Pravidlá

poskytovania dôveryhodnej služby vyhotovovania a overovania certifikátov - **časť:** RA

Disig, a.s.

Vypracoval	Ing. Peter **Miškovič**
Dátum platnosti	25.9.2017
Verzia	5.0
Typ	PRAVIDLÁ
Schválil	Ing. **Ľuboš Batěk**

Obsah

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

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 5.0 s platnosťou od 25.9.2017.

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]; Zákon č. 272/2014 Z.z. o dôveryhodných službách [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 [6], 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 [6].

1.2 Identifikácia

Názov:	Pravidlá Poskytovania dôveryhodnej služby vyhotovovania a overovania certifikátov - **časť:** RA
Skratka názvu:	CPS RA CA Disig
Verzia:	5.0
Schválené dňa:	18.9.2017
Platnosť od:	25.9.2017
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 (SSL 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); Miškovič
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); Miškovič
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	18.9.2017	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

1.3 Komunita a **použiteľnosť**

1.3.1 **Certifikačné** autority

Tieto CPS sa týkajú poskytovania dôveryhodných služieb podriadenými certifikačnými autoritami patriacich pod koreňové certifikačné autority CA Disig Root R2 a CA Disig Root R1 – 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

Poskytovateľa v zmysle týchto CPS vydáva koncovým klientom tieto typy certifikátov:

- certifikáty pre fyzické osoby určené najmä pre potreby zabezpečenia elektronickej pošty alebo podpisovanie elektronických dokumentov,
- certifikáty pre právnické osoby určené na vyhotovovanie elektronickej pečate,
- SSL certifikáty určené pre potreby zabezpečenia autentifikácie webového sídla.

1.4.1 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/

Zoznam ostatných registračných autorít Poskytovateľa je dostupný na jeho webovom sídle na adrese: http://eidas.disig.sk/sk/ralist/.

1.5.3 Osoba rozhodujúca o súlade CPS s CP

Pozri časť 1.5.3 CP CA Disig.

1.5.4 Postupy **schvaľovania** 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

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. *Zákon* ***č.*** *272/2016 Z.z. o dôveryhodných službách pre elektronické transakcie na vnútornom trhu a o zmenea doplnení niektorých zákonov (zákon o dôveryhodných službách).*

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. *CA/Browser Forum Baseline Requirements for the Issuance and Management of Publicly-Trusted Certificates v. 1.4.9.*

7. Zákon **č.** 122/2013 Z. z. o ochrane osobných údajov a o zmene a doplnení niektorých zákonov.

8. Všeobecné podmienky poskytovania a používania dôveryhodnej služby vyhotovovania a overovania certifikátov Disig, a.s.

9. *Electronic Signatures and Infrastructures (ESI); Policy and security requirements for Trust Service Providers issuing certificates; Part 1: General requirements.*

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.

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 neprirad'uje 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 obchodných **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 SSL 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 musí pre vydaním SSL certifikátu overiť, či Zákazník má kontrolu nad doménou (doménami), ktorých FQDN sa nachádza v položke žiadosti commonName (CN) resp. je požadované jeho umiestnenie v položke SubjectAltName (SAN). Overenie vykoná jedným zo spôsobov, ktoré sú uvedené v časti 3.2.2.4 aktuálnej verzie CP CA Disig, kde preferovaný je prvý spôsob – potvrdenie.

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“ SSL 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“ SSL 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“.

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 SSL 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 SSL 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.

3.2.7 Identifikácia a autentifikácia pri vydávaní následného certifikátu

Podmienky vydania následného certifikátu sú podrobne popísané v časti 3.2.7 aktuálnej verzie CP CA Disig.

RA vykoná vydanie certifikátu bez osobnej návštevy držiteľa len v prípade certifikátu pre fyzickú osobu resp. certifikátu pre právnickú osobu len po splnení podmienok uvedených v časti 3.2.7 aktuálnej verzie CP CA Disig. Overovanie zaslanej žiadosti, v prípade nepodpísaného e-mailu z e-mail adresy zhodnej z adresou uvedenou v prijatej žiadosti resp. zaslanej z iného e-mailu ako je v prijatej žiadosti, vykoná RA tak, že na danú e-mail adresu zašle elektronickú správu ktorá bude obsahovať tajnú nepredvídateľnú informáciu (overovacia informácia). Žiadateľ o certifikát musí zaslať späť overovaciu informáciu ako dôkaz kontroly zaslania žiadosti o vydanie následného certifikátu. Odpoveď musí byť zaslaná v stanovenom časovom úseku, dostatočnom na odoslanie elektronickej pošty. V prípade, že overenie zaslania žiadosti prebehne neúspešne, Poskytovateľ odmietne vydanie certifikátu.

3.2.8 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 Identifikácia a autentifikácia pri žiadaní o zrušenie certifikátu

Pozri časť 3.3 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.

4.1.3 Generovanie žiadosti

Pozri časť 4.1.3 aktuálnej verzie CP CA Disig.

4.1.4 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

1. Pracovník RA overí, či elektronicky zaslaná žiadosť o vydanie certifikátu daného Zákazníka (povinné pri certifikátoch s rozšírením „Secure Email (1.3.6.1.5.5.7.3.4)“), bola zaslaná z rovnakej e-mail adresy, aká sa nachádza v žiadosti o vydanie certifikátu. V prípade zistených rozdielov odmietne vydanie certifikátu.
2. V prípade, že vopred zaslaná žiadosť o vydanie certifikátu obsahuje rovnakú e-mail adresu z akej bola zaslaná, vykoná pracovník RA overenie kontroly tejto e-mailovej adresy. Overenie sa vykoná tak, že na danú e-mail adresu zašle elektronickú správu ktorá bude obsahovať tajnú nepredvídateľnú informáciu (overovacia informácia). Žiadateľ o certifikát musí zaslať späť overovaciu informáciu ako dôkaz kontroly danej e-mail adresy. Odpoveď musí byť zaslaná v stanovenom časovom úseku, dostatočnom na odoslanie elektronickej pošty. V prípade, že overenie e-mail adresy prebehne neúspešne Poskytovateľ odmietne vydanie certifikátu. Detailný postup je popísaný v príslušných príručkách pre pracovníkov RA a rovnako je predmetom úvodného školenia pracovníkov RA. Overovanie e-mailovej adresy nie je potrebné v prípade, že je zaslaná žiadosť o následný certifikát elektronicky e-mailom, ktorý je podpísaný platným certifikátom žiadateľa, vydaným certifikačnou autoritou Poskytovateľa a e-mailová adresa, z ktorej

bola žiadosť zaslaná je zhodná s e-mailovou adresou nachádzajúcou sa v žiadosti.

3. U zmluvných partnerov Poskytovateľa, ktorí zasielajú žiadosti na vydanie certifikátu so zmluvne dohodnutej domény sa overovanie vlastníctva e-mail adresy nevykonáva.

4.2.1.2 Postup pri registrácii zákazníka priamo na RA

1. Pracovník RA informuje prítomnú fyzickú osobu o Všeobecných podmienkach [7] 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. Žiadosť o vydanie osobného certifikátu určeného na podpisovanie a šifrovanie elektronickej pošty musí byť zaslaná na príslušnú RA elektronicky z adresy, ktorá bude uvedená v DN žiadosti v položke E-mail.
4. Pracovník RA skontroluje úplnosť a správnosť prijatej žiadosti o certifikát (napr. či niektoré položky neobsahujú zjavne chybné údaje).

   Upozornenie: Všetky položky musia byť vyplnené bez diakritiky. Malé a veľké písmená sa rozlišujú. Položky "Mesto:", "Firma:" a "Útvar vo firme:" sú nepovinné. Položka žiadosti zobrazovaná ako "E-mail" musí byť vyplnená povinne platnou email adresou zákazníka.

   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. Pracovník RA predloží Zákazníkovi na podpis zmluvu o vydaní a používaní certifikátu a služieb 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 vydaní 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 vydaní.

4.2.1.3 Detailný postup na získanie SSL 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 SSL 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 SSL certifikát resp. v nej sa nachádzajúci verejný kľúč, na ktorý už bol vydaný certifikát, nemôže byť z bezpečnostných dôvodov použitá opakovane na vydanie iného SSL certifikátu a bude na RA odmietnutá! Žiadosť o SSL 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 SSL 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 SSL certifikát. Všetky údaje sa musia zadávať bez diakritiky (mäkčene, dĺžne a pod.). V poli Organizácia sa nesmie použiť znak čiarka. Žiadateľom o SSL certifikát môže byť len štatutár organizácie resp. ním splnomocnená osoba, ktorej patrí entita, pre ktorú je SSL 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 SSL certifikát.

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

4.2.1.4 Postup RA pred vydaním SSL 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 SSL 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 SSL certifikát.

10. Bezprostredne po vydaní certifikátu bude môcť žiadateľ o certifikát prevziať svoj certifikát. Pritom podpíšu žiadateľ o certifikát a pracovník RA „Potvrdenie o vydaní certifikátu a jeho odovzdaní žiadateľovi o certifikát“, ktoré tvorí prílohu Zmluvy o vydaní a používaní certifikátu a službieb CA Disig. Toto potvrdenie sa vyhotoví v dvoch exemplároch – jeden pre žiadateľa a jeden zostane RA, ktorá ho potom postúpi vydávajúcej CA Disig.

4.2.2 Schválenie alebo zamietnutie žiadosti o certifikát

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.

4.2.3 **Čas** na spracovanie žiadosti o vydanie certifikátu

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.

4.2.4 **Doručenie** verejného **kľúča vydavateľovi** certifikátu

Pozri časť 4.1.4 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 v certifikáte resp. pokiaľ certifikát neobsahuje e-mailovú adresu, tak na e-mailovú adresu 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 http://eidas.disig.sk/sk/crtsearch/ 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.

4.6 Obnova certifikátu

Pozri časť 4.6 aktuálnej verzie CP CA Disig.

4.7 Vydanie certifikátu na nové **kľúče**

Pri vydávaní certifikátu na nové kľúče sa postupuje rovnako ako pri vydávaní prvotného certifikátu – pozri časť 4.3.

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

Vydanie nového certifikátu na pôvodné kľúče z dôvodu zmien týkajúcich sa obsahu certifikátu Poskytovateľ nepodporuje.

4.9 Zrušenie a suspendovanie 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).

4.9.4 Čas na podanie žiadosti 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

Poskytovateľ takúto službu neposkytuje.

4.9.14 Suspendovanie certifikátu

Poskytovateľ túto službu neposkytuje.

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 24/7/365.

Služba OCSP je dostupná v režime 24/7/365.

4.11 **Ukončenie** poskytovanie služieb

Pozri časť 4.11 aktuálnej verzie CP CA Disig.

4.12 Uchovávanie a obnova **kľúčov**

Pozri časť 4.12 aktuálnej verzie CP CA Disig.

5. Fyzické, procedurálne a personálne **bezpečnostné** opatrenia

5.1 Fyzické **bezpečnostné** opatrenia

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.

5.2 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.

5.3 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 musí vyberať 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.

5.4 Postupu získavania auditných záznamov

5.4.1 Typy zaznamenávaných udalosti

Žiadne ustanovenia.

5.4.2 Frekvencia spracovávania auditných záznamov

Žiadne ustanovenia.

5.4.3 Uchovávanie logov

Žiadne ustanovenia.

5.4.4 Ochrana auditných záznamov

Všetky záznamy musia byť 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 musí mať 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 musí uchovávať všetky záznamy o vydaných certifikátoch po dobu, ktorá je stanovená v príslušnej zmluve o RA a tieto odovzdávať Poskytovateľovi v intervaloch stanovených v zmluve o RA.

Záznamy môžu byť uchovávané v papierovej forme resp. v elektronickej forme. Súčasťou uchovávaných záznamov musia byť 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

Pozri časť 5.5.1.

5.5.3 Ochrana archívnych záznamov

Archívne záznamy RA musia byť až do ich odovzdania Poskytovateľovi uložené na bezpečnom mieste 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** 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 jednotlivé 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

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 – zákazník ani RA nemôžu meniť štruktúru certifikátov.

7.1 Profily certifikátov

Profily vydávaných certifikátov sú uvedené v aktuálne platnom CP CA Disig v časti 7.1.

7.2 Profily zoznamov zrušených certifikátov

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.

7.3 Profil OCSP

Pozri časť 7.3 aktuálnej verzie CP CA Disig.

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 Poskytovať 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 - http://eidas.disig.sk/sk/pricelist/.

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 zákona č. 122/2013 Z. z. [7].

9.4.2 Informácie považované 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 má k dispozícii súhlas so spracovaním osobných údajov Držiteľa certifikátu v súlade s požiadavkami Zákona č. 122/2013 Z. z. [7].

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. 18.9.2017 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 5.0, 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.