POLITIKA

poskytovania dôveryhodnej služby vyhotovovania a overovania certifikátov

Disig, a.s.

Vypracoval	**Ing. Peter Miškovič**
Dátum platnosti	**1 10. 2022**
Verzia	**5.7**
Typ	**POLITIKA**
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
E-mail	disig@disig.sk

1. Úvod

Tento dokument špecifikuje politiku (ďalej aj „CP“) spoločnosti Disig, a.s., so sídlom Záhradnícka 151, 821 08 Bratislava, IČO: 35975946, zapísanú v Obchodnom registri OS BA I, odd. Sa, vložka č. 3794/B, ako poskytovateľa dôveryhodných služieb (ďalej len „Poskytovateľ“) a platí pre všetky koreňové certifikačné autority a k nim podriadené certifikačné autority, prevádzkované Poskytovateľom, prostredníctvom ktorých poskytuje dôveryhodné služby, s výnimkou kvalifikovaných dôveryhodných služieb.

Certifikáty vyhotovované pre koncových používateľov jednoznačne identifikujú entitu, ktorej je certifikát vydávaný a túto entitu zväzujú s príslušným párom kľúčov. Pokiaľ v politike nie je vyslovene uvedené, že sa to týka certifikátu koreňovej certifikačnej autority resp. podriadenej certifikačnej autority, tak slovo certifikát znamená certifikát koncovej entity.

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

https://eidas.disig.sk

1.1 Prehľad

Táto CP definuje vytváranie a správu certifikátov s verejnými kľúčmi, podľa štandardu X.509 verzie 3 [1] v súlade s požiadavkami RFC 5280 „Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile“ [2], požiadavkami Baseline Requirements for the Issuance and Management of Publicly-Trusted Certificates [3] (ďalej aj „BR“) a požiadavkami Nariadenia Európskeho parlamentu a Rady (EÚ) č. 910/2014 z 23. júla 2014 o elektronickej identifikácii a dôveryhodných službách pre elektronické transakcie na vnútornom trhu a o zrušení smernice 1999/93/ES (ďalej len „Nariadenie eIDAS“) [4].

Táto politika je štruktúrovaná v súlade s RFC 3647 [5].

1.2 Názov dokumentu a jeho identifikácia

Názov	**POLITIKA poskytovania dôveryhodnej služby vyhotovovania a overovania certifikátov**
Skratka názvu:	**CP CA Disig***
Verzia:	**5.7**
Schválené dňa:	**26.9. 2022**
Platnosť od:	**1 10. 2022**
Tomuto dokumentu je priradený identifikátor objektu (OID):	**1.3.158.35975946.0.0.0.1.1**

* - v texte tohto dokumentu sa väčšinou používa pri odkaze len skrátená forma CP

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.**1** – **CP CA Disig**

1.2.1 História zmien

Verzia	Dátum revízie	Popis revízie; revidoval
1.0	25.03.2006	Prvá verzia dokumentu; Miškovič
1.5	20.12.2006	Formálne úpravy textu dokumentu – formátovanie, opravy odkazov, úpravy textu v kapitole 4 „Prevádzkové požiadavky“; Miškovič
2.0	23.01.2007	Rozšírenie CP v súvislosti s novým typom vydávaných certifikátov pre zmluvného klienta. Doplnenie kapitoly 7 „Profily certifikátov“; Miškovič.
2.1	29.03.2007	Opravy textu v kap. 2.8 a kap. 4.9 Úpravy textu v súvislosti s minoritnou zmenou v certifikáte pre zmluvného partnera; Miškovič
3.0	19.03.2008	Celková revízia CP vzhľadom k jednotlivým typom certifikátov; Ďurišová, Miškovič
3.1	24.06.2008	Pridanie nového typu certifikátu; Miškovič
3.2	10.11.2008	Zmena dĺžky platnosti certifikátov pre doménového používateľa PKI VšZP 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; Miškovič
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, doplnenie podpisových algoritmov 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	15.08.2013	Spresnenie profilu certifikátov koreňových certifikačných autorít CA Disig a ostatných vydávaných typov certifikátov; Miškovič
4.6	21.6.2013	Spresnenie OID dokumentu – vypustenie verzie dokumentu z OID (kap. 1.2). Úprava profilov pre vydávanie podriadených CA – certificatePolicies Identifier (kap.7.1.2); Povolenie vydávania

		„wildcard“ TLS/SSL certifikátov na tretej úrovni doménového mena; (3.1.2 Miškovič)
4.7	2.2.2015	Zapracovanie požiadaviek aktuálnej verzie dokumentu „Baseline Requirements for the Issuance and Management of Publicly-Trusted Certificates, v.1.2.3; Revízia CP v súvislosti s novelou zákona o elektronickom podpise v zmysle zákona č. 305/2013 Z. z.; Miškovič
4.8	22. 5. 2015	Overovanie CAA záznamov (4.1.5)
4.9	21. 10. 2016	Vykonané zmeny v súvislosti s Nariadením eIDAS a v súvislosti s ukončením platnosti zákona č. 215/2002 Z. z. a nadobudnutím účinnosti zákona č. 272/2016 Z. z.; Zapracovanie požiadaviek Baseline Requirements for the Issuance and Management of Publicly-Trusted Certificates, do verzie v.1.4.1; Miškovič
5.0	25. 9. 2017	Konverzia CP do formátu v zmysle RFC 3647; Zapracovanie požiadaviek nariadenia eIDAS [4] 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; Úprava znenia bodu 1.3.3; zmena znenia bodu 3.2.2.4 (nový spôsob overenia); doplnenie kapitoly 4.2.2 (gTLD); doplnenie bodu 4.9.11 (OCSP stapling); Miškovič
5.2	17. 5. 2019	Úprava bodu 4.9 v zmysle Baseline Requirements for the Issuance and Management of Publicly-Trusted Certificates, v.1.6.1; Úprava bodu 8.4 v zmysle Baseline Requirements for the Issuance and Management of Publicly-Trusted Certificates, v.1.6.5; Spresnenie definícii v bode 1.3.1; Doplnenie bodu 3.1,4; Miškovič
5.3	2.12.2019	Úprava profilu certifikátu pre elektronický podpis (3.1.4.1.); úprava dĺžky platnosti vydávaných certifikátov pre podpis/pečať (7.1.4); Aktualizácia odkazov (1.6.3.); Doplnenie skratiek a drobné úpravy textu.; Miškovič
5.4	1. 9. 2020	Úprava platnosti TLS/SSL certifikátov v zmysle požiadaviek [3] verzia 1.6.6 časť 6.3.2 a 7.1.4. Doplnenie sha256RSA odtlačku pre koreňovú Disig Root R2 a podriadene CA Disig R2I2 a VCA Disig R2I3 v časti 1.4.1. Spresnenie metód overovania vlastníctva domény v časti 3.2.2.4; Vypustenie povinného podporovania OCSP Stapling v časti 4.9.11 Miškovič
5.5	20. 5. 2021	Doplnenie spôsobu oznamovania incidentov (2.2); Čas použiteľnosti údajov použitých pri overovaní vlastníctva domény (3.2.2.4); Spôsob nahlasovania kompromitácie súkromného kľúča CA tretími stranami (4.9.12); Miškovič
5.6	20. 5. 2022	Vypustenie položky OU z profilu TLS certifikátu (3.1.4.3); úprava požiadaviek postupov získavania auditných záznamov v zmysle požiadaviek [3] verzia 1.8.4 (5.4); zmena označenia typu certifikátu TLS/SSL na TLS; Miškovič
5.7	1 10. 2022	Zmeny v súvislosti s požiadavkou uvádzania dôvodov zrušenia pri rušení vydaných TLS certifikátov (4.9.1.1; 4.9.2; 4.9.3;7.2.2)

1.3 Účastníci PKI

1.3.1 Certifikačné autority

Koreňová certifikačná autorita (Root Certification Authority – Root CA) je entita autorizovaná na vyhotovovanie certifikátov verejného kľúča pre podriadené certifikačné autority Poskytovateľa.

Podriadená certifikačná autorita (Subordinate Certification Authority – Sub CA) je entita na vyhotovovanie certifikátov verejného kľúča pre koncových používateľov Poskytovateľa.

1.3.2 Registračné autority

Registračná autorita (ďalej len „RA“) je entita, ktorá vykonáva niektoré vybrané činnosti pri poskytovaní dôveryhodných služieb v mene Poskytovateľa.

RA musí vykonávať svoje aktivity v súlade so schválenou CP a Pravidlami poskytovania dôveryhodnej služby vyhotovovania a overovania certifikátov (ďalej aj „CPS“) v aktuálnom znení.

Poskytovateľ môže zriadiť RA nasledovných typov:

- **Komerčná RA** – je určená na sprostredkovanie vybraných dôveryhodných služieb Poskytovateľa širokej verejnosti a je prevádzkovaná treťou stranou, na základe písomnej zmluvy s Poskytovateľom.
- **Firemná RA** – je určená na sprostredkovanie vybraných dôveryhodných služieb výhradne pre vlastné potreby konkrétnej právnickej osoby resp. pre potreby ňou prevádzkovaných systémov vyžadujúcich použitie certifikátov a je prevádzkovaná, na základe písomnej zmluvy s Poskytovateľom, danou konkrétnou právnickou osobou.
- **Interná RA** – je prevádzkovaná Poskytovateľom a je určená na poskytovanie dôveryhodných služieb pre všetkých záujemcov. Táto RA nie je samostatný právny subjekt.

1.3.3 Zákazník a Držiteľ certifikátu

Zákazníkom sa rozumie fyzická osoba resp. právnická osoba, ktorej Poskytovateľ poskytuje dôveryhodné služby na základe zmluvy.

Držiteľom certifikátu, teda subjektom uvedeným v certifikáte ako držiteľ súkromného kľúča prislúchajúcemu k verejnému kľúču, ku ktorému je vydaný certifikát, môže byť:

- fyzická osoba,
- fyzická osoba identifikovaná v spojení s právnickou osobou,
- právnická osoba, ktorou môže byť organizácia alebo jej jednotka resp. oddelenie,
- zariadenie alebo systém prevádzkovaný fyzickou alebo právnickou osobou alebo prevádzkovaný v mene fyzickej resp. právnickej osoby.

V prípade, že Zákazník je zároveň Držiteľom certifikátu, je priamo zodpovedný v prípade neplnenia si povinností kladených na zákazníka aj držiteľa certifikátu.

Keď Zákazník koná v mene jedného alebo viacerých Držiteľov, s ktorými je prepojený (napr. Zákazník je právnická osoba požadujúca vydanie certifikátov pre svojich zamestnancov) tak rozdielne zodpovednosti Zákazníka a Držiteľa sú definované v dokumente Všeobecné podmienky poskytovania a používania dôveryhodnej služby vydávania a overovania certifikátov“ (ďalej len „Všeobecné podmienky“) [6] zverejnené na webovom sídle Poskytovateľa (pozri kapitola 1).

Podmienky, ktoré musí splniť Zákazník, definuje táto CP.

Formálnym Držiteľom certifikátu sa rozumie fyzická osoba, ktorá sa zaviaže, že bude používať zodpovedajúci súkromný kľúč a certifikát v súlade s touto CP.

Vzťah medzi Zákazníkom a Držiteľom môže byť takýto:

- Pri žiadaní o certifikát fyzickej osoby (Držiteľ) je Zákazníkom
  - samotná fyzická osoba,
  - právnická osoba oprávnená na zastupovanie fyzickej osoby (Držiteľa), alebo
  - akýkoľvek subjekt, s ktorým je fyzická osoba (Držiteľ) spojená napr. právnická osoba, ktorá ju zamestnáva, nezisková organizácia ktorej je členom a pod.).
- Pri žiadaní o certifikát pre právnickú osobu je Zákazníkom
  - akýkoľvek subjekt, ktorý je podľa príslušného právneho poriadku oprávnený na zastupovanie právnickej osoby, alebo
  - štatutárny zástupca právnickej osoby, ktorá žiada za svoje dcérske spoločnosti alebo jednotky alebo oddelenia.
- Pri žiadaní o certifikát pre zariadenie alebo systém prevádzkovaný fyzickou alebo právnickou osobou je Zákazníkom:
  - fyzická alebo právnická osoba prevádzkujúca zariadenie alebo systém,
  - akýkoľvek subjekt, ktorý je podľa príslušného právneho poriadku oprávnený na zastupovanie právnickej osoby, alebo
  - štatutárny zástupca právnickej osoby, ktorá žiada za svoje dcérske spoločnosti alebo jednotky alebo oddelenia.

1.3.4 Spoliehajúca sa strana

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

1.3.5 Iní účastníci

Autorita pre správu CP (Policy Management Authority - PMA) je zložka ustanovená za účelom:

- dohľadu na vytváranie a aktualizáciu CP a CPS, vrátane vyhodnocovania zmien a plánov na implementovanie ľubovoľných prijatých zmien,
- revízie CPS, aby sa zaručilo, že prax Poskytovateľa vyhovuje príslušnej CP
- revízie výsledkov auditov zhody, aby sa určilo, či Poskytovateľ adekvátne dodržuje ustanovenia schváleného CPS,
- vydávania odporúčaní pre Poskytovateľa ohľadom nápravných akcií a iných vhodných opatrení,
- vydávania odporúčaní ohľadne vhodnosti certifikátov asociovaných s danou CP pre špecifické aplikácie riadenia a usmerňovania činnosti certifikačnej autority a registračných autorít,
- výkladu ustanovení CPS a svojich pokynov pre Poskytovateľa a RA,

- vykonávania interného auditu Poskytovateľa, pričom touto činnosťou poverí samostatného zamestnanca.
- zabezpečenia, že prijatá a schválená CP a CPS sú riadne a náležite realizované.

PMA predstavuje vrcholovú zložku, ktorá rozhoduje s konečnou platnosťou vo všetkých záležitostiach a aspektoch týkajúcich sa Poskytovateľa a jeho činnosti.

1.4 Použiteľnosť certifikátov

1.4.1 Vhodné použitie certifikátov

Certifikáty vyhotovované v zmysle tejto CP sú vydávané na účely identifikácie Držiteľa verejného kľúča z dvojice kryptografických kľúčov (verejný a súkromný), využívaných v rámci PKI infraštruktúry.

Kryptografický pár kľúčov (súkromný a verejný) a certifikát vydávaný Poskytovateľom môžu byť vo všeobecnosti použité bežným spôsobom, výhradne v súlade s ich účelovým určením, a to v závislosti od konkrétneho certifikátu najmä pre potreby:

- zabezpečenia elektronickej pošty (podpisovanie a/alebo šifrovanie správ posielaných elektronickou poštou),
- podpisovania elektronických dokumentov zdokonaleným elektronickým podpisom,
- opatrovania elektronických dokumentov zdokonalenou elektronickou pečaťou,
- zabezpečenia TLS komunikácie (autentifikácia webového sídla),
- zabezpečovacích mechanizmov pracovných staníc používateľov,
- interných procesov PKI (bezpečná komunikácia medzi komponentmi PKI a pod.).

Poskytovateľ vyhotovuje pre Zákazníkov tieto typy certifikátov:

- **certifikát pre fyzickú osobu resp. fyzickú osobu identifikovanú v spojení s právnickou osobou (ďalej len „certifikát pre fyzickú osobu“)** – kryptografické kľúče spojené s týmto typom certifikátu sú určené v prvom rade pre potreby zabezpečenia elektronickej pošty, vyhotovovanie zdokonaleného elektronického podpisu, autentifikáciu pri prístupe k rôznym IS;
- **certifikát pre právnickú osobu** - kryptografické kľúče spojené s týmto typom certifikátu sú určené na vyhotovovanie zdokonalenej elektronickej pečate právnickou osobou (pôvodca pečate) a slúžia ako dôkaz, že elektronický dokument vydala v certifikáte identifikovaná právnická osoba a zabezpečujú istotu, pokiaľ ide o pôvod a integritu dokumentu;
- **verejne dôveryhodný certifikát pre autentizáciu webového sídla (SSL certifikát)** - kryptografické kľúče spojené s týmto typom certifikátu sú určené pre autentizáciu serverov prístupných cez internet, čím je

zabezpečená efektívna a bezpečná elektronická komunikácia spĺňajúca záujmy používateľov týkajúce sa dôveryhodnosti; vydaný certifikát bude okrem iného obsahovať tieto identifikátory certifikačnej politiky pre validáciu organizácie v tvare:

- joint-iso-itu-t(2) international-organizations(23) ca-browser-forum(140) certificate-polcies(1) baselinerequirements(2) organization-validated(2) v zmysle Baseline Requirement [3];

Poskytovateľ pre svoje potreby vydáva **certifikáty na správu** (certifikáty podriadených certifikačných autorít, certifikáty pre službu časovej pečiatky (TS) resp. on-line overovanie stavu certifikátov (OCSP)).

Dôveryhodné služby vyhotovovania certifikátov uvedených v tejto časti sú poskytované týmito certifikačnými autoritami Poskytovateľa:

Názov	**CA Disig Root R2**
Sériové číslo certifikátu	0092b888dbb08ac163
Odtlačok (sha1)	B561EBEAA4DEE4254B691A98A55747C234C7D971
Odtlačok (sha256)	E23D4A036D7B70E9F595B1422079D2B91EDFBB1FB651A0633EAA8A9DC5F80703
Poznámka	Vydáva certifikáty len pre podriadené certifikačné autority Poskytovateľa.

Názov	**CA Disig R2I2 Certification Service**
Sériové číslo certifikátu	081792523668f5c8500000000000000003
Vydavateľ	CA Disig Root R2
Odtlačok (sha1)	19F2783DEDD8561A61C682932EE9D5B4D86B00CE
Odtlačok (sha256)	C96F24C45113FD91AE2F9E40E106653BFA0FFBCFA07E209524C844E7C8DA4148
Poznámka	Vydáva len TLS certifikáty pre koncových používateľov (pozri 3.1.4.3).

Názov	**CA Disig R2I3 Certification Service**
Sériové číslo certifikátu	08a2395ba703affdac0000000000000004
Vydavateľ	CA Disig Root R2
Odtlačok (sha1)	1432AC3C02C8C89D6179A40B2EFF6B5AD5DA5D7F
Odtlačok (sha256)	239FFA86D71033BA255914782057D87E8421AEDD5910B786928B6A1248C3E341
Poznámka	Vydáva certifikáty pre koncových používateľov - fyzické osoby (pozri 3.1.4.1) resp. právnické osoby (pozri 3.1.4.2).

1.4.2 Nedovolené použitie certifikátov

Certifikáty vydávané v zmysle tejto CP nie sú EÚ kvalifikované certifikáty v zmysle Nariadenia eIDAS [4] a nie je ich možné použiť tam, kde sú požadované EÚ kvalifikované certifikáty.

1.5 Správa politiky

1.5.1 Organizácia zodpovedná za správu dokumentu

Tabuľka č. 1 obsahuje údaje Poskytovateľa, ktorý je zodpovedný za prípravu, vytvorenie a udržiavanie tohto dokumentu.

Tabuľka č. 1: Kontaktné údaje Poskytovateľa

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

1.5.2 Kontaktná osoba

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

Tabuľka č. 2 obsahuje kontaktné údaje na zložku zodpovednú za prevádzku certifikačných autorít Poskytovateľa.

Tabuľka č. 2: Kontaktné údaje Poskytovateľa

Certifikačná autorita CA Disig	
Adresa:	**Záhradnícka 151, 821 08 Bratislava 2**
e-mail:	**caoperator@disig.sk**
telefón	**+421 2 20850150, +421 2 20820157**
webové sídlo:	**http://eidas.disig.sk**
Oznamovanie incidentov	**tspnotify@disig.sk** viac pozri: https://eidas.disig.sk/pdf/incident_reporting.pdf

1.5.3 Osoba rozhodujúca o súlade CPS s CP

Osobou, ktorá je zodpovedná za rozhodovanie o súlade postupov Poskytovateľa, ktoré sú uvedené v CPS s touto politikou je PMA (pozri časť 1.3.5).

1.5.4 Postupy schvaľovania CPS a externej politiky

Ešte pred začiatkom prevádzky má mať Poskytovateľ schválený svoj CP a príslušné CPS a musí spĺňať všetky jeho požiadavky. Obsah CP a CPS schvaľuje osoba menovaná do role PMA.

Po schválení zo strany PMA je príslušný dokument publikovaný v súlade s publikačnou a oznamovacou politikou.

PMA má informovať o svojich rozhodnutiach takým spôsobom, aby boli tieto informácie dobre prístupné Spoliehajúcim sa stranám.

1.6 Definície a skratky

1.6.1 Definície

TLS certifikát - je osvedčenie, ktoré umožňuje autentifikáciu webového sídla a spája toto webové sídlo s fyzickou alebo právnickou osobou, ktorej bol certifikát vydaný;

Dôveryhodná služba - elektronická služba, ktorá sa spravidla poskytuje za odplatu a spočíva:

a) vo vyhotovovaní, overovaní a validácii elektronických podpisov, elektronických pečatí alebo elektronických časových pečiatok, elektronických doručovacích služieb pre registrované zásielky a certifikátov, ktoré s týmito službami súvisia, alebo

b) vo vyhotovovaní, overovaní a validácii certifikátov pre autentifikáciu webových sídiel, alebo

c) v uchovávaní elektronických podpisov, pečatí alebo certifikátov, ktoré s týmito službami súvisia;

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

Elektronický podpis - údaje v elektronickej forme, ktoré sú pripojené alebo logicky pridružené k iným údajom v elektronickej forme a ktoré podpisovateľ používa na podpisovanie;

Elektronická pečať - údaje v elektronickej forme, ktoré sú pripojené alebo logicky pridružené k iným údajom v elektronickej forme s cieľom zabezpečiť pôvod a integritu týchto pridružených údajov;

Kľúčový pár - súčasť PKI systému, ktorá využíva asymetrickú kryptografiu a pozostávajúca z verejného a k nemu prislúchajúceho súkromného kľúča;

Oprávnený kontakt domény - registrátor domény, technický kontakt alebo administratívny kontakt (alebo ekvivalent v zmysle ccTLD) uvedený vo WHOIS zázname pre doménové meno uvedené ako prvé vľavo od riadeného registrového mena (napr. domena.sk) resp. registrového mena so suffixom (domena.co.uk) alebo v SOA (Start of Authority) zázname.

Poskytovateľ dôveryhodných služieb - fyzická alebo právnická osoba poskytujúca jednu alebo viacero dôveryhodných služieb buď ako kvalifikovaný alebo nekvalifikovaný poskytovateľ dôveryhodných služieb;

Pracovník RA – zamestnanec Poskytovateľa alebo inej právnickej osoby, ktorá má s Poskytovateľom uzavretú zmluvu o poskytovaní certifikačných služieb;

Spoliehajúca sa strana – fyzická osoba alebo právnická osoba, ktorá sa pri svojom konaní spolieha na dôveryhodné služby Poskytovateľa;

Verejne dôveryhodný certifikát - certifikát, ktorý je dôveryhodný na základe skutočnosti, že jej zodpovedajúci koreňový certifikát je distribuovaný ako dôveryhodný bod (trust anchor) v široko dostupnom aplikačnom softvéri.

„Wildcard“ certifikát – certifikát obsahujúci znak hviezdička („*“) v polohe úplne vľavo ktoréhokoľvek presne stanoveného doménového mena (FQDN) nachádzajúceho sa v certifikáte

„Wildcard“ doménové meno – doménové meno pozostávajúce z jednej hviezdičky, za ktorou nasleduje jeden znak bodka („*.“), za ktorými nasleduje presne stanovené doménové meno (FQDN)

Zákazník – fyzická osoba resp. právnická osoba, ktorá je oprávnená žiadať o certifikát v mene entity, ktorej meno sa objaví ako subjekt v certifikáte – Držiteľ certifikátu;

Zdokonalená elektronická pečať - elektronická pečať, ktorá spĺňa požiadavky stanovené v článku 36 Nariadenia eIDAS [4];

Zdokonalený elektronický podpis - elektronický podpis, ktorý spĺňa požiadavky stanovené v článku 26 Nariadenia eIDAS [4];

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

1.6.2 Skratky

CA	–	Certifikačná autorita (Certification Authority)
CAA	-	DNS záznam definujúci CA, ktoré môžu vydať certifikát pre danú doménu
CMA	–	Autorita pre správu certifikátov (Certificate Management Authority)
CP	–	Certifikačná politika (Certificate Policy)
CPS	–	Pravidlá poskytovania dôveryhodnej služby vyhotovovania a overovania certifikátov (Certificate Practice Statement)
CRL	–	Zoznam zrušených certifikátov (Certification Revocation List)
FQDN	-	Presne stanovené meno domény (Fully Qualified Domain Name) je jednoznačné meno domény, ktoré absolútne udáva pozíciu uzla v stromovej hierarchii DNS.
HSM	–	Hardware Security Modul
IČO	–	Identifikačné číslo organizácie
OID	–	Identifikátor objektu (Object Identifier)
PKCS#10	-	Formát žiadosti o certifikát podľa štandardu Public Key Cryptographic Standards (RFC 2986)

PKI		Infraštruktúra verejných kľúčov (Public Key Infrastructure)
PMA	–	Autorita pre správu CP (Policy Management Authority)
RA	–	Registračná autorita (Registration Authority)
QSCD	-	Zariadenie určené na bezpečné generovanie, uloženie a použitie páru kľúčov (súkromný aj verejný). Môže byť napr. vo forme čipovej karty, USB kľúča, HSM modulu.
SAN	-	Rozšírenie definované štandardom X.509 [1], ktoré umožňuje uviesť v certifikáte rôzne hodnoty (e-mail, URI, FQDN, IP adresa), ktorú budú umiestnené v položke subjAltName.
SSL	-	je protokol resp. vložená medzi vrstvu transportnú (napr. TCP/IP) a aplikačnú (napr. HTTP), ktorá poskytuje zabezpečení komunikácie šifrovaním a autentizáciou komunikujúcich strán. (Secure Sockets Layer)
TLS	-	Je nasledovníkom SSL protokolu (Transport Layer Security)
WHOIS	-	je v informatike označenie pre databázu, ktorá slúži k evidencii údajov o majiteľoch internetových domén a IP adries.

1.6.3 Odkazy

1. Recommendation ITU-T X.509; Information technology – Open Systems Interconnection – The Directory: Public-key and attribute certificate frameworks.
2. RFC5280, Request for Comments: 5280, Internet X.509 Public Key Infrastructure: Certificate and Certificate Revocation List (CRL) Profile.
3. CA/Browser Forum Baseline Requirements for the Issuance and Management of Publicly-Trusted Certificates v. 1.8.4.
4. 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 .
5. RFC3647, Request for Comments: 3647, Internet X.509 Public Key Infrastructure: Certificate Policy and Certification Practices Framework, Chokhani, et al, November 2003.
6. Všeobecné podmienky poskytovania a používania dôveryhodnej služby vyhotovovania a overovania certifikátov Disig, a.s.
7. Mozilla Root Store Policy version 2.7.1.
8. X.500 Information technology – Open Systems Interconnection – The Directory: Overview of concepts, models and services. 10/2012. s.l. : ITU-T.
9. X.501 Information technology – Open Systems Interconnection – The Directory: Models. s.l. : ITU-T, 10/2012.

10. X.520 Information technology – Open Systems Interconnection – The Directory: Selected attribute types. s.l. : ITU-T, 10/2012.
11. RFC5322 "Internet Message Format".
12. Informácia o spracúvaní osobných údajov, Disig, a.s.
13. ETSI EN 319 411-1 Electronic Signatures and Infrastructures (ESI); Policy and security requirements for Trust Service Providers issuing certificates; Part 1: General requirements.
14. RFC 5280 "Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile".
15. RFC 6960 „X.509 Internet Public Key Infrastructure Online Certificate Status Protocol – OCSP“.
16. ETSI EN 319 412-1 Electronic Signatures and Infrastructures (ESI);Certificate Profiles;Part 1: Overview and common data structures.
17. ETSI EN 319 412-3 Electronic Signatures and Infrastructures (ESI); Certificate Profiles;Part 3: Certificate profile for certificates issued to legal persons.
18. ETSI EN 319 412-2 Electronic Signatures and Infrastructures (ESI);Certificate Profiles;Part 2: Certificate profile for certificates issued to natural persons.

2. Zverejňovanie informácií a úložiská

Poskytovateľ musí vyhotoviť, implementovať, vynucovať a minimálne jedenkrát ročne aktualizovať svoju CP /CPS, ktoré popisujú podrobnosti ako sú implementované legislatívne požiadavky a požiadavky dokumentu [3].

2.1 Úložiská

Úložiská musia byť umiestnené tak, aby boli prístupné Držiteľom certifikátov a Spoliehajúcim sa stranám a v súlade s celkovými bezpečnostnými požiadavkami.

Funkciu úložiska Poskytovateľa bude zastávať jeho webové sídlo. Presná URL adresa je uvedená v časti 1. Webové sídlo Poskytovateľa je prostredníctvom Internetu verejne prístupné Zákazníkom, Držiteľom certifikátov, Spoliehajúcim sa stranám a verejnosti vôbec.

Verejne dostupné informácie uvedené na webovom sídle Poskytovateľa majú charakter riadeného prístupu.

2.2 Zverejňovanie informácií o CA

Poskytovateľ musí poskytovať v on-line režime úložisko, ktoré je prístupné Zákazníkom, Držiteľom certifikátov a Spoliehajúcim sa stranám v režime 24x7, ktorý bude obsahovať minimálne tieto informácie:

- certifikáty vydané v súlade s touto CP,
- aktuálne CRL ako aj všetky CRL vydané od začiatku činnosti vydávania certifikátov,
- certifikáty koreňových certifikačných autorít a podriadených certifikačných autorít, ktoré patria k jej verejným kľúčom, ktorým zodpovedajúce súkromné kľúče sú využívané pri podpisovaní vydávaných certifikátov a CRL
- aktuálnu verziu CP/CPS,
- informáciu o výsledku pravidelného auditu výkonu poskytovaných dôveryhodných služieb

Informácie o vydaných certifikátoch nemusí Poskytovateľ zverejňovať, pokiaľ sú tieto vydávané pre interné potreby zmluvných partnerov a s partnerom je zmluvne dohodnuté ich nezverejňovanie.

Poskytovateľ potvrdzuje, že v tejto CP sú zohľadnené všetky požiadavky aktuálnej verzie dokumentu [3], ktorý je publikovaný na stránke http://www.cabforum.org. V prípade akýchkoľvek rozporuplností medzi týmito požiadavkami a touto CP, majú prednosť požiadavky dané aktuálnou verziou dokumentu [3].

Poskytovateľ musí mať k dispozícii webové sídlo, ktoré umožní dodávateľom aplikácií testovať ich softvér s vydávanými TLS certifikátmi Poskytovateľa, ktoré sa naviazané k verejne dôveryhodnému koreňovému certifikátu.

V prípade, že Poskytovateľ nedodrží niektorú z požiadaviek stanovenú v aktuálnej verzii politiky „Mozilla Root Store Policy“ spoločnosti Mozilla [7] musí okamžite

hlásiť takýto incident spoločnosti Mozilla formou správy o incidente (Incident Report) a túto pravidelne aktualizovať, až kým predmetná chyba (bug) nie je označená zo strany spoločnosti Mozilla ako vyriešená v Bugzilla repozitári na stránke mozilla.org.

2.3 Frekvencia zverejňovania informácií

Certifikát sa musí publikovať čo najskôr po jeho vyhotovení. Informácie o vydanom certifikáte musia byť k dispozícii na webovom sídle Poskytovateľa (pozri časť 1). Certifikáty vydávané pre uzatvorené systémy resp. pre interné účely Poskytovateľa nemusia byť verejne dostupné.

Zoznam zrušených certifikátov (CRL) musí byť publikovaný ako je špecifikované v časti 4.9.7. Informácie o zrušenom certifikáte musia byť dostupné na webovom sídle Poskytovateľa (pozri časť 1), ktorý slúži ako jeho úložisko.

Všetky informácie, ktoré majú byť publikované v úložisku sa musia publikovať podľa možností, čo najskôr.

2.4 Kontroly prístupu

Poskytovateľ musí chrániť ľubovoľnú informáciu uloženú v úložisku, ktorá nie je určená na verejné rozšírenie. Poskytovateľ musí vynaložiť maximálne úsilie na to, aby zaistil integritu, dôvernosť a dostupnosť dát súvisiacich s poskytovaním dôveryhodných služieb. Taktiež musí vykonať logické a bezpečnostné opatrenia, aby zabránil neautorizovanému prístupu k úložisku osobám, ktoré by mohli akýmkoľvek spôsobom zmeniť, poškodiť, pridať resp. vymazať údaje uložené v úložisku.

3. Identifikácia a autentizácia

3.1 Mená

3.1.1 Typy mien

Každá CA musí byť schopná vytvárať certifikáty, ktoré obsahujú rozlišovacie mená v zmysle X.500 (X.500 Distinguished Name, ďalej ako „rozlišovacie meno“) [8], konkrétne s X.501 [9] resp. X.520 [10] a mená v zmysle RFC5322 Internet Message Format [11].

Zákazníci si musia sami zvoliť rozlišovacie meno, ktoré má byť uvedené v ich certifikáte.

3.1.2 Potreba zmysluplnosti mien

Pojem „zmysluplnosť“ znamená, že forma mena musí mať bežne používaný tvar na určenie identity Držiteľa (fyzickej osoby, právnickej osoby, orgánu verejnej moci, webového sídla)

Používané mená musia spoľahlivo identifikovať osoby, ktorým sú priradené.

3.1.3 Anonymita a používanie pseudonymov

Používanie pseudonymov, prezývok, krycích mien, aliasov a podobne (tzv. nicknames) v certifikátoch je dovolené len v prípade, že je v položke CN jednoznačne definované, že sa jedná o pseudonym uvedením textu „PSEUDONYM“ v položke CommonName (napr. CN= alias – PSEUDONYM“. Týmto nie sú dotknuté ustanovenia týkajúce sa jednoznačnej identifikácie Držiteľa takto vydaného certifikátu.

Poskytovateľ nesmie vydať certifikát pre anonymného Držiteľa.

Poskytovateľ má právo odmietnuť vydať certifikát, ktorý by obsahoval údaje porušujúce princíp zmysluplnosti mien.

3.1.4 Pravidlá na interpretáciu rôznych foriem mien

Interpretácia jednotlivých foriem mien v certifikátoch vydávaných Poskytovateľom musí byť v súlade s profilmi certifikátov, ktoré sú popísané v časti 7 tejto CP.

Rozlišovacie meno používané v jednotlivých typoch certifikátov vydávaných Poskytovateľom môže pozostávať z položiek, ktoré sú popísané v nasledovných častiach.

Položky rozlišovacieho mena nesmú obsahovať len meta údaje ako napr. znaky „.“ (ASCII 0x2E), „-„ (ASCII 0x2D) alebo iba medzeru „ „ (ASCII 0x20) alebo iné, ktoré by mali indikovať, že hodnota položky nie je vyplnená, je nekompletná alebo uvedenie položky nie je potrebné.

3.1.4.1 Certifikát pre fyzickú osobu

Tabuľka č. 3 obsahuje zoznam položiek, ktoré sa môžu nachádzať v DN certifikátu pre fyzickú osobu s vyznačením minimálneho rozsahu povinných položiek.

Podľa potreby Poskytovateľa môže byť tento typ certifikát rozšírený aj o ďalšie položky v zmysle RFC 5280 časť 4.1.2.6 [2].

Tabuľka č. 3: Položky certifikátu pre fyzickú osobu

Názov	OID	Skratka názvu	Popis	Poznámka
commonName	**2.5.4.3**	**CN**	**Meno a priezvisko vo forme, ktorú si zadá Zákazník**	**Údaj je povinný**
givenName	2.5.4.42	**G**	**Všetky mená fyzickej osoby okrem priezviska**	**Údaj je povinný**
Surname	2.5.4.4	**SN**	**Priezvisko fyzickej osoby - držiteľa**	**Údaj je povinný**
serialNumber	2.5.4.5		**Identifikátor zabezpečujúci jedinečnosť mena subjektu**	**Údaj je povinný**
organizationName	2.5.4.10	O	Názov organizácie	Údaj je nepovinný
organizationIdentifier resp. **serialNumber**	**2.5.4.97** resp. **2.5.4.5**		Odkaz na identifikačný údaj právnickej osoby[1]	Údaj je nepovinný
organizationUnitName	2.5.4.11	OU	Názov útvaru v organizácii	Údaj je nepovinný
localityName	2.5.4.7	L	Názov lokality	Údaj je nepovinný
countryName	**2.5.4.6**	**C**	**Dvojznaková skratka štátu, SK pre Slovenskú republiku**	**Údaj je povinný!!!**

Dôležité upozornenie!!!: Pokiaľ bude certifikát používaný na účely podpisovania a šifrovania elektronickej pošty musí žiadosť obsahovala platnú **e-mailovú adresu** Držiteľa certifikátu

3.1.4.2 Certifikáty pre právnickú osobu

Tabuľka č. 4 obsahuje zoznam položiek, ktoré sa môžu nachádzať v DN certifikátu pre právnickú osobu s vyznačením minimálneho rozsahu povinných položiek.

Podľa potreby Poskytovateľa môže byť certifikát rozšírený aj o ďalšie položky v zmysle RFC 5280 časť 4.1.2.6 [2].

[1] Pozri ETSI EN 319412-1 časť 5 [16]

Tabuľka č. 4: Položky certifikátu pre právnickú osobu

Názov	OID	Skratka názvu	Popis	Poznámka
commonName	**2.5.4.3**	**CN**	Bežne používaný názov právnickej osoby ktorý nemusí plne zodpovedať registrovanému menu	**Údaj je povinný!!!**
organizationName	**2.5.4.10**	**O**	Názov organizácie, pod ktorým je organizácia oficiálne zaregistrovaná	**Údaj je povinný!!!**
organizationIdentifier resp. **serialNumber**	**2.5.4.97** resp. **2.5.4.5**		Odkaz na identifikačný údaj právnickej osoby[2]	**Údaj je povinný pokiaľ existuje!!!**
organizationUnitName	2.5.4.11	OU	Názov útvaru v organizácii	Údaj je nepovinný
localityName	2.5.4.7	L	Názov lokality	Údaj je nepovinný
countryName	**2.5.4.6**	**C**	Dvojznaková skratka štátu, **SK** pre Slovenskú republiku	**Údaj je povinný!!!**

3.1.4.3 TLS certifikát

Tabuľka č. 5 obsahuje zoznam položiek, ktoré sa môžu nachádzať v DN TLS certifikátov. Podľa potreby Poskytovateľa môže byť TLS certifikát rozšírený aj o ďalšie položky v zmysle RFC 5280 časti 4.1.2.6 [2].

Každý TLS certifikát musí obsahovať rozšírenie „subjectAltName“, v ktorom bude uvedená minimálne jedna položka obsahujúca presne stanovené meno domény (FQDN), pre ktorú je certifikát určený.

Ako „wildcard“ doménové meno bude akceptované aj meno obsahujúce znak samostatný hviezdička („*“), nasledovaný znakom bodka („.“) na tretej a vyššej pozícii presne stanoveného doménového mena (FQDN) (napr. „*.disig.sk“; „*.mail.disig.sk“ ap.) a tento typ TLS certifikátu je označovaný ako „wildcard“ certifikát.

Presne stanovené meno domény (FQDN) nesmie byť obsiahnuté v žiadnej inej položke okrem položky CommonName (CN) a rozšírenia certifikátu SubjectAlternativeName.

[2] Pozri ETSI EN 319412-1 časť 5 [16]

Tabuľka č. 5: Položky TLS certifikátu a ich popis

Názov	OID	Skratka názvu	Popis	Poznámka
commonName	**2.5.4.3**	**CN**	Presne stanovené meno domény (FQDN), na ktoré je certifikát vydávaný	**Údaj je povinný!!!**
organizationName	**2.5.4.10**	O[1)]	Názov organizácie, pod ktorým je organizácia oficiálne zaregistrovaná	**Údaj je povinný!!!**[1)]
localityName	2.5.4.7	L[1)]	Názov lokality	**Údaj je povinný!!!**[1)]
countryName	**2.5.4.6**	**C**	Dvojznaková skratka štátu, **SK** pre Slovenskú republiku	**Údaj je povinný!!!**

[1)] - Pokiaľ je v žiadosti vyplnená položka O (organizationName), tak musí byť vyplnená aj položka L (localityName). Pokiaľ položka O (organizationName) nie je vyplnená, tak nesmie byť vyplnená položka L (localityName). V prvom prípade sa v certifikáte používa aj dodatočný identifikátor politiky 2.23.140.1.2.2, ktorý potvrdzuje, že certifikát bol vydaný v zmysle základných požiadaviek CA/Browser forum, časť 7.1.6.1 [3]. V druhom prípade sa použije dodatočný identifikátor politiky v tvare 2.23.140.1.2.1. Poskytovateľ preferuje u TLS certifikátov prvú možnosť s uvedením názvu organizácie a jej sídla.

[2)] - Musí byť vyplnená pokiaľ je vyplnená položka organizationName a nie je vyplnená položka localityName.

Presne stanovené meno domény (FQDN) nesmie obsahovať znak „_“ (ASCII kód 0x5F).

3.1.5 Jedinečnosť mien

Poskytovateľa zodpovedá za jednoznačnosť mien v rámci celej komunity Držiteľov certifikátov.

3.1.6 Rozpoznanie, autentizácia a rola obchodných značiek

Poskytovateľ žiadnej entite nemusí garantovať, že jej meno v certifikáte bude obsahovať jej obchodnú značku (trademark) a to ani na jej výslovnú žiadosť.

V certifikáte môžu byť použité len tie obchodné značky, ktorých vlastníctvo alebo prenájom Zákazník/Držiteľ uspokojivo doloží. Žiadnu inú autentizáciu obchodných značiek Poskytovateľ nevykonáva

Poskytovateľ nesmie vedome vydať certifikát obsahujúci meno, o ktorom kompetentný súd rozhodol, že porušuje obchodnú značku iného. Poskytovateľ nemá povinnosť skúmať obchodné značky ani riešiť spory týkajúce sa obchodných značiek.

3.2 Počiatočné overenie identity

Táto časť obsahuje politiky identifikácie a autentifikácie týkajúce sa jednotlivých subjektov (Zákazník, Držiteľ. RA, CA).

3.2.1 Preukazovanie vlastníctva súkromného kľúča

RA musí požadovať, aby Zákazník resp. fyzická osoba konajúca v mene Zákazníka potvrdili, že Zákazník/Držiteľ vlastní súkromný kľúč, ktorý zodpovedá verejnému kľúču nachádzajúcemu sa v žiadosti o certifikát.

V prípade žiadosti Držiteľa certifikátu o následný certifikát, ktorá bola vygenerované na nové kryptografické kľúče, je prípustné, aby Držiteľ potvrdil vlastníctvo nového súkromného kľúča tak, že svoju novú žiadosť o certifikát zašle na RA podpísaným e-mailom. Pri podpise e-mailu so žiadosťou musí Držiteľ použiť súkromný kľúč, na ktorý bol Poskytovateľom vydaný certifikát, a tento je v čase overovania prijatého e-mailu platný.

V prípade doručenia žiadosti o certifikát elektronickou cestou, od Držiteľa, ktorý už vlastnil certifikát vydaný Poskytovateľom, ktorá nemôže byť podpísaná súkromným kľúčom takéhoto certifikátu, musí byť vlastníctvo súkromného kľúča preverené kontaktovaním Držiteľa zo strany Poskytovateľa a overením, že je pôvodcom danej žiadosti.

CMA nesmie generovať kľúčové páry kľúčov pre cudzie subjekty. Výnimkou môže byť len generovanie kľúčov priamo v QSCD zariadení Zákazníka.

Žiadna zložka Poskytovateľa v nijakom prípade nearchivuje žiadne súkromné kľúče patriace Zákazníkom - cudzím subjektom.

3.2.2 Autentizácia identity právnickej osoby a identity domény

3.2.2.1 Autentizácia identity

Právnická osoba so sídlom v Slovenskej republike musí preukázať svoju totožnosť výpisom z obchodného registra príp. iného platného registra právnických osôb. Zo strany Poskytovateľa musí byť vyžadovaný 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 musí overiť 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).

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, zriaďovacou listinou ap.

V prípade vydávania certifikátu musí právnická osoba preukázať pravdivosť identifikačného údaja uvedeného v žiadosti o certifikát predložením k nahliadnutiu originálneho dokumentu preukazujúceho túto skutočnosť.

3.2.2.2 DBA/Obchodné meno

Ak je obsahom certifikátu identifikujúcim subjekt, ktorému je certifikát vydávaný DBA alebo obchodné meno musí Poskytovateľ overiť, či Zákazník má právo použiť dané TBA/obchodné meno minimálne za použitia:

1. Dokumentácia poskytnutej alebo komunikovanej s orgánom štátu, v ktorého jurisdikcii je daná právnická osoba vytvorená, existuje resp. je ju možno určiť
2. Dôveryhodného zdroja
3. Komunikáciou s orgánom, ktorý je zodpovedný za správu DBA resp. obchodných mien
4. Potvrdzujúcim listom spolu s relevantným dokumentom potvrdzujúcim oprávnenosť

3.2.2.3 Overenie krajiny Zákazníka/Držiteľa

Ak je v certifikáte uvedené pole countryName Poskytovateľ musí overiť krajinu, ktorá je spojená so Zákazníkom/Držiteľom jedným z nasledovných spôsobov:

a) Z informácií poskytovaných registrátorom domény

b) Niektorou z metód uvedených v časti 3.2.2.1

3.2.2.4 Overenie oprávnenia k doméne alebo kontroly nad doménou

V prípade použitia presne stanoveného doménového mena (FQDN) je podmienkou, aby príslušná doména druhej a vyššej úrovne patrila resp. bola pod kontrolou Zákazníka, ktorý žiada o vydanie TLS certifikátu.

Poskytovateľ musí potvrdiť, že v čase vydania TLS certifikátu overila všetky presne stanovené doménové mená (FQDN) nachádzajúce sa v certifikáte minimálne prostredníctvom jednej z metód uvedených ďalej.

Overenie musí byť vykonané v stanovenom čase ešte pred vydaním TLS certifikátu.

Overenie toho, že Zákazník je vlastníkom domény resp. má kontrolu nad danou doménou, ktorej FQDN sa nachádza v položke CN žiadosti resp. bude uvedené v položke Subject Alternative Name (SAN), sa musí vykonať jedným z nasledovných spôsobov:

- Zaslaním náhodne vygenerovanej hodnoty prostredníctvom emailu na emailovú adresu identifikovanú ako oprávnený kontakt pre danú doménu v registri oprávneného registrátora pre danú doménu (napr. pre doménu .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 bola zaslaná. 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. Túto metódu je možné použiť aj na validáciu žiadosti o vydanie „wildcard“ KC pre autentifikáciu webového sídla (táto metóda je uvedená v dokumente [3] v časti 3.2.2.4.2).
- Telefonicky, zavolaním na číslo identifikované ako oprávnený kontakt pre danú doménu v registri oprávneného registrátora pre danú doménu (napr. pre doménu .sk je to whois.sk-nic.sk) a overením oprávnenosti

žiadosti o vydanie TLS certifikátu zo strany Zákazníka. V prípade, že na telefonickom kontakte bude iná osoba ako kontakt uvedený pre danú doménu, musí CA požiadať o spojenie s osobou, ktorá je daným kontaktom. V prípade, že na telefonickom kontakte bude záznamník, tak CA zanechá na záznamníku náhodne vygenerovanú hodnotu a overovanú ADN (Authorization Domain Name). Ak prebehne úspešná validácia oprávnenosti použitia FQDN týmto spôsobom, tak Poskytovateľ môže vydať aj iné TLS certifikáty, ktoré končia rovnakým FQDN. Túto metódu je možné použiť aj na validáciu žiadosti o vydanie „wildcard“ KC pre autentifikáciu webového sídla (táto metóda je uvedená v dokumente [3] v časti 3.2.2.4.15).

Overenie v zmysle tejto kapitoly môže byť použité maximálne počas obdobia, ktoré je definované v aktuálnej verzii politiky „Mozilla Root Store Policy“ spoločnosti Mozilla [7].

Pokiaľ ani jednou z popísaných metód nebude možné dôveryhodne zistiť, že Zákazník má danú doménu pod oprávnenou kontrolou, Poskytovateľ musí odmietnuť vydanie certifikátu na danú žiadosť.

Poskytovateľ nevydáva TLS certifikáty pre FQDN s Onion Domain Name.

3.2.2.5 Autentifikácia IP adresy

Poskytovateľ nevydáva TLS certifikáty kde v poli commonName alebo v rozšírení subjectAlternativeName sa nachádza IP adresa.

3.2.2.6 Validácia domény obsahujúcej „wildcard“ znak

Pred vydaním certifikátu, ktorý obsahuje „wildcard“ znak „*“ v položke CN resp. položke SAN musí byť vykonaná kontrola, ktorá overí, či sa „wildcard“ znak nachádza na prvej pozícii vľavo od „registry-controlled“ názvu resp. „public suffix“.

3.2.2.7 Presnosť zdroja údajov

Pred použitím akéhokoľvek zdroja údajov ako dôveryhodného zdroja musí Poskytovateľ overiť hodnovernosť, správnosť, odolnosť voči zmenám alebo falzifikácie takéhoto zdroja, kde môže vziať do úvahy napr. aktuálnosť daných údajov, frekvenciu aktualizácie zdroja údajov, poskytovateľa údajov, verejnú dostupnosť, malú pravdepodobnosť možnosti zmeny alebo sfalšovania údajov ap.

3.2.2.8 CAA záznam

Ako súčasť procesu vydávania musí Poskytovateľ skontrolovať CAA záznam pre každé dNSName uvedené v rozšírení subjectAltName vydávaného certifikátu v zmysle postupu uvedeného v RFC 6844 a podľa pokynov na spracovanie ustanovených v dokumente RFC 6844 pre všetky nájdené záznamy.

3.2.3 Autentizácia identity fyzickej osoby

Poskytovateľ musí garantovať, že identita Držiteľa certifikátu a jeho verejný kľúč sú zodpovedajúco previazané. Poskytovateľ musí špecifikovať v príslušnom CPS procedúry na autentizáciu identity Držiteľa certifikátu. CA musí zaznamenávať

tento proces pre každý certifikát v písomnej alebo elektronickej forme. Dokumentácia o autentizácii musí minimálne obsahovať:

- identitu osoby, ktorá vykonáva autentizáciu,
- jednoznačné identifikačné údaje z dokladov preukazujúcich identitu Držiteľa certifikátu,
- dátum vykonania identifikácie.

Overenie identity musí vykonať CMA na základe dokladu, ktorý obsahujú tieto údaje Držiteľa:

- celé meno a priezvisko,
- adresu trvalého pobytu,
- rodné číslo (osoby, ktoré ho majú pridelené),
- dátum narodenia (osoby, ktoré nemajú pridelené rodné číslo).

Zákazník/Držiteľ musí zároveň poskytnúť ďalší doklad, ktorý obsahuje minimálne meno a priezvisko Držiteľa a ďalší jeho osobný údaj (dátum narodenia, rodné číslo). Toto neplatí v prípade, ak ide o služobný preukaz.

Poskytovateľ musí zaznamenať aj tieto údaje z dokladov:

- číslo preukazu totožnosti,
- vydavateľa preukazu totožnosti,
- dátum platnosti preukazu totožnosti, ak je vyznačený.

Poskytovateľ musí akceptovať pri overovaní identity Držiteľa nasledovné doklady:

- občiansky preukaz,
- cestovný pas,
- vodičský preukaz,
- rodný list,
- služobný preukaz,
- preukaz poistenca verejného zdravotného poistenia
- zbrojný preukaz.

V prípade poskytnutia rodného listu, zbrojného preukazu, služobného preukazu alebo preukazu poistenca verejného zdravotného poistenia sa musí poskytnúť aj jeden z týchto dokladov: občiansky preukaz, cestovný pas.

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

Súčasťou autentizácie Držiteľa je povinné poskytnutie zvolenej e-mailovej adresy, ktorá sa uloží spolu s jeho osobnými údajmi v IS Poskytovateľa, a ktorá bude slúžiť vyslovene na komunikáciu medzi Poskytovateľom a Držiteľom certifikátu a nebude súčasťou vydaného certifikátu. Poskytovateľ nebude vykonávať overenie, či uvedená e-mail adresa skutočne patrí Držiteľovi.

Pokiaľ je vydávaný certifikát pre fyzickú osobu určený na podpisovanie elektronickej pošty (rozšírenie Secure Email – OID 1.3.6.1.5.5.7.3.4), tak Poskytovateľ musí vykonať overenie vlastníctva príslušného e-mailového konta postupom, ktorý je uvedený v časti 4.1.2.

3.2.3.1 Autentizácia identity zariadenia alebo systému

Poskytovateľ musí garantovať aj v prípade, že certifikát je vydávaný pre zariadenie alebo systém, ktorý môže používať certifikát, že identita zariadenia resp. systému sa jeho verejným kľúčom sú zodpovedajúco previazané.

Z uvedeného dôvodu musí byť zariadenie resp. systém priradený fyzickej alebo fyzickej osobe konajúcej v mene právnickej osoby (Zákazník), ktorá ich spravuje.

Táto fyzická osoba musí poskytnúť CMA tieto informácie:

- identifikáciu zariadenia resp. systému,
- verejné kľúče zariadenia resp. systému (obsiahnuté v žiadosti o certifikát),
- autorizáciu zariadenia resp. systému a jeho atribúty (ak nejaké majú byť uvedené v certifikáte),
- kontaktné údaje, aby Poskytovateľ mohol v prípade potreby komunikovať s touto osobou,

Poskytovateľ musí overiť správnosť ľubovoľnej informácie (hodnoty položky rozlišovacieho mena), ktorá má byť uvedená v certifikáte.

Metódy na vykonanie overenia údajov zahrňujú:

- overenie identity fyzickej osoby v súlade s požiadavkami časti 3.2.3,
- overenie identity osoby, 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.

Poznámka: Typickou hodnotou tejto položky musí byť presne stanovené meno domény (FQDN).

Poskytovateľ musí zabezpečiť dôslednú kontrolu položky certifikátu subject:organizationUnitName (OU), tak aby táto neobsahovala názov právnickej osoby, obchodné meno, obchodnú značku, adresu, lokalitu, alebo iný text poukazujúc na určiteľnú fyzickú alebo právnickú osobu, bez toho aby si tieto informácie hodnoverne neoverila.

3.2.3.2 Autentizácia identity u zmluvných partnerov

Autentizácia identity fyzickej osoby resp. komponentu u zmluvných partnerov Poskytovateľa, sa musí vykonávať v spolupráci so zodpovednými osobami tohto zmluvného partnera.

3.2.3.3 Predkladané doklady

3.2.3.3.1 Všeobecne

Všetky doklady poskytované RA Zákazníkmi 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 osobnom doklade a vzhľadom Zákazníka, rozpornosť dvoch predložených dokladov a podobne), môže odmietnuť jeho registráciu.

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

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

Pri poskytovaní dokladov sa vyžaduje, aby na RA boli poskytnuté originály týchto dokladov slúžiace k nahliadnutiu a kópie originálov (nemusia byť overené), okrem osobných dokladov identifikujúcich totožnosť Zákazníka, slúžiace na archiváciu pre potreby Poskytovateľa. Poskytnutie 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.

3.2.3.3.2 Fyzická osoba

Pozri časť 3.2.3.

V prípade žiadosti o vydanie certifikát pre potreby zmluvného partnera, alebo žiadosti o jeho zrušenie postačuje, aby daná fyzická osoba preukázala svoju totožnosť jedným z nasledovných osobných dokladov – občiansky preukaz resp. pas. V prípade vydávania certifikátov pre zmluvného partnera musia byť splnené aj ďalšie podmienky pre vydanie certifikátu, ak sú stanovené samotným zmluvným partnerom.

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

Pokiaľ je Zákazníkom zákonný zástupca (spravidla rodič), musí navyše predložiť rodný list dieťaťa, osvojiteľ musí navyše predložiť rozhodnutie zo súdu alebo výpis z matriky.

3.2.3.3.3 Fyzická osoba - zamestnanec

Pokiaľ je Zákazníkom právnická osoba, ktorá žiada vydanie certifikátu pre fyzickú osobu, ktorá je jej zamestnancom a v žiadosti je uvedený názov tejto právnickej osoby, poskytuje okrem dokladov uvedených v časti 3.2.3.3.2 aj doklady podľa časti 3.2.2. Táto požiadavka sa netýka zamestnanca zmluvného partnera, kde je zmluvne dohodnutý iný mechanizmus overovania.

3.2.3.3.4 Právnická osoba

V tomto prípade Zákazník poskytuje doklady formálneho Držiteľa uvedené v časti 3.2.3. Súčasne musí predložiť doklad podľa časti 3.2.2.

3.2.3.3.5 Zariadenie alebo systém

Pozri časť 3.2.3.1.

3.2.3.4 Kontrola údajov na dokladoch

Pracovník RA musí skontrolovať na dokladoch najmä nasledovné:

- Osobné doklady fyzickej osoby:
  a) súlad údajov uvedených v žiadosti s údajmi uvedenými v osobných dokladoch,
  b) platnosť predloženého dokladu,
  c) plnoletosť fyzickej osoby (t. j. vek 18 rokov),
  d) súlad medzi fotografiou v osobnom doklade a vzhľadom majiteľa osobného dokladu,
  e) zhodu v predložených dokladoch t. j. či údaje na jednom doklade neodporujú údajom na inom doklade.
- Výpisy z obchodného registra príp. iného registra právnických osôb:
  a) platnosť výpisu – nesmie byť starší ako 3 mesiace,
  b) konanie za právnickú osobu - t. j., či má/majú fyzická/é osoba/y, ktoré predložili daný výpis, právo konať (podpisovať) za danú právnickú osobu,
  c) forma výpisu – originál alebo úradne (notárom/matrikou) overená kópia výpisu.
- Súhlas s vydaním certifikátu:
  a) oprávnenie konať za spoločnosť – osoba podpisujúca súhlas musí byť oprávnená zastupovať Zákazníka. Oprávnenosť sa kontroluje podľa výpisu z OR resp. iného zákonom určeného registra (príp. zriaďovacej listiny, poverovacej listiny, menovacieho dekrétu). Pokiaľ podpisujúca osoba nie je zapísaná v tomto výpise, musí poskytnúť iný doklad, na základe ktorého môže konať za Zákazníka (spravidla notárom overená plná moc).
  b) Platnosť – pokiaľ je v súhlase uvedená doba platnosti súhlasu, kontroluje sa aj tento údaj.
- Plné moci:
  a) overenie plnej moci (notárom/matrikou)

b) zhoda údajov uvedených v plnej moci, ktoré definujú zastupujúcu fyzickú resp. právnickú osobu, s údajmi uvedenými na osobných dokladoch zastupujúcej fyzickej osoby resp. s údajmi uvedenými na výpise z obchodného príp. iného registra zastupujúcej právnickej osoby,

c) 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,

d) časové obmedzenie príp. iná podmienka uvedené v plnej moci

- Čestné prehlásenia:

a) oprávnenie na podpis – osoba podpisujúca prehlásenie musí byť 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)

Poskytovateľ môže akceptovať aj dokumenty predkladané Zákazníkom v elektronickej podobe podpísané platným kvalifikovaným elektronickým podpisom alebo kvalifikovanou elektronickou pečaťou (výpis s obchodného registra, plná moc, prehlásenie, poverenie ap.).

3.2.4 Neoverované informácie o Držiteľovi

V priebehu prvotného vydania sa neoveruje e-mail adresa uvedená v žiadosti, u certifikátov, ktoré neobsahujú rozšírenie emailProtection.

3.2.5 Overovanie oprávnení

Pozri 3.2.3.

3.2.6 Kritériá interoperability

Poskytovateľ musí zverejniť všetky cross-certifikáty, ktoré identifikujú Poskytovateľa ako subjekt certifikátu.

3.3 Identifikácia a autentifikácia pri vydávaní následného certifikátu

3.3.1 Identifikácia a autentifikácia pri riadnom vydávaní následného certifikátu

Pri riadnom vydaní následného certifikátu dochádza k zmene páru kľúčov certifikátu – vytvorí sa nový certifikát, ktorý bude mať zhodné povinné položky rozlišovacieho mena, odlišný verejný kľúč (zodpovedajúci novému, odlišnému súkromnému kľúču), odlišné číslo certifikátu (Serial Number) a môže mať zmenenú dĺžku doby platnosti.

Držiteľ platného certifikátu môže požiadať o vydanie následného certifikátu len počas posledných 30 dní platnosti certifikátu, ku ktorému sa bude následný certifikát vydávať.

O vydanie následného certifikátu (certifikát pre fyzickú osobu, certifikát pre právnickú osobu) môže Držiteľ požiadať jedným z nasledovných spôsobov:

- Vygeneruje si novú žiadosť o certifikát, s totožným obsahom (s výnimkou položiek Organizačný útvar a Mesto) ako mal predchádzajúci certifikát, ktorú musí zaslať podpísaným e-mailom na kontaktnú e-mailovú adresu RA. Pri podpise e-mailu so žiadosťou musí využiť súkromný kľúč prislúchajúci k platnému certifikátu, na základe ktorého sa má následný certifikát vydať. V zasielanej e-mailovej správe zároveň musí oznámiť, že nedošlo k zmene jeho osobných údajov na základe, ktorých bol identifikovaný a autentifikovaný pri vydaní predchádzajúceho certifikátu. Pokiaľ nie je možné pri obnove certifikátu použiť podpísaný e-mail, je možné takúto žiadosť zaslať aj nepodpísaným e-mailom z rovnakej e-mail adresy aká sa nachádza v žiadosti. Súčasťou e-mailu musí byť aj oznámenie o nezmenených osobných údajoch. V danom prípade musí byť zo strany RA spustený proces overenia zaslanej žiadosti. V prípade zaslania žiadosti o vydanie následného certifikátu nepodpísaným e-mailom z inej adresy ako je uvedená v zaslanej žiadosti môže byť táto akceptovaná len v prípade dodatočného overenia zaslania žiadosti zo strany RA.
- Vygeneruje si novú žiadosť o certifikát, odošle ju e-mailom na kontaktnú adresu RA a osobne sa dostaví na RA, kde sa podrobí postupom a požiadavkám na overenie identity ako pri prvotnom vydaní certifikátu.
- Vytvorí si novú žiadosť o vydanie následného certifikátu a vydá si certifikát automatizovaným spôsobom prostredníctvom rozhrania prístupného na webovom sídle Poskytovateľa. Poskytovateľ si vyhradzuje právo umožniť vydanie následného certifikátu týmto spôsobom len vybraným zmluvným partnerom.
- Držiteľ platného certifikátu vydaného pre účely zmluvného partnera môže požiadať o vydanie následného certifikátu aj prostredníctvom iného mechanizmu, ktorý je dohodnutý medzi zmluvným partnerom a Poskytovateľom.

V prípade TLS certifikátov sa následné certifikáty nevydávajú.

Poskytovateľ vydáva všetky certifikáty s výnimkou TLS certifikátov s platnosťou maximálne na 60 mesiacov t. j. 5 rokov.

3.3.2 Identifikácia a autentifikácia pri vydávaní následného certifikátu po zrušení predchádzajúceho

V prípade, že po zrušení platnosti certifikátu chce mať Zákazník/Držiteľ nový platný certifikát vydaný Poskytovateľom, musí požiadať o vydanie nového certifikátu podľa časti 4.1. Pri tomto úkone sa podrobuje rovnakej autentizácii ako je uvedené v časti 3.2.

3.4 Identifikácia a autentifikácia pri žiadaní o zrušenie certifikátu

Žiadosť o zrušenie certifikátu musí byť autentizovaná, pozri časť 4.9.3. V prípade osobného certifikátu môže byť žiadosť o zrušenie certifikátu autentizovaná

využitím súkromného kľúča patriaceho k certifikátu bez ohľadu na to, či daný súkromný kľúč bol alebo nebol kompromitovaný.

4. Požiadavky na životný cyklus certifikátu

Obsahom tejto časti je popis prevádzkových požiadaviek životného cyklu certifikátu od žiadania o jeho vydanie.

4.1 Žiadanie o certifikát

4.1.1 Kto môže žiadať o vydanie certifikátu

Poskytovateľa môže požiadať o vydanie:

- certifikátu pre fyzickú osobu:
  - fyzická osoba resp. fyzická osoba splnomocnená Zákazníkom
  - akákoľvek entita, s ktorou je fyzická osoba spojená napr. jej zamestnávateľ, nezisková organizácia, ktorej je členom ap.
- certifikátu pre právnickú osobu:
  - akákoľvek entita, ktorá v zmysle platnej národnej legislatívy koná v mene danej právnickej osoby,
- TLS certifikátu pre autentifikáciu webového sídla:
  - fyzická alebo právnická osoba prevádzkujúca zariadenie resp. systém, ktorá preukáže oprávnenosť žiadať o certifikát pre FQDN nachádzajúce sa v žiadosti resp. pre FQDN, ktoré majú byť uvedené v SAN rozšírení.

Poskytovateľ musí udržiavať internú databázu všetkých revokovaných TLS certifikátov a odmietnutých žiadostí pre podozrenie z phishingu alebo iného podvodného konania.

4.1.2 Registračný proces a zodpovednosti

4.1.2.1 Príprava

Zákazník musí vykonať nasledovné kroky ako prípravu na návštevu Poskytovateľa:

- Oboznámiť sa so „Všeobecnými podmienkami poskytovania a používania dôveryhodnej služby vydávania a overovania certifikátov“ (ďalej len „Všeobecné podmienky“) [6] a Informáciou o spracúvaní osobných údajov [12], ktoré musia byť v čitateľnej podobe dostupné prostredníctvo trvalého komunikačného kanálu (pozri https://eidas.disig.sk/sk/documents/);
- Oboznámiť sa s týmto postupom, prípadne s princípmi a návodmi na získanie certifikátu;
- Pripraviť si hodnoty jednotlivých položiek žiadosti o certifikát tak, aby tieto hodnoty boli v súlade s touto CP (pozri časť 3.1.4);
- Pripraviť žiadosť o vydanie certifikátu vo formáte PKCS#10 resp. SPKAC, ktorú zašle vopred elektronickou poštou Poskytovateľovi (pozri časť 4.1.2.3);
- Pripraviť si zvolené doklady totožnosti resp. iné potrebné doklady, napr. výpis z obchodného registra, plné moci atď.;
- Dohodnúť si termín návštevy.

4.1.2.2 Generovanie žiadosti

4.1.2.2.1 Generovanie žiadosti o certifikát pre fyzickú osoby resp. právnickú osobu

O vydanie certifikátu pre fyzickú osobu resp. právnickú osobu je možné požiadať len na základe žiadosti vo formáte PKCS#10 resp. SPKAC. Zákazník je povinný na svojom počítači pomocou vyhovujúceho prehliadača a webového sídla Poskytovateľa (viď URL adresu v časť 1) vygenerovať žiadosť o certifikát a uložiť si ju na vhodné médium (HDD, USB disk, disketa ap.).

Žiadosť o certifikát pre fyzickú osobu, kde kryptografické kľúče sú určené na podpisovanie a šifrovanie elektronickej pošty musí byť zaslaná príslušnej RA elektronickou poštou vopred a z e-mailovej adresy, ktorá je uvedená v žiadosti o certifikát v položke E-mail. E-mailové adresy jednotlivých RA Poskytovateľa sú k dispozícii na webovom sídle Poskytovateľa (pozri časť 1).

Zákazník žiadajúci o následný certifikát si musí vytvoriť žiadosť podľa postupu popísaného v časti 4.7.3.

Žiadosť o certifikát resp. v nej sa nachádzajúci verejný kľúč, pre ktorý už bol vydaný certifikát, nemôže byť z bezpečnostných dôvodov použitá opakovane na vydanie iného certifikátu a musí byť na RA odmietnutá!

Pri zadávaní hodnôt do položiek žiadosti o certifikát musí mať Zákazník na zreteli, že na RA bude musieť uspokojivým spôsobom preukázať oprávnenosť všetkých údajov, ktoré sú uvedené v jednotlivých položkách žiadosti o certifikát.

Žiadosť o certifikát vydávaný fyzickej osobe, ktorá je zamestnancom zmluvného partnera, je možné generovať aj iným spôsobom, ako prostredníctvom webového sídla Poskytovateľa napr. vlastný web portál zmluvného partnera ap. Tento spôsob musí byť vopred dohodnutý so zmluvným partnerom a jednotlivý žiadatelia musia byť o spôsobe generovania a zasielania žiadosti informovaní ako zo strany zmluvného partnera, tak aj zo strany Poskytovateľa.

4.1.2.2.2 Generovanie žiadosti na vydanie TLS certifikátu

Zákazník si pomocou svojho softvéru (typicky napr. Microsoft IIS alebo Apache/Openssl) 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.

TLS certifikáty vydáva Poskytovateľ výhradne len v sídle spoločnosti v Bratislave.

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 Poskytovateľom, v opačnom prípade

si Poskytovateľ 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. Osobou žiadajúcou o vydanie TLS certifikát v mene Zákazníka 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 ukazujúci na určiteľnú fyzickú alebo právnickú osobu, pokiaľ použitie týchto informácií nie je žiadateľ schopný hodnoverne doložiť.

4.1.2.3 Zaslanie žiadosti o certifikát

Žiadosť o vydanie certifikátu zasiela Zákazník na RA (radisig@disig.sk) , ktorá musí vykonať všetky procedúry súvisiace s procesom vydávania certifikátu. V prípade, že certifikát je vydávaný priamo na QSCD zariadenie, tak kryptografický kľúčový pár a žiadosť musí pracovník RA vygenerovať priamo v QSCD zariadení prostredníctvom aplikácii RA Client.

4.2 Spracovanie žiadosti o vydanie certifikátu

4.2.1 Vykonanie identifikácie a autentifikácie

Pred vydaním certifikátu musí zamestnanec zastupujúci Poskytovateľa:

- informovať prítomnú fyzickú osobu o Všeobecných podmienkach [6],
- skontrolovať úplnosť a správnosť údajov v prijatej žiadosti o certifikát,
- overiť totožnosť budúceho Držiteľa certifikátu a vložiť jeho osobné údaje do IS Poskytovateľa, pričom je povinný vyplniť všetky povinné položky vyžadované systémom Poskytovateľa,
- overiť ďalšie doklady na overenie ľubovoľných identifikačných údajov, ktoré sa majú dostať do certifikátu.

V prípade certifikátu pre fyzickú osobu alebo právnickú osobu, kde kryptografické kľúče nie sú v QSCD musí pracovník RA pred overením totožnosti Držiteľa skontrolovať doručenú žiadosť, ktorá môže byť vo formáte PKCS#10 resp. SPKAC. Obsah položiek žiadosti a povinnosť ich vyplnenia pozri 3.1.4 (hrubo vyznačené položky sú povinné).

Pracovník RA musí overiť, či elektronicky zaslaná žiadosť o vydanie certifikátu daného Zákazníka bola zaslaná z rovnakej e-mailovej adresy, aká sa nachádza v žiadosti o vydanie certifikátu. V prípade zistených rozdielov môže odmietnuť vydanie certifikátu. Toto sa nepoužije v prípade, že vydávaný certifikát neobsahuje rozšírenie „Secure Email (1.3.6.1.5.5.7.3.4)“.

V súvislosti s overovaním e-mailu, ktorý má byť použitý na podpisovanie elektronických správ (rozšírenie „Secure Email (1.3.6.1.5.5.7.3.4)“) musí pracovník RA vykonať kontrolu e-mailovej adresy nachádzajúcej sa v žiadosti o vydanie certifikátu, odpoveďou na e-mail, z ktorého bola žiadosť zaslaná. Overenie sa vykoná tak, že na danú e-mailovú adresu musí zaslať elektronickú správu ktorá bude obsahovať tajnú nepredvídateľnú informáciu (overovacia informácia). Zákazník musí zaslať späť overovaciu informáciu ako dôkaz kontroly danej e-mailovej adresy. V prípade, že overenie e-mailovej adresy prebehne neúspešne, Poskytovateľ odmietne vydanie certifikátu. Overovanie e-mailovej adresy nie je

potrebné v prípade, že je zaslaná žiadosť o následný certifikát elektronicky e-mailom, ktorý je podpísaný platným certifikátom Držiteľa, vydaným certifikačnou autoritou Poskytovateľa a e-mailová adresa, z ktorej bola žiadosť zaslaná, je zhodná s e-mailovou adresou nachádzajúcou sa v žiadosti.

Pracovník RA musí overiť identitu a autenticitu Zákazníka v zmysle časti 3.2.

Zákazník musí na RA uspokojivým spôsobom preukázať všetky údaje, ktoré zadal do jednotlivých položiek žiadosti o certifikát.

Pracovník RA musí vložiť do informačného systému Poskytovateľa žiadosť o certifikát a ostatné požadované údaje.

V prípade žiadosti o následný certifikát sa musí postupovať podľa časti 4.7.

V prípade vydávania certifikátu pre zmluvného partnera, ktorý slúžia výhradne pre interné potreby zmluvného partnera, sú detailné postupy na získanie certifikátu týchto typov a postupy pri registrácii na RA pre daného zmluvného partnera, uvedené v príslušnom dokumente CPS alebo v interných dokumentoch zmluvného partnera.

4.2.2 Schválenie alebo zamietnutie žiadosti o certifikát

V prípade ľubovoľných odôvodnených pochybností o totožnosti Zákazníka, taktiež v prípade zistených nedostatkoch v dokladoch, resp. poskytnutí neúplných dokladov, musí pracovník RA registráciu Zákazníka odmietnuť.

Žiadosť musí byť zamietnutá aj v prípade, že jej formát resp. obsah nezodpovedá požiadavkám stanoveným v časti 3.1.4 a 4.1.2.2.

Ak na verejný kľúč obsiahnutý v žiadosti bol v minulosti vydaný systémom Poskytovateľa certifikát, vydanie nového certifikátu na túto žiadosť musí byť z bezpečnostných dôvodov zamietnuté, nakoľko už raz certifikovaný verejný kľúč nemôže byť použitý v inom certifikáte.

Poskytovateľ nesmie vydať TLS certifikáty pre FQDN, ktorá obsahuje doménu najvyššej (gTLD), ktoré nie je uvedená a v databáze „Root Zone Database“, ktorú vedie Internet Assigned Numbers Authority (IANA) (https://www.iana.org/domains/root/db).

Každá žiadosť spĺňajúca požiadavky tejto CP musí byť spracovaná okamžite, ak je vydávanie vykonávané za prítomnosti Zákazníka alebo najneskoršie do času, ktorý bol dohodnutý so Zákazníkom v procese žiadania o certifikát.

4.2.3 Doručenie verejného kľúča vydavateľovi certifikátu

Aby sa garantovala väzba overenej identity Držiteľa k verejnému kľúču na ktorý má byť vydaný certifikát, verejný kľúč (obsiahnutý v žiadostiach o certifikát) sa musí doručiť CA prostredníctvom RA. Zákazník musí doručiť žiadosť na RA buď osobne alebo na základe dohody s príslušnou RA môže zaslať žiadosť aj elektronickou poštou. V prípade certifikátu, ktorý je určený na podpisovanie elektronickej pošty (rozšírenie „Secure Email (1.3.6.1.5.5.7.3.4)“) musí byť žiadosť zaslaná na príslušnú RA vopred elektronicky, aby mohlo byť zo strany Poskytovateľa vykonané overenie kontroly daného e-mailového konta.

4.3 Vydanie certifikátu

4.3.1 Činnosť CA pri vydávaní certifikátu

Po odoslaní certifikátu z RA na CA musí systém CA vykonať overenie prijatej žiadosti za účelom overenia, či:

- bola odoslaná oprávneným pracovníkom RA,
- zodpovedá štandardu pre PKCS#10 resp. SPKAC,
- pre verejný kľúč nachádzajúci sa v predloženej žiadosti o certifikát už nebol v minulosti vydaný certifikát.

Vydanie certifikátu na kľúčový pár generovaný priamo na RA musí byť bezpečne naviazané na procedúru tohto generovania.

V prípade splnenia všetkých požiadaviek na vydanie certifikátu, musí systém CA certifikát vydať.

4.3.2 Informovanie Držiteľa o vydaní certifikátu

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

4.4 Prevzatie certifikátu

4.4.1 Spôsob prevzatia certifikátu

Certifikáty sa v systéme Poskytovateľa budú vytvárať a vydávať automatizovane a priebežne. Držiteľ si bude môcť bezprostredne po vydaní certifikátu prevziať vydaný certifikát.

Po vydaní certifikátu musí pracovník RA a Držiteľ podpísať príslušnú dokumentáciu súvisiacu s vydaním certifikátu.

4.4.2 Zverejňovanie certifikátu

Vydaný certifikát musí byť zverejnený v úložisku Poskytovateľa, ktorý je dostupný prostredníctvom webového sídla Poskytovateľa (pozri časť 1) pokiaľ Držiteľ certifikátu súhlasil so zverejnením.

4.4.3 Oznámenie o vydaní certifikátu iným subjektom

Poskytovateľ nezasiela oznámenie o vydaní certifikátu iným subjektom ako je Držiteľ certifikátu.

4.5 Kľúčový pár a používanie certifikátu

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

4.5.1 Používanie súkromného kľúča a certifikátu Držiteľom

Držiteľ certifikátu vo vzťahu k súkromnému kľúču a certifikátu musí:

- poskytnúť Poskytovateľovi pri žiadaní o vydanie certifikátu presné a úplné informácie zmysle tejto CP,
- používať kľúčový pár v súlade s obmedzeniami, na ktoré bol upozornený zo strany Poskytovateľa,
- neustále chrániť svoje súkromné kľúče v súlade s touto CP a v súlade so znením ustanovení Všeobecných podmienok [6],
- využívať súkromný kľúč až po tom ako dostane certifikát k verejnému kľúču s ktorým tvorí pár,
- bezodkladne upovedomiť Poskytovateľa, ak certifikát ešte neexspiroval, o podozrení, že:
  - jeho súkromný kľúč bol stratený, odcudzený alebo kompromitovaný,
  - stratil kontrolu nad súkromným kľúčom kompromitáciou jeho aktivačných údajov (PIN, PUK),
- bezodkladne požiadať o zrušenie certifikátu v prípade, že akýkoľvek údaj uvedený v subjekte certifikátu sa stal neplatným,
- dodržiavať všetky termíny, podmienky a obmedzenia uložené na využívanie svojho súkromného kľúča a certifikátu napr. ukončiť využívanie súkromného kľúča po exspirácii alebo zrušení certifikátu verejného kľúča,

Držiteľ certifikátu, ktorý nebude dodržiavať svoje povinnosti, nemá nárok na náhradu prípadnej škody.

4.5.2 Používanie verejného kľúča a certifikátu Spoliehajúcou sa stranou

Spoliehajúce sa strany, ktoré sa spoliehajú na certifikáty podľa tohto CP a v súlade so Všeobecnými podmienkami [6] sú povinné:

- zhodnotiť, či použitie certifikátu je v súlade s jeho účelovým určením a či je pre konkrétny účel vhodné,
- skontrolovať, či použitie certifikátu nie je v rozpore s obmedzeniami použitia certifikátu uvedenými v samotnom certifikáte, vo Všeobecných podmienkach [6] alebo v tejto CP,
- pri práci s certifikátom, vrátane jeho overovania, používať iba na to určený a vhodný hardvér resp. softvér,
- overiť platnosť predmetného certifikátu, tým, že skontroluje či:
  - bol certifikát v zmysle údaja o dobe platnosti certifikátu uvedeného v certifikáte platný v čase, keď spoliehajúca sa strana mala istotu, že certifikát, resp. ním vytvorený podpis/pečať existovali;
  - pred časom uvedeným v predchádzajúcom bode nedošlo k zrušeniu certifikátu pred uplynutím doby jeho platnosti podľa predchádzajúceho bodu, a to na základe aktuálneho CRL a prípadne OCSP odpovede poskytovaných Poskytovateľom - odkaz na umiestnenie aktuálneho CRL a prípadne na službu OCSP je uvedený v tele certifikátu;

- vykonať prípadne ďalšie overenia, ktoré môžu byť v zmysle tejto CP alebo štandardov vyžadované pre konkrétny druh certifikátu alebo jeho použitie a spôsobom podľa predchádzajúcich bodov overiť aj ostatné certifikáty v certifikačnej ceste až po tzv. „trust anchor“.

4.6 Obnova certifikátu

4.6.1 Okolnosti pre obnovenie certifikátu

Poskytovateľ neumožní obnovu (vydanie) certifikátu na verejný kľúč, na ktorý už bol v minulosti, ním prevádzkovanou CA, vydaný iný certifikát.

4.6.2 Kto môže požiadať o obnovenie

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 Zverejňovanie 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

V tejto časti sú popísané podmienky vydania nového certifikátu na nový kľúčový pár po exspirácii resp. zrušení používaného certifikátu vydaného Poskytovateľom pre existujúceho Zákazníka/Držiteľa, ktorého osobné údaje sú zavedené v systéme Poskytovateľa.

4.7.1 Podmienky vydania certifikátu na nové kľúče

Certifikát môže byť vydaný vždy, ak sú splnené podmienky pre vydávanie daného typu certifikátu.

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

Certifikát musí byť vydávaný rovnakým spôsobom ako bol vydávaný pôvodný certifikát za možnosti využitia modifikovaných spôsobov autentizácie popísaných v časti 3.

4.7.4 Oznámenie o vydaní certifikátu na nové kľúče Držiteľovi

Po vydaní certifikátu musí byť 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 musí uplatniť spôsob prevzatia popísaný v časti 4.4.

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

Po prevzatí certifikátu je Zákazník povinný zaplatiť za poskytnutú službu v zmysle cenníka Poskytovateľa vopred dohodnutým spôsobom.

4.7.6 Zverejňovanie certifikátov zo strany Poskytovateľa

Pozri časť4.4.2.

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

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

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 suspendovanie certifikátu

4.9.1 Podmienky zrušenia certifikátu

Certifikát sa musí zrušiť, keď sa väzba medzi subjektom a jeho verejným kľúčom definovaným v certifikáte už nepovažuje za platnú.

4.9.1.1 Zrušenie certifikátu Zákazníka/Držiteľa

Poskytovateľ je povinný do 24 hodín zrušiť certifikát, ktorý spravuje v prípade, že nastane jeden z nasledujúcich prípadov:

- Zákazník/Držiteľ certifikátu alebo iná oprávnená strana písomne požiada o zrušenie certifikátu,
- Zákazník/Držiteľ oznámi Poskytovateľovi, že pôvodná žiadosť o vydanie ním nebola autorizovaná a neposkytne spätnú autorizáciu vydania,
- Poskytovateľ získa dôkaz, že došlo ku kompromitácii súkromného kľúča, ktorý zodpovedá verejnému kľúču v certifikáte,
- v prípade TLS certifikátu:
  - Poskytovateľ získa dôkaz, že už sa nemôže spoliehať na overenie platnosti autorizácie domény alebo na kontrolu pre akúkoľvek uvedenú FQDN.

Poskytovateľ by mal zrušiť certifikát v priebehu 24 hodín a musí ho zrušiť do piatich (5) dní v prípade, že nastane niektorý z týchto prípadov:

- Certifikát už viac nespĺňa požiadavky v zmysle kapitoly 6.1.5 a 6.1.6,
- Poskytovateľ získa dôkaz, že došlo k jeho zneužitiu,
- Držiteľ certifikátu nedodržuje svoje povinnosti Držiteľa certifikátu, ktorými je zmluvne viazaný,
- je podozrenie, že certifikát nebol vydaný v súlade s touto CP resp. zodpovedajúcimi CPS,
- v prípade TLS certifikátu:
  - je Poskytovateľ oboznámený s okolnosťami, ktoré naznačujú, že používanie FQDN v certifikáte už nie je právne možné (napr. rozhodnutím súdu, ukončením zmluvy medzi registrátorom a jej držiteľom, alebo registrátor domény neobnovil jej registráciu apod.),
  - CA sa dozvie, že „wildcard“ certifikát bol použitý na autentifikáciu podvodnej zavádzajúcej podriadenej FQDN,
  - pokiaľ zanikne právo alebo je zrušené resp. ukončené právo vydávať certifikáty podľa BR CA/Browser forum [3] a Poskytovateľ neurobil opatrenia na pokračovanie v poskytovaní informácií z úložiska CRL/OCSP
  - Poskytovateľ je informovaný o preukázanej alebo overenej metóde, ktorá kompromituje súkromnému kľúču Držiteľa, že boli vyvinuté

metódy, ktoré ho môžu ľahko vypočítať na základe verejného kľúča (napríklad slabého Debian kľúča, alebo ak existuje jasný dôkaz, že konkrétna metóda použitá na vytvorenie súkromného kľúča bola chybná.

- Poskytovateľ je oboznámený, že došlo k podstatným zmenám informácií uvedených v certifikáte,
- CA sa dozvie, že „wildcard“ certifikát bol použitý na autentifikáciu podvodnej zavádzajúcej podriadenej FQDN
- Poskytovateľ je oboznámený s tým, že certifikát nebol vydaný v súlade s touto CP alebo príslušnými CPS,
- Poskytovateľ zistí, že niektorá z informácií uvedených v certifikáte je nepresná,
- Poskytovateľ ukončí z akéhokoľvek dôvodu svoju činnosť a zmluvne nezaisti u inej CA, aby poskytovala informácie o zrušených certifikátoch v jeho mene,
- skončili okolnosti, ktoré vyžadovali vydanie certifikátu (testovanie, overovanie aplikácií ap.),
- došlo ku strate súkromného kľúča,
- technické parametre alebo formát certifikátu by mohli viesť k neakceptovateľnému riziku z pohľadu dodávateľov softvéru alebo Spoliehajúcich sa strán (zmena kryptografických algoritmov na podpisovanie, dĺžka kryptografických kľúčov ap.),
- subjekt certifikátu zomrel ak ide o fyzickú osobu resp. ak ide o právnickú osobu zanikol a Poskytovateľ bude o tejto skutočnosti informovaný,
- zrušenie je vyžadované touto CP alebo príslušnými CPS.

Vždy, keď sa Poskytovateľ dozvie o niektorej z vyššie uvedených okolností, daný certifikát sa musí zrušiť a dať na zoznam zrušených certifikátov (ďalej len „CRL“).

Zrušený certifikát sa musí vyskytovať vo všetkých nových vydaniach CRL, minimálne dovtedy, kým danému certifikátu nepominie doba platnosti.

Zrušený certifikát nie je možné za žiadnych okolností obnoviť.

Pokiaľ dôjde k zrušeniu TLS certifikátu, ktorý bol vydaný pre koncového držiteľa na základe niektorého z týchto dôvodov:

- keyCompromise (RFC 5280 CRLReason #1),
- privilegeWithdrawn (RFC 5280 CRLReason #9),
- cessationOfOperation (RFC 5280 CRLReason #5),
- affiliationChanged (RFC 5280 CRLReason #3), alebor
- superseded (RFC 5280 CRLReason #4),

tak tento špecifický dôvod zrušenia (CRLReason) musí byť uvedený v položke reasonCode zoznamu zrušených certifikátov (CRL), ktorý je zverejňovaný po zrušení TLS certifikátu. V prípade, že je TLS certifikát zrušený z iných dôvodov ako sú vyššie uvedené, tak sa položka reasonCode v CRL nebude vyskytovať.

4.9.1.2 Zrušenie certifikátu podriadenej CA

Poskytovateľ musí zrušiť certifikát podriadenej CA v priebehu 7 dní v prípade že:

- dostane písomnú požiadavku na zrušenie podriadenej CA,
- podriadená CA informuje vydávajúcu CA Poskytovateľa, že pôvodná požiadavka nebola autorizovaná a neposkytne dodatočnú autorizáciu,
- Poskytovateľ získa dôkaz, že došlo ku kompromitácii súkromného kľúča zodpovedajúceho verejnému kľúču v certifikáte podriadenej CA resp. už nespĺňa požiadavky v zmysle kapitoly 6.1.5 a 6.1.6,
- Poskytovateľ získa dôkaz, že došlo k zneužitiu certifikátu podriadenej CA,
- Poskytovateľ je oboznámený s tým, že certifikát podriadenej CA nebol vydaný v súlade s týmto CP a príslušnými CPS,
- Poskytovateľ rozhodne, že niektorá z informácií uvedených v certifikáte podriadenej CA je nepresné alebo zavádzajúca,
- dôjde k ukončeniu činnosti CA a neexistuje možnosť, že iná CA bude poskytovať údaje o zrušených certifikátoch,
- zrušenie je vyžadované touto CP alebo príslušnými CPS,
- V prípade TLS certifikátu:
  - pokiaľ zanikne právo alebo je zrušené resp. ukončené právo vydávať certifikáty podľa BR CA/Browser forum [3] a Poskytovateľ neurobil opatrenia na pokračovanie v poskytovaní informácií z úložiska CRL/OCSP.

4.9.2 Kto môže žiadať o zrušenie certifikátu

Držiteľ certifikátu (alebo ním poverená fyzická alebo právnická osoba) môže kedykoľvek požiadať o zrušenie svojho vlastného certifikátu a to aj bez udania dôvodu žiadosti o zrušenie certifikátu.

V prípade žiadosti o zrušenie TLS certifikátu z dôvodov, ktoré musia byť publikované v CRL, musí žiadateľ tieto vo svojej žiadosti uviesť.

RA musí zrušiť certifikát daného Držiteľa, ak sa dozvie, že nastala niektorá z okolností uvedených v časti 4.9.1.

O zrušenie certifikátu môže ďalej požiadať:

- Poskytovateľ - daný pracovník musí písomne zdokumentovať túto skutočnosť vrátane dôvodu svojho konania,
- súd prostredníctvom svojho rozsudku alebo predbežného opatrenia (k dokumentom o zrušení certifikátu sa musí priložiť kópia príslušného súdneho rozhodnutia),
- subjekt (fyzická alebo právnická osoba) na základe dedičského konania (k dokumentom o zrušení certifikátu sa musí priložiť kópia dokladov, z ktorých vyplýva právo daného subjektu žiadať o zrušenie certifikátu),

- V prípade certifikátu RA môže o zrušenie certifikátu okrem jeho Držiteľa (pracovníka danej RA) požiadať tiež PMA, ak sa zistí závažná okolnosť (pozri časť 4.9.1) na zrušenie daného certifikátu.

4.9.3 Postup žiadosti o zrušenie certifikátu

V prípade splnenia podmienok autentifikácie Držiteľa certifikátu, ktorý žiada o jeho zrušenie (časť 3.2.3 resp.3.2.2), je možné žiadosť o zrušenie certifikátu podať:

- Osobne na pobočke RA prostredníctvom formulára „Žiadosť o zrušenie certifikátu“ dostupnom na RA – pracovník RA môže vyžiadať heslo na zrušenie certifikátu v prípade, ak osobou, ktorá žiada o zrušenie certifikátu nie je Držiteľ certifikátu, ale ním poverená osoba;
- Prostredníctvom elektronickej pošty – zaslaním elektronickej poštovej správy, podpísanej s využitím súkromného kľúča, tvoriaceho kľúčový pár s certifikátom, o zrušenie ktorého sa žiada. Obsahom správy musí byť jednoznačná vôľa na zrušenie certifikátu vyjadrená vetou „Žiadam týmto o zrušenie môjho certifikátu so sériovým číslom XXXXXX“;
- Prostredníctvom elektronickej pošty – zaslaním elektronickej poštovej správy (nemusí byť podpísaná). Obsahom správy musí byť jednoznačná vôľa na zrušenie certifikátu vyjadrená vetou „Žiadam týmto o zrušenie môjho certifikátu so sériovým číslom XXXXXX“. Pri takto zaslanej správe musí byť súčasťou mailu aj heslo na zrušenie certifikátu;
- Prostredníctvom poštovej zásielky spolu so zadaním hesla na zrušenie certifikátu zaslanej na adresu Poskytovateľa resp. príslušnej RA, ktorá sprostredkovala vydanie certifikátu, o zrušenie ktorého sa žiada;
- V prípade žiadosti o zrušenie TLS certifikátu z dôvodov, ktoré sú uvedené v časti 4.9.1.1 musí byť zo strany držiteľa certifikátu predložená/doručená „Žiadosť o zrušenie TLS certifikátu“, ktorá je dostupná na webovom sídle Poskytovateľa: https://dsrv.disig.sk/download/forms/tls_revoke_form.pdf.

Žiadosť o zrušenie certifikátu vydaného pre účely zmluvného partnera je možné podať buď priamo u Poskytovateľa alebo len na RA, ktorá je uvedená v príslušnej zmluve a pôsobí v mene Poskytovateľa u zmluvného partnera..

Certifikát, ktorému uplynula platnosť, nie je možné zrušiť.

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.

4.9.4 Čas na podanie žiadosti o zrušenie certifikátu

Žiadosť o zrušenie certifikátu v prípade hrozby kompromitácie súkromného kľúča musí podať Držiteľ certifikátu čo najskôr. Osobne je možné žiadať o zrušenie len v pracovnej dobe určenej jednotlivými RA, ktorých zoznam a pracovná doba je zverejnená na webovom sídle Poskytovateľa (pozri časť 1). Pri elektronickej žiadosti je túto možné zaslať na jednotlivé RA kedykoľvek.

4.9.5 Čas na spracovanie žiadosti o zrušenie certifikátu

Poskytovateľ musí:

- V priebehu 24 hodín od oznámenia problému s certifikátom je Poskytovateľ povinný preskúmať skutočnosti týkajúce sa oznámeného problému a poskytnúť Zákazníkovi/Držiteľov a spoliehajúcim sa stranám predbežnú informáciu o svojich zisteniach,
- Po preskúmaní faktov a okolností musí Poskytovateľ v súčinnosti so Zákazníkom/Držiteľom a koncovou entitou, ktorá oznámila problém rozhodnúť, či bude certifikát zrušený alebo nie a ak bude zrušený, tak v akom termíne.
- Čas medzi prevzatím oznámenia o probléme s certifikátom a publikovaním informácie o zrušení nesmie prekročiť časový rámec uvedený v kapitole 4.9.1.1, pričom stanovený termín by mal zohľadňovať tieto skutočnosti:
  - povahu údajného problému (rozsah, kontext, závažnosť, riziko poškodenia zainteresovaných strán)
  - dôsledky zrušenia (priame a vedľajšie vplyvy na Zákazníkov/Držiteľov
  - počet nahlásených problémov s predmetným certifikátom
  - subjekt, ktorý oznámil problém,
  - platné právne predpisy.
- zverejniť aktuálny zoznam zrušených certifikátov a všetky predchádzajúce zoznamy zrušených certifikátov na svojom webovom sídle (pozri časť 1),
- zverejniť v CRL všetky ním zrušené certifikáty t. j. aj tie, ktorých platnosť medzitým skončila,
- archivovať všetky CRL, ktoré vydal.

Poskytovateľ musí automaticky informovať Držiteľa certifikátu o zrušení jeho certifikátu, zaslaním e-mailu na e-mailovú adresu, ktorú poskytol Držiteľ v priebehu registrácie na RA.

Poskytovateľ musí CRL publikovať do úložiska v čo najrýchlejšom čase po jeho vydaní.

4.9.6 Overovanie platnosti zo strany spoliehajúcej sa strany

Spoliehajúca sa strana je povinná pri spoľahnutí sa na certifikát overiť si jeho platnosť v zmysle Všeobecných podmienok [6].

V čase medzi podaním oprávnenej žiadosti o zrušenie certifikátu a zverejnením zrušeného certifikátu na CRL nesie Zákazník/Držiteľ certifikátu všetku zodpovednosť za prípadné škody spôsobené zneužitím jeho certifikátu. Po zverejnení certifikátu v CRL nesie všetku zodpovednosť za prípadné škody spôsobené použitím zrušeného certifikátu strana, ktorá sa na daný zrušený certifikát spoľahla.

Neoverenie certifikátu pomocou CRL je považované za hrubé porušenie tejto CP.

4.9.7 Frekvencia vydávania CRL

Frekvencia vydávania zoznamu zrušených certifikátov (CRL) sa líši v závislosti na tom, či sa to týka koreňovej CA, podriadenej CA. Tabuľka č. 6 obsahuje informácie o maximálnych požiadavkách na vydávanie.

Tabuľka č. 6: Frekvencia vydávania CRL

Vydavateľ CRL	Frekvencia vydávania	nextUpdate vs. thisUpdate	Poznámka k vydávaniu
Koreňová CA	max 365 dní	< 365 dní	Vždy do 24 hodín po zrušení podriadenej CA
Podriadená CA	max 7 dní	< 10 dní	

Podriadené CA Poskytovateľa vydávajúce certifikáty koncovým používateľom musia vydávať CRL:

- minimálne každých 24 hodín, a to aj v prípade, keď za posledných 24 hodín nebol zrušený žiadny certifikát a s hodnotou nextUpdate 24 hodín

Koreňové CA Poskytovateľa vydávajúce certifikáty podriadeným CA musia vydávať CRL:

- minimálne každých 7 dní s hodnotou nextUpdate 14 dní
- vždy do 24 hodín po zrušení certifikátu podriadenej CA

4.9.8 Doba publikovania CRL

Maximálna doba latencie CRL od jeho vydania do jeho publikovania v úložisku nesmie presiahnuť 90 sekúnd.

4.9.9 Dostupnosť služby OCSP

Poskytovateľ môže pre vybrané typy certifikátov poskytovať službu OCSP. V prípade poskytovania služby OCSP musia byť URI adresy OSCP responderov obsiahnuté v rozšírení certifikátu Authority Information Access.

4.9.10 Požiadavky na OCSP overovanie

Tretie strany, ktoré majú záujem využívať službu OCSP musia zaslať požiadavku na príslušný OCSP responder, ktorého URI je publikovaná v certifikáte. Zaslaná žiadosť musí byť v súlade s požiadavkami RFC 6960.

4.9.11 Iné formy dostupnosti informácií o zrušení certifikátu

Overenie aktuálneho stavu certifikátu je možné vykonať manuálne prostredníctvom zoznamov aktuálnych CRL ako aj archívu všetkých vydaných CRL pre jednotlivé CA Poskytovateľa, ktoré musia byť dostupné na webovom sídle Poskytovateľa (pozri časť 1). RA musí odpovedať na dopyt týkajúci sa stavu konkrétneho certifikátu, ak bol tento dopyt urobený telefonicky, faxom alebo emailom.

RA musí na požiadanie zaslať aktuálne CRL prostredníctvom emailu na dohodnutú email adresu čo najskôr.

4.9.12 Špeciálne požiadavky na zmenu kľúčov po ich kompromitácii

Kompromitácia súkromného kľúča certifikačných autorít (koreňová, podriadené) prevádzkovaných Poskytovateľom (pozri 1.5.1) v zmysle tejto certifikačnej politiky môže byť tretími stranami oznámená Poskytovateľovi na kontaktné údaje uvedené v časti 1.5.1 resp. 1.5.2 podľa uváženia oznamovateľa (telefonicky, e-mailom, poštou ap.). Oznamovateľ si môže zvoliť aj akýkoľvek iným spôsob, ktorý uzná za vhodný pre takéto oznámenie.

4.9.13 Okolnosti pozastavenia platnosti certifikátu

Poskytovateľ takúto službu neposkytuje.

4.9.14 Kto môže žiadať o pozastavenie 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

CRL musí byť dostupný na webovom sídle Poskytovateľa (pozri časť 1) a musí byť prístupný prostredníctvom HTTP protokolu na porte 80.

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

4.10.2 Dostupnosť služieb

Distribučné body, na ktorých sú publikované CRL musia byť k dispozícii v režime 24/7/365.

Služba OCSP musí byť dostupná v režime 24/7/365.

4.10.3 Doplnkové funkcie

Žiadne ustanovenia.

4.11 Ukončenie poskytovanie služieb

Poskytovanie služieb Držiteľovi certifikátu zo strany Poskytovateľa bude ukončené skončením platnosti zmluvy, na základe ktorej bol certifikát vydaný.

Zmluva môže byť zrušená z oboch strán na základe dohody aj pred ukončením jej platnosti. Zrušenie zmluvy musí mať za následok okamžité zrušenie certifikátu, ktorý bol na základe danej zmluvy vydaný.

4.12 Uchovávanie a obnova kľúčov

4.12.1 Politika a postupy uchovávania a obnovy kľúčov

Poskytovateľ neposkytuje svojim Držiteľom žiadnu službu uchovávania resp. obnovy súkromných kľúčov.

4.12.2 Politika a postupy ochrany „session key“

Žiadne ustanovenia.

5. Fyzické, personálne a prevádzkové bezpečnostné opatrenia

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

Bezpečnostné opatrenia musia byť k dispozícii všetkým pracovníkom, ktorých sa týkajú.

Poskytovateľ musí:

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

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

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

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

5.1 Opatrenie týkajúce sa fyzickej bezpečnosti

5.1.1 Priestory

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

5.1.2 Fyzický prístup

Mechanizmy riadenia prístupu do chránených priestorov Poskytovateľa t. j. do priestorov zóny s najvyššou bezpečnosťou musí byť zabezpečený tak, že tieto 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

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

5.1.5 Ochrana pred ohňom

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

5.1.6 Úložisko médií

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

5.1.7 Nakladanie s odpadom

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

5.1.8 Zálohovanie off-site

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

5.2 Procedurálne bezpečnostné opatrenia

5.2.1 Dôveryhodné role

V rámci CA musia byť definované dôveryhodné role zodpovedné za jednotlivé aspekty poskytovaných dôveryhodných služieb ako napr. systémový administrátor, bezpečnostný manažér, interný audítor, manažér politík ap., ktoré formujú základ dôvery v celú PKI.

Zároveň musia byť definované zodpovednosti jednotlivých rolí.

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

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

5.2.2 Počet osôb v jednotlivých rolách

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

5.2.3 Identifikácia a autentizácia pre každú rolu

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

5.2.4 Role vyžadujúce oddelenie zodpovedností

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

5.3 Personálne bezpečnostné opatrenia

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

5.3.1 Požiadavky na kvalifikáciu, skúsenosti a previerky

Pracovníci v dôveryhodných roliach musia spĺňať kvalifikačné požiadavky, požiadavky na odbornú prax a musia mať bezpečnostné previerky stanovenej úrovne resp. musia byť v procese žiadania o bezpečnostnú previerku. Požiadavky na jednotlivé role sú popísané v samostatných listoch používaných pri nábore nových pracovníkov.

Osoby v manažérskych funkciách musia:

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

5.3.2 Požiadavky na previerky

Pracovník môže byť zaradený do dôveryhodnej roly Poskytovateľa len v prípade, že má bezpečnostnú previerku stanovenej úrovne t. j. minimálne na stupeň utajenia „Dôverné“ resp. je v procese žiadania o takúto previerku.

5.3.3 Požiadavky na školenia

Pre niektoré dôveryhodné role Poskytovateľa môžu byť špecifikované niektoré špeciálne požiadavky na školenia, ktoré by mali absolvovať pred zaradením prípadne v priebehu zaradenia. Témy majú obsahovať fungovanie softvéru

a hardvéru CMA, prevádzkové a bezpečnostné procedúry, ustanovenia tejto CP, CPS ap.

5.3.4 Požiadavky na frekvenciu obnovy školení

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

5.3.5 Rotácia rolí

Poskytovateľ nepraktizuje rotáciu jednotlivých rolí.

5.3.6 Postihy za neoprávnenú činnosť

Zlyhanie akéhokoľvek zamestnanca Poskytovateľa, 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.

5.3.7 Požiadavky na externých dodávateľov

V prípade, že by nezávislí dodávatelia boli priradení na vykonávanie dôveryhodných rolí, musia podliehať povinnostiam a špecifickým požiadavkám na tieto roly v zmysle ustanovení časti 5.3 a rovnako podliehajú sankciám uvedeným v časti 5.3.6.

5.3.8 Dokumentácia dodávané pre personál

Pracovníci v dôveryhodných rolách musia mať k dispozícii dokumenty potrebné pre výkon funkcie, na ktorú sa sú priradení, vrátane kópie tejto CP resp. CPS a všetky technické a prevádzkovej dokumentácie potrebné k zachovaniu integrity operácií Poskytovateľa.

5.4 Postupu získavania auditných záznamov

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

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

5.4.1 Typy zaznamenávaných udalosti

Poskytovateľ musí zaznamenávať a vyhodnocovať nasledovné dôležité udalosti:

- Udalosti týkajúce sa generovania a životného cyklu kľúčov vydávajúcich CA Poskytovateľa:
  - generovanie, zálohovanie, obnova, archivácia a likvidácia
  - žiadosť o vydanie, obnovu a zmenu kľúčov a ich zrušenie
  - schválenie a zamietnutie žiadosti na vydanie
  - vytváranie CRL

  - podpisovania OCSP odpovedí v zmysle požiadaviek BR [3] odsek 4.9 a 4.10
  - uvedenie nového profilu certifikátu a ukončenie používania existujúceho profilu
- Udalosti týkajúce sa životného cyklu certifikátov pre koncových používateľov:
  - žiadosť o vydanie certifikátu, jeho obnovu, zmenu kľúčov a ich rušenie
  - všetky aktivity týkajúce sa overovania stanovené v BR [3] a CPS CA Disig
  - schválenie a odmietnutie žiadosti o vydanie
  - vydanie certifikátu
  - vytvorenie CRL
  - podpisovania OCSP odpovedí v zmysle požiadaviek BR [3] odsek 4.9 a 4.10
- Udalosti týkajúce sa bezpečnosti:
  - úspešné a neúspešné prístupy do systému PKI
  - vykonané systémové bezpečnostné akcie v systéme PKI
  - zmeny bezpečnostných profilov
  - inštalácia, aktualizácia a odstránenie softvéru CA
  - havárie systému, poruchy HW a iné anomálie
  - aktivity na firewaloch a smerovačoch
  - vstupy a výstupy do priestorov umiestnenia CA

Záznam o udalosti musí obsahovať minimálne tieto informácie: dátum a čas udalosti, identitu osoby, ktorá záznam vykonala a popis udalosti.

5.4.2 Frekvencia spracovávania auditných záznamov

Žiadne ustanovenia.

5.4.3 Doba uchovávanie auditných záznamov

Poskytovateľ musí uchovávať auditné záznamy minimálne počas 2 rokov u:

- udalosti týkajúce sa generovania a životného cyklu kľúčov vydávajúcich CA Poskytovateľa v zmysle odseku 5.4.1, a to po výskyte niektorej z týchto udalosti, podľa toho, ktorá nastane neskoršie:
  - likvidácia súkromného kľúča CA,
  - zrušení alebo exspirácii posledného certifikátu v súbore certifikátov, ktoré majú rozšírenie X.509v3 basicConstraints s cA pole nastavené na hodnotu true a ktoré zdieľajú spoločný verejný kľúč zodpovedajúci súkromnému kľúču CA.
- udalostí správy životného cyklu certifikátu vydanému koncovému užívateľovi (ako je uvedené v časti 5.4.1 od skončenia jeho platnosti,
- akejkoľvek bezpečnostnej udalosti (ako je uvedené v časti 5.4.1), po tom, ako k udalosti došlo.

5.4.4 Ochrana auditných záznamov

Žiadne ustanovenia.

5.4.5 Postupy zálohovania auditných logov

Žiadne ustanovenia.

5.4.6 Systém zálohovania logov

Žiadne ustanovenia.

5.4.7 Notifikácia subjektu iniciujúceho log záznam

Žiadne ustanovenia.

5.4.8 Posudzovanie zraniteľností

Pozri 5.4.2.

5.5 Uchovávanie záznamov

5.5.1 Typy archivovaných záznamov

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

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.).

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

Prezeranie záznamov sa umožní jednotlivým zložkám Poskytovateľa v rozsahu týkajúcom sa nimi vykonávaných činností, v celom rozsahu PMA a osobám vykonávajúcim audit zhody.

5.5.2 Doba uchovávania záznamov

Poskytovateľ je povinný uchovávať zmluvu s držiteľom, resp. objednávateľom a potvrdenie o vydaní certifikátu podľa tejto zmluvy najmenej 7 rokov od skončenia platnosti certifikátu vydaného podľa tejto zmluvy.

5.5.3 Ochrana archívnych záznamov

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

5.5.4 Zálohovanie archívnych záznamov

Žiadne ustanovenia.

5.5.5 Požiadavky na pridávanie časových pečiatok k záznamom

Žiadne ustanovenia.

5.5.6 Archivačný systém

Žiadne ustanovenia.

5.5.7 Postup získania a overenia archívnych informácií

Žiadne ustanovenia

5.6 Zmena kľúčov CA

Poskytovateľ musí využívať svoje podpisové (súkromný) kľúče iba účel, na ktorý sú určené. Súkromné kľúče podriadených CA sa môžu využívať len pri podpisovaní certifikátov pre koncových klientov, a to len na účel, ku ktorému sú určené, prípadne pri podpisovaní certifikátov vydávaných pre technologické účely (časová pečiatka, OSCP responder ap.). Súkromný kľúče koreňovej CA sa môže využívať len pri podpisovaní certifikátov pre podriadené CA resp. technologických certifikátov (OCSP responder).

Po vytvorení nového certifikátu Poskytovateľa (koreňová CA, podriadená CA) sa tento musí zverejniť na webovom sídle Poskytovateľa.

5.7 Obnova po kompromitácia alebo havárii

5.7.1 Postupy riešenia incidentov a kompromitácie

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

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

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

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

5.7.2 Poškodenie hardvéru, softvéru alebo údajov

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

5.7.3 Postupy pri kompromitácii kľúča CA

V prípade kompromitácie súkromného kľúča CA musí mať Poskytovateľ k dispozícii postupy na obnovu bezpečného prostredia, postupy distribúcie verejného kľúča koncovým používateľom a akým spôsobom budú vydávané nové certifikáty jednotlivý koncovým používateľom.

5.7.4 Zachovanie kontinuity činnosti po havárii

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

5.8 Ukončenie činnosti CA resp. RA

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

Ešte pred ukončením poskytovania služieb musí Poskytovateľ:

- Vhodným spôsobom, minimálne 6 mesiacov vopred, oznámiť informácie o plánovanom ukončení svojej činnosti orgánu dohľadu, Držiteľom všetkých ním vydaných platných certifikátov, Spoliehajúcim sa stranám a verejnosti. Toto oznámenie sa musí vykonať prostredníctvom webového sídla Poskytovateľa, elektronickej pošty, obyčajnej pošty, registračných autorít, prípadne elektronických médií a tlače.
- Ukončiť všetky prípadné mandátne zmluvy, splnomocnenia a pod., na základe ktorých mohli iné právnické osoby konať v mene Poskytovateľa.
- Uzavrieť zmluvu s inou CA, ktorá by zabezpečila kontinuitu v poskytovaní dôveryhodných služieb, ak je to možné.
- Podľa pokynov PMA sústrediť a pripraviť na archiváciu všetky dokumenty spojené s poskytovanými dôveryhodnými službami.
- vykonať kontrolu dodržania predpisov o ochrane osobných údajov t. j. Nariadenie Európskeho Parlamentu a Rady (EÚ) 2016/679 o ochrane fyzických osôb pri spracúvaní osobných údajov a o voľnom pohybe takýchto údajov a zákon č. 18/2018 Z. z. o ochrane osobných údajov (ďalej len „Predpisy o ochrane osobných údajov“) [12]
- Vyradiť z používania všetky súkromné kľúče, vrátane všetkých ich kópií, takým spôsobom, že už nemôžu byť žiadnym spôsobom obnovené.

Po ukončení svojej činnosti Poskytovateľ nevydá žiadny certifikát a zabezpečí preukázateľné znemožnenie opätovného využitia súkromných kľúčov Poskytovateľa.

Pred ukončením svojej činnosti každá RA poskytne archivované dáta zložke Poskytovateľa podľa pokynu PMA.

Poskytovateľ musí mať riešenie na pokrytie všetkých nákladov spojených so splnením minimálnych požiadaviek pri ukončení činnosti v prípade bankrotu

alebo inej príčiny, kedy nebude schopná pokryť náklady vlastnými prostriedkami, a to v súlade s platnou legislatívou o bankrote.

6. Technické bezpečnostné opatrenia

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

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

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

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

Publikačné aplikácie musia zabezpečiť kontrolu prístupu pred pokusmi o pridanie alebo zmazanie certifikát alebo modifikovaním iných združených údajov.

Aplikácie súvisiace s udávaním stavu zrušenia musia zabezpečiť kontrolu prístupu pred pokusmi o modifikovanie informácií o stave zrušenia.

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

6.1 Generovanie a inštalácia páru kľúčov

6.1.1 Generovanie a inštalácia páru kľúčov pre jednotlivé subjekty

6.1.1.1 Vydavateľ certifikátov

Generovanie a inštalácia páru kľúčov Poskytovateľa sa musí vykonávať štandardizovaným spôsobom, ktorý je podrobne popísaný v dokumentácii Poskytovateľa. Spôsob generovania musí zabezpečiť dostatočnú dôveru v postup generovania a celý proces musí byť písomne zaznamenaný. Generovanie kľúčov musia zabezpečiť oprávnené osoby Poskytovateľa zaradení v rolách, ktoré majú oprávnenie na účasť na ceremóniu generovania kľúčov a žiadosti. Generovanie kľúčov musí byť vykonané v bezpečnom zariadení na uchovávanie kryptografických kľúčov.

6.1.1.2 Registračné autority

Generovanie kľúčových párov certifikátov pre registračné autority musí byť vykonávané pod kontrolou poverených zamestnancov Poskytovateľa a kľúče musia byť uložené v bezpečnom QSCD zariadení.

6.1.1.3 Koncoví používatelia

Pozri 4.1.

6.1.2 Doručenie súkromného kľúča Držiteľovi certifikátu

Vygenerovaný kľúčový pár obsahujúci súkromný kľúč pracovníka RA mu musí byť doručený bezpečným spôsobom.

Vygenerovaný kľúčový pár koncového Držiteľa certifikátu, ktorý je uložený v bezpečnom zariadení pre elektronický podpis musí byť odovzdaný osobne ihneď po vydaní certifikátu.

6.1.3 Doručenie verejného kľúča vydavateľovi certifikátu

Verejný kľúč musí byť počas vydávania doručený certifikačnej autorite bezpečne napr. on-line v TLS spojení prostredníctvom komunikácie autorizovanej registračnou autoritou.

6.1.4 Doručenie verejného kľúča CA spoliehajúcim sa stranám

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

6.1.5 Dĺžky kľúčov

CPS stanoví odporúčané dĺžky kľúčov resp. minimálne dĺžky kľúčov pre všetky typy entít a všetky používané algoritmy (napr. RSA).

6.1.6 Parametre a kvalita verejného kľúča

Parametre a kvalitu verejného kľúča Poskytovateľa (koreňové a podriadené CA) určuje PMA a kontrola kvality je kontrolovaná počas ceremónie generovania kľúčov. Poskytovateľ musí využívať na generovanie a uchovávanie kľúčov kryptografické hardvérové moduly spĺňajúce požiadavky FIPS 186-2, ktoré zabezpečujú náhodné generovanie RSA kľúčov veľkosti minimálne 2048 bit.

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

6.1.7 Použitie kľúčov

Certifikáty certifikačných autorít Poskytovateľa obsahujú rozšírenia, ktoré určujú k čomu môžu byť CA certifikáty použité.

6.2 Ochrana súkromného kľúča a technické opatrenia pre kryptografický modul

6.2.1 Štandardy a opatrenia pre kryptografický modul

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

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

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

HSM modul musí spĺňa ochranu pred odchytávaním elektromagnetického vyžarovania.

6.2.2 Opatrenia (K z N) pre manipuláciu so súkromným kľúčom

Pri operáciách so súkromnými kľúčmi Poskytovateľa (napr. generovanie, zálohovanie, likvidácia) musí byť vždy prítomný príslušný počet oprávnených osôb na princípe „K“ z „N“.

6.2.3 „Key escrow“ súkromného kľúča

Žiadne ustanovenia.

6.2.4 Zálohovanie súkromného kľúča

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

6.2.5 Archivácia súkromného kľúča

Žiadne ustanovenia

6.2.6 Prenos súkromných kľúčov z a do HSM modulu

Pozri časť 6.2.4

6.2.7 Uchovávanie súkromných kľúčov v HSM module

Súkromné kľúče podriadených CA, ktoré sú využívané na podpisovanie vydaných certifikátov pre koncových používateľov musia byť uchovávané v HSM module a modul môžu opustiť len v zašifrovanej podobe, ktorá neumožní ich obnovu bez prítomnosti príslušného počtu oprávnených osôb na princípe „K“ z „N“ Všetky HSM moduly Poskytovateľa musia byť prevádzkované v zabezpečených priestoroch s režimovým prístupom.

6.2.8 Spôsob aktivácie súkromných kľúčov

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

Pri aktivácií musí každá oprávnená osoba z potrebného počtu oprávnených osôb vložiť do HSM modulu svoju čipovú kartu a zadať k nej heslo.

Za ochranu súkromných kľúčov ich Držiteľmi, ktorým Poskytovateľ vydal certifikát na príslušný verejný kľúč, sú výhradne zodpovední ich Držitelia. Poskytovateľ musí

odporučiť všetkým Držiteľom, aby si chránili svoje súkromné kľúče používaním silného hesla, ktoré zabráni zneužitiu ich súkromného kľúča.

6.2.9 Spôsob deaktivácie súkromného kľúča

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

6.2.10 Spôsob zničenia súkromného kľúča

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

6.2.11 Charakteristika HSM modulu

Pozri časť 6.2.1.

6.3 Ďalšie aspekty manažmentu kľúčového páru

6.3.1 Archivácia verejných kľúčov

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

6.3.2 Dĺžka platnosti certifikátov a použiteľnosť kľúčového páru

Platnosť Poskytovateľom vydávaných certifikátov a použiteľnosť kľúčového páru nesmie prekročiť nasledovné:

Typ certifikátu	Platnosť (maximálne)
Koreňová CA	30 rokov
Podriadená CA	15 rokov
Certifikát pre koncového používateľa s výnimkou TLS certifikátu	5 rokov
TLS certifikát	maximálne 395 dní

6.4 Aktivačné údaje

6.4.1 Vytváranie a inštalácia aktivačných údajov

Aktivačné údaje sú údaje, ktoré sú nevyhnutné k tomu, aby bol umožnený prístup k súkromnému kľúču, ktorý je uložený buď v softvérovej podobe v súbore na počítači, v QSCD zariadení resp. v HSM module. Aktivačnú údaje môžu byť v podobe PIN, hesla alebo hesla rozdeleného na viacero častí na princípe K/N ap.

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

6.4.2 Ochrana aktivačných údajov

Za ochranu súkromných kľúčov Držiteľov sú zodpovední výhradne samotní Držitelia.

Pri vydávaní certifikátu musia byť Držitelia upozornení so strany Poskytovateľa o potrebe chrániť súkromný kľúč silným heslom, aby nemohlo dôjsť k jeho zneužitiu, počas celej doby jeho používania.

Kľúčový pár určený pre vydavateľa certifikátov:

- musí byť generovaný v bezpečnostnom module, ktorý spĺňa minimálne požiadavky štandardu FIPS 140-2 level 2,
- akákoľvek manipulácia so súkromným kľúčom môže byť umožnená len za princípu viacnásobnej kontroly, pričom minimálny počet potrebných osôb musí byť tri (3). Manipulácia sa týka obnovy kľúče do iného HSM modulu v prípade poškodenia modulu, v ktorom sú kľúče aktuálne uložené.

Ďalšie podrobnosti týkajúce sa súkromného kľúča certifikačnej autority Poskytovateľa sú uvedené v dokumente „Pravidlá práce s kryptografickými modulmi“.

6.4.3 Ostatné aspekty aktivačných údajov

Musí byť zabezpečené, aby sa asymetrické súkromné kľúče nikdy nedostali v nezašifrovanej forme mimo modul, kde sú uložené.

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

Počas zálohovania a prenosu musia byť kľúče zašifrované. Držiteľ kľúča zodpovedá za garanciu, že všetky kópie súkromných kľúčov sú chránené, vrátane ochrany všetkých pracovných staníc, na ktorých sa nachádza ľubovoľný z jeho súkromných kľúčov.

Pass-frázy, PINy, biometrické dáta alebo iné mechanizmy ekvivalentnej autentizačnej robustnosti sa musia použiť na ochranu prístupu k použitiu súkromného kľúča. Aktivačné dáta sa môžu Držiteľom distribuovať osobne alebo poštou, ale len oddelene od kryptografického modulu, ktorý aktivujú.

Ak sa aktivačné dáta zapíšu, musia byť zabezpečené na úrovni ochrany dát, na ochranu ktorých sa používa daný kryptografický modul a nesmú byť uložené spolu s ním.

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

Aktivačné dáta pre súkromné kľúče patriace k certifikátom potvrdzujúcim identitu organizácie majú byť známe len tým, ktorí sú v organizácii autorizovaní na použitie daných súkromných kľúčov.

6.5 Riadenie bezpečnosti počítačov

6.5.1 Špecifické požiadavky na bezpečnosť počítačov

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

Poskytovateľ vydávajúci certifikáty musí spĺňať špecifické požiadavky na bezpečnosť informácií kladené na dôveryhodného poskytovateľa služieb, ktoré sú definované v štandarde ETSI EN 319411-1 " Electronic Signatures and Infrastructures (ESI); Policy and security requirements for Trust Service Providers issuing certificates; Part 1: General requirements“ [13]

Všetky systému musí byť pravidelne overované na prítomnosť škodlivého kódu a chránené proti spyware a vírusom.

6.5.2 Hodnotenie bezpečnosti informácií

Žiadne ustanovenia.

6.6 Opatrenia v životnom cykle

6.6.1 Opatrenia pri vývoji systémov

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

6.6.2 Opatrenia na riadenie bezpečnosti

Poskytovateľ musí využívať nástroje a postupy na zaistenie, že operačné systémy a sieťové pripojenia zodpovedajú nastavenej bezpečnosti.

Tieto nástroje a postupy by mali zahŕňať kontrolu integrita bezpečnostného softvéru, firmvéru a hardvéru, čo zaisťuje ich správnu funkciu.

6.6.3 Bezpečnostné opatrenia v životnom cykle

Žiadne ustanovenia.

6.7 Sieťové bezpečnostné opatrenia

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

6.8 Využívanie časovej pečiatky

Žiadne ustanovenie

7. Profily certifikátov a zoznamov zrušených certifikátov

7.1 Profily certifikátov

7.1.1 Verzia

Táto CP povoľuje len vydávanie certifikátov vyhovujúcich štandardu X.509 verzie 3.

7.1.1.1 Certifikát koreňovej CA Poskytovateľa

Algoritmy a dĺžky kľúčov uplatňované v koreňovom certifikáte Poskytovateľa:

Algoritmus podpisu (Signature Algorithm)
sha256RSA
Verejný kľúč
RSA, dĺžka 2 048 bitov resp. 4 096 bitov
Doba platnosti certifikátu CA
maximálne 30 rokov

Tabuľka č. 7: Obsah položiek v certifikáte koreňovej certifikačnej autority Poskytovateľa

Skratka názvu	OID	Názov	Hodnota
C	2.5.4.6	countryName	**SK**
L	2.5.4.7	localityName	**Bratislava**
	2.5.4.97	organizationIdentifier	Odkaz na identifikačný údaj právnickej osoby prevádzkujúcej CA[1)]
O	2.5.4.10	organizationName	**Disig a.s.**
CN	2.5.4.3	commonName	*v závislosti od typu CA* [2)]

[1)] Musí byť súčasťou certifikátu koreňovej CA Poskytovateľa, ktorého platnosť začína po 1.7.2016

[2)] Súčasťou CN musí byť obchodné meno certifikačnej autority t. j. CA Disig doplnené podľa potreby o rozlišovacie meno typu koreňovej CA Disig napr. Root R1, Root R2 ap.

Tabuľka č. 8: Použité rozšírenia (certificate extensions) v certifikáte koreňových CA Poskytovateľa

Rozšírenie / OID	Prítomnosť	Kritickosť
basicConstraints / 2.5.29.19	ÁNO	**ÁNO**
keyUsage / 2.5.29.15	ÁNO	**ÁNO**
subjectKeyIdentifier / 2.5.29.14	ÁNO	NIE

7.1.1.2 Podriadené certifikačné autority Poskytovateľa

Algoritmy a dĺžky kľúčov uplatňované v certifikátoch podriadených CA Poskytovateľa:

Algoritmus podpisu (Signature Algorithm)
sha256RSA
Verejný kľúč
RSA, dĺžka 2 048 bitov
Doba platnosti certifikátu CA
maximálne 15 rokov

Tabuľka č. 9: Obsah položiek v certifikáte podriadenej certifikačnej autority Poskytovateľa

Skratka názvu	OID	Názov	Hodnota
C	2.5.4.6	countryName	**SK**
L	2.5.4.7	localityName	**Bratislava**
	2.5.4.97	organizationIdentifier	Odkaz na identifikačný údaj právnickej osoby prevádzkujúcej CA[1)]
O	2.5.4.10	organizationName	**Disig a.s.**
CN	2.5.4.3	commonName	*v závislosti od typu CA*[2)]

[1)] Musí byť súčasťou certifikátu podriadenej CA Poskytovateľa, ktorého platnosť začína po 1.7.2016

[2)] Súčasťou CN musí byť obchodné meno certifikačnej autority t. j. CA Disig doplnené podľa potreby o rozlišovacie meno typu podriadenej CA Disig napr. R2I2 Certification Service, R2I3 Certification Service ap.

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

Rozšírenie / OID	Prítomnosť	Kritickosť
authorityInfoAccess / 1.3.6.1.5.5.7.1.1	ÁNO	NIE
Authority Key Identifier / 2.5.29.35	ÁNO	NIE
basicConstraints / 2.5.29.19	ÁNO	**ÁNO**
keyUsage / 2.5.29.15	ÁNO	**ÁNO**
subjectKeyIdentifier / 2.5.29.14	ÁNO	NIE
crlDistributionPoints / 2.5.29.31	ÁNO	NIE
certificatePolicies / 2.5.29.32	ÁNO	NIE
subjectAltName / 2.5.29.17	ÁNO	NIE

7.1.1.3 Certifikáty vydávané Poskytovateľom pre koncových používateľov

Podrobnosti o obsahu rozlišovacieho mena (DN) jednotlivých typov certifikátov vydávaných v zmysle tejto CP sú uvedené v časti 3.1.4

7.1.2 Rozšírenia v certifikátoch

Tabuľka č. 11 obsahuje použité rozšírenia nachádzajúce sa vo všetkých typoch vydávaných certifikátov

Tabuľka č. 11: Základné rozšírenia (certificate extensions) vo vydávaných certifikátoch

Názov rozšírenia	ASN.1 názov a OID / Popis	Prítomnosť	Kritickosť
Subject Key Identifier	{id-ce-subjectKeyIdentifier} {2.5.29.14} Identifikátor verejného kľúča Držiteľa certifikátu.	ÁNO	NIE
Authority Key Identifier	{id-ce-authorityKeyIdentifier} {2.5.29.35} Identifikátor verejného kľúča certifikačnej autority CA, ktorá vydala tento certifikát.	ÁNO	NIE
Key Usage	{id-ce-keyUsage} {2.5.29.15} Definuje účel použitia súkromného kľúča, ktorého verejný kľúč je súčasťou tohto certifikátu.	ÁNO	NIE
CRL Distribution Points	{id-ce-CRLDistributionPoints} {2.5.29.31} Určuje, akým spôsobom a odkiaľ je možné získať CRL.	ÁNO	NIE
Extended Key Usage	{id-ce-extKeyUsage}	ÁNO	NIE

	[2.5.29.37] Rozširuje účel použitia súkromného kľúča definovaný v rozšírení „Key Usage“		
Certificate Policies	{id-ce-certificatePolicies} {2.5.29.32} Identifikuje certifikačné politiky, pod ktorými bol certifikát vydaný.	ÁNO	NIE
subjectAltName	id-ce-subjectAltName [2.5.29.17] Obsahuje jedno alebo viac alternatívnych mien entity, ktorú CA zviaže s verejným kľúčom certifikátu.	ÁNO	NIE
AuthorityInfoAccess	{id-pe-authorityInfoAccess} {1.3.6.1.5.5.7.1.1} Určuje (http:// … p7c, certifikát alebo aj ldap://...) adresu na získanie certifikátov vydaných pre vydavateľa tohto certifikátu a adresu na OCSP.	ÁNO	NIE

7.1.3 Identifikátory použitých algoritmov

Algoritmus podpisu vydávaných certifikátov (Signature Algorithm)
sha256RSA
OID: 1.2.840.113549.1.1.11

7.1.4 Formy mien

Požiadavky na formy mien pre jednotlivé typy certifikátov sú uvedené v časti 3.1.4.

V certifikáte vydávajúcej CA Poskytovateľa, ktorej certifikačná cesta obsahuje koreňový certifikát distribuovaný ako dôveryhodný bod (trust anchor) v široko dostupnom aplikačnom softvéri, sa vždy uvádza názov „CA Disig“.

Vo všetkých certifikátoch vyhotovovaných pre koncových používateľov v zmysle tejto CP, s výnimkou TLS certifikátov, sú uplatňované nasledovné algoritmy a dĺžky kľúčov:

Algoritmus podpisu (Signature Algorithm)
sha256RSA

Verejný kľúč
RSA, dĺžka je minimálne 2 048 bitov

Doba platnosti certifikátu pre fyzickú resp. právnickú osobu
Maximálne 60 mesiacov t. j. 5 rokov (5*365 dní)

U TLS certifikátov vyhotovovaných v zmysle tejto CP sú uplatňované nasledovné algoritmy a dĺžky kľúčov:

Algoritmus podpisu (Signature Algorithm)
sha256RSA
Verejný kľúč
RSA, dĺžka je minimálne 2 048 bitov
Doba platnosti TLS certifikátu
Maximálne 395 dní

7.1.5 Obmedzenia týkajúce sa mien

Žiadne ustanovenia.

7.1.6 Identifikátor certifikačnej politiky

Pozri časť 1.2.

7.1.7 Použitie rozšírení na obmedzenie politiky

Toto rozšírenie nie je používané.

7.1.8 Syntax a sémantika politiky

Každý certifikát vyhotovený v zmysle tejto CP musí obsahovať jej identifikátor v podobe OID (pozri 1.2) v rozšírení id-ce-certificatePolicies (2.5.29.32).

Každý TLS certifikát naviac musí obsahovať identifikátor v podobe OID (2.23.140.1.2.2), že certifikát je vydávaný ako TLS certifikát, kde bola overená organizácia (právnická osoba resp. fyzická osoba), ktorá má pod kontrolou presne stanovené meno domény (FQDN) v ňom uvedené.

Každý certifikát pre elektronickú pečať musí mať v položke NoticeText (OID 1.3.6.1.5.5.7.2.2) uvedený text, že ide o certifikát pre elektronickú pečať v zmysle Nariadenia eIDAS [4].

7.1.9 Sémantika spracovania kritických certifikačných politík

Žiadne ustanovenia.

7.1.10 Ostatné ustanovenia

Štruktúra (profil) ostatných certifikátov vydávaných Poskytovateľom, ktoré sú určené výhradne pre interné používanie u zmluvných partnerov je detailne popísaná v príslušných CPS, vrátane používaných rozšírení certifikátov (Certificate Extensions).

Štruktúra certifikátov vydávaných Poskytovateľom sa môže meniť len na základe rozhodnutia PMA, v prípade osobných certifikátov vydávaných pre účely zmluvných partnerov na základe dohody so zmluvným partnerom.

Použité základné rozšírenia (Certificate Extensions) u jednotlivých typov certifikátov môžu byť rozširované podľa aktuálnej potreby na základe rozhodnutia

PMA. Takéto rozšírenie sa nepovažuje za zmenu profilu certifikátov tak ako sú definované v ods. 7.1.

Podľa potreby Poskytovateľa môžu byť všetky vydávané typy certifikátov rozšírené aj o ďalšie položky v zmysle RFC 5280 časť 4.1.2.6.

7.2 Profil zoznamu zrušených certifikátov (CRL)

7.2.1 Verzia

Všetky CRL vydávané Poskytovateľom musia byť CRL verzie 2.

CRL musia byť vydávané a podpisované tou istou CA Poskytovateľa ako certifikáty, ktoré sú v CRL uvedené.

Vydávané CRL musia byť v súlade s RFC 5280 „Internet X.509 Public Key Infrastructure Certificate and CRL Profile“ [14]

7.2.2 Použité rozšírenia (CRL extensions) v CRL vydávanom Poskytovateľom

Tabuľka č. 12 obsahuje zoznam rozšírení uvádzaných v CRL vydávaných certifikačnými autoritami Poskytovateľa, pre ktoré platí táto CP spolu s informáciou o povinnosti uvádzania ich kritickosti.

Tabuľka č. 12: Rozšírenia vydávaného CRL

Názov rozšírenia	Vyžadované	Kritickosť
Authority Key Identifier (OID: 2.5.29.35)	ÁNO	NIE
CRL Number (OID: 2.5.29.20)	ÁNO	NIE
ReasonCode* (OID 2.5.29.21)	ÁNO	NIE

* Uvádza sa v CRL len v prípade zrušenia TLS certifikátu z týchto dôvodov: keyCompromise (RFC 5280 CRLReason #1); privilegeWithdrawn (RFC 5280 CRLReason #9); cessationOfOperation (RFC 5280 CRLReason #5); affiliationChanged (RFC 5280 CRLReason #3), alebo superseded (RFC 5280 CRLReason #4).

7.3 Profil OCSP

7.3.1 Verzia

Poskytovateľ musí vydávať OCSP odpovede v zmysle RFC 6960 „X.509 Internet Public Key Infrastructure Online Certificate Status Protocol – OCSP“ [15]. OCSP odpovede pre jednotlivé certifikačné autority vydávajúce verejne dôveryhodné certifikáty musia byť vydávané samostatnými OCSP respondermi, ktorých podpisové certifikáty budú podpísané zodpovedajúcimi vydávajúcimi certifikačnými autoritami Poskytovateľa a musia obsahovať rozšírenie na použitie kľúča OCSP Signing (1.3.6.1.5.5.7.3.9).

V zmysle požiadaviek definovaných v dokumente [3], ak OCSP responder dostane požiadavku na certifikát, ktorý certifikačná autorita v mene, ktorej odpovedá, nevydala, nesmie odpovedať statusom „good“.

7.3.2 OCSP rozšírenia

Tabuľka č. 13 obsahuje možné rozšírenia v OCSP odpovedi OCSP responderov Poskytovateľa, povinnosť ich uvádzania a ich kritickosť.

Tabuľka č. 13: Rozšírenia v OCSP odpovedi

Názov rozšírenia	Vyžadované	Kritickosť
id-pkix-ocsp-nonce (OID: 1.3.6.1.5.5.7.48.1.2)	NIE	NIE
Online Certificate Status Protocol (OCSP) Stapling TLS extension SignedCertificateTimestampList* (OID 1.3.6.1.4.1.11129.2.4.5)	ÁNO	NIE

* - Toto rozšírenie je vložené len v OSCP odpovediach, ktoré boli vydané OCSP responderom poskytujúcim odpovede v mene CA Disig R2I2 Certification Service

8. Audit zhody

Účelom auditu o zhode má byť záruka, že Poskytovateľ má vyhovujúci systém práce, ktorý garantuje kvalitu dôveryhodných služieb, ktoré Poskytovateľ poskytuje a taktiež garantuje, že koná v súlade so všetkými požiadavkami tejto CP, svojho CPS, požiadaviek Nariadenia eIDAS [4] a CA/Browser fórum [3]. Všetky aspekty prevádzky CA vzťahujúce sa k tejto CP majú byť predmetom auditov zhody.

8.1 Frekvencia auditu zhody pre danú entitu

Všetky certifikačné autority, ktoré sú definované v časti 1.4.1 musia byť auditované minimálne jedenkrát ročne, pričom audity musia byť na seba naviazané tak, že auditované obdobie nepresiahne 1 kalendárny rok.

8.2 Identita audítora a kvalifikačné požiadavky na neho

Audítor musí byť kompetentný v oblasti auditov o zhode a musí byť dôkladne oboznámený s CP a CPS CMA, u ktorej vykonáva audit a musí spĺňať kvalifikačné požiadavky popísané v dokumente [3].

8.3 Vzťah audítora k auditovanému subjektu

Pozri časť 8.2.

8.4 Témy pokryté audiom

Poskytovateľ bude auditovaný v zmysle národnej schémy, ktorá posudzuje zhodu s požiadavkami najnovších verzií ETSI EN 319 411-1, pričom musí zahŕňať aj normatívne odkazy z ETSI EN 319 401.

Audit musí byť vykonaný kvalifikovaným audítorom v zmysle odseku 8.2.

8.5 Akcie vykonané na odstránenie nedostatkov

Keď audítor zistí rozpor medzi prevádzkou CMA a ustanoveniami jej CPS, musia sa uskutočniť nasledujúce akcie:

- audítor zaznamená rozpor,
- audítor upovedomí o rozpore subjekty definované v časti 8.6,
- CA navrhne PMA zodpovedajúce opatrenie na nápravu vrátane očakávaného času potrebného na jeho realizáciu.

PMA určí vhodné opatrenie na nápravu a to prípadne až po zrušenie certifikátu CA.

8.6 Zaobchádzanie s výsledkami auditu

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

V správa z auditu musí byť vyslovene uvedené, že sa vzťahuje na príslušné systémy a postupy používané pri vydávaní všetkých certifikátov, ktoré uplatňujú jeden alebo viac identifikátorov politík uvedených v časti 1.1. Správa z auditu musí byť verejne dostupná. Poskytovateľ nemusí verejne sprístupnil akékoľvek všeobecné zistenia z auditu, ktoré nemajú vplyv na celkové stanovisko audítora. Poskytovateľ musí verejne sprístupniť svoju správu o audite najneskôr tri mesiace po ukončení auditu. V prípade oneskorenia dlhšieho ako tri mesiace, a ak o to požiada dodávateľ aplikačného softvéru, musí Poskytovateľ poskytnúť vysvetľujúci list k tejto skutočnosti, podpísaný kvalifikovaným audítorom.

Poskytovateľ je povinný predložiť výslednú správu o posúdení zhody všetkým tvorcom aplikačného softvéru, ktorý distribuujú jeho koreňové certifikáty ako dôveryhodný bod v zmysle ich podmienok.

8.7 Interný audit

Počas obdobia, v ktorom CA vydáva certifikáty, musí Poskytovateľ monitorovať dodržiavanie svojej CP a CPS a požiadaviek uvedených v dokumente [3] a kontrolovať poskytované služby vykonávaním interných auditov minimálne na štvrťročnej báze na náhodne vybranej vzorke vydaných certifikátov v počte vyššom ako jeden a najviac v počte tri percentá z vydaných certifikátov v období od predchádzajúceho interného auditu.

9. Iné obchodné a právne záležitosti

9.1 Poplatky

Povinnosťou Poskytovateľa je vhodným spôsobom zverejniť platný cenník svojich dôveryhodných služieb resp. informáciu, za akých zmluvných podmienok je možné tieto služby objednať.

9.1.1 Poplatky za vydanie certifikátu

Poplatky za certifikáty sa musia platiť na základe podmienok dohodnutých so Zákazníkom/Držiteľom.

Poskytovateľ musí zverejniť platný cenník svojich služieb prostredníctvom svojho webového sídla spoločnosti (pozri časť 1).

V prípade poskytovania svojich služieb len zmluvným partnerom cenník služieb nemusí byť zverejňovaný.

9.1.2 Poplatok za prístup k certifikátu

Pozri 9.1.1

9.1.3 Poplatky za služby vydávania CRL a OCSP

Pozri 9.1.1

9.1.4 Poplatky za ostatné služby

Pozri 9.1.1

9.1.5 Vrátenie platby

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

9.2 Finančná zodpovednosť

Poskytovateľ musí mať dostatočné zdroje na výkon ním poskytovaných dôveryhodných služieb, aby zostal solventným a bol schopný zaplatiť náhradu škody v prípade súdneho rozhodnutia resp. vyrovnania z nárokov vyplývajúcich z poskytovania týchto služieb.

9.2.1 Poistenie

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

Poskytovateľ musí zodpovedať za škody vzniknuté používaním ním vydaného certifikátu v zmysle platnej legislatívy (napr. Obchodný zákonník, Občiansky zákonník). Predpokladom pritom je, že boli dodržané príslušné ustanovenia tejto CP.

Zodpovednosť za škodu a z nej vyplývajúce plnenie, je možné uznať len za predpokladu, že

- Držiteľ neporušil svoje povinnosti (hlavne ochranu svojho súkromného kľúča),
- každý, kto sa v danom prípade spoliehal na certifikát vydaný Poskytovateľom, urobil všetko, aby prípadnej škode zabránil, hlavne tým, že si overil aktuálny stav predmetného certifikátu t. j. či daný certifikát nebol v rozhodujúcom čase, keď sa na neho spoliehal zrušený.

Poskytovateľ nemá žiadnu finančnú zodpovednosť za prípadné škody, ktoré by vznikli Držiteľovi certifikátu alebo strane spoliehajúcej sa na certifikát v súvislosti s používaním certifikátu s konkrétnou aplikáciou resp. hardvérom alebo v súvislosti s tým, že certifikát nie je možné používať s konkrétnou aplikáciou resp. hardvérom.

Akákoľvek žiadosť o náhradu škody musí byť podaná písomne.

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

Dôvernými informáciami podliehajúcimi zodpovedajúcej ochrane musia byť:

- súkromné kľúče Poskytovateľa používané na podpisovanie vydávaných certifikátov pre podriadené CA,
- súkromné kľúče podriadených CA používané na podpisovanie vydávaných certifikátov pre koncových používateľov
- súkromné kľúče poskytovaných služieb TSA resp. OCSP služieb
- súkromné kľúče patriace výkonným zložkám Poskytovateľa (pracovníci RA),
- infraštruktúra (napr. dokumenty, procedúry, postupy, súbory, skripty, heslá a pod.) slúžiaca na zabezpečenie prevádzky CA Poskytovateľa, vrátane všetkých jej RA,
- osobné údaje Držiteľov certifikátov podliehajúce ochrane v zmysle Predpisov o ochrane osobných údajov. [12]

Certifikát môže obsahovať len také informácie, ktoré sú dôležité a nevyhnutné na vykonávanie bezpečnej komunikácie pomocou certifikátu.

Za účelom náležitej správy certifikátov CMA môže požadovať, aby sa pri správe certifikátov Poskytovateľom používali aj informácie, ktoré nie sú uvedené v certifikátoch (napr. identifikačné čísla dokladov, adresy, telefónne čísla).

Ľubovoľná takáto informácia musí byť explicitne definovaná v CPS.

So všetkými informáciami uloženými u Poskytovateľa, ktoré nie sú v úložisku, sa musí zaobchádzať ako s citlivými informáciami a prístup k nim musí byť obmedzený len na osoby, ktoré tieto informácie nevyhnutne potrebujú na výkon svojich oficiálnych povinností.

Všetky informácie, ktoré sú uvedené v certifikáte a teda sú zverejňované prostredníctvom úložiska, nie sú klasifikované ako dôverné a považujú sa za verejné.

Zoznam zrušených certifikátov (CRL) nie je považovaný za dôverný.

9.3.2 Nechránené informácie

Poskytovateľ nesmie zverejniť informácie týkajúce sa Zákazníka alebo Držiteľa certifikátu žiadnej tretej strane, pokiaľ to nie je povolené touto CP, požadované zákonom alebo príkazom kompetentného súdu resp. je to predmetom zmluvy medzi Poskytovateľom a jeho Zákazníkom. Každá požiadavka na uvoľnenie informácií musí byť autentizovaná a zadokumentovaná.

Poskytovateľ musí s osobnými údajmi Zákazníka zaobchádzať v súlade s platnými zákonmi a nesmie ich poskytnúť žiadnej tretej strane s výnimkou subjektov, ktoré zo zákona majú právo kontrolovať činnosť Poskytovateľa a kompetentných štátnych orgánov ako sú polícia, súdy, prokuratúra.

9.3.3 Zodpovednosť za ochranu dôverných informácií

Účastníci, ktorí získajú dôverné informácie sú zodpovední za ich ochranu pred prezradením a musia sa zdržať ich poskytnutia tretej strane.

9.4 Ochrana osobných údajov

9.4.1 Politika ochrany osobných údajov

Poskytovateľ musí spracovávať osobné údaje Zákazníkov/Držiteľov certifikátov, resp. nimi splnomocnených osôb v súlade s požiadavkami Predpisov o ochrane osobných údajov [12].

9.4.2 Informácie považované za osobné údaje

Poskytovateľ musí mať definovaný rozsah osobných údajov, ktorý spracováva pri poskytovaní kvalifikovaných dôveryhodných služieb.

9.4.3 Informácie, ktoré nie sú považované za osobné údaje

Poskytovateľ môže v súlade s Predpismi na ochranu osobných údajov [12] definovať typy informácií, ktorý spracováva pri poskytovaní dôveryhodných služieb a nie sú považované za osobné údaje.

9.4.4 Zodpovednosť za ochranu osobných údajov

Účastníci, ktorí získajú osobné údaje sú zodpovední za ich ochranu pred prezradením a musia sa zdržať ich poskytnutia tretej strane.

9.4.5 Súhlas so spracovaním osobných údajov

Poskytovateľ je povinný pri plnení informačnej povinnosti voči dotknutým osobám a pri získavaní ich súhlasu so spracovaním osobných údajov postupovať v súlade s Predpismi na ochranu osobných údajov [12].

9.4.6 Zverejnenie na základe súdneho alebo správneho procesu

Poskytovateľ môže tieto údaje poskytovať aj tretím stranám, ak mu to ukladajú alebo umožňujú príslušné právne predpisy.

9.4.7 Ďalšie okolnosti zverejňovania informácií

Žiadne ustanovenia.

9.5 Práva duševného vlastníctva

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

Poskytovateľ je nositeľom výlučných práv k IS Poskytovateľa a k obsahu jeho webového sídla.

9.6 Vyhlásenie a záruky

Poskytovateľ prostredníctvom tejto CP, Všeobecných podmienok [6] a prípadne zmluvy o poskytovaní služby vydania certifikátu vyjadruje právne predpoklady používania vydaných certifikátov Zákazníkmi/Držiteľmi a spoliehajúcimi sa stranami.

9.6.1 Vyhlásenia a záruky Poskytovateľa

Pokiaľ ide o poskytované dôveryhodné služby Poskytovateľ neposkytuje žiadne vyhlásenia ani záruky s výnimkou prípadov uvedených v tejto CP a Všeobecných podmienkach [6] a v časti 9.6.1 dokumentu [3].

9.6.2 Vyhlásenia a záruky RA

Všetky externé registračné autority Poskytovateľa musia poskytovať dôveryhodné služby na základe zmluvného vzťahu s poskytovateľom a v súlade s touto CP.

Ďalej pozri ustanovenia v časti 9.6.

9.6.3 Vyhlásenie a záruky Držiteľa

Zákazník/Držiteľ certifikátu používajú dôveryhodné služby Poskytovateľa na vlastnú zodpovednosť a nesú všetky náklady na komunikačné prostriedky na diaľku alebo iných technické prostriedky potrebné na použitie týchto služieb (napr. na softvér potrebný na vyhotovovanie elektronického podpisu/pečate, na autentifikáciu webového sídla, na základe certifikátu vydaného Poskytovateľom). Zákazník/Držiteľ musí dodržiavať všetky ustanovenia tákajúce sa vyhlásení a záruk ako sú uvedené vo Všeobecných podmienkach [6].

9.6.4 Vyhlásenia a záruky spoliehajúcej sa strany

Spoliehajúce sa strany musia brať na vedomie, že je výhradne na ich slobodnom rozhodnutí, či sa rozhodnú dôverovať a spoľahnúť sa na certifikát vydaný Poskytovateľom a teda na informácie v ňom obsiahnuté. V prípade, rozhodnutia dôverovať certifikátom Poskytovateľa sú spoliehajúce sa strany povinné dodržať povinnosti popísané v 10. časti Všeobecných podmienok [6], v opačnom prípade sú výhradne zodpovedné za právne následky tým spôsobené.

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

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

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

a) porušenia povinností Zákazníkom/Držiteľom certifikátu alebo spoliehajúcou sa stranou uvedených v právnych predpisoch, zmluve, Všeobecných podmienkach alebo v politikách Poskytovateľa, vrátane povinnosti vynaložiť primeranú starostlivosť pri používaní certifikátov a pri spoliehaní sa na ne;

b) neposkytnutia potrebnej súčinnosti zo strany Zákazníka/Držiteľa certifikátu;

c) technickými vlastnosťami, konfiguráciou, nekompatibilitou, nevhodnosťou alebo inými vadami nimi použitých softvérových alebo hardvérových prostriedkov;

d) používania, resp. spoliehania sa na certifikát, ktorého platnosť uplynula alebo ktorý bol zrušený;

e) použitia certifikátu Zákazníkom/Držiteľom certifikátu v rozpore so zmluvou, Všeobecnými podmienkami alebo politikami Poskytovateľa;

f) že certifikát bol použitý v rozpore s jeho účelovým určením alebo obmedzeniami uvedenými v certifikáte, v týchto Všeobecných podmienkach resp. v politikách Poskytovateľa;

g) omeškania alebo nedoručenia požiadaviek na overenie statusu certifikátu Poskytovateľovi, z dôvodov, ktoré nie sú na strane Poskytovateľa (najmä

prípady nedostupnosti alebo preťaženosti siete internet alebo vady zariadenia alebo technického vybavenia používaného overovateľom);

h) neposkytnutia niektorej z dôveryhodných služieb alebo jej nedostupnosti v priebehu plánovanej údržby alebo reorganizácie oznámenej na webovom sídle Poskytovateľa;

i) pôsobenia vyššej moci;

Poskytovateľ nezodpovedá za škody, ktoré vznikli spoliehajúcej sa strane z dôvodu, že pri spoliehaní sa na certifikát a dôveryhodné služby Poskytovateľa, resp. na elektronický podpis alebo pečať vyhotovené na ich základe nepostupovala podľa 10. časti Všeobecných podmienok [6] a v zmysle tejto politiky.

9.9 Náhrada škody

Kto poruší svoju povinnosť alebo akýkoľvek záväzok, vyplývajúci z tejto CP, Zmluvy a Všeobecných podmienok je povinný nahradiť škodu tým spôsobenú druhej strane, okrem prípadov kde je vylúčená zodpovednosť daného subjektu za škody. Za škodu sa považuje skutočná škoda, ušlý zisk a náklady vzniknuté poškodenej strane v súvislosti so škodovou udalosťou.

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

9.10 Doba platnosti, ukončenie platnosti

9.10.1 Doba platnosti

Tato verzia CP platí odo dňa nadobudnutia jej platnosti t. j. 1 10. 2022 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 CP skončí dňom publikovania novej verzie s vyšším číslom ako je 5.7, prípadne ukončením činnosti poskytovania dôveryhodných služieb Poskytovateľom v čase jej platnosti.

9.10.3 Dôsledky ukončenia platnosti

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

9.11 Jednotlivé oznámenia a komunikácia s účastníkmi

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

9.12 Zmeny

9.12.1 Postup vykonávania zmien

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

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

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

Všetky schválené zmeny CP musia byť dané na vedomie subjektom, ktorých sa týkajú, v lehote jedného týždňa pred nadobudnutím ich účinnosti, a to prostredníctvom kanálov publikačnej a oznamovacej politiky (pozri 2).

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

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

9.12.2 Postup a periodicita oznamovania zmien

Poskytovateľ musí publikovať informácie týkajúce sa aktuálnej verzie CP prostredníctvom svojho webového sídla (pozri 1.5.2).

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

Aktuálna verzia CP musí byť k dispozícii na každej zmluvne viazanej RA Poskytovateľa minimálne v elektronickej forme. Interní zamestnanci musia byť rovnako informovaní o novej verzii tejto CP.

9.12.3 Okolnosti zmeny OID

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

9.13 Riešenie sporov

Zákazník/Držiteľ má právo zaslať Poskytovateľovi sťažnosť, podnet alebo reklamáciu na poskytnutú dôveryhodnú služby emailom na radisig@disig.sk. Poskytovateľ vybaví reklamáciu najneskôr do 30 dní od jej prijatia, pokiaľ sa strany nedohodnú inak. Vybavenie reklamácie sa vzťahuje len k popisu vady uvedenej Zákazníkom. Poskytovateľ na ňu musí odpovedať do 30 dní od jej prijatia, v prípade komplikovanejších sťažností alebo reklamácií si vyhradzuje právo túto dobu predĺžiť.

Súdy Slovenskej republiky majú výlučnú právomoc na rozhodovanie akýchkoľvek sporov medzi Poskytovateľom a Zákazníkom/Držiteľom certifikátu. V prípade, že Zákazník/Držiteľ certifikátu je spotrebiteľom, prípadný spor môže riešiť taktiež mimosúdnou cestou. V takomto prípade je oprávnený kontaktovať subjekt mimosúdneho riešenia sporov, napr. Slovenskú obchodnú inšpekciu alebo inú právnickú osobu zapísanú v zozname podľa § 5 ods. 2 zákona č. 391/2015 Z. z. o alternatívnom riešení spotrebiteľských sporov, v znení neskorších predpisov. Pred pristúpením k súdnemu alebo mimosúdnemu riešeniu sporu sú zmluvné strany povinné pokúsiť sa najskôr vyriešiť tento spor vzájomnou dohodou.

9.14 Rozhodné právo

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

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

9.15 Súlad s platnými právnymi predpismi

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

9.16 Rôzne ustanovenia

9.16.1 Rámcová dohoda

Žiadne ustanovenia.

9.16.2 Postúpenie práv

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

9.16.3 Salvatórska klauzula

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

9.16.4 Uplatnenie práv

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

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

9.16.5 Vyššia moc

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

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

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

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

9.17 Iné ustanovenia

Žiadne ustanovenia.