovedá štandardu PKCS#10.

V prípade splnenia všetkých požiadaviek na vydanie CERTIFIKÁTU, musí Poskytovateľ CERTIFIKÁT vydať.

4.4 Prevzatie CERTIFIKÁTU

4.4.1 Spôsob prevzatia CERTIFIKÁTU

Poskytovateľ vydáva CERTIFIKÁTY na eID v režime on-line, tzn. žiadateľ si môže prevziať vydané CERTIFIKÁTY spolu s eID v rámci procedúry ich vydávania.

Pri prevzatí CERTIFIKÁTOV musí elektronicky podpísať potvrdenie o prevzatí certifikátov na eID. Pokiaľ nedôjde zo strany držiteľa k podpísaniu potvrdenia okamžite po vydaní resp. pri opakovaných pokusoch, tak je Poskytovateľ oprávnený predmetné certifikáty, ktorých vydania sa potvrdenie týka, v primeranej dobe zrušiť.

4.4.2 Zverejnenie CERIFIKÁTU

Kvalifikovaný certifikát pre elektronický podpis vydávaný na eID obsahuje citlivé osobné údaje Držiteľa a z dôvodu ochrany osobných údajov nesmie byť zverejňovaný.

4.4.3 Oznámenie o vydaní CERTIFIKÁTU iným stranám

O vydaní kvalifikovaného certifikátu musí Poskytovateľ v zmysle požiadaviek §6 ods. 2 zákona č. 272/2016 Z. z. informovať Národný bezpečnostný úrad.

4.5 Kľúčový pár a používanie CERTIFIKÁTU

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

4.5.1 Používanie súkromného kľúča a CERTIFIKÁTU Držiteľom

Povinnosťou Držiteľa CERTIFIKÁTU vo vzťahu k súkromnému kľúču a CERTIFIKÁTU je:

- používať kľúčový pár v súlade s obmedzeniami, ktoré sú uvedené v tejto CP,
- neustále chrániť svoje súkromné kľúče v súlade s touto CP tak, aby boli výhradne pod jeho kontrolou,
- bezodkladne upovedomiť Poskytovateľa o podozrení, že:
  - jeho súkromný kľúč bol stratený, odcudzený alebo kompromitovaný,
  - stratil kontrolu nad súkromným kľúčom kompromitáciou jeho aktivačných údajov (BOK, KEP PIN, KEP PUK),
  - nepresnostiach alebo zmenách v obsahu CERTIFIKÁTU,
- bezodkladne požiadať o zrušenie CERTIFIKÁTU v prípade, že akýkoľvek údaj uvedený v subjekte CERTIFIKÁTU sa stal neplatným,
- dodržiavať všetky termíny, podmienky a obmedzenia uložené na používanie svojich súkromných kľúčov a CERTIFIKÁTOV napr. ukončiť používanie súkromného kľúča po exspirácii alebo zrušení CERTIFIKÁTU verejného kľúča,
- používať poskytnuté CERTIFIKÁTY len na príslušné účely,
- okamžite ukončiť používanie súkromného kľúča po jeho kompromitácii.

4.5.2 Používanie verejného kľúča a CERTIFIKÁTU Spoliehajúcou sa stranou

Spoliehajúce sa strany sú povinné:

- používať CERTIFIKÁT na účel, pre ktorý bol vydaný,
- predtým, ako sa na CERTIFIKÁT spoľahnú, overovať každý na platnosť t. j. overovať, že CERTIFIKÁT je v danom čase platný a že sa nenachádza na aktuálnom zozname zrušených CERTIFIKÁTOV vydanom Poskytovateľom,
- vytvoriť vzťah dôvery k CA, ktorá vydala daný CERTIFIKÁT, verifikovaním, že ide oprávneného poskytovateľa kvalifikovaných dôveryhodných služieb, ktorý je uvedená v dôveryhodnom zozname Slovenskej republiky (SK TLS),
- uchovávať originálne podpísané údaje, aplikácie potrebné na čítanie a spracovanie týchto údajov a kryptografické aplikácie potrebné na overovanie zdokonalených elektronických podpisov resp. kvalifikovaných elektronických podpisov týchto údajov, pokiaľ môže byť potrebné overovať podpis týchto údajov.

4.6 Obnova certifikátu

Poskytovateľ nesmie vydať CERTIFIKÁT na verejný kľúč, na ktorý už bol ním v minulosti CERTIFIKÁT vydaný.

4.7 Vydanie následného CERTIFIKÁTU

V tejto časti sú popísané podmienky vydania následného CERTIFIKÁTU vydaného Poskytovateľom. Pod pojmom následný CERTIFIKÁT sa myslí vydanie nového CERTIFIKÁTU rovnakého druhu a s rovnakým obsahom pre existujúceho Držiteľa, ktorého osobné údaje sú zavedené v systéme Poskytovateľa.

4.7.1 Podmienky vydania následného CERTIFIKÁTU

Následný CERTIFIKÁT je možné vydať v prípade, že

- došlo k ukončeniu platnosti predchádzajúceho (exspirácia) certifikátu
- bol tento zrušený z dôvodov, pre ktoré už nemohol byť používaný napr. neplatnosť údajov v CERTIFIKÁTE, kompromitácia súkromného kľúča
- sa držiteľ eID rozhodol vydať si nový certifikát prostredníctvom aplikácie pre eID a systém mu to umožnil.

4.7.2 Kto môže žiadať o vydanie následného CERTIFIKÁTU

O vydanie následného CERTIFIKÁTU môže požiadať existujúci Zákazník, ktorému bol Poskytovateľom v minulosti vydaný predchádzajúci CERTIFIKÁT.

4.7.3 Postup žiadania o vydanie následného KC

Následný CERTIFIKÁT musí byť vydaný rovnakým spôsobom ako bol vydávaný predchádzajúci CERTIFIKÁT.

4.7.4 Oznámenie o vydaní následného KC

Poskytovateľ musí vhodným spôsobom informovať Držiteľa o vydaní následného CERTIFIKÁTU.

4.7.5 Spôsob prevzatia následného KC

Pozri kapitola 4.4.1.

4.7.6 Zverejňovanie následného KC

Pozri kapitola 4.4.2.

4.7.7 Oznámenie o vydaní následného CERTIFIKÁTU iným subjektom

Pozri kapitola 4.4.3.

4.8 Modifikácia CERTIFIKÁTU

Vydanie nového CERTIFIKÁTU z dôvodu zmien týkajúcich sa jeho obsahu, bez zmeny kľúčového páru, Poskytovateľ nepodporuje.

4.9 Zrušenie CERTIFIKÁTU

4.9.1 Okolnosti zrušenia CERTIFIKÁTU

CERTIFIKÁT sa musí zrušiť, keď sa väzba medzi Držiteľom a jeho verejným kľúčom v certifikáte už nepovažuje za platnú. Poskytovateľ je zo zákona povinný zrušiť CERTIFIKÁT, ktorý spravuje, v týchto prípadoch:

- zistí, že pri vydaní CERTIFIKÁTU neboli splnené v čase vydania platné legislatívne požiadavky,
- zistí, že CERTIFIKÁT bol vydaný na základe nepravdivých údajov,
- o zrušenie CERTIFIKÁTU požiada Držiteľ, ktorého údaje sú v ňom uvedené,
- zrušenie CERTIFIKÁTU nariadi Poskytovateľovi svojím rozhodnutím súd,
- dozvie sa, že subjekt CERTIFIKÁTU zomrel,
- zistí, že došlo ku kompromitácii súkromného kľúča patriaceho k danému CERTIFIKÁTU, napr. ak súkromný kľúč patriaci k verejnému kľúču uvedenému v CERTIFIKÁTE pozná resp. má pod kontrolou iná osoba, než Držiteľ uvedený v CERTIFIKÁTE,
- dozvie sa, že údaje uvedené v CERTIFIKÁTE sa stali neaktuálnymi,
- Držiteľ porušil svoje povinnosti stanovené touto CP prípade Poskytovateľom,
- dozvie sa, že sa Držiteľ stal nesvojprávnym na základe rozhodnutia súdu,
- došlo ku kompromitácii súkromného kľúča Poskytovateľa,
- zistí, že kvalifikované zariadenie, v ktorom sú generované kľúče je zraniteľné takým spôsobom, že je možné, za splnenia podmienok umožňujúcich využitie danej zraniteľnosti, získať kópiu súkromného kľúča Držiteľa,
- bola ukončená certifikácia kvalifikovaného zariadenia pre elektronický podpis (QSCD), na ktorom bol kvalifikovaný certifikát uložený.

Vždy, keď sa Poskytovateľ dozvie o niektorej z uvedených okolností, daný CERTIFIKÁT sa musí zrušiť a zverejniť na zozname zrušených CERTIFIKÁTOV (CRL) resp. informácia o jeho zrušení môže byť dostupná prostredníctvom služby OCSP.

Zrušený CERTIFIKÁT nie je možné za žiadnych okolností obnoviť.

4.9.2 Kto môže žiadať o zrušenie CERTIFIKÁTU

Držiteľ CERTIFIKÁTU môže kedykoľvek požiadať spôsobom stanoveným v tejto CP o zrušenie svojich vlastných CERTIFIKÁTOV, a to aj bez udania dôvodu v žiadosti o zrušenie.

O zrušenie CERTIFIKÁTOV môže tiež požiadať:

- Poskytovateľ – pracovník oprávnený konať vo veci zrušenia v mene Poskytovateľa je povinný písomne zdokumentovať túto skutočnosť vrátane dôvodu svojho konania,

- súd prostredníctvom svojho rozsudku alebo predbežného opatrenia (k dokumentom o zrušení CERTIFIKÁTU musí Poskytovateľ priložiť kópiu príslušného súdneho rozhodnutia),
- subjekt (fyzická osoba) na základe dedičského konania (k dokumentom o zrušení CERTIFIKÁTU musí Poskytovateľ priložiť kópiu dokladov, z ktorých vyplýva právo daného subjektu žiadať o zrušenie CERTIFIKÁTU),
- súdom poverená osoba, napr. poručník subjektu CERTIFIKÁTU, ktorý sa má zrušiť (k dokumentom o zrušení CERTIFIKÁTU musí Poskytovateľ priložiť kópiu príslušného súdneho rozhodnutia),

4.9.3 Postup pri žiadosti o zrušenie CERTIFIKÁTU na eID

Žiadosť o zrušenie CERTIFIKÁTU na eID podáva oprávnená osoba (držiteľ eID) buď:

- osobne u Poskytovateľa (RA) na jednotnom pracovisku, kde pracovník RA musí overiť, že žiadateľ o zrušenie CERTIFIKÁTU na eID je oprávneným držiteľom daného eID,
- prostredníctvom verejne dostupnej elektronickej služby poskytovanej MV SR.

Pri strate eID, ktoré je nahlásené vydavateľovi eID (MV SR), sa vykoná automatické zrušenie všetkých CERTIFIKÁTOV nachádzajúcich sa na danom eID.

Poskytovateľ (RA) musí posúdiť oprávnenosť žiadosti o zrušenie CERTIFIKÁTU a v prípade, ak je jasné, že žiadateľ o zrušenie nie je oprávnenou osobou, Poskytovateľ musí danú žiadosť o zrušenie odmietnuť.

Ak žiadosť o zrušenie vyhovuje príslušným ustanoveniam tejto CP, bezodkladne sa vykoná zrušenie CERTIFIKÁTU, aby sa dostal na najbližšie CRL.

O zrušení CERTIFIKÁTU bude Držiteľ informovaný prostredníctvom vydaného CRL.

4.9.4 Čas na podanie žiadosti o zrušenie CERTIFIKÁTU

V prípade hrozby kompromitácie súkromného kľúča musí oprávnená osoba (pozri kapitola 4.9.2) podať žiadosť o zrušenie CERTIFIKÁTU čo najskôr. Osobne je možné žiadať o zrušenie len v pracovnej dobe určenej jednotlivými RA (MV SR).

4.9.5 Čas na zrušenie CERTIFIKÁTU

Poskytovateľ musí:

- zrušiť CERTIFIKÁT, čo najskôr od momentu prijatia platnej žiadosti o zrušenie a vyhodnotenia jej oprávnenosti, najneskôr však do 24 hodín od vyhodnotenia oprávnenosti žiadosti o zrušenie,
- zverejňovať aktuálny zoznam zrušených CERTIFIKÁTOV a všetky predchádzajúce zoznamy zrušených CERTIFIKÁTOV, tak aby boli prístupné Zákazníkovi/Držiteľom a všetkým Spoliehajúcim sa stranám,
- archivovať všetky CRL, ktoré vydal.

4.9.6 Overovanie platnosti zo strany Spoliehajúcej sa strany

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

Neoverenie platnosti CERTIFIKÁTU pomocou CRL je brané ako hrubé porušenie tejto CP.

4.9.7 Frekvencia vydávania CRL

Poskytovateľ musí vydávať a publikovať nove CRL pre všetky ním vydávané CERTIFIKÁTY na eID minimálne jeden krát za 24 hodín.

Poskytovateľ musí zverejňovať CRL prostredníctvom stanoveného adresára (URL), ktorý je uvedený v samotnom CERTIFIKÁTE

4.9.8 Doba publikovania CRL

Poskytovateľ musí zabezpečiť, aby čas od vydania CRL do jeho publikovania v úložisku nepresiahol 90 sekúnd.

4.9.9 Dostupnosť služby OCSP

URI adresy OSCP responderov jednotlivých vydávajúcich certifikačných autorít Poskytovateľa musia byť obsiahnuté v rozšírení certifikátu Authority Information Access. V zmysle Nariadenia eIDAS musí byť služba OCSP poskytovaná bezodplatne.

4.9.10 Požiadavky na on-line overenie platnosti certifikátu

Spoliehajúce sa strany, ktoré majú záujem využívať službu OCSP musia zaslať požiadavku na príslušný OCSP responder, ktorého URI je publikovaná v CERTIFIKÁTE, ktorého platnosť požadujú overiť. Zaslaná žiadosť musí byť v súlade s požiadavkami RFC 6960.

4.9.11 Iné formy dostupnosti informácií o zrušení CERTIFIKÁTU

Overenie aktuálneho stavu CERTIFIKÁTU je možné vykonať manuálne prostredníctvom:

- Zoznamov aktuálnych CRL ako aj archívu všetkých vydaných CRL pre certifikačné autority Poskytovateľa vydávajúce kvalifikované certifikáty, ktoré sú k dispozícii na adrese:

https://eidas.disig.sk/sk/kvalifikovane-certifikaty/crl/

- Zoznamov aktuálnych CRL ako aj archívu všetkých vydaných CRL pre certifikačné autority Poskytovateľa vydávajúce certifikáty, ktoré sú k dispozícii na adrese:

https://eidas.disig.sk/sk/certifikaty/crl/

4.9.12 Špeciálne požiadavky na zmenu kľúčov po ich kompromitácii

Žiadne ustanovenia.

4.9.13 Okolnosti pozastavenia platnosti CERTIFIKÁTU

Poskytovateľ pozastavenie platnosti CERTIFIKÁTU nepodporuje.

4.9.14 Kto môže žiadať o pozastavenie CERIFIKÁTU

Žiadne ustanovenia.

4.9.15 Postup pozastavenia CERTIFIKÁTU

Žiadne ustanovenia.

4.9.16 Obmedzenia počas pozastavenia CERTIFIKÁTU

Žiadne ustanovenia.

4.10 Služby súvisiace so stavom certifikátu

4.10.1 Prevádzkové požiadavky

Zoznam zrušených certifikátov musí byť dostupný na URL adrese uvedenej v kapitole 4.9.11 a musí byť prístupný prostredníctvom.

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

4.10.2 Ukončenie poskytovania služieb

V prípade, že sa Zákazník/Držiteľ rozhodne ukončiť zmluvný vzťah s Poskytovateľom pred uplynutím doby platnosti vydaného CERTIFIKÁTU musí zároveň požiadať o zrušenie CERTIFIKÁTU.

4.10.3 Úschova a obnova kľúčov

Poskytovateľ takúto službu neposkytuje.

5. Fyzické, procedurálne a personálne bezpečnostné opatrenia

Bezpečnosť Poskytovateľa musí byť založená na súhrne bezpečnostných opatrení v oblasti fyzickej a objektovej, procedurálnej a personálnej bezpečnosti. Tieto bezpečnostné opatrenia musia byť navrhnuté, dokumentované a aplikované na základe bezpečnostných pravidiel.

Poskytovateľ musí:

- niesť plnú zodpovednosť za súlad svojej činnosti s postupmi definovanými vo svojej bezpečnostnej politike, vrátane jej dodržiavania zo strany externých registračných autorít.
- definovať zodpovednosť externých registračných autorít a zaviazať ich dodržiavaním stanovených bezpečnostných opatrení,
- mať zoznam všetkých svojich aktív s vyznačením ich klasifikácie v zmysle vykonaného posúdenia rizika.

Bezpečnostná politika Poskytovateľa a súhrn aktív týkajúci sa bezpečnosti musia byť preskúmavané v pravidelných intervaloch, prípade pri významných zmenách na zaistenie ich kontinuity, vhodnosti, dostatočnosti a účinnosti.

Všetky zmeny, ktoré môžu ovplyvniť úroveň poskytovanej bezpečnosti musia byť schválené manažmentom Poskytovateľa.

Nastavenie systémov Poskytovateľa musí byť pravidelne preskúmavané na zmeny, ktoré ohrozujú bezpečnostnú politiku Poskytovateľa.

5.1 Opatrenia týkajúce sa fyzickej bezpečnosti

5.1.1 Priestory

Technologické priestory, v ktorých je umiestnená základná infraštruktúra Poskytovateľa musia byť v chránených priestoroch, ktoré sú prístupné len autorizovaným osobám a od ostatných priestorov sú oddelené prostredníctvom primeraných bezpečnostných prvkov (bezpečnostné dvere, mreže, pevné múry ap.). Vybavenie Poskytovateľa má pozostávať len z vybavenia vyhradeného na poskytovanie dôveryhodných služieb a kvalifikovaných dôveryhodných služieb a nemá slúžiť na žiadne účely, ktoré sa netýkajú týchto služieb.

5.1.2 Fyzický prístup

Mechanizmy riadenia prístupu do chránených priestorov Poskytovateľa t. j. do priestorov zóny s najvyššou bezpečnosťou musia byť zabezpečené tak, že tieto priestory musia byť chránené bezpečnostným alarmom a vstup do nich môže byť umožnený len osobám, ktoré vlastnia bezpečnostný token a sú uvedené na zozname oprávnených osôb na vstup do chránených priestorov Poskytovateľa. Vybavenie Poskytovateľa musí byť neprestajne chránené pred neautorizovaným prístupom a to aj pred neautorizovaným fyzickým prístupom. Vstup iných osôb môže byť povolený len v sprievode oprávnenej osoby a každý takýto vstup musí byť zaznamenaný.

5.1.3 Zásobovanie elektrickou energiou a klimatizácia

Priestory, v ktorých je umiestnené vybavenie Poskytovateľa, majú byť postačujúco zásobované elektrickou energiou a klimatizované na vytvorenie spoľahlivého operačného prostredia.

5.1.4 Ochrana pre vodou

Priestory, v ktorých je umiestnené vybavenie Poskytovateľa, majú byť umiestnené tak, aby nemohlo dôjsť k ich ohrozeniu vodou s akýchkoľvek zdrojov. V prípade, že to nie je úplne možné musia byť prijaté opatrenia, ktoré minimalizujú riziko ohrozenia priestorov vodou na minimum.

5.1.5 Ochrana pred ohňom

Priestory, v ktorých je umiestnené vybavenie Poskytovateľa musia byť spoľahlivo chránené od zdrojov priameho ohňa resp. tepla, ktoré by mohli spôsobiť požiar v priestoroch.

5.1.6 Úložisko médií

Médiá musia byť uskladnené v priestoroch, ktorú sú chránené pred náhodným, neúmyselným poškodením (vodou, ohňom, elektromagneticky). Médiá, ktoré obsahujú informácie týkajúce sa bezpečnostného auditu, archív alebo zálohované informácie musia byť uložené v lokalite oddelenej od vybavenia CMA.

5.1.7 Nakladanie s odpadom

S odpadom vznikajúcim v súvislosti s prevádzkou Poskytovateľa musí byť nakladané tak, aby v žiadnom prípade nedošlo k znečisťovaniu životného prostredia.

5.1.8 Zálohovanie mimo hlavnú lokalitu

Pre prípad nenávratného poškodenia priestorov hlavnej lokality, v ktorých je umiestnená infraštruktúra Poskytovateľa je potrebné mať k dispozícii minimálne kópie najdôležitejších aktív Poskytovateľa zálohované mimo túto hlavnú lokalitu.

5.2 Procedurálne bezpečnostné opatrenia

5.2.1 Dôveryhodné role

Poskytovateľ musí mať definované dôveryhodné role zodpovedné za jednotlivé aspekty poskytovaných dôveryhodných služieb ako napr. systémový administrátor, bezpečnostný manažér, interný audítor, manažér politík ap.), ktoré formujú základ dôvery v celú PKI.

Zároveň musia byť definované zodpovednosti jednotlivých rolí.

Osoby vybrané na zastávanie rolí, ktoré si vyžadujú dôveryhodnosť, musia byť zodpovedné a dôveryhodné.

Všetky osoby v dôveryhodných roliach musí byť bez konfliktu záujmov na zabezpečenie nestrannosti služieb poskytovaných Poskytovateľom.

5.2.2 Počet osôb v jednotlivých úlohách

Pre každú úlohu musí byť identifikovaný počet jednotlivcov, ktorí sú určení na vykonávanie jednotlivých úloh (pravidlo K z N).

5.2.3 Identifikácia a autentizácia pre každú rolu

Každá rola musí mať definovaný spôsob identifikácie a autentifikácie pri prístupe k IS Poskytovateľa.

5.2.4 Roly vyžadujúce oddelenie zodpovedností

Každá rola musí mať stanovené kritériá, ktoré zohľadňujú potrebu oddelenia funkcií z hľadiska samotnej roly t. j. musia byť uvedené roly, ktoré nemôžu byť vykonávané rovnakými jednotlivcami.

5.3 Personálne bezpečnostné opatrenia

Pracovníci Poskytovateľa musia byť formálne menovaní do dôveryhodných rolí výkonným manažmentom zodpovedným za bezpečnosť.

5.3.1 Požiadavky na kvalifikáciu, skúsenosti a previerky

Zamestnanci v dôveryhodných rolách musia spĺňať kvalifikačné požiadavky, požiadavky na odbornú prax a musia mať bezpečnostné previerky stanovenej úrovne.

Osoby v manažérskych funkciách musia:

- mať príslušné školenia alebo skúsenosti v oblasti dôveryhodných služieb, ktoré Poskytovateľ poskytuje,
- byť oboznámené s bezpečnostnými opatreniami pre role zodpovedné za bezpečnosť
- mať skúsenosti s informačnou bezpečnosťou a odhadom rizika v rozsahu potrebnom na výkon manažérskej funkcie.

5.3.2 Požiadavky na previerky

Zamestnanec môže byť zaradený do dôveryhodnej roly Poskytovateľa len v prípade, že má bezpečnostnú previerku stanovenej úrovne. Personálne bezpečnostné opatrenia sú zabezpečované internými mechanizmami Poskytovateľa.

5.3.3 Požiadavky na školenia

Pre niektoré dôveryhodné roly Poskytovateľa môžu byť špecifikované niektoré špeciálne požiadavky na školenia, ktoré by mali absolvovať pred zaradením prípadne v priebehu zaradenia. Témy majú obsahovať fungovanie softvéru a hardvéru CMA, prevádzkové a bezpečnostné postupy, ustanovenia tohto CP, CPS ap.

5.3.4 Požiadavky na frekvenciu obnovy školení

Pre roly, kde sú stanovené požiadavky na absolvovanie predpísaných školení je možné stanoviť potrebu ich opakovania po absolvovaní primárneho školenia.

5.3.5 Rotácia rolí

Žiadne ustanovenia.

5.3.6 Postihy za neoprávnenú činnosť

Zlyhanie akéhokoľvek zamestnanca Poskytovateľa, ktorého výsledok by mohol byť stav, ktorý nie je v súlade s ustanoveniami tejto CP resp. prijatých CPS, či už sa jedná o nedbanlivosť alebo zlý úmysel, musí byť predmetom zodpovedajúcich administratívnych a disciplinárnych konaní, ktoré môžu viesť až k ukončeniu zamestnaneckého pomeru, prípadne občianskym resp. trestnoprávnym postihom.

Akékoľvek neoprávnené alebo nevhodné konanie zamestnanca v dôveryhodnej role označené vedením Poskytovateľa musí viesť k bezodkladnému odvolaniu z dôveryhodnej roly až do ukončenia prebiehajúceho preskúmania manažmentom. Následne po preskúmaní manažmentom a vzájomnej diskusii alebo preskúmaní výsledkov vyšetrovania so zamestnancom, môže byť tento podľa potreby znovu pridelený do dôveryhodnej roly, alebo prepustený zo zamestnania.

5.3.7 Požiadavky na externých dodávateľov

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

5.3.8 Dokumentácia poskytovaná zamestnancom

Zamestnanci v dôveryhodných rolách musia mať k dispozícii dokumenty potrebné pre výkon funkcie, na ktorú sa sú priradení, vrátane kópie tejto CP resp. CPS a všetky technické a prevádzkovej dokumenty potrebné k zachovaniu integrity operácií Poskytovateľa. Tieto informácie musia zahŕňať aj dokumentáciu interného systému a bezpečnostnú dokumentáciu, politiky a postupy overovania identity a ďalšie informácie pripravené Poskytovateľom, dokumenty tretích strán resp. dokumenty dostupné prostredníctvom internetu.

5.4 Postup získavania auditných záznamov

Poskytovateľ musí zaznamenávať a mať k dispozícii počas nevyhnutnej doby, aj po ukončení činnosti, všetky dôležité informácie týkajúce sa vydaných CERTIFIKÁTOV.

Poskytovateľ musí v systéme na poskytovanie dôveryhodných služieb zaznamenávať presný čas. Čas zaznamenávaný pri jednotlivých udalostí musí byť synchronizovaný s UTC minimálne každých 24 hodín.

5.4.1 Typy zaznamenávaných udalosti

Poskytovateľ musí zaznamenávať a vyhodnocovať nasledovné dôležité udalosti:

- Procesy týkajúce sa životného cyklu kľúčov Poskytovateľa (generovanie, zálohovanie, obnova, likvidácia ap.)
- Procesy týkajúce sa samotného HSM modulu
- Údaje získané pri poskytovaní dôveryhodných služieb od Zákazníka/Držiteľov,
- Systémové logy jednotlivých častí systému Poskytovateľa

5.4.2 Frekvencia spracovávania auditných záznamov

Administrátori Poskytovateľa sú povinní sledovať zasielané systémové logy priebežne, tak aby včas odhalili potenciálne nebezpečenstvo ohrozenia poskytovania služieb Poskytovateľa. Všetky zaznamenávané logy v elektronickej podobe musia byť v pravidelných intervaloch, minimálne 1 krát mesačne, ukladané na záznamové médiá, aby mohli byť k dispozícii audítorom. Rovnako musia byť audítorom k dispozícii všetky písomné auditné záznamy z procesov týkajúcich sa životného cyklu kľúčov certifikačných autorít Poskytovateľa, autorít časovej pečiatky a OCSP reponderov.

5.4.3 Uchovávanie logov

Poskytovateľ musí uchovávať auditné logy v súlade s požiadavkami aktuálne platnej legislatívy. Auditné logy musia byť zároveň uchovávané minimálne do času ukončenia nasledovného pravidelného externého auditu svojich služieb.

5.4.4 Ochrana auditných záznamov

Auditné záznamy musia byť uchovávané a chránené tak, aby nedošlo k ich znehodnoteniu najlepšie vo viacerých kópiách umiestnených v rozdielnych priestoroch.

5.4.5 Postupy zálohovania auditných logov

Žiadne ustanovenia.

5.4.6 Systém zálohovania logov

Žiadne ustanovenia

5.4.7 Notifikácia subjektu iniciujúceho log záznam

Žiadne ustanovenia.

5.4.8 Posudzovanie zraniteľností

Pozri kapitola 5.4.2.

5.5 Uchovávanie záznamov

5.5.1 Typy archivovaných záznamov

Poskytovateľ musí uchovávať všetky záznamy o vydaných CERTIFIKÁTOCH ako aj samotné CERTIFIKÁTY v zmysle požiadaviek aktuálne platnej legislatívy po dobu, ktorá je stanovená v bode 5.5.2.

Záznamy môžu byť v zmysle zákona uchovávané v papierovej forme resp. v elektronickej forme.

Poskytovateľ musí uchovávať aj všetky auditné záznamy (logy), písomné záznamy z udalostí CA (generovanie kľúčov CA, vydávanie TSA certifikátov a certifikátov pre OCSP respondery ap.).

5.5.2 Doba uchovávania záznamov

Poskytovateľ musí uchovávať originály žiadosti o vydanie CERTIFIKÁTU spolu s príslušnými dokumentami potvrdzujúcimi totožnosť žiadateľa v papierovej resp. elektronickej podobe po dobu 10 rokov.

5.5.3 Ochrana archívnych záznamov

Archívne záznamy Poskytovateľa musia byť uložené na bezpečnom mieste mimo prevádzkových priestorov a musia byť udržiavané spôsobom, ktorý zabraňuje ich neoprávnenej modifikácii, nahradenia alebo zničenia.

5.5.4 Zálohovanie archívnych záznamov

Žiadne ustanovenia.

5.5.5 Požiadavky na pridávanie časových pečiatok k záznamom

Žiadne ustanovenia.

5.5.6 Archivačný systém

Žiadne ustanovenia.

5.5.7 Postup získania a overenia archívnych informácií

Žiadne ustanovenia

5.6 Zmena kľúčov CA

Celý proces musí prebehnúť bez negatívneho vplyvu na úroveň zabezpečenia.

K zmene kľúčov Poskytovateľa môže dôjsť z nasledovných dôvodov:

- Blíži sa čas skončenia platnosti aktuálne používaných kľúčov Poskytovateľa. Toto je normálny stav - 14 dní pred uplynutím platnosti doteraz používaného páru kľúčov Poskytovateľa sa musí na webovom sídle Poskytovateľa zverejniť

oznam o blížiacej sa zmene kľúčov Poskytovateľa. Po tom, čo sa vygeneruje nový kľúčový pár a vydá sa nový certifikát pre Poskytovateľa, tento sa musí zverejniť na webovom sídle Poskytovateľa.

- Je nutné vymeniť aktuálne používané kľúče Poskytovateľa z dôvodu ich kompromitácie. Toto je výnimočný, havarijný stav – Poskytovateľ musí bezodkladne oznámiť orgánu dohľadu, všetkým Držiteľom vydaných CERTIFIKÁTOV a verejnosti, že došlo ku kompromitácii kľúčov Poskytovateľa. Bezodkladne tiež musí zrušiť kompromitovaný certifikát, ako aj všetky platné CERTIFIKÁTY podpísané kompromitovaným kľúčom. Poskytovateľa musí upozorniť prostredníctvom svojho webového sídla Držiteľov CERTIFIKÁTOV, ktoré boli podpísané zrušeným certifikátom Poskytovateľa ako aj Spoliehajúcim sa stranám, že zrušený certifikát Poskytovateľa sa má odstrániť z každej aplikácie, ktorú používajú Spoliehajúce sa strany a má byť nahradený novým certifikátom Poskytovateľa.
- Došlo k zmene kľúčov koreňovej certifikačnej autority, ktorá vydala certifikát certifikačnej autorite Poskytovateľa.
- Je nutné vymeniť aktuálne používané kľúče Poskytovateľa z dôvodu, že je potrebné synchronizovať dĺžku platnosti vydávaného kvalifikovaného certifikátu pre elektronický podpis s časom exspirácie certifikačných autorít nachádzajúcich sa v celej jeho certifikačnej ceste.

5.7 Obnova po kompromitácii alebo havárii

5.7.1 Postupy riešenia incidentov a kompromitácie

Na zabezpečenie integrity služieb musí Poskytovateľ implementovať postupy zálohovania údajov a ich obnovy.

Poskytovateľ musí mať vypracované havarijné postupy a plány obnovy pre poskytovanie dôveryhodných služieb.

Dôveryhodné služby by mali byť poskytované z dvoch geograficky oddelených CA systémov, z ktorých je jeden vedený ako hlavný a druhý ako záložný v prípade zlyhania alebo havárii hlavného.

Postupy v prípade havárie a obnovy musia byť pravidelne preskúmavané a testované (minimálne na ročnej báze) a mali by byť revidované a aktualizované podľa potreby.

5.7.2 Poškodenie hardvéru, softvéru alebo údajov

V prípade poškodenia alebo podozrenia z poškodenia hardvéru, softvéru alebo údajov musí Poskytovateľ použiť postupy určené k obnove poškodených aktív. Postupy musia zahŕňať aktivity, ktoré zabezpečia kompletnú obnovu prostredia.

5.7.3 Postupy pri kompromitácii kľúča CA

V prípade kompromitácie súkromného kľúča CA musí mať Poskytovateľ k dispozícii postupy na obnovu bezpečného prostredia, postupy distribúcie verejného kľúča

koncovým používateľom a akým spôsobom budú vydávané nové certifikáty jednotlivým koncovým používateľom.

5.7.4 Zachovanie kontinuity činnosti po havárii

Poskytovateľ musí mať prijaté postupy na zabezpečenie kontinuity činnosti v prípade havárie v dôsledku napr. prírodnej katastrofy, ktoré zabezpečia jej schopnosť obnoviť svoju činnosť. Postupy musia zahŕňať miesto obnovy, postupy na ochranu aktív v mieste havárie resp. prírodnej katastrofy ap.

5.8 Ukončenie činnosti CA resp. RA

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

Ešte pred ukončením poskytovania služieb Poskytovateľ musí:

- vhodným spôsobom, minimálne 6 mesiacov vopred, oznámiť plánované ukončenie svojej činnosti orgánu dohľadu, Držiteľom všetkých ňou vydaných platných CERTIFIKÁTOV, Spoliehajúcim sa stranám a verejnosti,
- ukončiť všetky prípadné mandátne zmluvy, splnomocnenia a pod., na základe ktorých mohli iné osoby konať v mene Poskytovateľa (napr. poskytovať služby RA),
- pokúsiť sa uzavrieť zmluvu s iným kvalifikovaným poskytovateľom dôveryhodných služieb, ktorý by zabezpečil kontinuitu v poskytovaní jeho kvalifikovaných dôveryhodných služieb,
- sústrediť a archivovať všetky dokumenty Poskytovateľa,
- vykonať kontrolu dodržania predpisov o ochrane osobných údajov t. j. Nariadenie Európskeho Parlamentu a Rady (EÚ) 2016/679 o ochrane fyzických osôb pri spracúvaní osobných údajov a o voľnom pohybe takýchto údajov a zákon č. 18/2018 Z. z. o ochrane osobných údajov (ďalej len „Predpisy o ochrane osobných údajov“) [5],
- vyradiť z používania všetky súkromné kľúče, vrátane ich kópií takým spôsobom, že nebude možné ich žiadnym spôsobom obnoviť.

Ak je dôvodom ukončenia činnosti Poskytovateľa nejaký dôvod bez vzťahu k bezpečnosti, potom ani certifikáty vydávajúcich CA, ktoré končia činnosť a ani CERTIFIKÁTY podpísané týmito CA nemusia byť zrušené.

Po ukončení svojej činnosti Poskytovateľ nesmie vydať žiaden CERTIFIKÁT a musí zabezpečiť preukázateľné znemožnenie opätovného použitia podpisových dát (súkromných kľúčov) CA.

Poskytovateľ musí mať riešenie na pokrytie všetkých nákladov spojených so splnením minimálnych požiadaviek pri ukončení činnosti v prípade bankrotu alebo inej príčiny, kedy nebude schopná pokryť náklady vlastnými prostriedkami, a to v súlade s platnou legislatívou o bankrote.

6. Technické bezpečnostné opatrenia

Technická časť infraštruktúry Poskytovateľa (hardvér a softvér) musí pozostávať len z bezpečných systémov a oficiálneho softvéru. Architektúru infraštruktúry Poskytovateľa musí byť navrhnutá s použitím komponentov, ktoré vyhovujú bezpečnostným štandardom na úrovni súčasných poznatkov.

Osobitná pozornosť musí byť venovaná kryptografickému modulu (HSM modulu), ktorý slúži na generovanie, úschovu a použitie súkromných kľúčov Poskytovateľa, a ktorý patrí k najcitlivejším aktívam. Súkromné kľúče Poskytovateľa musia byť uložené v HSM module, ktorý je certifikovaný minimálne podľa štandardu FIPS 140-2 level 3.

Poskytovateľ musí používať na ochranu svojho súkromného kľúča kombináciu fyzických, logických a procedurálnych opatrení, ktoré zaručujú jeho bezpečnosť. Tieto opatrenia musia byť popísané napr. vo vydanom CPS.

Súčasťou systému Poskytovateľa musia byť zariadenia na nepretržitú detekciu, monitorovanie a signalizáciu neautorizovaných a neobvyklých pokusov o prístup k jej prostriedkom.

Aplikácie súvisiace s informáciou o stave certifikátu musia byť zabezpečené tak, zabezpečiť, že zabránia akýmkoľvek neoprávneným pokusom o modifikovanie informácií o stave certifikátu.

Všetky funkcie Poskytovateľa, pri ktorých sa používa počítačová sieť, musia byť zabezpečené pred neautorizovaným prístupom a inými škodlivými činnosťami.

6.1 Generovanie a inštalácia páru kľúčov

6.1.1 Generovanie a inštalácia páru kľúčov pre jednotlivé subjekty

6.1.1.1 Vydavateľ certifikátov

Generovanie a inštalácia páru kľúčov Poskytovateľa sa musí vykonávať štandardizovaným spôsobom, ktorý je podrobne popísaný v dokumentácii Poskytovateľa. Spôsob generovania musí zabezpečiť dostatočnú dôveru v postup generovania a celý proces musí byť písomne zaznamenaný. Generovanie kľúčov musia zabezpečiť zamestnanci Poskytovateľa zaradení v rolách, ktoré majú oprávnenie na účasť na ceremónii generovania. Generovanie kľúčov musí byť vykonané v bezpečnom zariadení na uchovávanie kryptografických kľúčov, ktoré spĺňa legislatívne požiadavky dané na takýto typ zariadenia..

6.1.1.2 Registračné autority

Kľúčový pár certifikátov pracovníkov registračných autorít musí byť uložený v bezpečnom zariadení.

6.1.1.3 Koncoví používatelia

Pozri kapitola 4.1.3.

6.1.2 Doručenie súkromného kľúča Držiteľovi CERTIFIKÁTU

Vygenerovaný kľúčový pár Držiteľa CERTIFIKÁTU, ktorý je uložený v eID musí byť odovzdaný osobne ihneď po vydaní CERTIFIKÁTU.

6.1.3 Doručenie verejného kľúča vydavateľovi CERTIFIKÁTU

Žiadne ustanovenia.

6.1.4 Poskytovanie verejných kľúčov Poskytovateľa Spoliehajúcim sa stranám

Pre Spoliehajúce sa strany musí Poskytovateľ bezpečným spôsobom poskytnúť verejné kľúče všetkých vydávajúcich certifikačných autorít Poskytovateľa, ktoré vydávajú CERTIFIKÁTY.

6.1.5 Dĺžka kľúčového páru

Musí byť stanovená odporúčaná dĺžka kľúčového páru resp. minimálna dĺžka kľúčov pre všetky typy entít a všetky používané algoritmy (napr. RSA).

6.1.6 Parametre a kvalita verejného kľúča

Parametre a kvalitu verejných kľúčov Poskytovateľa musí určiť PMA. Počas ceremónie generovania kľúčov musia byť stanovené parametre dodržiavané. Poskytovateľ musí využívať na generovanie a uchovávanie kľúčov kryptografické hardvérové moduly spĺňajúce požiadavky FIPS 140-2, ktoré zabezpečujú náhodné generovanie RSA kľúčov veľkosti minimálne 4096 bitov.

Pre jednotlivé typy KC vydávaných koncovým používateľom musí mať Poskytovateľ stanovené parametre a kvalitu verejného kľúča (dĺžka, typ) a pred samotným vydaním musí kontrolovať ich dodržanie.

6.1.7 Použitie kľúčov

Certifikáty certifikačných autorít Poskytovateľa musia obsahovať rozšírenia, ktoré určujú k čomu môžu byť tieto certifikáty použité.

6.2 Ochrana súkromného kľúča a technické opatrenia pre kryptografický modul

6.2.1 Štandardy a opatrenia pre kryptografický modul

Poskytovateľ musí využívať na ochranu súkromných kľúčov svojich vydávajúcich CA hardvérové kryptografické moduly, ktoré sú certifikované podľa štandardu FIPS 140-2 level 3. Moduly musia byť uložené v zabezpečených priestoroch, do ktorých majú prístup len osoby v dôveryhodných rolách.

Súkromné kľúče Poskytovateľa sa môžu používať výlučne na podpisovanie certifikátov a CRL vydávaných Poskytovateľom.

Vybavenie CA musí byť neprestajne chránené pred neautorizovaným prístupom a to aj pred neautorizovaným fyzickým prístupom.

6.2.2 Opatrenia (k z n) pre manipuláciu so súkromným kľúčom

Pri operáciách správy súkromných kľúčov Poskytovateľa (napr. generovanie, zálohovanie, zničenie) musí byť vždy prítomný príslušný počet oprávnených osôb na princípe „k“ z „n“ určených oprávnených osôb

6.2.3 „Key escrow“ súkromného kľúča

Žiadne ustanovenia.

6.2.4 Zálohovanie súkromného kľúča

Súkromné kľúče Poskytovateľa sú generované a uchovávané vo vnútri hardvérových kryptografických modulov. V prípade potreby ich prenosu pre proces zálohovania a obnovy, musia byť súkromné kľúče prenášané vždy v zašifrovanej podobe. Prenášanie súkromných kľúčov a ich obnova v inom hardvérovom kryptografickom module môže byť vykonaná len oprávnenými zamestnancami v zmysle pravidiel uvedených v bode 6.2.2.

6.2.5 Archivácia súkromného kľúča

Žiadne ustanovenia.

6.2.6 Prenos súkromných kľúčov z a do HSM modulu

Pozri 6.2.4

6.2.7 Uchovávanie súkromných kľúčov v HSM module

Súkromné kľúče Poskytovateľa, ktoré sú využívané na podpisovanie vydaných CERTIFIKÁTOV pre koncových používateľov môžu byť v samotnom HSM module uchovávané v čitateľnej forme. Všetky HSM moduly Poskytovateľa musia byť prevádzkované v zabezpečených priestoroch s režimovým prístupom.

6.2.8 Spôsob aktivácie súkromných kľúčov

Súkromné kľúče Poskytovateľa môžu aktivovať len oprávnené osoby v zmysle bodu 6.2.2.

Pri aktivácií musí každý držiteľ z potrebného počtu držiteľov vložiť do HSM modulu svoju čipovú kartu a zadať k nej heslo.

Po aktivácii sú kľúče v HSM module aktívne až do doby, kým nedôjde k ich deaktivácii. oprávnenou osobou (administrátor CA) alebo výpadkom elektrického napájania HSM modulu.

6.2.9 Spôsob deaktivácie súkromného kľúča

Deaktiváciu súkromného kľúča v HSM module môže vykonať len oprávnená osoba (administrátor CA) alebo sú kľúče deaktivované automaticky pri výpadku relácie alebo výpadkom elektrického napájania HSM modulu.

6.2.10 Spôsob zničenia súkromného kľúča

Poskytovateľ musí technickými a organizačnými opatreniami zabezpečiť, že súkromné kľúče vydávajúcich CA Poskytovateľa nebude možné po ukončení jeho životného cyklu ďalej používať. O ukončení životného cyklu súkromného kľúča CA a prijatých technických a organizačných opatreniach musí byť vykonaný záznam podpísaný všetkými prítomnými aktérmi.

6.2.11 Charakteristika HSM modulu

Pozri bod 6.2.1.

6.3 Ďalšie aspekty manažmentu páru kľúčov

6.3.1 Archivácia verejných kľúčov

Poskytovateľ musí uchovávať všetky verejné kľúče, na ktoré bol ňou vydaný certifikát v zmysle bodu 5.5.2.

6.3.2 Dĺžka platnosti certifikátov a použiteľnosť kľúčového páru

Pre platnosť vydávaných CERTIFIKÁTOV Poskytovateľom a použiteľnosť páru kľúčov platia tieto hodnoty:

Typ certifikátu	**Platnosť**
Koreňová CA	30 rokov
Vydávajúca CA Disig	30 rokov
Kvalifikovaný certifikát pre koncového používateľa	maximálne 1856 dní
Certifikát pre elektronický podpis	maximálne 3650 dní
Certifikát na šifrovanie	maximálne 3650 dní

6.4 Aktivačné údaje

6.4.1 Vytváranie a inštalácia aktivačných údajov

Aktivačné údaje Držiteľov CERTIFIKÁTOV (BOK, KEP PIN a KEP PUK), ktoré sa viažu ku konkrétnemu eID musia byť zvolené vlastníkom eID ešte pred procesom vydania CERTIFIKÁTOV.

Aktivačné údaje k používaným kryptografickým modulom CA Poskytovateľa musia byť vytvárané v zmysle bodu 6.2.2.

6.4.2 Ochrana aktivačných údajov

Za ochranu súkromných kľúčov Držiteľov sú zodpovední výhradne samotní Držitelia.

Kľúčový pár určený pre vydavateľa CERTIFIKÁTOV:

- musí byť generovaný v bezpečnostnom module, ktorý spĺňa minimálne požiadavky štandardu FIPS 140-2 level 3,
- akákoľvek manipulácia so súkromným kľúčom môže byť umožnená len za princípu viacnásobnej kontroly, pričom minimálny počet potrebných osôb musí byť tri (3).

6.4.3 Ostatné aspekty aktivačných údajov

Musí byť zabezpečené, že sa súkromné kľúče vydávajúcich CA nikdy nedostali v nezašifrovanej forme mimo modul, kde sú uložené.

Nikto nemá mať prístup k súkromnému podpisovému kľúču okrem jeho Držiteľa.

Aktivačné dáta pre súkromné kľúče patriace k CERTIFIKÁTOM potvrdzujúcim individuálnu identitu nesmú byť nikdy zdieľané.

6.5 Riadenie bezpečnosti počítačov

6.5.1 Špecifické požiadavky na bezpečnosť počítačov

Poskytovateľ musí vykonáva všetky funkcie kvalifikovaného poskytovateľa dôveryhodných služieb za použitia dôveryhodného systému, ktorý spĺňa požiadavky definované v bezpečnostnom projekte IS Poskytovateľa.

Poskytovateľ vydávajúci kvalifikované certifikáty sa môže riadiť pri poskytovaní svojich služieb požiadavkami na bezpečnosť informácií, ktoré sú kladené na dôveryhodného poskytovateľa služieb a sú definované v štandarde ETSI EN 319411-2 " Electronic Signatures and Infrastructures (ESI); Policy and security requirements for Trust Service Providers issuing certificates; Part 2: Requirements for trust service providers issuing EU qualified certificates. [6]

Všetky systémy musia byť pravidelne overované na prítomnosť škodlivého kódu a chránené proti spyware a vírusom.

6.5.2 Hodnotenie bezpečnosti informácií

Žiadne ustanovenia.

6.6 Opatrenia v životnom cykle

6.6.1 Opatrenia pri vývoji systémov

Aplikácie Poskytovateľa pre potreby systému Poskytovateľa musia zohľadňovať opatrenie týkajúce sa bezpečnosti vývojového prostredia, personálnej bezpečnosti, bezpečnosti riadenia konfigurácie pri údržbe systémov, v rámci technických postupov vývoja softvéru, v rámci metodológie vývoja softvéru a jeho modularite a vrstvení.

6.6.2 Opatrenia na riadenie bezpečnosti

Poskytovateľ musí využívať nástroje a postupy, ktoré umožnia určiť, či operačné systémy využívané v rámci CA Poskytovateľa a využívané sieťové pripojenia stále zodpovedajú nastavenej úrovni bezpečnosti.

Tieto nástroje a postupy by mali zahŕňať kontrolu integrity bezpečnostného softvéru, firmvéru a hardvéru na zaistenie ich správnej funkčnosti.

6.6.3 Bezpečnostné opatrenia v životnom cykle

Žiadne ustanovenia.

6.7 Sieťové bezpečnostné opatrenia

Poskytovateľ musí mať prijaté opatrenia na zabezpečenie sieťovej bezpečnosti vrátane bezpečnosti firewalov.

6.8 Využívanie časovej pečiatky

Žiadne ustanovenie

7. Profily CERTIFIKÁTOV, CRL a OCSP

7.1 Kvalifikované dôveryhodné služby

V rámci poskytovania kvalifikovaných dôveryhodných služieb bude na eID vydávaný kvalifikovaný certifikát pre elektronický podpis v zmysle Nariadenia eIDAS článok 3 bod 15.

7.1.1 Certifikát vydávajúcej CA

Certifikát musí podporovať nasledovné:

Algoritmus podpisu (Signature algorithm)
sha256RSA

Algoritmus fingerprintu podpisu (Signature hash algorithm)
sha256

Verejný kľúč
RSA, 4096 bitov

Tabuľka č. 1: Položky použité v certifikáte CA Disig vydávajúcej KC

Položka / OID položky	Skratka názvu položky	Povinnosť uvádzania
CN (commonName) {id-at-commonName} { 2.5.4.3 }	Identifikácia certifikačnej služby	**Povinná**
OU (organizationUnitName) {id-at-organizationalUnit} { 2.5.4.11}	Identifikácia CA	Nepovinná
O (organizationName) {id-at-organization} { 2.5.4.10}	Oficiálny názov právnickej osoby poskytujúcej dôveryhodné služby a kvalifikovane dôveryhodné služby	**Povinná**
(organizationIdentifier) { id-at-organizationIdentifier } { 2.5.4.97}	Identifikátor právnickej osoby uvedenej v položke „O“	Nepovinná
L (localityName) {joint-iso-itu-t(2) ds(5) attributeType(4) localityName(7)}	Sídlo právnickej osoby uvedenej v položke „O“	Nepovinná
C (countryName) {id-at-countryName} { 2.5.4.6 }	Krajina pôvodu poskytovateľa služby uvedeného v položke „O“	**Povinná**

Certifikát musí obsahovať aj nasledovné údaje:

Tabuľka č. 2: Základné položky v certifikáte vydávajúcej CA

Názov	**Popis**
Verzia certifikátu (*Version*)	Táto položka obsahuje verziu formátu certifikátu. V prípade KC musí byť verzia X.509 v3
Sériové číslo certifikátu (*serialNumber*)	Položka obsahuje sériové číslo certifikátu, ktoré musí byť jedinečné pre všetky vydané certifikáty danou CA. Obsah určuje vydávajúca CA resp. u self-signed certifikátu je zvolený Poskytovateľom.
Algoritmus podpisovania (*signatureAlgorithm*)	Položka obsahuje šifrovací algoritmus, ktorý CA využíva pri podpisovaní vydávaných certifikátov. Algoritmus určuje vydávajúca CA resp. u self-signed certifikátu je zvolený Poskytovateľom.
Platnosť certifikátu (*validity*)	Platnosť certifikátu určuje obdobie, počas ktorého vydávajúca KCA zaručuje poskytovanie dôveryhodných služieb pre daný certifikát. Obdobie platnosti určuje vydávajúca CA resp. u self-signed certifikátu je zvolený Poskytovateľom.
Verejný kľúč v certifikáte (*subjecPublicKeyInfo*)	Táto položka obsahuje verejný kľúč Držiteľa certifikátu a použitý algoritmus

Tabuľka č. 3: Rozšírenia v certifikáte CA Disig vydávajúcej KC

Názov rozšírenia	**ASN.1 názov a OID / Popis**	**Prítomnosť?**	**Kritickosť?**
authorityKeyIdentifier	{id-ce-authorityKeyIdentifier} {2.5.29.35} Identifikátor verejného kľúča certifikačnej autority CA, ktorá vydala tento certifikát resp. u self-signed certifikátu sa táto hodnota rovná hodnote subjectKeyIdentifier.	Áno	Nie
subjectKeyIdentifier	{id-ce-subjectKeyIdentifier} {2.5.29.14} Identifikátor verejného kľúča Držiteľa certifikátu.	Áno	Nie
keyUsage	{id-ce-keyUsage} {2.5.29.15} Definuje účel súkromného kľúča, ktorého verejný kľúč je súčasťou tohto certifikátu.	Áno	Áno
certificatePolicies	id-ce-certificatePolicies} {2.5.29.32} Identifikuje certifikačné politiky, pod ktorými bol certifikát vydaný.	Áno	Áno
Policy Mappings	{id-ce-policyMappings} {2.5.29.33} Potvrdzuje, že vydávajúca CA považuje svoju politiku za ekvivalentnú politike CA, pre ktorú je certifikát vydaný.	Áno U self-signed certifikátu sa táto položka nevyskytuje.	Nie
BasicConstraints	{id-ce-basicConstraints} {2.5.29.19} Identifikuje CA certifikát.	Áno	Áno
Policy Constraints	{id-ce-policyConstraints} {2.5.29.36}	Áno	Áno

	Môže byť použitý v CA certifikátoch na obmedzenie overovania certifikačnej cesty.	U self-signed certifikátu sa táto položka nevyskytuje.	
crlDistributionPoints	{id-ce-CRLDistributionPoints} {2.5.29.31} Určuje, akým spôsobom a odkiaľ je možné získať CRL.	Áno U self-signed certifikátu sa táto položka nevyskytuje.	Nie
AuthorityInfoAccess	{id-pe-authorityInfoAccess} {1.3.6.1.5.5.7.1.1} Určuje (http:// … p7c, certifikát alebo aj ldap://...) adresu na získanie certifikátov vydaných pre vydavateľa tohto certifikátu a adresu na OCSP.	Áno U self-signed certifikátu sa táto položka nevyskytuje	Nie

7.1.1.1 Profil KC

Táto CP povoľuje len KC vyhovujúce štandardu X.509 verzie 3. Štruktúra KC vydávaného na eID sa môže meniť len na základe rozhodnutia PMA.

Algoritmy a dĺžky kľúčov uplatňované v KC:

Algoritmus podpisu (Signature Algorithm)
sha256RSA

Verejný kľúč
RSA, minimálna dĺžka je 3 072 bitov

Algoritmus fingerprintu (Thumbprint Algorithm)
SHA1

Dĺžka platnosti
maximálne 1856 dní

V tabuľke č. 4 sú uvedené možné položky rozlišovacieho mena a ich popis v prípade KC vydávaných na eID.

Tabuľka č. 4: Obsah položiek rozlišovacieho mena v KC vydávanom na eID

Názov položky / OID/ Uvádzanie	Skratka názvu položky	Popis položky	Príklad hodnoty položky	Typ a maximálna dĺžka položky
Meno a priezvisko (commonName) OID (2.5.4.3) Povinná položka	CN	Meno a priezvisko	Peter Test	DirectoryString (UTF8String) 64 znakov

Meno(á) (givenName) OID (2.5.4.42)	G	Všetky mená použité v položke CN okrem priezviska	Peter	DirectoryString (UTF8String) 64 znakov
Priezvisko (Surname) OID (2.5.4.4) Povinná položka	SN	Priezvisko z položky CN	Test	DirectoryString (UTF8String) 64 znakov
Mesto (localityName) OID (2.5.4.7) Povinná položka	L	Názov mesta/obce trvalého pobytu Držiteľa	Bratislava	DirectoryString (UTF8String) 128 znakov
Štát (countryName) OID (2.5.4.6) Povinná položka	C	Dvojznaková skratka štátu – dvojmiestny kód podľa ISO 3166	SK	PrintableString 2 znaky
SerialNumber OID (2.5.4.5) Povinná položka		Odkaz na identitu fyzickej osoby *	PNOSK-1234567890 Položka je súčasťou KC	PrintableString 64 znakov
Sériové číslo (serialNumber - CertificateSerialNumber)		Položka slúži na zabezpečenie jednoznačnosti rozlišovacieho mena (pozri kapitola 3.1.3)	Položka nebude súčasťou žiadosti o KC – jej hodnotu určí vydávajúca CA	INTEGER max 20 Byte 1 ≤ serialNumber ≤ 2159

* Odkaz na identitu sa skladá z dvoch častí. Prvá časť pozostáva z troch úvodných znakov určujúcich typ odkazu na identitu a dvoch znakov krajiny. Tri úvodné znaky potom budú „PNO“ (identifikácia na základe rodného čísla u občanov SR, alebo cudzincov, ktorí majú pridelené rodné číslo podľa zákona o rodnom čísle 301/1995 Z. z. Nasledujúce dva znaky obsahujú kód krajiny podľa ISO 3166 (pre Slovensko „SK“). Druhá časť položky pozostáva z údajov, ktorých typ určujú prvé tri úvodné znaky, pri rodnom čísle sa uvedie rodné číslo bez lomky (napr. PNOSK 7701011111). Upozornenie - Prvá a druhá časť sú oddelené pomlčkou!!!

Tabuľka č. 5: Použité rozlíšenia v KC vydávanom na eID

Názov rozšírenia	ASN.1 názov a OID / Popis	Prítomnosť?	Kritickosť?
authorityKeyIdentifier	{id-ce-authorityKeyIdentifier} {2.5.29.35} Identifikátor verejného kľúča certifikačnej autority CA, ktorá vydala tento certifikát.	Áno	Nie
subjectKeyIdentifier	{id-ce-subjectKeyIdentifier} {2.5.29.14} Identifikátor verejného kľúča Držiteľa certifikátu.	Áno	Nie
keyUsage	{id-ce-keyUsage} {2.5.29.15} Definuje účel súkromného kľúča, ktorého verejný kľúč je súčasťou tohto certifikátu.	Áno	Áno
certificatePolicies	id-ce-certificatePolicies} {2.5.29.32} Identifikuje certifikačné politiky, pod ktorými bol certifikát vydaný.	Áno	Nie
BasicConstraints	{id-ce-basicConstraints} {2.5.29.19} Identifikuje CA certifikát.	Áno	Áno
crlDistributionPoints	{id-ce-CRLDistributionPoints}	Áno	Nie

	{2.5.29.31} Určuje, akým spôsobom a odkiaľ je možné získať CRL.		
AuthorityInfoAccess	{id-pe-authorityInfoAccess} {1.3.6.1.5.5.7.1.1} Určuje (http:// … p7c, certifikát alebo aj ldap://...) adresu na získanie certifikátov vydaných pre vydavateľa tohto certifikátu a adresu na OCSP.	Áno	Nie
QCstatements	{id-pe-qcStatements}* {1.3.6.1.5.5.7.1.3} Prehlásenie o tom, že certifikát je kvalifikovaný v súlade s konkrétnym technickým štandardom a obsahuje obmedzenia použitia kvalifikovaného certifikátu.	Áno	Nie

* V prípade vydávania kvalifikovaného certifikátu, kde sa údaje na vyhotovenie elektronického podpisu súvisiace s údajmi na validáciu elektronického podpisu nachádzajú v kvalifikovanom zariadení na vyhotovenie elektronického podpisu, je táto o skutočnosť uvedená v tomto rozšírení, v podobe OID 0.4.0.1862.1.4.

7.1.2 Certifikát na potvrdenie existencie a platnosti certifikátu (OCSP)

Certifikát, ktorý je určený na potvrdenie existencie a platnosti certifikátu (OCSP) musí podporovať nasledovné:

Algoritmus podpisu (Signature Algorithm)
sha256RSA

Verejný kľúč
RSA, dĺžka je minimálne 2 048 bitov

Dĺžka platnosti certifikátu pre OCSP responder
Maximálne 1095 dní (3 roky= 3*365 dní)

Tabuľka č. 6: Položky použité v certifikáte OCSP respondera

Položka / OID položky	Skratka názvu položky	Povinnosť uvádzania
CN (commonName) {id-at-commonName} { 2.5.4.3 }	Identifikácia poskytovanej služby	Povinná
OU (organizationUnitName) {id-at-organizationalUnit} { 2.5.4.11}	Identifikácia služby	Nepovinná
OU (organizationUnitName) {id-at-organizationalUnit} { 2.5.4.11}	Identifikácia CA	Nepovinná
O (organizationName) {id-at-organization} { 2.5.4.10}	Oficiálny názov právnickej osoby poskytujúcej dôveryhodné služby a kvalifikovane dôveryhodné služby	Povinná

	(organizationIdentifier) { id-at-organizationIdentifier } { 2.5.4.97}	Identifikátor právnickej osoby uvedenej v položke „O“	Nepovinná
L	(localityName) {joint-iso-itu-t(2) ds(5) attributeType(4) localityName(7)}	Sídlo právnickej osoby uvedenej v položke „O“	Nepovinná
C	(countryName) {id-at-countryName} { 2.5.4.6 }	Krajina pôvodu poskytovateľa služby uvedeného v položke „O“	Povinná

Tabuľka č. 7: Použité rozšírenia v certifikáte OCSP respondera na potvrdenie existencie a platnosti kvalifikovaného certifikátu (OCSP)

Názov rozšírenia	ASN.1 názov a OID / Popis	Prítomnosť?	Kritickosť?
authorityKeyIdentifier	{id-ce-authorityKeyIdentifier} {2.5.29.35} Identifikátor verejného kľúča certifikačnej autority CA, ktorá vydala tento certifikát.	Áno	Nie
subjectKeyIdentifier	{id-ce-subjectKeyIdentifier} {2.5.29.14} Identifikátor verejného kľúča Držiteľa certifikátu.	Áno	Nie
keyUsage	{id-ce-keyUsage} {2.5.29.15} Definuje účel súkromného kľúča, ktorého verejný kľúč je súčasťou tohto certifikátu.	Áno	Nie
certificatePolicies	id-ce-certificatePolicies} {2.5.29.32} Identifikuje certifikačné politiky, pod ktorými bol certifikát vydaný.	Áno	Nie
BasicConstraints	{id-ce-basicConstraints} {2.5.29.19} Identifikuje CA certifikát.	Áno	Áno
crlDistributionPoints	{id-ce-CRLDistributionPoints} {2.5.29.31} Určuje, akým spôsobom a odkiaľ je možné získať CRL.	Áno	Nie
AuthorityInfoAccess	{id-pe-authorityInfoAccess} {1.3.6.1.5.5.7.1.1} Určuje (http:// … p7c, certifikát alebo aj ldap://...) adresu na získanie certifikátov vydaných pre vydavateľa tohto certifikátu a adresu na OCSP.	Áno	Nie
SubjectAltnames	{2.5.29.17} Alternatívne (technické) meno Držiteľa certifikátu: napríklad OtherName, e-mail, DNS meno, IP adresa, URI	Možná	Nie
Extended Key Usage	{2.5.29.37} Definuje ďalší možný účel použitia súkromného kľúča, ktorého verejný kľúč je súčasťou tohto certifikátu, ako doplnok alebo náhrada rozšírenia keyUsage. OCSP Signing (1.3.6.1.5.5.7.3.9)	Áno	Nie

7.2 Dôveryhodné služby

V rámci poskytovania dôveryhodných služieb bude na eID vydávaný certifikát na šifrovanie a certifikát na podpisovanie.

7.2.1 Certifikát koreňovej CA

Algoritmy a dĺžky kľúčov uplatňované v certifikáte koreňovej CA:

Algoritmus podpisu (Signature Algorithm)
sha256RSA

Verejný kľúč
RSA, dĺžka 4 096 bitov

Doba platnosti certifikátu CA
maximálne 30 rokov (30*365 dní)

Tabuľka č. 8: Základné položky v certifikáte koreňovej CA

Názov	**Popis**
Verzia certifikátu (*Version*)	Táto položka obsahuje verziu formátu certifikátu. V prípade KC musí byť verzia X.509 v3
Sériové číslo certifikátu (*serialNumber*)	Položka obsahuje sériové číslo certifikátu, ktoré musí byť jedinečné pre všetky vydané certifikáty danou CA. Obsah určuje vydávajúca KCA.
Algoritmus podpisovania (*signatureAlgorithm*)	Položka obsahuje šifrovací algoritmus, ktorý CA využíva pri podpisovaní vydávaných certifikátov. Algoritmus určuje vydávajúca KCA.
Platnosť certifikátu (*validity*)	Platnosť certifikátu určuje obdobie, počas ktorého vydávajúca KCA zaručuje poskytovanie certifikačných služieb pre daný certifikát. Obdobie platnosti určuje vydávajúca KCA.
Verejný kľúč v certifikáte (*subjecPublicKeyInfo*)	Táto položka obsahuje verejný kľúč Držiteľa certifikátu a použitý algoritmus

Tabuľka č. 9: Obsah položiek v rozlišovacom mene koreňovej CA

Položka / OID položky	**Skratka názvu položky**
C (countryName) {id-at-countryName} { 2.5.4.6 }	Krajina pôvodu poskytovateľa služby uvedeného v položke „O“
L (localityName) {joint-iso-itu-t(2) ds(5) attributeType(4) localityName(7)}	Sídlo právnickej osoby uvedenej v položke „O“
O (organizationName) {id-at-organization} { 2.5.4.10}	Oficiálny názov právnickej osoby poskytujúcej dôveryhodné služby a kvalifikovane dôveryhodné služby
CN (commonName) {id-at-commonName} { 2.5.4.3 }	Identifikácia koreňovej CA

Tabuľka č. 10: Použité rozšírenia (certificate extensions) v certifikáte koreňovej CA

Názov rozšírenia	ASN.1 názov a OID / Popis	Prítomnosť?	Kritickosť?
subjectKeyIdentifier	{id-ce-subjectKeyIdentifier} {2.5.29.14} Identifikátor verejného kľúča Držiteľa certifikátu.	Áno	Nie
keyUsage	{id-ce-keyUsage} {2.5.29.15} Definuje účel súkromného kľúča, ktorého verejný kľúč je súčasťou tohto certifikátu.	Áno	Áno
BasicConstraints	{id-ce-basicConstraints} {2.5.29.19} Identifikuje CA certifikát.	Áno	Áno

7.2.2 Podriadené certifikačné autority vydávané koreňovou CA

Algoritmy a dĺžky kľúčov uplatňované v certifikáte podriadených CA:

Algoritmus podpisu (Signature Algorithm)
sha256RSA

Verejný kľúč
RSA, dĺžka 2 048 bitov

Doba platnosti certifikátu CA
maximálne 20 rokov (20*365 dní)

Tabuľka č. 11: Obsah položiek v DN podriadených certifikačných autorít

Položka / OID položky	Skratka názvu položky
C (countryName) {id-at-countryName} { 2.5.4.6 }	Krajina pôvodu poskytovateľa služby uvedeného v položke „O“
L (localityName) {joint-iso-itu-t(2) ds(5) attributeType(4) localityName(7)}	Sídlo právnickej osoby uvedenej v položke „O“
O (organizationName) {id-at-organization} { 2.5.4.10}	Oficiálny názov právnickej osoby poskytujúcej dôveryhodné služby a kvalifikovane dôveryhodné služby
CN (commonName) {id-at-commonName} { 2.5.4.3 }	Identifikácia koreňovej CA

Tabuľka č. 12: Použité rozšírenia (certificate extensions) v certifikáte podriadených CA

Názov rozšírenia	ASN.1 názov a OID / Popis	Prítomnosť?	Kritickosť?
authorityKeyIdentifier	{id-ce-authorityKeyIdentifier} {2.5.29.35} Identifikátor verejného kľúča certifikačnej autority CA, ktorá vydala tento certifikát.	Áno	Nie
subjectKeyIdentifier	{id-ce-subjectKeyIdentifier} {2.5.29.14} Identifikátor verejného kľúča Držiteľa certifikátu.	Áno	Nie
keyUsage	{id-ce-keyUsage} {2.5.29.15} Definuje účel súkromného kľúča, ktorého verejný kľúč je súčasťou tohto certifikátu.	Áno	Áno
certificatePolicies	id-ce-certificatePolicies} {2.5.29.32} Identifikuje certifikačné politiky, pod ktorými bol certifikát vydaný.	Áno	Áno
BasicConstraints	{id-ce-basicConstraints} {2.5.29.19} Identifikuje CA certifikát.	Áno	Áno
crlDistributionPoints	{id-ce-CRLDistributionPoints} {2.5.29.31} Určuje, akým spôsobom a odkiaľ je možné získať CRL.	Áno	Nie
AuthorityInfoAccess	{id-pe-authorityInfoAccess} {1.3.6.1.5.5.7.1.1} Určuje (http:// … p7c, certifikát alebo aj ldap://...) adresu na získanie certifikátov vydaných pre vydavateľa tohto certifikátu a adresu na OCSP.	Áno	Nie
SubjectAltnames	{2.5.29.17} Alternatívne (technické) meno Držiteľa certifikátu: napríklad OtherName, e-mail, DNS meno, IP adresa, URI	Áno	Nie

7.2.3 Certifikáty vydávané koncovým užívateľom

7.2.3.1 Certifikát na šifrovanie

Algoritmy a dĺžky kľúčov uplatňované v certifikáte na šifrovanie:

Algoritmus podpisu (Signature Algorithm)
sha256RSA

Verejný kľúč
RSA, dĺžka je minimálne 3 072 bitov

Doba platnosti osobného certifikátu

maximálne 3650 dní

Tabuľka č. 13: Obsah štandardných položiek v certifikáte na šifrovanie

Položka / OID položky	Skratka názvu položky
(SerialNumber) {id-at-countryName} { 2.5.4.5 }	Jedinečné sériové číslo
C (countryName) {id-at-countryName} { 2.5.4.6 }	Krajina vydavateľa eID
L (localityName) {joint-iso-itu-t(2) ds(5) attributeType(4) localityName(7)}	Názov lokality – mesto (obec) trvalého bydliska
CN (commonName) {id-at-commonName} { 2.5.4.3 }	Meno a priezvisko Držiteľa

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

Názov rozšírenia	ASN.1 názov a OID / Popis	Prítomnosť?	Kritickosť?
authorityKeyIdentifier	{id-ce-authorityKeyIdentifier} {2.5.29.35} Identifikátor verejného kľúča certifikačnej autority CA, ktorá vydala tento certifikát.	Áno	Nie
subjectKeyIdentifier	{id-ce-subjectKeyIdentifier} {2.5.29.14} Identifikátor verejného kľúča Držiteľa certifikátu.	Áno	Nie
keyUsage	{id-ce-keyUsage} {2.5.29.15} Definuje účel súkromného kľúča, ktorého verejný kľúč je súčasťou tohto certifikátu.	Áno	Nie
certificatePolicies	id-ce-certificatePolicies} {2.5.29.32} Identifikuje certifikačné politiky, pod ktorými bol certifikát vydaný.	Áno	Nie
crlDistributionPoints	{id-ce-CRLDistributionPoints} {2.5.29.31} Určuje, akým spôsobom a odkiaľ je možné získať CRL.	Áno	Nie
AuthorityInfoAccess	{id-pe-authorityInfoAccess} {1.3.6.1.5.5.7.1.1} Určuje (http:// … p7c, certifikát alebo aj ldap://...) adresu na získanie certifikátov vydaných pre vydavateľa tohto certifikátu a adresu na OCSP.	Áno	Nie

7.2.3.2 Certifikát na podpisovanie

Algoritmy a dĺžky kľúčov uplatňované v certifikáte na podpisovanie:

Algoritmus podpisu (Signature Algorithm)
sha256RSA

Verejný kľúč
RSA, dĺžka je minimálne 3 072 bitov

Doba platnosti osobného certifikátu
maximálne 3650 dní

Tabuľka č. 15: Obsah štandardných položiek v certifikáte na podpisovanie

Položka / OID položky	Skratka názvu položky
(SerialNumber) {id-at-countryName} { 2.5.4.5 }	Jedinečné sériové číslo
C (countryName) {id-at-countryName} { 2.5.4.6 }	Krajina vydavateľa eID
L (localityName) {joint-iso-itu-t(2) ds(5) attributeType(4) localityName(7)}	Názov lokality – mesto (obec) trvalého bydliska
CN (commonName) {id-at-commonName} { 2.5.4.3 }	Meno a priezvisko Držiteľa

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

Názov rozšírenia	ASN.1 názov a OID / Popis	Prítomnosť?	Kritickosť?
authorityKeyIdentifier	{id-ce-authorityKeyIdentifier} {2.5.29.35} Identifikátor verejného kľúča certifikačnej autority CA, ktorá vydala tento certifikát.	Áno	Nie
subjectKeyIdentifier	{id-ce-subjectKeyIdentifier} {2.5.29.14} Identifikátor verejného kľúča Držiteľa certifikátu.	Áno	Nie
keyUsage	{id-ce-keyUsage} {2.5.29.15} Definuje účel súkromného kľúča, ktorého verejný kľúč je súčasťou tohto certifikátu.	Áno	Nie
certificatePolicies	id-ce-certificatePolicies} {2.5.29.32} Identifikuje certifikačné politiky, pod ktorými bol certifikát vydaný.	Áno	Nie
crlDistributionPoints	{id-ce-CRLDistributionPoints} {2.5.29.31} Určuje, akým spôsobom a odkiaľ je možné získať CRL.	Áno	Nie
AuthorityInfoAccess	{id-pe-authorityInfoAccess} {1.3.6.1.5.5.7.1.1}	Áno	Nie

	Určuje (http:// … p7c, certifikát alebo aj ldap://...) adresu na získanie certifikátov vydaných pre vydavateľa tohto certifikátu a adresu na OCSP.		
Extended Key Usage	{2.5.29.37} Definuje ďalší možný účel použitia súkromného kľúča, ktorého verejný kľúč je súčasťou tohto certifikátu, ako doplnok alebo náhrada rozšírenia keyUsage. Client Authentication (1.3.6.1.5.5.7.3.2)	Áno	Nie

7.2.4 Certifikát na potvrdenie existencie a platnosti certifikátu (OCSP)

Algoritmy a dĺžky kľúčov uplatňované v certifikátoch CA, ktorý je určený na potvrdenie existencie a platnosti certifikátu na šifrovanie a certifikátu na podpisovanie (OCSP):

Algoritmus podpisu (Signature Algorithm)
sha256RSA

Verejný kľúč
RSA, dĺžka je 2 048 bitov

Dĺžka platnosti certifikátu OCSP respondera
Maximálne 1095 dní (3 roky t. j. 3*365 dní)

Tabuľka č. 17: Obsah položiek v certifikáte na potvrdenie existencie a platnosti certifikátu (OCSP)

Položka / OID položky	Skratka názvu položky
C (countryName) {id-at-countryName} { 2.5.4.6 }	*Krajina pôvodu poskytovateľa služby uvedeného v položke „O“*
L (localityName) {joint-iso-itu-t(2) ds(5) attributeType(4) localityName(7)}	Sídlo právnickej osoby uvedenej v položke „O“
O (organizationName) {id-at-organization} { 2.5.4.10}	Oficiálny názov právnickej osoby poskytujúcej dôveryhodné služby a kvalifikovane dôveryhodné služby
OU (organizationUnitName) {id-at-organizationalUnit} { 2.5.4.11}	Identifikácia CA
OU (organizationUnitName) {id-at-organizationalUnit} { 2.5.4.11}	Identifikácia služby
CN (commonName) {id-at-commonName} { 2.5.4.3 }	Identifikácia poskytovanej služby

Tabuľka č. 18: Použité rozšírenia v certifikáte na potvrdenie existencie a platnosti certifikátu (OCSP)

Názov rozšírenia	ASN.1 názov a OID / Popis	Prítomnosť?	Kritickosť?
authorityKeyIdentifier	{id-ce-authorityKeyIdentifier} {2.5.29.35} Identifikátor verejného kľúča certifikačnej autority CA, ktorá vydala tento certifikát.	Áno	Nie
subjectKeyIdentifier	{id-ce-subjectKeyIdentifier} {2.5.29.14} Identifikátor verejného kľúča Držiteľa certifikátu.	Áno	Nie
keyUsage	{id-ce-keyUsage} {2.5.29.15} Definuje účel súkromného kľúča, ktorého verejný kľúč je súčasťou tohto certifikátu.	Áno	Nie
certificatePolicies	id-ce-certificatePolicies} {2.5.29.32} Identifikuje certifikačné politiky, pod ktorými bol certifikát vydaný.	Áno	Nie
crlDistributionPoints	{id-ce-CRLDistributionPoints} {2.5.29.31} Určuje, akým spôsobom a odkiaľ je možné získať CRL.	Áno	Nie
AuthorityInfoAccess	{id-pe-authorityInfoAccess} {1.3.6.1.5.5.7.1.1} Určuje (http:// … p7c, certifikát alebo aj ldap://...) adresu na získanie certifikátov vydaných pre vydavateľa tohto certifikátu a adresu na OCSP.	Áno	Nie
Extended Key Usage	{2.5.29.37} Definuje ďalší možný účel použitia súkromného kľúča, ktorého verejný kľúč je súčasťou tohto certifikátu, ako doplnok alebo náhrada rozšírenia keyUsage. OCSP Signing (1.3.6.1.5.5.7.3.9)	Áno	Nie

7.2.5 Obmedzenia týkajúce sa mien

Žiadne ustanovenia.

7.2.6 Identifikátor certifikačnej politiky

Pozri kapitola 1.2.

7.2.7 Použitie rozšírení na obmedzenie politiky

Toto rozšírenie nie je používané.

7.2.8 Syntax a sémantika politiky

Každý KC vydaný v zmysle tejto politiky musí obsahovať jej identifikátor v podobe OID (pozri 1.2) v rozšírení id-ce-certificatePolicies (2.5.29.32).

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

Každý certifikát pre podpisovanie resp. certifikát na šifrovanie vydaný v zmysle tejto musí obsahovať jej identifikátor v podobe OID (pozri 1.2) v rozšírení id-ce-certificatePolicies (2.5.29.32).

7.2.9 Sémantika spracovania kritických certifikačných politík

Žiadne ustanovenia.

7.3 Profily zoznamu zrušených certifikátov

7.3.1 Verzia

CRL vydávané Poskytovateľom musia byť CRL verzie 2.

CRL musia byť vydávané tou istou CA Poskytovateľa ako CERTIFIKÁT.

Vydávané CRL musia byť v súlade s RFC 5280 „Internet X.509 Public Key Infrastructure Certificate and CRL Profile“ [7]

7.3.2 Použité rozšírenia (CRL extensions) v CRL

Tabuľka č. 19 obsahuje zoznam rozšírení uvádzaných v CRL vydávaných Poskytovateľom, povinnosť ich uvádzania a ich kritickosť.

Tabuľka č. 19: Rozšírenia vydávaného CRL

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

7.4 Profil OCSP

7.4.1 Verzia

V prípade, že Poskytovateľ vydáva OCSP odpovede, tieto musia byť v zmysle RFC 6960 „X.509 Internet Public Key Infrastructure Online Certificate Status Protocol – OCSP“ [8]. Ak budú OCSP odpovede pre jednotlivé certifikačné autority Poskytovateľa, ktoré vydávajú CERTIFIKÁTY, vydávané samostatnými OCSP

respondermi, ich podpisové certifikáty musia byť podpísané zodpovedajúcimi CA Poskytovateľa a musia obsahovať rozšírenie na použitie kľúča OCSP Signing (1.3.6.1.5.5.7.3.9).

7.4.2 OCSP rozšírenia

Tabuľka č. 20 obsahuje možné rozšírenia v OCSP odpovedi OCSP responderov Poskytovateľa, povinnosť ich uvádzania a ich kritickosť.

Tabuľka č. 20: Rozšírenia v OCSP odpovedi

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

* - toto rozšírenie je uvádzané len v odpovedi týkajúcej sa požiadavky na overenie stavu kvalifikovaného certifikátu

8. Audit zhody

8.1 Témy pokrývané auditom zhody

Účelom auditu je potvrdiť, že Poskytovateľ ako kvalifikovaný poskytovateľ dôveryhodných služieb a kvalifikované dôveryhodné služby, ktoré poskytuje, spĺňajú požiadavky stanovené v Nariadení eIDAS [1].

8.2 Frekvencia auditu zhody

Poskytovateľ sa musí aspoň každých 24 mesiacov podrobiť auditu ním poskytovaných kvalifikovaných dôveryhodných služieb.

8.3 Identita audítora a kvalifikačné požiadavky kladené na túto rolu

Orgán posudzovania zhody a nim poverené osoby na výkon auditu musí spĺňať požiadavky ETSI EN 319 403 „Electronic Signatures and Infrastructures (ESI); Trust Service Provider Conformity Assessment - Requirements for conformity assessment bodies assessing Trust Service Providers“ [9] minimálne vo verzii 2.2.2.

8.4 Vzťah audítora k Poskytovateľovi

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

8.5 Akcie vykonané na odstránenie nedostatkov

Keď audítor zistí rozpor medzi prevádzkou Poskytovateľa a platnými požiadavkami Nariadenia eIDAS alebo ustanoveniami CP a vydaných CPS, musia sa uskutočniť tieto akcie:

- rozpor musí byť zaznamenaný,
- audítor musí upovedomiť o rozpore subjekty definované v 8.6,
- PMA musí určiť vhodné opatrenie na nápravu.

8.6 Zaobchádzanie s výsledkami auditu

Orgán posudzovania zhody musí výsledky auditu predložiť v písomnej forme auditovanému subjektu, ktorý na ich základe musí prijať a vykonať potrebné nápravné opatrenia. Vykonanie opatrení na nápravu musí byť dané na vedomie orgánu posudzovania zhody.

Poskytovateľ je povinný predložiť výslednú správu o posúdení zhody orgánu dohľadu v lehote troch pracovných dní od jej doručenia.

9. Iné obchodné a právne záležitosti

9.1 Poplatky

Poplatky za kvalifikované dôveryhodné služby poskytované Poskytovateľom uhrádza Zákazník.

9.1.1 Poplatky za vydanie certifikátu

Poskytovateľ zverejňuje platný cenník svojich služieb prostredníctvom svojho webového sídla (pozri kapitola 1).

9.1.2 Poplatok za prístup k CERTIFIKÁTU

Žiadne ustanovenia

9.1.3 Poplatky za zrušenie alebo overenie statusu CERTIFIKÁTU

Poskytovateľ poskytuje službu zrušenia CERTIFIKÁTOV ako aj službu overenia statusu CERTIFIKÁTOV spočívajúcu vo vydávaní CRL a OCSP odpovede pre Spoliehajúce sa strany zadarmo.

9.1.4 Poplatky za ostatné služby

Poskytovateľ môže účtovať poplatky aj za ďalšie pridružené dôveryhodné služby požadované Zákazníkom v zmysle platného cenníka alebo na základe individuálnej dohody so Zákazníkom.

9.1.5 Vrátenie poplatku

Poskytovateľ môže v odôvodnených prípadoch na základe individuálneho posúdenia vrátiť platbu za poskytnuté služby Zákazníkovi.

9.2 Finančná zodpovednosť

Poskytovateľ musí mať dostatočné zdroje na výkon ním poskytovaných dôveryhodných služieb a/alebo získať vhodné poistenie zodpovednosti, aby zostal solventný a bol prípadne schopný nahradiť škodu v prípade súdneho rozhodnutia resp. uzavretia zmieru, v súvislosti s poskytovaním týchto služieb.

9.2.1 Poistenie zodpovednosti

Poskytovateľ musí byť poistený v súvislosti s možnými škodami, ktoré môžu byť spôsobené Držiteľom CERTIFIKÁTOV resp. tretím stranám v súvislosti s poskytovaním dôveryhodných služieb.

9.2.2 Iné aktíva

Žiadne ustanovenia.

9.2.3 Poistenie a záruky pre koncových používateľov

Žiadne ustanovenia.

9.3 Dôvernosť obchodných informácií

Poskytovateľ ako aj Zákazník sú povinní pristupovať k údajom získaným v súvislosti s poskytovanými kvalifikovanými dôveryhodnými službami v súlade s príslušnými právnymi predpismi.

9.3.1 Dôverné informácie

Dôvernými informáciami podliehajúcimi zodpovedajúcej ochrane sú:

- súkromný kľúč Poskytovateľa používaný na podpisovanie vydávaných CERTIFIKÁTOV,
- súkromný kľúč OCSP respondera, používaný na podpisovanie odpovedí na požiadavky na potvrdenie existencie a platnosti CERTIFIKÁTOV,
- súkromné kľúče patriace k služobným certifikátom (napr. certifikáty patriace pracovníkom RA a pod.),
- interná infraštruktúra (napr. dokumenty, postupy, súbory, skripty, heslá, pass frázy a pod.) slúžiaca na prevádzku Poskytovateľa, vrátane jej RA,
- osobné údaje Držiteľov CERTIFIKÁTOV podliehajúce ochrane v zmysle Predpisov o ochrane osobných údajov [5],

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

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

9.3.2 Informácie nepovažované za dôverné

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

- sú v dobe ich prijatia druhou stranou verejne dostupnými alebo sa takými stanú následne bez toho, aby druhá strana porušila povinnosti podľa tejto CP, alebo
- boli druhej strane známe ich sprístupnením v súvislosti s poskytovanými dôveryhodnými službami, alebo
- boli druhou stranou preukázateľne získané od tretej osoby, ktorá je preukázateľne oprávnená šíriť takéto informácie, alebo

- boli druhou stranou nezávisle vyvinuté bez toho, aby došlo k neoprávnenej manipulácii s dôvernými informáciami alebo
- sú všeobecne známe aj napriek ich označeniu druhou stranou ako dôverné.

9.3.3 Zodpovednosť za ochranu dôverných informácií

Zákazník ako aj Poskytovateľ sú v prípade získania dôverných informácií alebo prístupu k nim, povinní chrániť ich pred prezradením a zdržať sa ich použitia alebo poskytnutia/prezradenia tretej strane.

V prípade, ak by mali byť tretej strane v rámci výkonu jej činnosti pre Poskytovateľa poskytnuté alebo sprístupnené dôverné informácie, Poskytovateľ uzatvorí s touto treťou stranou zmluvu o mlčanlivosti, resp. zmluvu o poskytnutí dôverných informácii, ktorej obsahom sú aj vyššie uvedené povinnosti.

Poskytovateľ môže za určitých okolností poskytnúť určité dôverné informácie tretej strane, najmä v prípade:

- povinného poskytnutia informácii orgánu dozoru,
- povinného poskytnutia informácii v trestnom konaní, občianskom súdnom konaní alebo správnom konaní,
- poskytnutia informácii na požiadanie dotknutej osoby.

9.4 Ochrana osobných údajov a súkromia

9.4.1 Politika ochrany osobných údajov

Poskytovateľ musí pri spracovaní osobných údajov dodržiavať požiadavky Predpisov o ochrane osobných údajov. [5]

Poskytovateľ zabezpečí dôvernosť a integritu osobných údajov získaných v rámci procesu vydávania CERTIFIKÁTU, a to aj v prípade ich prenosu medzi Poskytovateľom a Zákazníkom či medzi jednotlivými komponentmi systému Poskytovateľa.

Niektoré osobné údaje bude Poskytovateľ uchovávať, aby splnil svoje zákonné povinnosti a aby zabezpečil chod svojich podnikateľských aktivít.

9.4.2 Informácie považované za súkromné

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

9.4.3 Informácie, ktoré nie sú považované za súkromné

Poskytovateľ môže v súlade s Predpismi na ochranu osobných údajov [5] definovať typy informácií, ktoré spracováva pri poskytovaní dôveryhodných a kvalifikovaných dôveryhodných služieb a nie sú považované za osobné údaje.

Poskytovateľ môže na základe písomného súhlasu Držiteľa certifikátu na svojom webovom sídle zverejniť alebo sprístupniť informáciu o vydaní CERTIFIKÁTU s menom jeho Držiteľa.

9.4.4 Zodpovednosť za ochranu osobných údajov

Poskytovateľ bude bezpečne uchovávať a ochraňovať osobné údaje spracúvané v súvislosti s vydávaním CERTIFIKÁTU. Tieto údaje bude chrániť prijatím vhodných bezpečnostných opatrení, a to najmä pred neautorizovaným prístupom, zmenou alebo prezradením.

9.4.5 Informačná povinnosť a súhlas

Poskytovateľ je povinný pri plnení informačnej povinnosti voči dotknutým osobám a pri získavaní ich súhlasu so spracovaním osobných údajov postupovať v súlade s Predpismi na ochranu osobných údajov. [5]

9.5 Ochrana práv duševného vlastníctva

Poskytovateľ je nositeľom autorských práv k všetkým dokumentom, databázam, postupom, politikám, poriadkom, pravidlám, CERTIFIKÁTOM a súkromným kľúčom, ktoré sú súčasťou infraštruktúry Poskytovateľa a ktoré boli vytvorené Poskytovateľom.

9.6 Vyhlásenie a záruky

Poskytovateľ prostredníctvom tejto CP a Potvrdenia o prevzatí certifikátov na eID vyjadruje právne predpoklady používania vydaných CERTIFIKÁTOV ich Držiteľmi a Spoliehajúcimi sa stranami.

9.6.1 Vyhlásenia a záruky Poskytovateľa

Pokiaľ ide o poskytované dôveryhodné služby Poskytovateľ neposkytuje žiadne vyhlásenia ani záruky s výnimkou prípadov uvedených v tejto CP a nadväzujúcich CPS.

Poskytovateľ si vyhradzuje právo, ak to uzná za vhodné, na zmenu týchto vyhlásení a to na základe vlastného uváženia alebo v súlade s platnou legislatívou.

Poskytovateľ v rozsahu stanovenom v jednotlivých častiach tejto CP resp. vydaných CPS deklaruje:

- dodržiavanie svojich povinností v zmysle tejto CP, vydaných CPS ako aj ďalších publikovaných politík a postupov, vrátane politiky informačnej bezpečnosti,

- plnenie svojich povinností v zmysle platnej legislatívy SR a Nariadenia eIDAS,
- zavedenie bezpečnostných mechanizmov, vrátane mechanizmov pri generovaní a ochrane súkromného kľúča, týkajúcich sa ochrany svojej PKI infraštruktúry,
- okamžité informovanie dotknutých subjektov v prípade kompromitácie svojich súkromných kľúčov v súlade s touto CP,
- dostupnosť tlačenej resp. elektronickej verzie tejto CP a ďalších publikovaných politík online,
- správnosť informácii nachádzajúcich sa vo vydávaných CERTIFIKÁTOCH podľa najlepšieho vedomia Poskytovateľa a súlad vydaných CERTIFIKÁTOV s požiadavkami Nariadenia eIDAS,
- skutočnosť, že Držiteľ je vlastníkom súkromného kľúča v čase vydávania CERTIFIKÁTU v zmysle tejto CP,
- dodržiavanie Predpisov na ochranu osobných údajov [5] pri zaobchádzaní s osobnými údajmi Držiteľov.

9.6.2 Vyhlásenia a záruky RA

Registračné autority poskytujúce dôveryhodné a kvalifikované dôveryhodné služby Poskytovateľa na základe zmluvného vzťahu deklarujú, že:

- ich aktivity sú vykonávané s použitím vhodného hardvérového vybavenia a softvéru odporúčaného Poskytovateľom,
- vynaložia maximálnu snahu na zabezpečenie toho, že identifikačné údaje Držiteľa CERTIFIKÁTU uložené v IS Poskytovateľa budú správne a potvrdené v čase ich zadania,
- ich služby sú poskytované na základe postupov, ktoré sú prispôsobené tejto CP a CPS vydaným pre potreby RA,
- budú chrániť osobné údaje Držiteľov certifikátov v zmysle požiadaviek Predpisov na ochranu osobných údajov [5],
- súkromné kľúče pracovníkov RA budú používané v súlade s bezpečnostnými požiadavkami špecifikovanými Poskytovateľom,
- umožnia Poskytovateľovi prístup do svojich priestorov za účelom overenia, čí sú všetky postupy RA vykonávané v súlade s touto CP resp. ďalšími relevantnými požiadavkami.

9.6.3 Vyhlásenie a záruky Držiteľa

Ak nie je v tejto CP alebo príslušnej zmluve so Zákazníkom/Držiteľom uvedené inak, Držiteľ je výlučne zodpovedný za:

- poskytnutie správnych a presných informácií v komunikácii s Poskytovateľom,
- oboznámenie sa a súhlas so všetkými podmienkami danými v tejto CP a s ňou spojenými politikami, ktoré sú dostupné v úložisku Poskytovateľa (pozri kapitola 1),

- používanie vydaných CERTIFIKÁTOV len na účely, na ktoré sú určené a v súlade s touto CP,
- ukončenie používania CERTIFIKÁTU, pokiaľ sa ukáže, že akákoľvek informácia v nich je zavádzajúca, neaktuálna alebo nesprávna,
- vyvinutie maximálneho úsilia na zabránenie kompromitácie, straty, odtajnenie, modifikácie alebo akéhokoľvek neautorizovaného použitia súkromného kľúča zodpovedajúceho verejnému kľúču, ktorý sa nachádza v CERTIFIKÁTE vydanom Poskytovateľom.

9.6.4 Vyhlásenia a záruky Spoliehajúcej sa strany

Spoliehajúca sa strana akceptuje, že v prípade spoliehania sa na CERTIFIKÁT vydaný Poskytovateľom sa musí:

- oboznámiť sa a súhlasiť s podmienkami Poskytovateľa uvedenými v informácii pre Spoliehajúce sa strany, ktorá je dostupná na webovom sídle Poskytovateľa (pozri kapitola 1) resp. stránke: https://www.slovensko.sk/sk/obciansky-preukaz-s-cipom/_obciansky-preukaz-s-cipom1
- overiť platnosť vydaného CERTIFIKÁTU prostredníctvom informácií na overenie stavu certifikátu (CRL, OCSP),
- akceptovať CERTIFIKÁT len v prípade, že je platný a nebol zrušený alebo exspirovaný,
- dôverovať certifikátu vydávajúcej CA Poskytovateľa len v prípade, že je platný a nebol zrušený alebo nie je exspirovaný,
- mať na pamäti akékoľvek obmedzenie použitia CERTIFIKÁTU, či už je obsiahnuté v samotnom CERTIFIKÁTE alebo v tejto CP resp. publikovaných CPS,
- prijať akékoľvek iné kroky na minimalizáciu rizika pri spoľahnutí sa na elektronický podpis alebo elektronickú pečať vytvorenú prostredníctvom kľúčov, kde verejný kľúč je neplatný, zrušený, exspirovaný,
- vziať do úvahy akékoľvek iné indície dôveryhodnosti resp. nedôveryhodnosti, alebo iné fakty, s ktorými je Spoliehajúca sa strana oboznámená alebo bola na tieto upozornená.

9.6.5 Vyhlásenia a záruky iných strán

Žiadne ustanovenia.

9.7 Odmietnutie poskytnutia záruky

Poskytovateľ zodpovedá v zmysle čl. 13 Nariadenia eIDAS za škodu spôsobenú nesplnením svojich povinností podľa Nariadenia eIDAS.

9.8 Obmedzenie zodpovednosti

Poskytovateľ nezodpovedá za nepriame alebo podmienené straty alebo škody, ktoré Zákazníkom alebo Spoliehajúcim sa stranám vznikli v súvislosti s používaním dôveryhodných služieb.

Poskytovateľ nezodpovedá za škodu (vrátane ušlého zisku), ktorá vznikla Zákazníkovi/Držiteľovi CERTIFIKÁTU, Spoliehajúcej sa strane príp. akýmkoľvek tretím stranám z dôvodu:

- porušenia povinností Zákazníkom/Držiteľom CERTIFIKÁTU alebo Spoliehajúcou sa stranou uvedených v právnych predpisoch, zmluve, Všeobecných podmienkach [4] alebo v politikách Poskytovateľa, vrátane povinnosti vynaložiť primeranú starostlivosť pri používaní CERTIFIKÁTOV a pri spoliehaní sa na ne,
- neposkytnutia potrebnej súčinnosti zo strany Zákazníka/Držiteľa CERTIFIKÁTU,
- technickými vlastnosťami, konfiguráciou, nekompatibilitou, nevhodnosťou alebo inými vadami nimi použitých softvérových alebo hardvérových prostriedkov,
- používania, resp. spoliehania sa na CERTIFIKÁT, ktorého platnosť uplynula alebo ktorý bol zrušený,
- použitia CERTIFIKÁTU Zákazníkom/Držiteľom CERTIFIKÁTU v rozpore so zmluvou, Všeobecnými podmienkami [4] alebo politikami Poskytovateľa,
- že CERTIFIKÁT bol použitý v rozpore s jeho účelom, určením alebo obmedzeniami uvedenými v CERTIFIKÁTE v tejto CP alebo vo Všeobecných podmienkach [4] Poskytovateľa,
- omeškania alebo nedoručenia požiadaviek na overenie statusu CERTIFIKÁTU Poskytovateľovi, z dôvodov, ktoré nie sú na strane Poskytovateľa (najmä prípady nedostupnosti alebo preťaženosti siete internet alebo vady zariadenia alebo technického vybavenia používaného overovateľom),
- neposkytnutia niektorej z dôveryhodných služieb alebo jej nedostupnosti v priebehu plánovanej údržby alebo reorganizácie oznámenej na webovom sídle Poskytovateľa,
- pôsobenia vyššej moci.

Poskytovateľ nezodpovedá za škody, ktoré vznikli Spoliehajúcej sa strane z dôvodu, že pri spoliehaní sa na CERTIFIKÁT a dôveryhodné služby Poskytovateľa, resp. na elektronický podpis resp. kvalifikovaný elektronický podpis vyhotovené na ich základe nepostupovala podľa 10. časti Všeobecných podmienok [4] a v zmysle tejto CP.

9.9 Náhrada škody

Kto poruší svoju povinnosť alebo akýkoľvek záväzok, vyplývajúci z tejto CP, Zmluvy a Všeobecných podmienok [4] je povinný nahradiť škodu tým spôsobenú druhej

strane, okrem prípadov kde je vylúčená zodpovednosť daného subjektu za škody. Za škodu sa považuje skutočná škoda, ušlý zisk a náklady vzniknuté poškodenej strane v súvislosti so škodovou udalosťou.

Kto poruší svoju povinnosť alebo akýkoľvek záväzok, vyplývajúci z tejto CP, Zmluvy a Všeobecných podmienok [4], sa môže zbaviť zodpovednosti na náhradu škody, jedine ak preukáže, že k porušeniu povinnosti alebo akéhokoľvek záväzku, došlo v dôsledku okolností vylučujúcich zodpovednosť – vyššej moci.

9.10 Doba platnosti, ukončenie platnosti

9.10.1 Doba platnosti

Tato verzia CP platí odo dňa nadobudnutia jej platnosti t. j. 29. 11. 2022 až do jej nahradenia novou verziou. Podrobnosti o histórii zmien tejto CP sú uvedené na konci dokumentu v časti „História zmien“.

9.10.2 Ukončenie platnosti

Platnosť tejto verzie CP skončí dňom publikovania novej verzie s vyšším číslom ako je 1.8, prípadne ukončením činnosti poskytovania dôveryhodných služieb Poskytovateľom v čase jej platnosti.

9.10.3 Dôsledky ukončenia platnosti

V prípade, že tento dokument nebude nahradený novou verziou a v čase jeho platnosti dôjde k ukončeniu poskytovania dôveryhodných služieb zo strany Poskytovateľa, musia byť dodržané všetky ustanovenia tejto CP týkajúce sa Poskytovateľa, ktoré je povinný dodržať po ukončení svojej činnosti (pozri kapitola 9).

9.11 Jednotlivé oznámenia a komunikácia s účastníkmi

Komunikácia Poskytovateľa s jednotlivých RA musí prebiehať oficiálne prostredníctvom autorizovanej e-mailovej komunikácie medzi poverenou osobou Poskytovateľa a poverenou osobou RA.

9.12 Zmeny

9.12.1 Postup vykonávania zmien

Aktualizácia CP sa vykonáva na základe jeho preskúmania, ktoré musí byť vykonané minimálne 1x ročne od schválenia aktuálne platnej verzie. Preskúmanie musí vykonať poverený pracovník Poskytovateľa, ktorý na základe výsledkov preskúmania musí spracovať písomný návrh na prípadné navrhované zmeny.

Schválenie navrhovaných zmien musí vykonať poverený člen PMA. Navrhované zmeny musia byť posúdené v lehote 14 dní od ich doručenia. Po uplynutí lehoty určenej na posúdenie návrhu na zmenu musí PMA navrhovanú zmenu prijať, prijať s úpravou alebo odmietnuť.

Chyby, požiadavky na aktualizáciu alebo navrhované zmeny CP sa musia oznámiť kontaktu uvedenému v 1.5.2. Takáto komunikácia musí obsahovať opis zmeny, zdôvodnenie zmeny a kontaktné údaje osoby, ktorá zmenu požaduje resp. navrhuje.

Všetky schválené zmeny CP musia byť dané na vedomie subjektom, ktorých sa týkajú, v lehote jedného týždňa pred nadobudnutím ich účinnosti, a to prostredníctvom kanálov publikačnej a oznamovacej politiky (pozri 2.2).

Každá zmenená verzia tejto CP musí byť očíslovaná a evidovaná, tak že novšia verzia musí mať vyššie číslo verzie ako tá, ktorú nahradzuje .

Opravy preklepov, gramatických a štylistických chýb sa nepovažujú za zmeny iniciujúce zmenu verzie tejto CP.

9.12.2 Postup a periodicita oznamovania zmien

Poskytovateľ musí publikovať informácie týkajúce sa aktuálnej verzie CP prostredníctvom svojho webového sídla (pozri kapitola 1).

Poverený zástupca Poskytovateľa musí informovať všetky zmluvne viazané RA Poskytovateľa o schválení novej verzie CP, zaslaním jeho verzie elektronickou poštou ešte pred nadobudnutím jeho účinnosti v zmysle časti 9.12.1. Poskytovateľ si musí vyžiadať od RA spätnú väzbu v podobe potvrdzujúcej e-mailovej správy o prevzatí elektronickej verzie CP Poskytovateľa.

9.12.3 Okolnosti zmeny OID

Každá politika musí mať stanovený svoj OID Poskytovateľom. OID tejto politiky je uvedený v časti 1.2 a pre každú novú verziu CP zostáva nezmenený.

9.13 Riešenie sporov

Zákazník/Držiteľ má právo zaslať Poskytovateľovi sťažnosť, podnet alebo reklamáciu na poskytnutú kvalifikovanú dôveryhodnú služby emailom na eid_podpora@disig.sk. Poskytovateľ vybaví reklamáciu najneskôr do 30 dní od jej prijatia, pokiaľ sa strany nedohodnú inak. Vybavenie reklamácie sa vzťahuje len k popisu vady uvedenej Zákazníkom.

Súdy Slovenskej republiky majú výlučnú právomoc na rozhodovanie akýchkoľvek sporov medzi Poskytovateľom a Zákazníkom/Držiteľom certifikátu. V prípade, že Zákazník/Držiteľ certifikátu je spotrebiteľom, prípadný spor môže riešiť taktiež mimosúdnou cestou. V takomto prípade je oprávnený kontaktovať subjekt mimosúdneho riešenia sporov, ktorým je Slovenská obchodná inšpekcia alebo iná právnická osoba zapísaná v zozname subjektov alternatívneho riešenia spotrebiteľských sporov vedenom Ministerstvom hospodárstva Slovenskej republiky a dostupnom na jeho webovom sídle; Zákazník/Držiteľ má právo voľby, na ktorý z uvedených subjektov alternatívneho riešenia spotrebiteľských sporov sa obráti. Pred pristúpením k súdnemu alebo mimosúdnemu riešeniu sporu sú zmluvné strany povinné pokúsiť sa najskôr vyriešiť tento spor vzájomnou dohodou.

9.14 Rozhodné právo

Právne vzťahy medzi Poskytovateľom a Zákazníkom/Držiteľom certifikátu sa riadia právnymi predpismi Slovenskej republiky.

Práva a povinnosti zmluvných strán výslovne neupravené Všeobecnými podmienkami [4] a touto CP sa riadia najmä príslušnými ustanoveniami zákona č. 513/1991 Zb., Obchodný zákonník, v znení neskorších predpisov, zákona č. 40/1964 Zb., Občiansky zákonník v znení neskorších predpisov a ďalšími všeobecne záväznými právnymi predpismi Slovenskej republiky.

9.15 Súlad s platnými právnymi predpismi

Poskytovateľ poskytuje dôveryhodné služby v súlade s platnými právnymi predpismi platnými v Slovenskej republike.

9.16 Rôzne ustanovenia

9.16.1 Rámcová dohoda

Žiadne ustanovenia.

9.16.2 Postúpenie práv

Zákazník/Držiteľ nesmie svoje práva, povinnosti ako aj pohľadávky z tejto CP, Zmluvy alebo Všeobecných podmienok [4] postúpiť alebo previesť (ani s nimi akokoľvek inak obchodovať) tretej osobe bez písomného súhlasu Poskytovateľa.

9.16.3 Salvatórska klauzula

Pokiaľ akékoľvek ustanovenie tejto CP je alebo sa stane neplatným alebo nevymáhateľným, nespôsobí to neplatnosť alebo nevymáhateľnosť celej CP, ak je úplne oddeliteľným od ostatných ustanovení tejto CP. Poskytovateľ bezodkladne nahradí neplatné alebo nevymáhateľné ustanovenie CP novým platným a vymáhateľným ustanovením, ktorého predmet bude v najvyššej možnej miere zodpovedať predmetu pôvodného ustanovenia a zároveň bude zachovaný účel tejto CP a obsah jednotlivých ustanovení tejto CP.

9.16.4 Uplatnenie práv

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

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

9.16.5 Vyššia moc

Poskytovateľ, Zákazník a Držiteľ nie sú zodpovední za omeškanie so splnením svojich záväzkov spôsobené okolnosťami vylučujúcimi zodpovednosť (vyššou mocou).

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

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

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

9.17 Iné ustanovenia

Žiadne ustanovenia.

10. Odkazy

1. Nariadenie Európskeho parlamentu a Rady (EÚ) č. 910/2014 z 23. júla 2014 o elektronickej identifikácii a dôveryhodných službách pre elektronické transakcie na vnútornom trhu a o zrušení smernice 1999/93/ES. s.l. : Úradný vestník Európskej únie, 28.8.2014. Zv. L 257/73.

2. Zákon č. 272/2016 Z. z. o dôveryhodných službách pre elektronické transakcie na vnútornom trhu a o zmene a doplnení niektorých zákonov (zákon o dôveryhodných službách). s.l. : Zbierka zákonov Slovenskej republiky, 18.10.2016.

3. Certifikačná politika pre koreňovú CA a dôveryhodnú službu vyhotovovania kvalifikovaných certifikátov, ktorej kvalifikovaný štatút udelil Národný bezpečnostný úrad. s.l. : Národný bezpečnostný úrad.

4. Všeobecné podmienky poskytovania a používania dôveryhodnej služby vydávania a overovania certifikátov na eID.

5. Nariadenie Európskeho Parlamentu a Rady (EÚ) 2016/679 o ochrane fyzických osôb pri spracúvaní osobných údajov a o voľnom pohybe takýchto údajov a zákon č. 18/2018 Z. z. o ochrane osobných údajov.

6. ETSI EN 319411-2 " Electronic Signatures and Infrastructures (ESI); Policy and security requirements for Trust Service Providers issuing certificates; Part 2: Requirements for trust service providers issuing EU qualified certificates.

7. RFC 5280 "Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile".

8. RFC 6960 „X.509 Internet Public Key Infrastructure Online Certificate Status Protocol – OCSP“.

9. „Electronic Signatures and Infrastructures (ESI); Trust Service Provider Conformity Assessment - Requirements for conformity assessment bodies assessing Trust Service Providers.

História zmien

Verzia	Dátum revízie	Popis revízie; revidoval
1.0	25.11.2013	Prvá verzia dokumentu; Miškovič
1.1	31.12.2014	Zmena vo formáte vydávaného KC (7.1.2); Miškovič
1.2	18.10.2016	Vykonané zmeny v súvislosti s Nariadením eIDAS a v súvislosti s ukončením platnosti zákona č. 215/2002 Z. z. a nadobudnutím účinnosti zákona č. 272/2016 Z. z.; Miškovič
1.3	18.4.2017	Revízia dokumentu a úprava obsahu v zmysle RFC 3647; Miškovič, Vydrová
1.4	27.10.2017	Zmena dĺžky kľúčov a platnosti vydávaných CERTIFIKÁTOV na eID a s tým súvisiace úpravy; Miškovič
1.5	25.5.2018	Nadobudnutie účinnosti Nariadenia č. 2016/679 – GDPR; Miškovič
1.6	1. 9. 2020	Úprava znenia kapitoly1.4.1; Úprava obsahu tabuliek v kapitole 7; Miškovič
1.7	16. 6. 2021	Doplnenie novej vydávajúcej SVK eID ACA2 (1.1, 1.5.2); Spresnenie vydania následného certifikátu (4.7.1); Doplnenie okolnosti zrušenia certifikátu (4.9.1); Spresnenie zmeny kľúčov CA (5.6); Miškovič
1.8	29. 11. 2022	Doplnenie možnosti vydávania KC aj na zariadenie, ktoré nie je kvalifikovaným zariadením pre elektronický podpis v zmysle požiadaviek nariadenia eIDAS (1.4.1; 7.1.1.1;) ; spresnenie kapitoly o spôsobe preberania CERTIFIKÁTU (4.4.1); úprava tabuľku s platnosťami vydávaných certifikátov (6.3.2;); Miškovič