Pravidlá

poskytovania dôveryhodnej služby
vyhotovovania a overovania certifikátov -
časť: RA

Disig, a.s.

Vypracoval	**Ing. Peter Miškovič**
Dátum platnosti	1. 9. 2023
Verzia	5.9
Typ	PRAVIDLÁ
Schválil	**Ing. Ľuboš Batěk**

Obsah

Obchodné meno	Disig, a.s.
Sídlo	Záhradnícka 151, 821 08 Bratislava
Zapísaná v OR	OR Mestského súdu Bratislava III, odd. Sa 3794/B
Telefón	+ 421 2 208 50 140
Fax	+ 421 2 208 50 141
E-mail	disig@disig.sk

Tento dokument neprešiel jazykovou úpravou.

1. Úvod

Tento dokument definuje pravidlá poskytovania dôveryhodnej služby vyhotovovania a overovania certifikátov - časť: RA (Certificate Practice Statement, ďalej len „CPS“) pre registračné autority (ďalej len „RA“) spoločnosti Disig ako poskytovateľa dôveryhodných služieb (ďalej len „Poskytovateľ“). CPS vychádzajú z dokumentu „Politika poskytovania dôveryhodnej služby vyhotovovania a overovania certifikátov“ (OID=1.3.158.35975946.0.0.0.1.1) [1] Poskytovateľa (ďalej len „CP CA Disig“). Aktuálna verzia CP CA Disig, na ktorú sa viažu tieto CPS je verzia 5.9 s platnosťou od 1. 9. 2023.

Webové sídlo Poskytovateľa k poskytovaným dôveryhodným službám je dostupné na adrese:

http://eidas.disig.sk

1.1 Prehľad

CPS boli vytvorené na základe materiálov Internet X.509 Public Key Infrastructure - Certificate Policy and Certification Practices Framework (RFC3647) [2]; Internet X.509 Public Key Infrastructure - Certificate and Certificate Revocation List (CRL) Profile (RFC5280) [3], Baseline Requirements for the Issuance and Management of Publicly-Trusted Certificates [4] a Nariadenie Európskeho parlamentu a Rady EU č. 910/2014 [5].

Poskytovateľ potvrdzuje, že v týchto CPS sú zohľadnené všetky požiadavky aktuálnej verzie dokumentu [4], ktorý je publikovaný na stránke http://www.cabforum.org. V prípade akýchkoľvek rozporuplností medzi týmito požiadavkami a týmito CPS, majú prednosť požiadavky dané aktuálnou verziou dokumentu [4].

Tieto pravidlá sú štruktúrované v súlade s RFC 3647 [2].

1.2 Identifikácia

Názov:	Pravidlá **Poskytovania dôveryhodnej služby** vyhotovovania a overovania certifikátov - **časť: RA**
Skratka názvu:	CPS RA CA Disig
Verzia:	5.9
Schválené dňa:	25. 8. 2023
Platnosť od:	1. 9. 2023
Tomuto dokumentu je priradený identifikátor objektu (OID):	1.3.158.35975946.0.0.0.1.3

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, a. s.

1.3.158.35975946.0.0.0.1.– CA Disig

1.3.158.35975946.0.0.0.1.3. – CPS RA CA Disig

Tieto CPS sa týkajú certifikátov pre fyzickú osobu, certifikátov pre právnickú osobu a verejne dôveryhodných certifikátov pre autentizáciu webového sídla (TLS certifikát) vydávaných Poskytovateľom. Ostatné typy certifikátov sú popísané v samostatných CPS.

Pojmom certifikát resp. certifikát Poskytovateľa sa v tomto dokumente označuje ľubovoľný z vyššie uvedených certifikátov vydaný Poskytovateľom.

1.2.1 História zmien

Verzia	Dátum revízie	Popis revízie; revidoval
1.0	25.03.2006	Prvá verzia dokumentu; Mišković
1.5	20.12.2006	Formálne úpravy textu dokumentu – formátovanie, opravy odkazov, úpravy textu v kapitole 4 „Prevádzkové požiadavky“; Mišković
3.0	19.03.2008	Celková revízia CP vzhľadom k jednotlivým typom certifikátov; Ďurišová, Mišković.
3.1	24.06.2008	Pridanie nového typu certifikátu; Mišković
3.2	10.11.2008	Zrušenie prevádzky na Záhradníckej 153.
3.3	25.11.2008	Úprava znenia: ods. 3.1.9 - overovanie vlastníctva domény ods. 4.1.1, 4.1.2, - overovanie platnosti e-mail adresy žiadateľa
3.4	02.06.2009	Úprava v súvislosti s požiadavkou na minimálnu dĺžku verejného kľúča, na ktorý CA Disig vydá certifikát (ods.5.1.3; 6.1.2); Zmena umiestnenia e-mail adresy v profile certifikátu (ods. 3.1.2; 6.1.2); Mišković
4.0	14.10.2009	Úprava v súvislosti s požiadavkami Mozilla Foundation pri uchádzaní sa o umiestnenie certifikátu CA Disig do Mozilla Root Certificate Store
4.1	11.05.2010	Zapracovanie navrhnutých nápravných opatrení z auditu zo dňa 13.11.2009 (audit podľa ETSI TS 102042 V1.3.4); Mišković
4.2	11.03.2011	Zmena dĺžky platnosti certifikátov; zapracovanie požiadaviek novej bezpečnostnej politiky Mozilla Foundation a

		požiadaviek Microsoft (code signing); formálne úpravy tabuliek a textov; Miškovič
4.3	25.01.2012	Doplnenie možnosti vydávania podriadených CA a pravidelná ročná revízia obsahu; Miškovič
4.4	22.06.2012	Zapracovanie požiadaviek dokumentu „Baseline Requirements for the Issuance and Management of Publicly-Trusted Certificates, v.1.0, ktorý vydala CA/Browser Forum; Miškovič
4.5	15.08.2012	Spresnenie profilu certifikátov koreňových certifikačných autorít CA Disig a ostatných vydávaných typov certifikátov; Miškovič
4.6	21.06.2013	Spresnenie OID dokumentu – vypustenie verzie dokumentu z OID (kap. 1.2); drobné úpravy textov v kapitole 3.1.9; Miškovič
4.7	16.03.2015	Zapracovanie požiadaviek aktuálnej verzie dokumentu „Baseline Requirements for the Issuance and Management of Publicly-Trusted Certificates, v.1.2.3; Zmena certifikátu vydávaného právnickej osobe na systémový certifikát pre elektronický pečať (3.1.2); Miškovič
4.8	22.05.2015	Overovanie CAA záznamov (4.1.3)
4.9	21.11.2016	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.; Zmeny v profiloch vydávaných certifikátov; Zapracovanie požiadaviek Baseline Requirements for the Issuance and Management of Publicly-Trusted Certificates, do verzie 1.4.1; Miškovič
5.0	25.9.2017	Konverzia CP do formátu v zmysle RFC 3647; Zapracovanie požiadaviek nariadenia eIDAS [5] a zapracovanie požiadaviek aktuálnej verzie Baseline Requirements for the Issuance and Management of Publicly-Trusted Certificates, v.1.5.2; Miškovič
5.1	23.5.2018	Nadobudnutie účinnosti Nariadenia č. 2016/679 – GDPR; Zmena znenia bodu 3.2.2.4 (nový spôsob overenia); doplnenie kapitoly 4.2.2 (gTLD); Miškovič
5.2	17.5.2019	Revízia dokumentu a modifikácia v zmysle požiadaviek [4], zmeny v bodoch 4.9.3; 5; 5.2; 5.3;5.4 and 5.5; Miškovič
5.3	2.12.2019	Revízia dokumentu; Zmena názvov dokumentov súvisiacich s vydávaním certifikátov (4.2.1.2); Miškovič
5.4	1.9.2020	Spresnenie overovania vlastníctva domény 4.2.2.4); Aktualizácia odkazov (1.6.3); Miškovič

5.5	20.5.2021	Doplnenie zodpovednej osoby za hlásenie incidentov (2.2); Miškovič
5.6	18.6.2021	Aktualizácia znenia časti 3.2.2.4; Miškovič
5.7	20.5.2022	Zmena označenia typu certifikátu TLS/SSL na TLS; Doplnenie a úpravy v časti 5.4 týkajúce sa uchovávania záznamov; Miškovič
5.8	1. 10. 2022	Zmena v súvislosti s požiadavkou zverejnenia dôvodu zrušenia v CRL pri zrušení vydaných TLS certifikátov (4.9.3); Miškovič
5.9	1. 9. 2023	Zmeny v súvislosti s nadobudnutím účinnosti „Baseline Requirements for the Issuance and Management of Publicly-Trusted S/MIME Certificates“; Miškovič

1.3 **Komunita a použiteľnosť**

1.3.1 **Certifikačn**é autority

Tieto CPS sa týkajú poskytovania dôveryhodných služieb podriadenými certifikačnými autoritami patriacich pod koreňové certifikačné autority CA Disig Root R2 – pozri časť 1.4.1 aktuálnej verzie CP CA Disig.

1.3.2 **Registračné autority**

Zložkou Poskytovateľa, o ktorej detailne pojednávajú tieto pravidlá sú:

- Komerčná registračná autorita
- Interná registračná autorita

Pokiaľ sú vytvárané registračné autority na základe písomnej zmluvy s obchodným partnerom a tento bude prevádzkovať vlastné registračné autority, pre takýto typ budú vydávané samostatné CPS danej registračnej autority.

Spoločný termín pre CA a RA je autority na správu certifikátov (Certificate Management Authority, ďalej len „CMA“). Termín CMA sa bude používať, keď funkciu možno priradiť buď CA alebo RA, prípadne keď sa požiadavka týka súčasne CA aj RA.

1.3.3 Zákazník a **Držiteľ certifikátu**

Pozri časť 1.3.3 CP CA Disig.

1.3.4 Strany spoliehajúce sa na certifikáty

Pozri časť 1.3.4 CP CA Disig.

1.3.5 **Iní účastníci**

Pozri časť 1.3.5 CP CA Disig

1.4 **Použiteľnosť** certifikátov

1.4.1 **Vhodné použitie certifikátov**

Pozri časť 1.4.1 CP CA Disig.

1.4.2 **Nedovolené použitie certifikátov**

Pozri časť 1.4.2 CP CA Disig.

1.5 Správa pravidiel

1.5.1 Organizácia zodpovedná za správu pravidiel

Poskytovateľ	
Spoločnosť:	Disig, a.s.
Adresa sídla:	Záhradnícka 151, 821 08 Bratislava 2
IČO:	359 75 946
telefón	+421 2 20850140
fax:	+421 2 20828141
e-mail:	disig@disig.sk
webové sídlo:	http://www.disig.sk

1.5.2 Kontaktná osoba

Kontaktná osoba zodpovedná za prevádzku registračných autorít Poskytovateľa je:

Registračná autorita	
Adresa:	Záhradnícka 151, 821 08 Bratislava 2
e-mail:	radisig@disig.sk
telefón	+421 2 20850140
fax:	+421 2 20850141
webové sídlo:	http://eidas.disig.sk/
oznamovanie incidentov	tspnotify@disig.sk viac pozri: https://eidas.disig.sk/pdf/incident_reporting.pdf

Zoznam ostatných registračných autorít Poskytovateľa je dostupný na jeho webovom sídle na adrese: https://eidas.disig.sk/sk/kontakt/registracne-autority/.

1.5.3 Osoba rozhodujúca o súlade CPS s CP

Pozri časť 1.5.3 CP CA Disig.

1.5.4 **Postupy schvaľo**vania CPS a externej politiky

Tieto CPS sú schválené osobou, ktorá je menovaná do role PMA.

CPS sú publikovaný v súlade s publikačnou a oznamovacou politikou na webovom sídle Poskytovateľa (pozri časť 1).

1.6 Definície a skratky

1.6.1 Definície

Zmluvný partner – právnická osoba, s ktorou ma s Poskytovateľom uzatvorenú písomnú zmluvu o poskytovaní dôveryhodných služieb.

1.6.2 Skratky

CP	–	Politika poskytovania dôveryhodnej služby vyhotovovania a overovania certifikátov
CPS	–	Pravidlá poskytovania dôveryhodnej služby vyhotovovania a overovania certifikátov
CA	–	Certifikačná autorita (Certification Authority)
OID	–	Identifikátor objektu (Object Identifier)
PKI		Infraštruktúra verejných kľúčov (Public Key Infrastructure)
PMA	–	Autorita pre správu CP (Policy Management Authority)
RA	–	Registračná autorita (Registration Authority)
CRL	–	Zoznam zrušených certifikátov (Certification Revocation List)
HSM	–	Hardware Security Modul
CMA	–	Autorita pre správu certifikátov (Certificate Management Authority)
IČO	–	Identifikačné číslo organizácie
TLS	-	Je nasledovníkom SSL protokolu (Transport Layer Security)
SWACA	-	Softvér certifikačnej autority Poskytovateľa

1.6.3 Odkazy

[1] Politika poskytovania dôveryhodnej služby vyhotovovania a overovanie certifikátov. s.l. : Disig, a.s.

[2] RFC 3647 - Internet X.509 Public Key Infrastructure Certificate Policy and Certification Practices Framework. November 2003.

[3] RFC 5280 - Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile. Máj 2008.

[4] CA/Browser Forum Baseline Requirements for the Issuance and Management of Publicly-Trusted Certificates v. 2.0.0.

[5] 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 .

[6] Všeobecné podmienky poskytovania a používania dôveryhodnej služby vyhotovovania a overovania certifikátov Disig, a.s.

[7] Informácia o spracúvaní osobných údajov, Disig, a.s.

2. Zverejňovanie informácií a úložisko

2.1 Úložiská

Funkciu úložiska Poskytovateľa zastáva jej webové sídlo, ktorého URL adresa je uvedená v časti 1. Úložisko je verejne prístupný držiteľom certifikátov, stranám spoliehajúcim sa na certifikáty a verejnosti vôbec.

2.2 Zverejňovanie informácií o CA/RA

Pozri časť 2.2 CP CA Disig.

Informácie o registračných autoritách poskytujúcich dôveryhodné služby v mene Poskytovateľa sú dostupné na webovom sídle Poskytovateľa – pozri časť 1.5.2.

Pokiaľ dôjde k nedodržaniu podmienok stanovených aktuálnou politikou „Mozilla Root Store Policy“, tak za hlásenie vniknutého incidentu je zodpovedný manažér certifikačnej autority Poskytovateľa menovaný do roly PMA.

2.3 Frekvencia zverejňovania informácií

Certifikát sa publikuje ihneď po jeho vydaní a okamžite je možné jeho prevzatie Zákazníkom/Držiteľom certifikátu. Informácie o vydanom certifikáte sú dostupné v úložisku Poskytovateľa – pozri časť 2.1.

CRL sa publikuje ako je špecifikované v časti 4.9.8. Informácie o zrušenom certifikáte možno nájsť v úložisku Poskytovateľa.

Všetky informácie v úložisku sú publikované čo možno najskôr po ich vzniku (vydanie, zrušenie ap.).

Certifikáty vydávané pre uzatvorené systémy resp. pre interné účely Poskytovateľa nie sú verejne dostupné a informácie o ich vydaní nie sú publikované v úložisku.

2.4 Kontroly prístupu

Poskytovateľ prostredníctvom technických a prijatých organizačných opatrení chráni ľubovoľnú informáciu uloženú v úložisku, ktorá nie je určená na verejné rozšírenie. K tomuto účelu má vypracované presné pravidlá zahrnuté v bezpečnostnom projekte Poskytovateľa a s ním súvisiacich smerniciach.

Verejne dostupné informácie uvedené v repári Poskytovateľa majú charakter riadeného prístupu.

3. Identifikácia a autentizácia

3.1 Mená

CA Disig prijíma len tie žiadosti o certifikát, ktoré vyhovujú štandardu PKCS #10 alebo SPKAC a sú vo formáte PEM, ak nebolo so zákazníkom vopred dohodnuté inak.

3.1.1 Typy mien

Vo všeobecnosti CA neprirađuje pre certifikáty zákazníkov rozlišovacie mená v zmysle X.500 (X.500 Distinguished Name, ďalej len „rozlišovacie meno“).

Žiadatelia o certifikát si sami zvolia rozlišovacie meno, ktoré má byť v ich certifikáte.

3.1.2 Potreba zmysluplnosti mien

Pozri časť 3.1.2 aktuálnej verzie CP CA Disig.

3.1.3 **Anonymita a používanie pseudonymov**

Pozri časť 3.1.3 aktuálnej verzie CP CA Disig.

3.1.4 Pravidlá na interpretáciu rôznych foriem mien

Pozri časť 3.1.4 aktuálnej verzie CP CA Disig.

3.1.5 **Jedinečnosť mien**

Pozri časť 3.1.5 aktuálnej verzie CP CA Disig.

V prípade, že by mohlo dôjsť k vyhotoveniu certifikátu pre dva rôzne subjekty, ktorý by obsahoval rovnaké rozlišovacie meno daného subjektu sa do certifikátu vkladá jedinečný identifikátor v podobe položky serialNumber.

3.1.6 Rozpoznanie, autentizácia a rola obc**hodných značiek**

Poskytovateľ vedome nevydá certifikát obsahujúci meno v prípade podozrenia, že Zákazník/Držiteľ zodpovedajúcim spôsobom nedoložil oprávnenie takúto obchodnú značku v žiadosti o certifikát použiť.

3.2 **Počiatočné overenie identity**

3.2.1 Preukazovanie vlastníctva súkromného **kľúča**

Pracovník RA musí overiť, že Zákazník/Držiteľ vlastní súkromný kľúč, ktorý zodpovedá verejnému kľúču nachádzajúcemu sa v žiadosti o certifikát.

V prípade žiadosti o nový (následný) certifikát, ktorá bola vygenerované na nové kryptografické kľúče v softvérovom úložisku Zákazníka/Držiteľa sa vlastníctvo súkromného kľúča Zákazníkom/Držiteľom formálne potvrdzuje jej zaslaním ako

prílohy podpísanej správy z e-mailovej adresy, ktorá je uvedená v žiadosti o certifikát. Pracovník RA overí, či žiadosť o certifikát doručená na RA podpísaným e-mailom bola podpísaná prostredníctvom súkromného kľúča, na ktorý bol certifikačnou autoritou Poskytovateľa vydaný certifikát danému Zákazníkovi/Držiteľovi, a tento je v čase overovania prijatého e-mailu platný. Rovnako overí, či bola doručená z e-mailovej adresy, ktorá je totožná z adresou uvedenou v žiadosti.

V prípade doručenia žiadosti o certifikát elektronickou cestou, od Zákazníka/Držiteľa, ktorý už vlastnil certifikát vydaný Poskytovateľom, avšak nemôže byť podpísaná súkromným kľúčom takéhoto certifikátu (certifikát neobsahuje rozšírenie na podpisovanie elektronickej pošty), sa vlastníctvo súkromného kľúča vykonáva kontaktovaním žiadateľa zo strany RA na e-mailovú adresu, z ktorej bola žiadosť zaslaná a overením, že je pôvodcom danej žiadosti.

V prípade, keď Poskytovateľ generuje kľúč priamo do kvalifikovaného zariadenia na vyhotovovanie elektronického podpisu/pečate (Qualified Signature/Seal Creation Device - QSCD) nie je potrebné osobitne overovanie vlastníctva súkromného kľúča.

3.2.2 Autentizácia identity právnickej osoby a identity osoby

3.2.2.1 Autentizácia identity

U Zákazníka/Držiteľa, ktorý žiada o certifikát pre právnickú osobu RA kontroluje predložené doklady dokazujúce existencie danej právnickej osoby, čo je spravidla výpis z obchodného registra resp. iný rovnocenný výpis z iného oficiálneho platného registra právnických osôb.

Predložené doklady musia byť buď originál alebo úradne overená kópia originálu, nie starší/ia ako tri mesiace. Doklad musí obsahovať úplné obchodné meno alebo názov, identifikačný údaj (spravidla IČO), sídlo, meno/á osoby/osôb konajúcej/ich za právnickú osobu a spôsob konania a podpisovania za danú právnickú osobu.

V prípade, že právnická osoba nemá sídlo na území Slovenskej republiky, jej totožnosť sa overuje rovnakým spôsobom ako je uvedené vyššie. Výpis z platného registra právnických osôb musí byť úradne preložený do slovenského jazyka (okrem organizácií so sídlom v Českej republike).

Fyzické osoby, ktoré na základe predloženého výpisu z obchodného registra konajú na RA za danú právnickú osobu vo veci získania certifikátu, musia preukázať svoju totožnosť podľa časti 3.2.3.

V mene právnickej osoby môže na RA konať len oprávnená osoba používateľa t. j. osoba, ktorá je jej štatutárom (alebo viac takýchto osôb súčasne, ak to vyžaduje predložený výpis z obchodného registra), prípadne sa právnická osoba môže nechať zastupovať fyzickou alebo inou právnickou osobou.

Ak sa právnická osoba nechá zastupovať na RA, zastupujúca fyzická alebo právnická osoba musí vždy predložiť k nahliadnutiu overený výpis z obchodného registra zastupovanej právnickej osoby nie starší ako tri mesiace.

Ak sa právnická osoba nechá zastupovať na RA fyzickou osobou, táto zastupujúca fyzická osoba musí preukázať svoju totožnosť podľa časti 3.2.3 a navyše sa musí

preukázať úradne overenou (notárom alebo matrikou) plnou mocou, z textu ktorej je jednoznačne jasné, že zastupujúca fyzická osoba bola splnomocnená splnomocňujúcou právnickou osobou konať v danej veci v jej mene.

Ak sa právnická osoba nechá zastupovať na RA inou právnickou osobou, táto zastupujúca právnická osoba okrem príslušnej plnej moci (viď predošlý odsek) musí preukázať svoju totožnosť rovnakým spôsobom ako zastupovaná právnická osoba, ako je to požadované vyššie.

Subjekt (fyzická alebo právnická osoba), ktorý zastupuje právnickú osobu, sa vo veci právnickej osoby, ktorú zastupuje, v žiadnom prípade nemôže nechať zastupovať iným subjektom.

V prípade, že právnická osoba nemôže preukázať svoju totožnosť výpisom z obchodného registra (platí pre nepodnikateľské subjekty ako sú napr. obec, cirkev, občianske združenie, nadácia, štátny orgán a podobne), musí takáto právnická osoba písomne preukázať okrem svojej totožnosti aj legálnosť (resp. „dôvod“) svojej existencie (s využitím a poukázaním na zákon alebo iný predpis, ktorý o subjekte daného typu pojednáva, zriaďovaciu listinu ap.).

3.2.2.2 DBA/Obchodné meno

Ak je obsahom certifikátu DBA/Obchodné meno, tak pracovník RA overuje, či má Zákazník/Držiteľ právo použiť dané TBA/Obchodné meno na základe preloženia jedného z dokladov uvedených v časti 3.2.2.2 aktuálnej verzie CP CA Disig.

3.2.2.3 Overenie krajiny Zákazníka/Držiteľa

V prípade vydávania TLS certifikátu kde je v položke countryName uvedený kód krajiny pracovník RA overuje oprávnenosť spojenia danej krajiny so Zákazníkom/Držiteľom na základe informácií poskytovaných registrátorom domény resp. na základe iných predkladaných dokumentov – pozri časť 3.2.2.1 týchto CPS.

3.2.2.4 Overenie oprávnenia k doméne alebo kontroly nad doménou

Pracovník RA vykoná overenie oprávnenia k doméne alebo kontroly nad doménou metódou, ktorá je uvedená v dokumente [4] v časti 3.2.2.4.2 resp. v prípade, že nie je možné využiť túto metódu, tak alternatívne použije metódu, ktorá je uvedená v dokumente [4] v časti 3.2.2.4.15.

V prípade overenia v zmysle časti 3.2.2.4.2 [4] pracovník RA prostredníctvom softvérovej aplikácie KeePass vygeneruje náhodný textový reťazec s minimálnou dĺžkou 20 znakov, ktorý bude obsahovať veľké a malé písmená, čísla a špeciálne znaky. Takto vygenerovanú hodnotu zašle prostredníctvom emailu na emailovú adresu identifikovanú ako oprávnený kontakt pre danú doménu v registri oprávneného registrátora pre danú doménu (napr. pre doménu najvyššej úrovne „.sk“ je to whois.sk-nic.sk). Náhodne vygenerovaná hodnota musí byť zaslaná spolu s potvrdením oprávnenosti žiadosti o vydanie TLS certifikátu v spätne zaslanej emailovej správe z emailovej adresy, na ktorú bol overovací email zaslaný. Náhodná hodnota musí byť pre každú odoslanú emailovú správu jedinečná. Ak prebehne úspešná validácia oprávnenosti použitia FQDN týmto spôsobom, tak Poskytovateľ môže vydať aj iné TLS certifikáty, ktoré končia rovnakým FQDN

na druhej a vyššej úrovni. Pracovník RA potom archivuje príslušnú emailovú komunikáciu k vydaným TLS certifikátom v elektronickej podobe. Túto metódu je možné použiť aj na validáciu žiadosti o vydanie „wildcard“ TLS certifikátu.

V prípade overenia v zmysle časti 3.2.2.4.15 [6] pracovník RA overí oprávnenosť žiadosti o vydanie TLS certifikátu zo strany Zákazníka telefonicky, tak že zavolá na telefónne číslo oprávneného kontaktu, ktoré je uvedené ako oprávnený kontakt pre danú doménu v registri oprávneného registrátora pre danú doménu (napr. pre doménu najvyššej úrovne „.sk“ je to whois.sk-nic.sk). Ak prebehne úspešná validácia oprávnenosti použitia FQDN týmto spôsobom, tak Poskytovateľ môže vydať aj iné TLS certifikáty, ktoré končia rovnakým FQDN na druhej a vyššej úrovni. V prípade, že na telefonickom kontakte bude iná osoba ako kontakt uvedený pre danú doménu, musí pracovník RA požiadať o spojenie s osobou, ktorá je daným kontaktom. V prípade, že na telefonickom kontakte bude záznamník, tak pracovník RA zanechá na záznamníku informáciu s obsahom náhodne vygenerovanej hodnoty (pozri postup podľa metódy 3.2.2.4.2 [6]) a overovanú ADN (Authorization Domain Name). Pracovník RA vykoná záznam v elektronickej podobe o telefonickom rozhovore s vyznačením telefónneho čísla, na ktoré bolo vykonaný a menom osoby, ktorá potvrdila oprávnenosť žiadosti o vydanie TLS certifikátu prípadne zaznamená náhodne vygenerovanú hodnotu, ak na telefónnom čísle bol záznamník a rovnako zaznamená odpoveď na takto zanechaný odkaz. Túto metódu je možné použiť aj na validáciu žiadosti o vydanie „wildcard“ TLS certifikátu.

3.2.2.5 Autentifikácia IP adresy

Žiadne ustanovenia.

3.2.2.6 Validácia domény obsahujúcej „wildcard“ znak

Pracovník RA vykoná validáciu žiadosti o vyhotovenie „wildcard“ TLS certifikátu, tým spôsobom, že skontroluje, či v položke CN resp. SAN sa wildcard znak hviezdička („*“) nachádza na prvej pozícii zľava, a či za ním ihneď nasleduje znak bodka („.“). Zároveň skontroluje, či je „wildcard“ TLS certifikát vydávaný pre doménu tretej a vyššej úrovne, kde prvá úroveň môže byť len úroveň národnej domény „.sk“ t. j. akceptovateľná žiadosť musí mať tvar „wildcard“ doménového mena pre tretiu úroveň „*.názovdomény.sk“. Overenie oprávnenia k doméne sa vykoná v zmysle bodu 3.2.2.4.

3.2.2.7 Presnosť zdroja údajov

Pracovník RA musí pred použitím akéhokoľvek zdroja ako dôveryhodného zdroja postupovať v zmysle časti 3.2.2.7 aktuálnej verzie CP CA Disig.

3.2.2.8 CAA záznam

Pracovník RA musí pred vydaním TLS certifikátu skontrolovať publikovaný CAA záznam. Ak zistí, že takýto záznam existuje nesmie vydať certifikát pokiaľ sa nepotvrdí, že žiadosť o certifikát je v súlade s príslušnou množinou záznamov v CAA.

Overovanie záznamu sa vykonáva pre každé FQDN uvedené v CN žiadosti resp. to, ktoré má byť uvedené v SAN takým spôsobom, že sa postupuje v mennom strome od ľavej strany až po pravú napr. pre kontrolu CAA záznamu žiadosti, ktorá

obsahuje FQDN v tvare X.Y.X sa kontrola vykoná v poradí X.Y.X -> Y.Z -> Z, pokiaľ Z nie je národná úroveň napr. „.sk“.

O vykonaní kontroly CAA záznamu sa vytvorí písomný záznam obsahujúci všetky kontrolované FQDN aj s výsledkom kontroly.

3.2.3 Autentizácia identity fyzickej osoby

Fyzickou osobou môže byť plnoletý občan Slovenskej republiky alebo cudzí štátny príslušník.

Fyzická osoba musí preukázať svoju totožnosť dvomi z týchto osobných dokladov:

- občiansky preukaz,
- cestovný pas,
- vodičský preukaz,
- rodný list,
- povolenie na prechodný pobyt (resp. trvalý pobyt) v prípade cudzinca
- zbrojný preukaz
- služobný preukaz

Požaduje sa pritom, aby aspoň jeden z predkladaných dokladov bol dokladom, ktorého súčasťou je fotografia danej osoby. V prípade predloženia rodného listu, zbrojného preukazu alebo služobného preukazu sa musí predložiť aj jeden z týchto dokladov: občiansky preukaz alebo cestovný pas.

Ak fyzická osoba zastupuje na RA inú fyzickú osobu, musí sa navyše preukázať úradne overenou (notárom alebo matrikou) plnou mocou, z textu ktorej je jednoznačne jasné, že zastupujúca fyzická osoba bola splnomocnená splnomocňujúcou fyzickou osobou konať v danej veci v jej mene.

Ak právnická osoba zastupuje fyzickú osobu, okrem plnej moci (viď predošlý odsek) musí splnomocnená právnická osoba preukázať svoju totožnosť podľa časti 3.2.2.

Subjekt (fyzická alebo právnická osoba), ktorý zastupuje fyzickú osobu, sa vo veci fyzickej osoby, ktorú zastupuje, v žiadnom prípade nemôže nechať zastupovať iným subjektom.

3.2.3.1 Autentizácia identity komponentu

CMA musí garantovať aj v takomto prípade, že identita komponentu a jeho verejný kľúč sú zodpovedajúco previazané.

Hardvérový alebo softvérový komponent, ktorý bude používať certifikáty, bude predmetom certifikácie a je možné vytvoriť preň TLS certifikát. V takom prípade komponent musí byť priradený fyzickej alebo právnickej osobe (organizácii), ktorá ho spravuje.

Táto osoba alebo organizácia je povinná poskytnúť RA tieto informácie:

- identifikáciu zariadenia (názov softvérového komponentu),
- verejný kľúč zariadenia (obsiahnutý v žiadosti o certifikát),

- autorizáciu zariadenia a jeho atribúty (ak nejaké majú byť uvedené v certifikáte),
- kontaktné údaje, aby CMA mohla v prípade potreby komunikovať s touto osobou,

RA musí autentizovať správnosť ľubovoľnej autorizácie (hodnoty položky rozlišovacieho mena), ktorá má byť uvedená v certifikáte a overuje predložené údaje.

Metódy na vykonanie tejto autentizácie a kontroly údajov zahrňujú:

- overenie identity danej osoby v súlade s požiadavkami časti 3.2,
- overenie identity organizácie, ktorej patrí daný komponent, v súlade s požiadavkami časti 3.2.2,
- overenie oprávnenosti použitia údajov, ktoré majú byť uvedené v jednotlivých položkách certifikátu, s dôrazom na obsah položky commonName.

Typickou hodnotou tejto položky bude úplné doménové meno.

RA vykoná overenie všetkých položiek nachádzajúcich sa v DN certifikátu, s výnimkou položky organizationUnitName (Názov útvaru v organizácii). V prípade tejto položky sa vykoná len kontrola, či neobsahuje názov právnickej osoby, obchodné meno, obchodnú značku, adresu, lokalitu, alebo iný text poukazujúc na určiteľnú fyzickú alebo právnickú osobu.

3.2.3.2 Autentizácia identity u zmluvných partnerov

Autentizácia identity fyzickej osoby resp. komponentu u zmluvných partnerov spoločnosti Disig (obchodní partneri), sa vykonáva v spolupráci so zodpovednými osobami tejto spoločnosti.

Niektoré postupy sú v tomto prípade zjednodušené a nemusia sa vykonávať napr. overovanie vlastníctva domény, overovanie kontroly e-mail konta ap.

3.2.3.3 Predkladané doklady

3.2.3.3.1 Všeobecne

Všetky doklady predkladané na RA žiadateľmi o služby musia byť buď originály alebo úradne overené kópie originálov. Nesmie v nich byť žiaden údaj doplňovaný, pozmeňovaný, prečiarknutý a podobne. Doklady, na ktorých je vyznačená doba ich platnosti, musia byť platné.

Ak má pracovník RA pochybnosti o totožnosti potenciálneho zákazníka (napr. zjavný nesúlad medzi fotografiou v predloženom osobnom doklade a vzhľadom zákazníka, rozpornosť dvoch predložených dokladov a podobne), môže odmietnuť jeho registráciu.

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

Na žiadosť potenciálneho zákazníka alebo RA sa prípadné sporné prípady pri preukazovaní totožnosti riešia postupom podľa časti 9.13.

Pri predkladaní dokladov sa vyžaduje, aby na pobočke RA boli predložené originály týchto dokladov slúžiace k nahliadnutiu a kópie originálov (nemusia byť overené), okrem osobných dokladov identifikujúcich totožnosť žiadateľa resp. splnomocnenej osoby, slúžiace na archiváciu pre potreby Poskytovateľa. Predloženie výpisu z obchodného registra resp. živnostenského registra získaného z Internetu, zo strany žiadateľa, nie je postačujúce, nakoľko tento má len informatívny charakter a nie je použiteľný na právne úkony.

3.2.3.3.2 Fyzická osoba

Pozri časť 3.2.3 a časť 3.2.3.3.2 aktuálnej verzie CP CA Disig.

3.2.3.3.3 Fyzická osoba - zamestnanec

Pozri časť 3.2.3.3.4 aktuálnej verzie CP CA Disig.

3.2.3.3.4 Právnická osoba

V tomto prípade žiadateľ o certifikát predkladá doklady uvedené v časti 3.2.3.3.2. Súčasne musí predložiť doklad podľa časti 3.2.2.

3.2.3.4 Zariadenie alebo systém

Pozri časť 3.2.3.1.

3.2.3.5 Kontrola údajov na predložených dokladoch

V prípade ľubovoľných odôvodnených pochybností o totožnosti potenciálneho zákazníka môže RA jeho registráciu odmietnuť. Pracovník RA kontroluje na predložených dokladoch najmä nasledovné:

- Osobné doklady fyzickej osoby:
  - platnosť predloženého dokladu - v prípade neplatného osobného dokladu sa postupuje ako pri chýbajúcom osobnom doklade - RA registráciu odmietne
  - plnoletosť fyzickej osoby (t. j. vek 18 rokov) - RA odmietne registráciu neplnoletých osôb pričom za neplnoleté osoby má právo konať ich zákonný zástupca (obvykle rodič).
  - či nie je zjavný nesúlad medzi fotografiou v osobnom doklade a vzhľadom držiteľa osobného dokladu – v prípade, že áno, RA môže odmietnuť registráciu.
  - rozpornosť predložených dokladov, t. j. či údaje na jednom doklade neodporujú údajom na inom doklade
- Výpisy z obchodného registra:
  - či výpis nie je starší ako 3 mesiace
  - či majú fyzické osoby (stačí jedna fyzická osoba, ak na výpise nie je uvedené inak), ktoré predložili daný výpis, právo konať (podpisovať) za danú právnickú osobu (t. j. či sú jej štatutárnymi zástupcami)
  - či je výpis úradne overený (notárom alebo matrikou), ak sa nejedná o originál

- Plné moci:
  - či je plná moc úradne overená (notárom alebo matrikou)
  - či sa údaje, uvedené v plnej moci, ktoré definujú zastupujúcu fyzickú resp. právnickú osobu, zhodujú s údajmi uvedenými na osobných dokladoch zastupujúcej fyzickej osoby resp. s údajmi uvedenými na výpise z obchodného registra zastupujúcej právnickej osoby
  - rozsah plnej moci - t. j. či plná moc oprávňuje splnomocnenú fyzickú alebo právnickú osobu k požadovanému úkonu na RA v mene splnomocňujúcej fyzickej alebo právnickej osoby
  - či plná moc nie je časovo obmedzená alebo ak obsahuje inú podmienku, či je táto splnená
- Čestné prehlásenia:
  - oprávnenie na podpis – či osoba podpisujúca prehlásenie je oprávnená zastupovať právnickú osobu. Oprávnenosť sa kontroluje podľa výpisu z OR resp. iného registra právnických osôb. Pokiaľ podpisujúca osoba nie je zapísaná v tomto výpise, musí predložiť iný doklad, na základe ktorého môže konať za spoločnosť (spravidla notárom overená plná moc)

Druh predložených dokladov (napr. občiansky preukaz, pas) a príslušné údaje z nich zaznamená pracovník RA elektronicky do informačného systému CA.

V prípade zistených nedostatkoch na predložených dokladoch, resp. predložení neúplných dokladov, musí pracovník RA registráciu žiadateľa odmietnuť. Služba vydania certifikátu bude v tomto prípade zamietnutá.

Pracovník RA musí akceptovať aj dokumenty predkladané žiadateľom v elektronickej podobe podpísané platným ZEP (výpis s obchodného registra, plná moc, prehlásenie, poverenie ap.)

3.2.3.6 Prvotná registrácia RA

Prvotná registrácia osoby v role RA sa vykoná za rovnakých, vyššie popísaných podmienok ako v prípade zákazníka - žiadateľa o osobný certifikát. Vlastné overenie identity pracovníkov RA vykonajú pracovníci Poskytovateľa, pokiaľ nie je zmluvne dohodnutý iný mechanizmus.

3.2.4 Neoverované informácie o **Držiteľovi**

Pozri časť 3.2.4 aktuálnej verzie CP CA Disig.

3.2.5 Overovanie oprávnení

Pozri časť 3.2.3.

3.2.6 Kritériá interoperability

Žiadne ustanovenia.

3.3 Identifikácia a autentifikácia pri vydávaní následného certifikátu

Podmienky vydania následného certifikátu sú podrobne popísané v časti 3.3 aktuálnej verzie CP CA Disig.

RA vykoná vydanie certifikátu bez osobnej návštevy držiteľa v prípade certifikátu pre fyzickú osobu resp. certifikátu pre právnickú osobu len po splnení podmienok uvedených v časti 3.3 aktuálnej verzie CP CA Disig.

3.3.1 Identifikácia a autentifikácia pri vydávaní následného certifikátu po **zrušení predchádzajúceho**

Po zrušení certifikátu musí žiadateľ o následný certifikát podrobiť všetkým požiadavkám prvotnej registrácie.

3.3.2 Identifikácia a autentifikácia pri vydávaní následného certifikátu po **zrušení predchádzajúceho**

Žiadne ustanovenia.

3.4 Identifikácia a **autentifikácia pri žiadaní o zrušenie certifikátu**

Pozri časť 3.4 aktuálnej verzie CP CA Disig.

4. Požiadavky na životný cyklus certifikátu

4.1 Žiadanie o certifikát

4.1.1 Kto môže žiadať o vydanie certifikátu

Pozri časť 4.1.1 aktuálnej verzie CP CA Disig.

4.1.2 Registračný proces a zodpovednosti

4.1.2.1 Príprava

Pozri časť 4.1.2.1 aktuálnej verzie CP CA Disig.

4.1.2.2 Generovanie žiadosti

Pozri časť 4.1.3 aktuálnej verzie CP CA Disig.

4.1.2.3 Zaslanie žiadosti o certifikát

Pozri časť 4.1.4 aktuálnej verzie CP CA Disig.

4.2 Spracovanie žiadosti a vydanie certifikátu

4.2.1 Vykonanie identifikácie a autentifikácie

4.2.1.1 Postup RA pri zaslaní žiadosti elektronicky

Pracovník RA overí, či elektronicky zaslaná žiadosť o vydanie certifikátu daného Zákazníka obsahom zodpovedá požiadavkám na jej obsah, ktorý je daný v časti 3.1.4.1 CP CA Disig v prípade certifikátu pre fyzickú osobu, v časti 3.1.4.2 CP CA Disig v prípade certifikátu pre právnickú osobu resp. časti 3.1.4.3 CP CA Disig v prípade TLS certifikátu.

4.2.1.2 Postup pri registrácii zákazníka priamo na RA

1. Pracovník RA informuje prítomnú fyzickú osobu o Všeobecných podmienkach [6] poskytovania dôveryhodných služieb
2. Pracovník RA overí totožnosť Zákazníka resp. subjektu, ktorý ho zastupuje, podľa ustanovení častí 3.2.2 a 3.2.3.
3. Pracovník RA vyberie vopred zaslanú žiadosť o certifikát identifikovanú Zákazníkom.
4. Pracovník RA skontroluje úplnosť a správnosť prijatej žiadosti o certifikát (napr. či niektoré položky neobsahujú zjavne chybné údaje).

Upozornenie: Položky "Mesto:", "Firma:" a "Útvar vo firme:" sú nepovinné. Zákazník musí na RA uspokojivým spôsobom preukázať všetky údaje, ktoré zadal do jednotlivých položiek žiadosti o certifikát. Ak Zákazník predloží aj iné doklady (okrem osobných dokladov fyzických osôb, napr. výpis z obchodného registra alebo iný doklad o právnickej osobe, plná moc v prípade zastupovania iného subjektu), pracovník RA prevezme a uschová kópie (nemusia byt overené) všetkých predložených dokladov, porovná ich s originálmi a na každú kópiu napíše text

„Potvrdzujem zhodu s originálom“ a doplní dátum a svoj podpis. Predloženie výpisu z obchodného registra získaného z Internetu, zo strany Zákazníka, nie je postačujúce, nakoľko tento výpis má len informatívny charakter a nie je použiteľný na právne úkony.

5. Prostredníctvom informačného systému Poskytovateľa sa automatizovane overí, či pre verejný kľúč nachádzajúci sa v predloženej žiadosti o certifikát už nebol v minulosti vydaný certifikát. Ak bol, RA žiadosť o certifikát odmietne z bezpečnostných dôvodov prijať, nakoľko už raz certifikovaný verejný kľúč nemôže byť použitý v inom certifikáte.
6. V prípade, že Poskytovateľ nemá so Zákazníkom platnú zmluvu o poskytovaní dôveryhodnej služby vydávania certifikátov, pracovník RA predloží Zákazníkovi na podpis zmluvu o poskytovaní dôveryhodnej služby vydávania certifikátov v dvoch exemplároch – jeden pre Poskytovateľa a jeden pre zákazníka. Súhlas Zákazníka s textom tejto zmluvy je podmienkou na prijatie žiadosti o certifikát a vyhotovenie certifikátu.
7. Zákazník zaplatí za certifikát sumu podľa platného cenníka služieb Poskytovateľa, pokiaľ nie je dohodnutý iný spôsob platby.
8. Pracovník RA vloží do informačného systému Poskytovateľa žiadosť o certifikát a ostatné požadované údaje.
9. Bezprostredne po vydaní certifikátu bude môcť žiadateľ o certifikát prevziať svoj certifikát. Pritom podpíšu žiadateľ o certifikát a pracovník RA potvrdenie o prevzatí certifikátu. Toto potvrdenie sa vyhotoví v dvoch exemplároch – jeden pre žiadateľa a jeden zostane RA, ktorá ho potom postúpi Poskytovateľovi V prípade zmluvných partnerov, ktorých zamestnancom sú vydávané certifikáty na zmluvnom základe je podpisované len potvrdenie o prevzatí.

4.2.1.3 Detailný postup na získanie TLS certifikátu

4.2.1.3.1 Príprava na návštevu na RA

Zákazník vykoná nasledovné kroky:

- oboznámi sa s týmto postupom, prípadne s princípmi a návodmi na získanie certifikátu,
- pomocou svojho softvéru (typicky napr. Microsoft IIS alebo Apache/Openssl) si vygeneruje žiadosť o TLS certifikát a túto odošle elektronicky na RA (radisig@disig.sk) a zároveň si ju uloží z dôvodov zálohy na vhodné prenosné médium,

Poznámky a upozornenia: Upozorňujeme, že žiadosť o TLS certifikát resp. v nej sa nachádzajúci verejný kľúč, na ktorý už bol vydaný certifikát, nemôže byť z bezpečnostných dôvodov použitá opakovane na vydanie iného TLS certifikátu a bude na RA odmietnutá! Žiadosť o TLS certifikát musí povinne obsahovať vhodne vyplnenú položku subject:commonName (tzv. názov entity). Jednotlivé položky je potrebné vyplniť tak, aby zadané hodnoty boli v súlade s týmto dokumentom s dôrazom na jeho časť 3.1.2, a aby jednoznačne identifikovali entitu, ktorá bude používať daný TLS certifikát (typicky úplné doménové meno (FQDN)). Pokiaľ je v žiadosti vyplnená položka O (subject:organizationName), tak musí byť vyplnená aj položka L (subject:localityName). Pokiaľ položka O (subject:organizationName) nie je vyplnená, tak nesmie byť vyplnená položka L (subject:localityName).

Použitie špeciálnych znakov (napr. čiarka, pomlčka, =, / a iné) treba obmedziť na minimálnu nutnú mieru, odporúčame prípadne tieto znaky použiť až po dohode s CA Disig, v opačnom prípade si CA Disig vyhradzuje právo odmietnuť takúto žiadosť o TLS certifikát. Všetky údaje sa musia zadávať bez diakritiky (mäkčene, dĺžne a pod.). V poli Organizácia sa nesmie použiť znak čiarka. Žiadateľom o TLS certifikát môže byť len štatutár organizácie resp. ním splnomocnená osoba, ktorej patrí entita, pre ktorú je TLS certifikát vydávaný. Všetky údaje v žiadosti musia byť zo strany žiadateľa hodnoverne preukázané, okrem položky subject:organizationUnitName (OU). Položka OU nesmie obsahovať názov právnickej osoby, obchodné meno, obchodnú značku, adresu, lokalitu, alebo iný text poukazujúci na určiteľnú fyzickú alebo právnickú osobu, pokiaľ použitie týchto informácií nie je žiadateľ schopný hodnoverne doložiť.

- pripraví si zvolené doklady totožnosti resp. iné potrebné doklady, napr. výpis z obchodného registra (odporúčame overiť platnosť dokladov) podľa ustanovení časti 3.

Poznámka: Je potrebné, aby si zákazník pripravil kópie (nemusia byt overené) všetkých dokladov (okrem osobných dokladov fyzických osôb), ktoré mieni predložiť na RA (napr. výpis z obchodného registra a iné doklady o právnickej osobe, splnomocnenie, ak sa dá zastupovať na RA), aby ich mohol odovzdať na RA. Predloženie výpisu z obchodného registra získaného z Internetu, zo strany žiadateľa, nie je postačujúce, nakoľko tento výpis má len informatívny charakter a nie je použiteľný na právne úkony.

Odporúča sa, aby si zákazník na RA ešte pred návštevou RA overil a vyjasnil prípadné pochybnosti a problémy, najmä tie, ktoré týkajú vhodnosti hodnôt jednotlivých položiek v žiadosti o TLS certifikát.

- dohodne si termín návštevy RA (telefonicky, e-mailom).

4.2.1.4 Postup RA pred vydaním TLS certifikátu

Na základe vopred zaslanej žiadosti pracovník RA vykoná overenie vlastníctva domény v zmysle ods. 3.2.2.4 a zároveň skontroluje úplnosť a správnosť prijatej žiadosti o TLS certifikát. Ak má pracovník RA vážne podozrenie na neoprávnené použitie niektorého FQDN Zákazníkom, má právo požadovať, aby Zákazník dôveryhodným spôsobom dokladoval oprávnenosť použitia daného FQDN, v opačnom prípade môže RA odmietnuť prijať danú žiadosť o TLS certifikát.

4.2.2 **Schválenie alebo zamietnutie žiadosti o** certifikát

Žiadosť o vydanie certifikátu začne pracovník RA spracovávať ihneď po jej prijatí v zmysle postupov uvedených v časti 4.2.1 a ak sú splnené všetky podmienky na vydanie, tak certifikát vydá, ak ide o žiadosť zaslanú elektronicky. V prípade potreby osobnej účasti Zákazníka/Držiteľa sa vydanie uskutoční pri jeho osobnej účasti za predpokladu predloženia všetkých požadovaných dokumentov.

Pracovník RA zamietne žiadosť o vydanie certifikátu v prípade, že má odôvodnenú pochybnosť o totožnosti zákazníka a tiež v prípade, že zistí nedostatky v identifikačných dokladoch, poskytnutí neúplných informácii alebo v prípade, že v minulosti už bol Poskytovateľom vydaný certifikát na daný verejný kľúč.

Pokiaľ najvyššia doména (gTLD) uvedená v zaslanej žiadosti na vydanie TLS certifikátu (napríklad „.ipsum“) je pre pracovníka neznáma, musí si overiť či sa nachádza v databáze „Root Zone Database“, ktorú vedie Internet Assigned Numbers

Authority (IANA) (https://www.iana.org/domains/root/db). Ak zistí, že daná gTLD sa v zozname nenachádza, tak odmietne vydať certifikát.

4.2.3 **Doručenie verejného kľúča vydavateľovi certifikátu**

Pozri časť 4.2.3 aktuálnej verzie CP CA Disig.

4.3 Vydanie certifikátu

4.3.1 **Činnosť CA pri vydávaní certifikátu**

Pozri časť 4.3.1 aktuálnej verzie CP CA Disig.

4.3.2 **Informovanie Držiteľa o** vydaní certifikátu

Držiteľ je upozornený na vydanie certifikátu zaslaním e-mailovej správy priamo zo systému CA na e-mailovú adresu uvedenú uvedenú v osobných údajoch Držiteľa certifikátu.

4.4 Prevzatie certifikátu

4.4.1 Spôsob prevzatia certifikátu

V prípade, že certifikát nie je vydávaný na QSCD, tak vydaný certifikát je k dispozícii na prevzatie prostredníctvom úložiska Poskytovateľa na adrese https://eidas.disig.sk/sk/poskytovatel/certifikacna-autorita/vyhladavanie-certifikatov/ resp. v upozorňujúcom e-maile je priamo uvedená linka, kde si Držiteľ môže vydaný certifikát stiahnuť.

V prípade vydania certifikátu na QSCD je tento odovzdaný Zákazníkovi/Držiteľovi ihneď po vydaní spolu s QSCD.

4.4.2 **Zverejňovanie certifikátu**

Každý vydaný certifikát je zverejňovaný v úložisku Poskytovateľa ihneď po vydaní, pokiaľ so Zákazníkom/Držiteľom nebolo dohodnuté jeho nezverejňovanie.

4.4.3 Oznámenie o vydaní certifikátu iným subjektom

Pozri časť 4.4.3 aktuálnej verzie CP CA Disig.

4.5 **Kľúčový pár a používanie certifikátu**

Pozri časť 4.5 aktuálnej verzie CP CA Disig.

4.5.1 **Používanie súkromného kľúča a certifikátu Držiteľom**

Žiadne ustanovenia.

4.5.2 **Používanie verejného kľúča a certifikátu Spoliehajúcou sa stranou**

Žiadne ustanovenia.

4.6 Obnova certifikátu

Pozri časť 4.6 aktuálnej verzie CP CA Disig.

4.6.1 Okolnosti pre obnovenie certifikátu

Žiadne ustanovenia.

4.6.2 **Kto môže požiadať o obnove**nie

Žiadne ustanovenia.

4.6.3 **Spracovanie žiadostí o obnovenie certifikátu**

Žiadne ustanovenia.

4.6.4 **Oznámenie o vydaní nového certifikátu držiteľovi**

Žiadne ustanovenia.

4.6.5 Spôsob prevzatia obnoveného certifikátu

Žiadne ustanovenia

4.6.6 Z**verejňovanie obnoveného certifikátu zo strany Poskytovateľa**

Žiadne ustanovenia.

4.6.7 Oznámenie o vydaní obnoveného certifikátu iným subjektom

Žiadne ustanovenia.

4.7 **Vydanie certifikátu na nové kľúče**

4.7.1 **Podmienky vydania certifikátu na nové kľúče**

Žiadne ustanovenia

4.7.2 **Kto môže žiadať o** vydanie certifikátu na **nové kľúče**

O vydanie certifikátu na nové kľúče môže požiadať existujúci Držiteľ, ktorému bol v minulosti vydaný certifikát Poskytovateľom, a ktorý splní požiadavky na identifikáciu a autentifikáciu v zmysle časti 3.

4.7.3 **Postup žiadania o vydanie certifikátu na nové kľúče**

Pracovník RA vydá certifikát rovnakým spôsobom ako bol vydávaný pôvodný certifikát.

4.7.4 Oznámenie o **vydaní certifikátu na nové kľúče Držiteľovi**

Po vydaní certifikátu je Držiteľ upozornený na jeho vydanie zaslaním e-mailovej správy na e-mailovú adresu oznámenú v procese autentifikácie a identifikácie.

4.7.5 **Spôsob prevzatia certifikátu vydaného na nové kľúče**

V prípade vydávania za osobnej prítomnosti Držiteľa na RA sa uplatní spôsob prevzatia popísaný v časti 4.4.

V prípade podania žiadosti o certifikát na nové kľúče elektronickou cestou je Držiteľovi certifikát doručený na e-mailovú adresu uvedenú v certifikáte.

4.7.6 **Zverejňovanie certifikátov zo strany Poskytovateľa**

Pozri časť 4.4.2.

4.7.7 Oznámenie o vydaní certifikátu CA iným subjektom

Pozri časť 4.4.3.

4.8 Modifikácia certifikátu

4.8.1 Okolnosti pre modifikovanie certifikátu

Žiadne ustanovenia

4.8.2 **Kto môže požiadať o modifikáciu certifikátu**

Žiadne ustanovenia.

4.8.3 **Spracovanie žiadostí o modifikáciu certifikátu**

Žiadne ustanovenia.

4.8.4 **Oznámenie o vydaní nového certifikátu držiteľovi**

Žiadne ustanovenia.

4.8.5 Spôsob prevzatia modifikovaného certifikátu

Žiadne ustanovenia

4.8.6 **Zverejňovanie modifikovaného certifikátu zo strany Poskytovateľa**

Žiadne ustanovenia.

4.8.7 Oznámenie o vydaní modifikovaného certifikátu iným subjektom

Žiadne ustanovenia.

4.9 **Zrušenie a s**uspendovanie certifikátu

4.9.1 **Podmienky zrušenia certifikátu**

Pozri časť 4.9.1 aktuálnej verzie CP CA Disig.

4.9.1.1 Zrušenie certifikátu Zákazníka/Držiteľa

Pozri časť 4.9.1.1 aktuálnej verzie CP CA Disig.

4.9.2 **Kto môže žiadať o zrušenie certifikátu**

Pozri časť 4.9.2 aktuálnej verzie CP CA Disig.

4.9.3 Postup **žiadosti o zrušenie certifikátu**

Osoba požadujúca zrušenie certifikátu sa buď musí na RA podrobiť rovnakému procesu autentizácie, aký je požadovaný pri prvotnej registrácii žiadateľa o certifikát alebo musí hodnoverným spôsobom preukázať, že je oprávnenou osobou, ktorá môže žiadať o zrušenie daného certifikátu.

Ak sa držiteľ certifikátu nechá na RA zastupovať vo veci zrušenia certifikátu, zastupujúci subjekt sa musí preukázať overenou plnou mocou (notárom alebo matrikou), z textu ktorej je jednoznačne zrejmá vôľa držiteľa certifikátu zrušiť svoj certifikát. Zastupujúci subjekt je povinný nechať na RA doklad potvrdzujúci jeho plnú moc alebo jeho kópiu (nemusí byť overená). Pracovník RA prevezme a uschová tento doklad, v prípade neoverenej kópie túto porovná s originálom a napíše na ňu text „Potvrdzujem zhodu s originálom“ a doplní dátum a svoj podpis.

Pracovník RA posúdi oprávnenosť žiadosti o zrušenie certifikátu a v prípade, že je zrejmé, že žiadateľ o zrušenie nie je oprávnenou osobou, RA môže danú žiadosť o zrušenie odmietnuť.

Pracovník RA odmietne žiadosť, ak žiadateľ nesplní podmienky autentizácie svojej identity (pozri časti 3.2.2 resp. 3.2.3).

Kontakty pre nahlasovania a postup nahlasovania incidentov v prípade možnej kompromitácie súkromného kľúča, zneužitia certifikátu alebo iného druhu podvodu, neoprávneného vydania alebo inej záležitosti týkajúcej sa vydaného Certifikátu sú uvedené v kapitole 1.5.2.

V prípade požiadavky na zrušenie TLS certifikátu z niektorého z dôvodov uvedených v časti 4.9.1.1 aktuálneho CP CA Disig (keyCompromise (RFC 5280 CRLReason #1), privilégiumWithdrawn (RFC 5280 CRLReason #9), cessationOfOperation (RFC 5280 CRLReason #5), affiliationChanged (RFC 5280 CRLReason #3) alebo superseded (RFC 5280 CRLReason #4) musí RA požadovať zaslanie písomnej požiadavky v zmysle časti 4.9.3 aktuálneho CP CA Disig.

4.9.4 **Čas na podanie žiado**sti o **zrušenie certifikátu**

Pozri časť 4.9.4 aktuálnej verzie CP CA Disig.

4.9.5 **Čas na zrušenie certifikátu**

Pozri časť 4.9.5 aktuálnej verzie CP CA Disig.

Po prijatí žiadosti o zrušenie certifikátu, ktorú Pracovník RA považuje za oprávnenú (t. j. ktorá vyhovuje príslušným ustanoveniam týchto pravidiel), Pracovník RA vloží prijatú žiadosť o zrušenie certifikátu prostredníctvom aplikácie RA Client do informačného systému Poskytovateľa, aby sa daný certifikát mohol automatizovane zrušiť. Zrušenie je vykonané najneskoršie do 24 hodín od overenia oprávnenosti žiadosti o zrušenie.

Po zrušení certifikátu je zo systému Poskytovateľa automaticky zaslaná držiteľovi e-mailová notifikáciu o zrušení jeho certifikátu aj s informáciou o dôvodoch jeho zrušenia.

4.9.6 Overovanie platnosti zo strany spoliehajúcej sa strany

Pozri časť 4.9.6 aktuálnej verzie CP CA Disig.

4.9.7 Frekvencia vydávania CRL

Žiadne ustanovenia.

4.9.8 Doba publikovania CRL

Žiadne ustanovenia.

4.9.9 **Dostupnosť služby OCSP**

Žiadne ustanovenia.

4.9.10 **Požiadavky na OCSP overovanie**

Žiadne ustanovenia.

4.9.11 Iné formy dostupnosti informácií o **zrušení certifikátu**

Žiadne ustanovenia

4.9.12 **Špeciálne požiadavky na zmenu kľúčov po ich kompromitácii**

Žiadne ustanovenia.

4.9.13 Okolnosti pozastavenia platnosti certifikátu

Žiadne ustanovenia.

4.9.14 Suspendovanie certifikátu

Žiadne ustanovenia.

4.9.15 Postup pre pozastavenie platnosti certifikátu

Žiadne ustanovenia.

4.9.16 Limity pre obdobie pozastavenia

Žiadne ustanovenia.

4.10 **Služby** súvisiace so stavom certifikátu

4.10.1 Prevádzkové charakteristiky

Aktuálne CRL je dostupné na webovom sídle Poskytovateľa (pozri časť 1) a je prístupné prostredníctvom HTTP protokolu na porte 80.

Služba OCSP je dostupná na URL adrese uvedenej vo vydanom certifikáte.

4.10.2 **Dostupnosť služieb**

Distribučné body, na ktorých sú publikované CRL sú k dispozícii v režime 24x7.

Služba OCSP je dostupná v režime 24x7.

4.10.3 Doplnkové funkcie

Žiadne ustanovenia.

4.11 **Ukončenie poskytovanie služieb**

Pozri časť 4.11 aktuálnej verzie CP CA Disig.

4.12 **Uchovávanie a obnova kľúčov**

4.12.1 **Politika a postupy uchovávania a obnovy kľúčov**

Žiadne ustanovenia.

4.12.2 **Politika a postupy ochrany „session key“**

Žiadne ustanovenia.

5. Fyzické, procedurálne a personálne bezpečnostné opatrenia

5.1 Opatrenie týkajúce sa fyzickej bezpečnosti

5.1.1 Priestory

Základná infraštruktúra Poskytovateľa je umiestnená 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 pozostáva len z vybavenia vyhradeného na poskytovanie dôveryhodných služieb a neslúži 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 sú zabezpečené tak, že priestory sú chránené bezpečnostným alarmom a vstup do nich je umožnený len osobám, ktoré vlastnia bezpečnostný token a sú uvedené na zozname oprávnených osôb na vstup do chránených priestorov Poskytovateľa. Vybavenie Poskytovateľa je neprestajne chránené pred neautorizovaným prístupom a to aj pred neautorizovaným fyzickým prístupom.

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, sú umiestnené tak, že ohrozeniu vodou s akýchkoľvek zdrojov je málo pravdepodobné.

5.1.5 **Ochrana pred ohňom**

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

5.1.6 **Úložisko médií**

Médiá sú 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 sú uložené v lokalite oddelenej od vybavenia CMA.

5.1.7 Nakladanie s odpadom

S odpadom vznikajúcim v súvislosti s prevádzkou Poskytovateľa je nakladané tak, že v žiadnom prípade nemôže dôjsť k znečisteniu životného prostredia.

5.1.8 Zálohovanie off-site

Pre prípad nenávratného poškodenia priestorov hlavnej lokality, v ktorých je umiestnená infraštruktúra Poskytovateľa má tento k dispozícii kópiu všetkých najdôležitejších aktív v záložnej lokalite, ktorá je geograficky vzdialená od hlavnej lokality.

5.2 **Procedurálne bezpečnostné opatrenia**

Pri výbere osôb na zastávanie roly Pracovník RA sa kladie dôraz, aby boli zodpovedné a dôveryhodné, lebo táto rola si vyžaduje dôveryhodnosť. Funkcie vykonávané touto rolou patria k funkciám, ktoré formujú v personálnej rovine základ dôvery v Poskytovateľa.

Každá RA, ktorá pracuje v súlade s týmito CPS, je povinná dodržiavať ich ustanovenia. Zodpovednosťou Pracovníka RA je v prvom rade:

- overovanie identity buď prostredníctvom osobného kontaktu alebo prostredníctvom zastupujúceho subjektu,
- zaznamenávanie informácií od žiadateľov o certifikát a overovanie ich správnosti,
- bezpečná komunikácia s Poskytovateľom,
- komunikácia so Zákazníkom/Držiteľom a dokumentovanie tejto komunikácie.

5.2.1 Dôveryhodné role

V rámci CA sú definované dôveryhodné role zodpovedné za jednotlivé aspekty poskytovaných dôveryhodných služieb a rovnako sú definované zodpovednosti jednotlivých rolí.

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

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

5.2.2 **Počet osôb v jednotlivých rolách**

Pre každú úlohu je identifikovaný počet jednotlivcov, ktorí sú určení na ich vykonávanie (pravidlo K z N).

5.2.3 **Identifikácia a autentizácia pre každú** rolu

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

5.2.4 Role vyžadujúce oddelenie zodpovedností

Každá rola má stanovené kritériá, ktoré zohľadňujú potrebu oddelenie funkcií z hľadiska samotnej roly t. j. sú uvedené roly, ktoré nemôžu byť vykonané rovnakými jednotlivcami.

5.3 Personálne bezpečnostné opatrenia

Personálne bezpečnostné opatrenia sú zabezpečované internými mechanizmami právnickej osoby, ktorá má zmluvu s Poskytovateľom o poskytovaní jeho služieb prostredníctvom svojej registračnej autority.

Personál pre rolu Pracovník RA sa vyberá na základe spoľahlivosti, lojality a dôveryhodnosti.

Všetky osoby zastávajúce rolu Pracovníka RA sú náležite poučené a zaškolené v rozsahu potrebnom na výkon činnosti Pracovníka RA a vždy majú k dispozícii aktuálne verzie dokumentov Poskytovateľa určených na výkon činnosti Pracovníka RA, ktoré sú dostupne na webovom sídle https://razona.disig.sk.

Prístup Pracovníka RA k IS Poskytovateľa prostredníctvom aplikácie RA Client, ktoré RA využíva pri svojej činnosti, je chránený pred neautorizovaným prístupom tým, že RA používa na autentizáciu vlastný certifikát RA, prostredníctvom ktorého sa identifikuje a autorizuje.

Dôležitým bezpečnostným opatrením, ktoré podstatným spôsobom obmedzuje možnosť zneužitia elektronickej identity Pracovníka RA (certifikátu RA a najmä k nemu patriaceho súkromného kľúča), je to, že daný pár kľúčov RA je uložený na čipovej karte. Prístup k súkromnému kľúču uloženému na karte je chránený heslom.

Na ochranu vybavenia RA sa použijú aj ďalšie bezpečnostné mechanizmy primerané úrovni hrozby v prostredí vybavenia RA.

5.3.1 Požiadavky na kvalifikáciu, skúsenosti a previerky

Pracovníci v roly registračnej autority spĺňajú kvalifikačné požiadavky požadované pre túto rolu.

5.3.2 Požiadavky na previerky

U roly Pracovník RA sa nepožaduje bezpečnostná previerka.

5.3.3 Požiadavky na školenia

Každý pracovník RA musí prejsť, pred tým ako začne vykonávať svoju funkciu, povinným školením, ktoré vykonávajú poverení pracovníci Poskytovateľa. Tieto školenia sú povinné pre všetky typy RA (pozri časť 1.3.2 CP CA Disig).

5.3.4 Požiadavky na frekvenciu obnovy školení

Obnova školenia pracovníkov RA sa vykonáva na základe rozhodnutia PMA v tých prípadoch, kedy dochádza k významným zmenám, či už v legislatíve alebo

v softvérovom vybavení RA.

5.3.5 Rotácia rolí

Žiadne ustanovenia.

5.3.6 Postihy za neoprávnenú činnosť

Zlyhanie akéhokoľvek pracovníka RA, ktorého výsledok je stav, ktorý nie je v súlade s ustanoveniami tejto CP resp. prijatých CPS, či už sa to týka nedbanlivosti alebo zlého úmyslu, bude predmetom zodpovedajúcich administratívnych a disciplinárnych konaní zo strany Poskytovateľa na základe interných predpisov resp. existujúcich zmlúv s externými RA

5.3.7 Požiadavky na externých dodávateľov

Žiadne ustanovenia.

5.3.8 Dokumentácia dodávané pre personál

Pracovníci RA majú k dispozícii dokumenty potrebné pre výkon funkcie, na ktorú sa sú priradení, vrátane kópie tejto CP resp. CPS a všetky technické a prevádzkovej dokumentácie potrebné k zachovaniu integrity operácií Poskytovateľa. Táto dokumentácia je pre nich dostupná na portáli razona.disig.sk.

5.4 Postupu získavania auditných záznamov

5.4.1 Typy zaznamenávaných udalosti

Všetky udalosti týkajúce sa vykonaných operácií v aplikácii RA Client sú zaznamenávané priamo aplikáciou. Rovnako, všetky informácie zasielané z aplikácie RA Client sú zaznamenávané na serverovej strane u Poskytovateľa služby.

Udalosti týkajúce sa životného cyklu certifikátov pre koncových používateľov v rozsahu:

- žiadosť o vydanie certifikátu,
- schválenie žiadosti o vydanie,
- vydanie certifikátu,
- rušenie certifikátu,

sú zaznamenávané v databáze SWACA.

5.4.2 Frekvencia spracovávania auditných záznamov

Auditné záznamy týkajúce sa činnosti RA sa analyzujú pravidelne v prípade nahlásenia problému pri vydávaní certifikátov zo strany pracovníkov RA.

5.4.3 Uchovávanie logov

Zaznamenávané udalosti v zmysle odseku 5.4.1 sú uchovávané minimálne 2 roky od skončenia platnosti vydaného certifikátu.

5.4.4 Ochrana auditných záznamov

Všetky záznamy sú na RA uchovávané a chránené tak, aby nedošlo k ich znehodnoteniu.

5.4.5 Postupy zálohovania auditných logov

Žiadne ustanovenia.

5.4.6 Systém zálohovania logov

Poskytovateľ má vybudovaný systém na zálohovania logov.

5.4.7 Notifikácia subjektu iniciujúceho log záznam

Žiadne ustanovenia.

5.4.8 **Posudzovanie zraniteľností**

Žiadne ustanovenia.

5.5 Uchovávanie záznamov

5.5.1 Typy archivovaných záznamov

RA uchováva všetky záznamy o vydaných certifikátoch po dobu, ktorá je stanovená v príslušnej zmluve o RA a tieto odovzdáva Poskytovateľovi v intervaloch stanovených v zmluve o RA.

Záznamy sú uchovávané v papierovej forme resp. v elektronickej forme. Súčasťou uchovávaných záznamov sú aj všetky dokumenty, ktoré musí Zákazník/Držiteľ predložiť k tomu, aby mu bol vydaný požadovaný typ certifikátu (napr. výpis z obchodného registra, plná moc potvrdenie o vlastníctve domény ap.).

5.5.2 Doba uchovávania záznamov

Záznamy sú u externých RA uchovávané do doby pokiaľ nie sú odovzdané Poskytovateľovi. Poskytovateľ uchováva záznamy v súlade s požiadavkou v časti 5.5.2 CP CA Disig.

Poskytovateľ uchováva záznamy v súlade s požiadavkou v bode 5.5.2 CP CA Disig.

5.5.3 Ochrana archívnych záznamov

Archívne záznamy RA sú uchovávané až do ich odovzdania Poskytovateľovi na bezpečnom mieste a sú 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 pracovníka RA**

Pracovník RA môže používať svoje prístupové kľúče iba na prístup k IS Poskytovateľa prostredníctvom aplikácie RA Client, podpisovanie operácií v aplikácii RA Client a prístup k portálu razona.disig.sk.

Prístupové kľúče Pracovníka RA sú pravidelne obmieňané v intervale cca 1 rok.

5.7 Obnova po kompromitácia alebo havárii

5.7.1 **Postupy riešenia incidentov a kompromitácie**

V prípade, že dôjde ku kompromitácii kľúča pracovníka RA napr. stratou kľúča, prezradením prístupových hesiel ap., musí byť tento incident zo strany Pracovníka RA okamžite nahlásený Poskytovateľ, aby mohli byť prijaté príslušné opatrenia na minimalizáciu možnosti zneužitia prístupových práv k IS Poskytovateľa.

5.7.2 **Poškodenie hardvéru, softvéru alebo** údajov

Žiadne ustanovenia.

5.7.3 **Postupy pri kompromitácii kľúča CA**

V prípade kompromitácie súkromného kľúča Pracovníka RA musí Poskytovateľ okamžite zrušiť príslušný certifikát a zrušiť jeho autorizáciu vo svojom IS.

5.7.4 **Zachovanie kontinuity činnosti po havárii**

Žiadne ustanovenia.

5.8 **Ukončenie činnosti RA**

Pri ukončení činnosti RA musí RA:

- Vhodným spôsobom, v zmysle zmluvy o RA, vopred, oznámiť úmysel ukončiť svoju činnosť Poskytovateľovi
- Podľa pokynov Poskytovateľa sústrediť a pripraviť na odovzdanie všetky dokumenty spojené s poskytovanými dôveryhodnými službami.
- Vyradiť z používania všetky súkromné kľúče Pracovníkov RA a tieto odovzdať Poskytovateľovi.

6. Technické bezpečnostné opatrenia

6.1 Generovanie a **inštalácia páru kľúčov**

6.1.1 Generovanie a **inštalácia páru pre jednot**livé subjekty

6.1.1.1 Vydavateľ certifikátov

Žiadne ustanovenia.

6.1.1.2 Registračné autority

Generovanie prístupových kľúčov a vydávanie autentifikačných certifikátov pre Pracovníkov RA vykonávajú poverení pracovníci Poskytovateľa. Všetky prístupové kľúče sú uložené na kvalifikovanom zariadení pre elektronický podpis, kde prístup ku kľúčom je chránený prístupovým heslo, ktoré si volí Pracovník RA. Takto je zabezpečená dvojfaktorová autentifikácia pri vydávaní certifikátu prostredníctvom IS Poskytovateľa.

6.1.1.3 Koncoví používatelia

Žiadne ustanovenia.

6.1.2 **Doručenie súkromného kľúča držiteľovi certifikátu**

Pozri časť 6.1.2 aktuálnej verzie CP CA Disig.

Všetky kvalifikované zariadenia pracovníkov RA sú buď odovzdávané osobne v sídle Poskytovateľa alebo sú zasielané doporučenou poštou do vlastných rúk Pracovníka RA. Pri zasielaní doporučenou poštou je inicializácia prístupových práv pre Pracovníkov RA v IS Poskytovateľa vykonaná až po potvrdení doručenia kvalifikovaného zariadenia zo strany Pracovníka RA.

6.1.3 **Doručenie verejného kľúča vydavateľovi certifikátu**

Verejný kľúč je pri vydávaní certifikátu doručený certifikačnej autorite bezpečne prostredníctvom aplikácie RA Client v on-line režime počas procesu vydávania certifikátu. Komunikácia medzi aplikáciou RA Client a vydávajúcou CA je autorizovaná podpísaním všetkých zasielaných údajov pracovníkom RA, kde oprávnenie na vydanie daným pracovníkom RA je kontrolované na strane CA v automatickom režime.

6.1.4 **Doručenie verejného kľúča CA spoliehajúcim sa stranám**

Všetky certifikáty vydávajúcich certifikačných autorít sú dostupné prostredníctvom webového sídla poskytovateľa na adrese: https://eidas.disig.sk/sk/cacert/.

6.1.5 **Dĺžky kľúčov**

Algoritmy a dĺžky kľúčov uplatňované v certifikátoch AdmCA:

Algoritmus podpisu (Signature Algorithm)
sha256RSA

Verejný kľúč
RSA, dĺžka je 2048 bitov

Algoritmy a dĺžky kľúčov uplatňované v certifikáte koreňovej CA Disig:

Algoritmus podpisu (Signature Algorithm)
sha256RSA

Verejný kľúč
RSA, dĺžka 4096 bitov

Algoritmy a dĺžky kľúčov uplatňované v certifikáte podriadených CA Disig:

Algoritmus podpisu (Signature Algorithm)
sha256RSA

Verejný kľúč
RSA, dĺžka je minimálne 2 048 bitov

Doba platnosti certifikátu
Maximálne 15 rokov*

* - hodnota „Valid to“ certifikátu podriadenej CA nesmie prekročiť hodnotu poľa „Valid to“ nadriadenej (koreňovej) CA.

Dĺžky kľúčov v certifikátoch pre koncových používateľov sú uvedené v časti 7.1.4 aktuálnej verzie CP CA Disig.

6.1.6 Parametre a **kvalita verejného kľúča**

Pozri časť 6.1.5 týchto CPS a rovnako aj časť 7 aktuálnej verzie CP CA Disig.

6.1.7 **Použitie kľúčov**

Kľúče vydané pracovníkom RA je možné využívať len na prístup k IS Poskytovateľa prostredníctvom aplikácie RA Client a tiež na podpisovanie zasielaných údajov v procese vydávania certifikátu v aplikácii RA Client. Tiež môžu byť použité na prístup k portálu razona.disig.sk, kde sú dostupné všetky potrebné informácie pre Pracovníkov RA.

6.2 **Ochrana súkromného kľúča** a technické opatrenia pre kryptografický modul

6.2.1 **Štandardy a opatrenia pre kryptografický modul**

Žiadne ustanovenia.

6.2.2 O**patrenia (K z N) pre manipuláciu so súkromným kľúčom**

Žiadne ustanovenia.

6.2.3 **„Key escrow“ súkromného kľúča**

Žiadne ustanovenia.

6.2.4 **Zálohovanie súkromného kľúča**

Žiadne ustanovenia..

6.2.5 **Archivácia súkromného kľúča**

Žiadne ustanovenia

6.2.6 **Prenos súkromných kľúčov z a do HSM modulu**

Žiadne ustanovenia.

6.2.7 **Uchovávanie súkromných kľúčov v HSM module**

Žiadne ustanovenia.

6.2.8 **Spôsob aktivácie súkromných kľúčov**

Žiadne ustanovenia.

6.2.9 Spô**sob deaktivácie súkromného kľúča**

Žiadne ustanovenia.

6.2.10 **Spôsob zničenia súkromného kľúča**

Žiadne ustanovenia.

6.2.11 Charakteristika HSM modulu

Žiadne ustanovenia.

6.3 Ďalšie aspekty manažmentu kľúčového páru

6.3.1 Archivácia verejných kľúčov

Žiadne ustanovenia.

6.3.2 Dĺžka platnosti certifikátov a použiteľnosť kľúčového páru

Platnosť Poskytovateľom vydávaných certifikátov pre Pracovníkov RA nesmie prekročiť nasledovné:

Typ certifikátu	Platnosť (maximálne)
Certifikát Pracovníka RA	maximálne 365 dní

6.4 Aktivačné údaje

6.4.1 Vytváranie a inštalácia aktivačných údajov

Aktivačné údaje k súkromnému kľúču pracovníka RA si volí sám Pracovník RA sám ihneď po prebratí kvalifikovaného zariadenia ešte pred jeho prvým použitím na prístup k IS Poskytovateľa prostredníctvom aplikácie RA Client.

6.4.2 Ochrana aktivačných údajov

Za ochranu súkromných kľúčov Pracovníka RA je zodpovedný výhradne samotný Pracovník RA.

Pri vydávaní certifikátu je každý Pracovník RA upozornený so strany zodpovednej osoby Poskytovateľa o potrebe chrániť súkromný kľúč silným heslom, aby nemohlo dôjsť k jeho zneužitiu, počas celej doby jeho používania.

6.4.3 Ostatné aspekty aktivačných údajov

Pozri časť 6.4.3 aktuálnej verzie CP CA Disig.

6.5 Riadenie bezpečnosti počítačov

6.5.1 Špecifické požiadavky na bezpečnosť počítačov

Pozri časť 6.5.1 aktuálnej verzie CP CA Disig..

6.5.2 Hodnotenie bezpečnosti informácií

Žiadne ustanovenia.

6.6 Opatrenia v životnom cykle

6.6.1 Opatrenia pri vývoji systémov

Pozri časť 6.6.1 aktuálnej verzie CP CA Disig.

6.6.2 Opatrenia na riadenie bezpečnosti

Žiadne ustanovenia.

6.6.3 Bezpečnostné opatrenia v životnom cykle

Žiadne ustanovenia.

6.7 Sieťové bezpečnostné opatrenia

Žiadne ustanovenia.

6.8 Využívanie časovej pečiatky

Žiadne ustanovenie

7. Profily certifikátov a zoznamov zrušených certifikátov

Profily certifikátov a zoznamov zrušených certifikátov sú stanovené centrálne – pracovníci RA nemôžu meniť štruktúru certifikátov.

7.1 Profily certifikátov

7.1.1 Verzia

Pozri časť 7.1.1 CP CA Disig.

7.1.2 **Rozšírenia v** certifikátoch

Pozri časť 7.1.2 CP CA Disig.

7.1.3 **Identifikátory použitých algoritmov**

Pozri časť 7.1.3 CP CA Disig.

7.1.4 Formy mien

Pre pracovníkov RA sú vydávané certifikáty pre FO s uvedením názvu príslušnej RA v časti organizationUnit certifikátu.

7.1.5 Obmedzenia týkajúce sa mien

Žiadne ustanovenia.

7.1.6 Identifikátor pravidiel CPS

Pozri časť 1.2.

7.1.7 **Použitie rozšírení na obmedzenie politiky**

Žiadne ustanovenia.

7.1.8 Syntax a sémantika politiky

Žiadne ustanovenia

7.1.9 **Sémantika spracovania kritických certifikačných politík**

Žiadne ustanovenia.

7.1.10 Ostatné ustanovenia

Žiadne ustanovenia.

7.2 Profily zoznamov zrušených certifikátov

7.2.1 Verzia

Pozri časť 7.2 aktuálnej verzie CP CA Disig.

CRL vydávané CA Disig sú CRL verzie 2.

Algoritmus podpisu (Signature Algorithm):	sha256RSA

CRL obsahuje všetky zrušené certifikáty vrátane tých, ktoré už v čase vydania daného CRL nie sú platné.

7.2.2 **Použité rozšírenia (CRL extensions) v CRL vydávanom Poskytovateľom**

Žiadne ustanovenia

7.3 Profil OCSP

7.3.1 Verzia

Žiadne ustanovenia.

7.3.2 **OCSP rozšírenia**

Žiadne ustanovenia.

8. Audit zhody

Pozri časť 8 aktuálnej verzie CP CA Disig.

Na základe rozhodnutia externej organizácie, ktorá vykonáva posúdenie zhody poskytovaných dôveryhodných služieb Poskytovateľa, sa musí každá externá RA podrobiť auditu poskytovaných služieb a poskytnúť maximálnu súčinnosť, pokiaľ bude o umožnenie auditu požiadaná. Prípadné odmietnutie bude mať za následok ukončenie zmluvy a spolupráce s predmetnou RA.

8.1 Frekvencia auditu zhody pre danú entitu

Pozri časť 8.1 aktuálnej verzie CP CA Disig.

8.2 Identita audítora a kvalifikačné požiadavky na neho

Pozri časť 8.2 aktuálnej verzie CP CA Disig.

8.3 Vzťah audítora k auditovanému subjektu

Žiadne ustanovenia.

8.4 Témy pokryté audiom

Pozri časť 8.4 aktuálnej verzie CP CA Disig.

8.5 Akcie vykonané na odstránenie nedostatkov

Pozri časť 8.5 aktuálnej verzie CP CA Disig.

8.6 Zaobchádzanie s výsledkami auditu

Pozri časť 8.2 aktuálnej verzie CP CA Disig.

8.7 Interný audit

Počas obdobia, v ktorom externá RA vykonáva svoju činnosť musí Poskytovateľ monitorovať jej činnosť a kontrolovať ňou poskytované služby vykonávaním pravidelnej kontroly dodaných podkladov k vydaným certifikátom. V prípade zistenia závažnejších nedostatkov môže Poskytovateľ kedykoľvek vykonať audit predmetnej RA na zistenie príčin daných nedostatkov.

9. Iné obchodné a právne záležitosti

9.1 Poplatky

Cenník dôveryhodných služieb resp. informáciu, za akých zmluvných podmienok je možné tieto služby objednať je zverejnený na webovom sídle Poskytovateľa: https://eidas.disig.sk/sk/poskytovatel/cenniky/.

9.1.1 Poplatky za vydanie certifikátu

Pozri časť 9.1.1. aktuálnej verzie CP CA Disig.

9.1.2 Poplatok za prístup k certifikátu

Žiadne ustanovenia.

9.1.3 **Poplatky za služby vydávania CRL a** OCSP

Tieto služby sú poskytované bezodplatne.

9.1.4 **Poplatky za ostatné služby**

Žiadne ustanovenia.

9.1.5 Vrátenie platby

Žiadne ustanovenia.

9.2 **Finančná zodpovednosť**

Poskytovateľ má dostatočné zdroje na výkon ním poskytovaných dôveryhodných služieb.

9.2.1 Poistenie

Poskytovateľ je poistený v súvislosti s možnými škodami, ktoré môžu byť spôsobené Zákazníkom/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 Zákazníkov

Žiadne ustanovenia.

9.3 **Dôvernosť**

9.3.1 **Typy informácií, ktoré sa majú chrániť**

Pozri časť 9.3.1 aktuálnej verzie CP CA Disig.

9.3.2 Nechránené informácie

Pozri časť 9.3.2 aktuálnej verzie CP CA Disig.

9.3.3 **Zodpovednosť za ochranu dôverných informácií**

Externé RA sú zodpovedné za ich ochranu dôverných informácií v zmysle zmluvy, ktorú majú uzavretú s Poskytovateľom.

9.4 Ochrana osobných údajov

9.4.1 Politika ochrany osobných údajov

Pozri časť 9.4.1 aktuálnej verzie CP CA Disig.

Poskytovateľ spracováva osobné údaje Zákazníkov/Držiteľov certifikátov, resp. nimi splnomocnených osôb v súlade s požiadavkami 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“) [7].

9.4.2 **Informácie považ**ované za osobné údaje

Poskytovateľ má definovaný rozsah osobných údajov, ktorý spracováva pri poskytovaní dôveryhodných služieb.

9.4.3 **Informácie, ktoré nie sú považované za osobné údaje**

Žiadne ustanovenia.

9.4.4 **Zodpovednosť za ochranu osobných údajov**

Externé RA sú zodpovedné za ochranu osobných údajov Zákazníkov/Držiteľov certifikátov a musia ich chrániť pred prezradením a musia sa zdržať ich poskytnutia tretej strane.

9.4.5 Súhlas so spracovaním osobných údajov

Poskytovateľ si plní informačnú povinnosť voči dotknutým osobám v súlade s požiadavkami predpisov o ochrane osobných údajov [7].

9.4.6 Zverejnenie na základe súdneho alebo správneho procesu

Žiadne ustanovenia.

9.4.7 **Ďalšie okolnosti zverejňovania informácií**

Žiadne ustanovenia.

9.5 **Práva duševného** vlastníctva

Táto CPS a s ňou súvisiace dokumenty predstavujú významné know-how Poskytovateľa a sú chránené jeho autorskými právami.

9.6 Vyhlásenie a záruky

Pozri časť 9.6, aktuálnej verzie CP CA Disig.

9.6.1 Vyhlásenia a **záruky Poskytovateľa**

Pozri časť 9.6.1 aktuálnej verzie CP CA Disig.

9.6.2 Vyhlásenia a záruky RA

Všetky externé registračné autority Poskytovateľa poskytujú dôveryhodné služby na základe zmluvného vzťahu s poskytovateľom a v súlade s týmito CPS.

Ďalej pozri ustanovenia v časti 9.6.

9.6.3 Vyhlásenie a **záruky Držiteľa**

Žiadne ustanovenia.

9.6.4 Vyhlásenia a záruky spoliehajúcej sa strany

Žiadne ustanovenia.

9.6.5 Vyhlásenia a záruky iných strán

Žiadne ustanovenia.

9.7 Odmietnutie poskytnutia záruky

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

9.8 Obmedzenie zodpovednosti

Pozri časť 9.6.1 aktuálnej verzie CP CA Disig.

9.9 Náhrada škody

Pre tieto CPS platí v plnom rozsahu časť 9.9 aktuálnej verzie CP CA Disig.

9.10 Doba platnosti, ukončenie platnosti

9.10.1 Doba platnosti

Tato verzia CPS platí odo dňa nadobudnutia jej platnosti t. j. 1. 9. 2023 až do jej nahradenia novou verziou. Podrobnosti o histórii zmien tejto CP sú uvedené v časti 1.2.1 „História zmien“.

9.10.2 Ukončenie platnosti

Platnosť tejto verzie CPS skončí dňom publikovania novej verzie s vyšším číslom ako je 5.9, prípadne ukončením činnosti poskytovania dôveryhodných služieb Poskytovateľom v čase ich 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 týchto CPS týkajúce sa Poskytovateľa, ktoré je povinný dodržať po ukončení svojej činnosti (pozri časť 9).

9.11 Jednotlivé oznámenia a komunikácia s účastníkmi

Komunikácia Poskytovateľa s jednotlivých RA oficiálne prebieha prostredníctvom autorizovanej e-mailovej komunikácie medzi poverenými osobami Poskytovateľa a poverenou osobou RA.

9.12 Zmeny

9.12.1 Postup vykonávania zmien

Aktualizácia CPS sa vykonáva na základe ich preskúmania, ktoré je vykonané minimálne 1x ročne od schválenia aktuálne platnej verzie. Preskúmanie vykonáva poverený pracovník Poskytovateľa, ktorý na základe výsledkov preskúmania pripravuje písomný návrh na prípadné navrhované zmeny.

Schválenie navrhovaných zmien vykonáva poverený člen PMA v zmysle požiadaviek daných V časti 9.12.1 aktuálnej verzie CP CA Disig.

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

Všetky schválené zmeny CPS sú dávané na vedomie subjektom, ktorých sa týkajú, v lehote jedného týždňa pred nadobudnutím ich účinnosti, a to prostredníctvom kanálov publikačnej a oznamovacej politiky.

Každá zmenená verzia týchto CPS 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 týchto CPS.

9.12.2 Postup a periodicita oznamovania zmien

Poskytovateľ publikuje informácie týkajúce sa aktuálnej verzie CPS prostredníctvom svojho webového sídla (pozri časť 1).

Poverený zástupca Poskytovateľa informuje všetky zmluvne viazané RA Poskytovateľa o schválení novej verzie CPS, zaslaním jeho verzie elektronickou poštou.

9.12.3 Okolnosti zmeny OID

Všetky pravidlá majú stanovený svoj OID Poskytovateľom. OID týchto CPS je uvedený v časti 1.2 a pre každú novú verziu CPS zostáva nezmenený.

9.13 **Riešenie sporov**

Pozri časť 9.13 aktuálnej verzie CP CA Disig.

9.14 Rozhodné právo

Pozri časť 9.14 aktuálnej verzie CP CA Disig.

9.15 Súlad s platnými právnymi predpismi

Pozri časť 9.13 aktuálnej verzie CP CA Disig.

9.16 Rôzne ustanovenia

9.16.1 Rámcová dohoda

Žiadne ustanovenia.

9.16.2 Postúpenie práv

RA nesmie svoje práva, povinnosti z týchto CPS postúpiť alebo previesť (ani s nimi akokoľvek inak obchodovať) tretej osobe bez písomného súhlasu Poskytovateľa.

9.16.3 Salvatórska klauzula

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

9.16.4 Uplatnenie práv

Pozri časť 9.16.4 aktuálnej verzie CP CA Disig.

9.16.5 **Vyššia moc**

Pozri časť 9.16.5 aktuálnej verzie CP CA Disig.

9.17 Iné ustanovenia

Žiadne ustanovenia.