POLITIKA

poskytovania dôveryhodnej služby vyhotovovania a overovania verejne dôveryhodných certifikátov

Disig, a.s.

Vypracoval	**Disig, a.s.**
Dátum platnosti	**18. 7. 2024**
Verzia	**1.1**
Typ	**POLITIKA**
Schválil	**Ing. Ľuboš Batěk**

Obsah

Obchodné meno	Disig, a.s.
Sídlo	Galvaniho 17/C, 821 04 Bratislava
Zapísaná v OR	Mestského súdu Bratislava III, odd. Sa 3794/B
Telefón	+ 421 2 208 50 140
E-mail	disig@disig.sk

Tento dokument neprešiel jazykovou úpravou.

Ochranné známky
Mená produktov uvádzané v tomto dokumente môžu byť registrované ochranné známky príslušných firiem

1. Úvod

Tento dokument špecifikuje politiku (ďalej aj „CP“) spoločnosti Disig, a.s., so sídlom Galvaniho 17/C, 821 04 Bratislava, IČO: 35975946, zapísanú v Obchodnom registri Mestského súdu Bratislava III, odd. Sa, vložka č. 3794/B, ako poskytovateľa dôveryhodných služieb (ďalej len „Poskytovateľ“) a platí pre koreňové certifikačné autority a k nim podriadené certifikačné autority uvedené v kapitole 1.4.1, prevádzkované Poskytovateľom, prostredníctvom ktorých poskytuje dôveryhodné služby vyhotovovania verejne dôveryhodných certifikátov.

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 programov pre koreňové certifikačné autority Microsoft Trusted Root Program [3]. Mozilla Root Store Policy [4], Apple Root Certificate Program [5], Chrome Root Program Policy [6] 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“) [7] a požiadavkami štandardu ETSI EN 319 411-1 [8].

Táto politika je štruktúrovaná v súlade s RFC 3647 [9].

1.2 Názov dokumentu a jeho identifikácia

Názov	**POLITIKA poskytovania dôveryhodnej služby vyhotovovania a overovania verejne dôveryhodných certifikátov**
Skratka názvu:	**CP PT CA Disig***
Verzia:	**1.1**
Schválené dňa:	**18.7.2024**
Platnosť od:	**18. 7. 2024**
Tomuto dokumentu je priradený identifikátor objektu (OID):	**1.3.158.35975946.0.0.0.1.13**

* - 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.**13** – **CP PT CA Disig**

1.2.1 História zmien

Verzia	Dátum revízie	Popis revízie; revidoval
1.0	1.2.2024	Prvá verzia dokumentu; Miškovič
1.1	18. 7. 2024	Zmena sídla spoločnosti Disig, a.s.; Miškovič

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,

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“) [10] 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.

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:

- autentifikácie držiteľa certifikátu,
- podpisovania elektronických dokumentov zdokonaleným elektronickým podpisom,
- opatrovania elektronických dokumentov zdokonalenou elektronickou pečaťou,
- 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 na vyhotovovanie zdokonaleného elektronického podpisu, autentifikáciu pri prístupe k rôznym IS; vydávaný certifikát spĺňa požiadavky dané v [8]

pre NCP (Normalized Certificate Policy; OID 0.4.0.2042.1.1) resp. NCP+ (extended Normalized Certificate Policy; OID 0.4.0.2042.1.2).

- **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; vydávaný certifikát spĺňa požiadavky dané v [8] pre NCP (Normalized Certificate Policy; OID 0.4.0.2042.1.1) resp. NCP+ (extended Normalized Certificate Policy; OID 0.4.0.2042.1.2).

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)(DER)	B561EBEAA4DEE4254B691A98A55747C234C7D971
Odtlačok (sha256)(DER)	E23D4A036D7B70E9F595B1422079D2B91EDFBB1FB651A0633EAA8A9DC5F80703
Poznámka	Vydáva certifikáty len pre podriadené certifikačné autority Poskytovateľa.

Názov	**CA Disig R2I3 Certification Service**
Sériové číslo certifikátu	08a2395ba703affdac0000000000000004
Vydavateľ	CA Disig Root R2
Odtlačok (sha1)(DER)	1432AC3C02C8C89D6179A40B2EFF6B5AD5DA5D7F
Odtlačok (sha256)(DER)	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 [7] a nie je ich možné použiť tam, kde sú požadované EÚ kvalifikované certifikáty. V zmysle tejto CP nie je možné vydať certifikáty obsahujúce v rozšírení „*Extended key Usage (EKU)*“ hodnotu „*id-kp-serverAuth*“ resp. „*id-kp-emailProtection*“.

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:	**Galvaniho 17/C, 821 04 Bratislava**
IČO:	**359 75 946**
telefón	**+421 2 20850140**
e-mail:	**disig@disig.sk**
webové sídlo:	**https://www.disig.sk**

1.5.2 Kontaktná osoba

Na účel tvorby politík má Poskytovateľ vytvorenú autoritu pre správu politík (PMA), 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:	**Galvaniho 17/C, 821 04 Bratislava**
e-mail:	**caoperator@disig.sk**
telefón	**+421 2 20850150, +421 2 20820157**
webové sídlo:	**https://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

Autentifikácia - je proces overovania udanej identity užívateľa s využitím verejne dôveryhodného certifikátu pri prístupe k informačným systémom;

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;

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.

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 [7];

Zdokonalený elektronický podpis - elektronický podpis, ktorý spĺňa požiadavky stanovené v článku 26 Nariadenia eIDAS [7];

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)
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)
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)

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] Microsoft Trusted Root Program.

[4] Mozilla Root Store Policy, Version 2.9, Effective September 1, 2023.

[5] Apple Root Certificate Program, Effective August 15,2023. https://www.apple.com/certificateauthority/ca_program.html.

[6] Chrome Root Program Policy, Version 1.5. s.l. : https://www.chromium.org/Home/chromium-security/root-ca-policy/.

[7] 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 .

[8] ETSI EN 319 411-1 Electronic Signatures and Infrastructures (ESI); Policy and security requirements for Trust Service Providers issuing certificates; Part 1: General requirements.

[9] RFC3647, Request for Comments: 3647, Internet X.509 Public Key Infrastructure: Certificate Policy and Certification Practices Framework, Chokhani, et al, November 2003.

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

[11] X.500 Information technology – Open Systems Interconnection – The Directory: Overview of concepts, models and services. 10/2012. s.l. : ITU-T.

[12] X.501 Information technology – Open Systems Interconnection – The Directory: Models. s.l. : ITU-T, 10/2012.

[13] X.520 Information technology – Open Systems Interconnection – The Directory: Selected attribute types. s.l. : ITU-T, 10/2012.

[14] RFC5322 "Internet Message Format".

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

[16] Network and Certificate System Security Requirements Version 2.0. s.l. : CA/Browser Forum.

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

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

[19] ETSI EN 319 401 Electronic Signatures and Infrastructures (ESI); General Policy Requirements for Trust Service Providers.

[20] ETSI EN 319 412-1 Electronic Signatures and Infrastructures (ESI);Certificate Profiles;Part 1: Overview and common data structures.

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 dané v jednotlivých programov pre koreňové CA [3], [4] , [5] a [6].

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.

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“) [11], konkrétne s X.501 [12] resp. X.520 [13] a mená v zmysle RFC5322 Internet Message Format [14].

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)

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 subjekte 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**
pseudonym	2.5.4.65		Pseudonym zvolený Žiadateľom	**Údaj je povinný** (ak sa v CN nachádza pseudonym)
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
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!!!**

3.1.4.2 Certifikáty pre právnickú osobu

Tabuľka č. 4 obsahuje zoznam položiek, ktoré sa môžu nachádzať v subjekte 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 [20]

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	**2.5.4.97**		Odkaz na identifikačný údaj právnickej osoby[2]	**Údaj je povinný pokiaľ existuje!!!**
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!!!**

3.1.5 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).

[2] Pozri ETSI EN 319412-1 časť 5 [20]

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.

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

3.2.2 Autentizácia identity právnickej osoby

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 niektorou z metód uvedených v časti 3.2.2.1

3.2.2.4 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.

3.2.3 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.

3.2.3.1 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.

3.2.3.2 Predkladané doklady

3.2.3.2.1 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.

3.2.3.2.2 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.

3.2.3.2.3 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 0 aj doklady podľa časti 3.2.2. Táto požiadavka sa netýka zamestnanca zmluvného partnera, kde je zmluvne dohodnutý iný mechanizmus overovania.

3.2.3.2.4 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 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 zapisovaná do osobných údajov držiteľa v IS Poskytovateľa.

3.2.5 Overovanie oprávnení

Žiadne ustanovenia.

3.2.6 Kritériá interoperability

Žiadne ustanovenia.

3.3 Identifikácia a autentifikácia pri vydávaní následného certifikátu

3.3.1 Identifikácia a autentifikácia pri riadnom vydávaní následného certifikátu

Žiadne ustanovenia.

3.3.2 Identifikácia a autentifikácia pri vydávaní následného certifikátu po zrušení predchádzajúceho

Žiadne ustanovenia.

3.4 Identifikácia a autentifikácia pri žiadaní o zrušenie certifikátu

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,

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“) [10] a Informáciou o spracúvaní osobných údajov [15], 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 musí byť zaslaná príslušnej RA elektronickou poštou. E-mailové adresy jednotlivých RA Poskytovateľa sú k dispozícii na webovom sídle Poskytovateľa (pozri časť 1).

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.

4.1.2.3 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.

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 [10],
- 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, 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 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 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.

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.

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

Žiadne ustanovenia.

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 [10],
- 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,
- 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 [10] 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 [10] 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

Žiadne ustanovenia.

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

Žiadne ustanovenia.

4.7.1 Podmienky vydania certifikátu na nové kľúče

Žiadne ustanovenia.

4.7.2 Kto môže žiadať o vydanie certifikátu na nové kľúče

Žiadne ustanovenia.

4.7.3 Postup žiadania o vydanie certifikátu na nové kľúče

Žiadne ustanovenia.

4.7.4 Oznámenie o vydaní certifikátu na nové kľúče Držiteľovi

Žiadne ustanovenia.

4.7.5 Spôsob prevzatia certifikátu vydaného na nové kľúče

Žiadne ustanovenia.

4.7.6 Zverejňovanie certifikátov zo strany Poskytovateľa

Žiadne ustanovenia.

4.7.7 Oznámenie o vydaní certifikátu CA iným subjektom

Žiadne ustanovenia.

4.8 Modifikácia certifikátu

4.8.1 Okolnosti pre modifikovanie certifikátu

Žiadne ustanovenia.

4.8.2 Kto môže požiadať o modifikáciu certifikátu

Žiadne ustanovenia.

4.8.3 Spracovanie žiadostí o modifikáciu certifikátu

Žiadne ustanovenia.

4.8.4 Oznámenie o vydaní nového certifikátu držiteľovi

Žiadne ustanovenia.

4.8.5 Spôsob prevzatia modifikovaného certifikátu

Žiadne ustanovenia

4.8.6 Zverejňovanie modifikovaného certifikátu zo strany Poskytovateľa

Žiadne ustanovenia.

4.8.7 Oznámenie o vydaní modifikovaného certifikátu iným subjektom

Žiadne ustanovenia.

4.9 Zrušenie a 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,

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,
- Poskytovateľ je oboznámený, že došlo k podstatným zmenám informácií uvedených v certifikáte,
- 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.

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,

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.

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 (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;
- Prostredníctvom online služby dostupnej na webovom sídle Poskytovateľa. Linka na online službu zrušenia certifikátu je uvedená v potvrdení o prevzatí certifikátu, ktoré dostáva držiteľ pri jeho prevzatí. Online zrušenie certifikátu je podmienené poskytnutím sériového čísla predmetného certifikátu a hesla na jeho zrušenie.

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

Žiadne ustanovenia.

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 [10].

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. 5 obsahuje informácie o maximálnych požiadavkách na vydávanie.

Tabuľka č. 5: 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.

Údaje pre OSCP službu musí byť aktualizovať minimálne každé štyri dni [4]

Odpovede musia mať definovanú hodnotu v položke *nextUpdate* a táto musí byť najviac desať dní po hodnote v položke *thisUpdate* [4]

Hodnota v položke *nextUpdate* musí byť pred alebo rovná dátumu *notAfter* všetkých certifikátov zahrnutých v položke *BasicOCSPResponse.certs* alebo, ak je pole *certs* vynechané, pred alebo rovná dátumu *notAfter* certifikátu CA, ktorý vydal certifikát, pre ktorý je poskytovaná OCSP odpoveď (*BasicOCSPResponse*) [4].

Všetky certifikáty vydané koreňovou certifikačnou autoritou musia podporovať rozšírenie distribučného bodu CRL a/alebo AIA obsahujúcu adresu URL, kde je možné získať OCSP odpoveď [3].

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

Žiadne ustanovenia.

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 24x7.

Služba OCSP musí byť dostupná v režime 24x7.

4.10.3 Doplnkové funkcie

Žiadne ustanovenia.

4.11 Ukončenie poskytovanie služieb

Žiadne ustanovenia.

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:

5.4.1.1 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,
- uvedenie nového profilu certifikátu a ukončenie používania existujúceho profilu

5.4.1.2 Udalosti týkajúce sa životného cyklu certifikátov pre koncových používateľov:

- žiadosť o vydanie certifikátu, jeho obnovu, zmenu kľúčov a ich rušenie,
- schválenie a odmietnutie žiadosti o vydanie,
- vydanie certifikátu,
- vytvorenie CRL,

5.4.1.3 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

Žiadne ustanovenia.

5.5 Uchovávanie záznamov

5.5.1 Typy archivovaných záznamov

Poskytovateľ musí archivovať všetky auditné logy uvedené v sekcii 5.4.1.

Okrem toho musí archivovať:

- dokumentáciu týkajúcu sa bezpečnosti systémov certifikačnej autority, systémov správy certifikátov, systémov koreňových CA,
- dokumentáciu týkajúcu sa overovaniam vydávania a zrušovania žiadosti o certifikát a samotných certifikátov.

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 musí archivovať záznamy po dobu najmenej dvoch (2) rokov od ich času ich vytvorenia alebo tak dlho, ako sa vyžaduje, aby boli archivované podľa časti 5.4.3, podľa toho, čo dlhšie.

Okrem toho Poskytovateľ archivuje aspoň dva (2) roky:

- všetku archivovanú dokumentáciu týkajúcu sa bezpečnosti systémov certifikačnej autority, systémov správy certifikátov, systémov koreňových CA,
- všetku archivovanú dokumentáciu týkajúcu sa overovaniam vydávania a zrušovania žiadosti o certifikát a samotných certifikátov.

5.5.3 Ochrana archívnych záznamov

Žiadne ustanovenia.

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

Žiadne ustanovenia.

5.7 Obnova po kompromitácia alebo havárii

5.7.1 Postupy riešenia incidentov a kompromitácie

Poskytovateľ musí mať zdokumentované postupy na zabezpečenie kontinuity činnosti a obnovy po havárii určené na informovanie a primeranú ochranu dodávateľov aplikačného softvéru, zákazníkov a spoliehajúce sa strany v prípade havárie, narušenia bezpečnosti alebo zlyhania podnikateľskej činnosti. Poskytovateľ nie je povinný zverejniť svoje plány kontinuity činnosti, ale na požiadanie musí sprístupniť tento plán audítorom. Poskytovateľ musí tieto plány testovať, kontrolovať a aktualizovať na ročnej báze.

Plán kontinuity činnosti by musí zahŕňať:

1. Podmienky aktivácie plánu;
2. Núdzové postupy;
3. Záložné postupy;
4. Postupy obnovenia;
5. Plán údržby plánu;
6. Požiadavky na informovanosť a vzdelanie;
7. Zodpovednosti jednotlivcov;
8. Ciele doby obnovy (RTO);
9. Pravidelné testovanie pohotovostných plánov;
10. Plán Poskytovateľa na udržiavanie alebo obnovu podnikateľských činností CA včas po prerušení alebo zlyhaní kritických podnikateľských procesov;

11. Požiadavku uchovávať kritické kryptografické materiály (t. j. bezpečné kryptografické zariadenie a aktivačné materiály) na záložnom mieste;
12. Prijateľné časy výpadku systému a času obnovy;
13. Ako často sa vytvárajú záložné kópie základných obchodných informácií a softvéru;
14. Vzdialenosť zariadení na obnovu od hlavného miesta prevádzky CA;
15. Postupy na zabezpečenie svojich priestorov v možnom rozsahu počas obdobia po havárii a pred obnovením bezpečného prostredia buď na pôvodnom mieste, alebo na vzdialenom mieste.

5.7.2 Poškodenie hardvéru, softvéru alebo údajov

Žiadne ustanovenia.

5.7.3 Postupy pri kompromitácii kľúča CA

Žiadne ustanovenia.

5.7.4 Zachovanie kontinuity činnosti po havárii

Žiadne ustanovenia.

5.8 Ukončenie činnosti CA resp. RA

Žiadne ustanovenia.

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 Generovanie kľúčového páru certifikačnej autority

V prípade kľúčových párov, ktoré sú určené pre prevádzkovateľa koreňovej CA musí Poskytovateľ:

- pripraviť a riadiť sa skriptom pre generovanie kľúčového páru
- zabezpečiť buď:
  - vykonať generovanie kľúčového páru za prítomnosti kvalifikovaného audítora, alebo
  - zaznamenať celý proces generovania kľúčového páru na video pre kontrolu procesu zo strany audítora

Poskytovateľ musí ďalej zabezpečiť:

- vygenerovať kľúčový pár CA vo fyzicky zabezpečenom prostredí, ako je popísané v CP a/alebo CPS CA;
- generovať kľúčový pár CA pomocou osôb v dôveryhodných rolách podľa princípov kontroly viacerými osobami a rozdelených znalostí;

- vygenerovať pár kľúčov CA v rámci kryptografických modulov, ktoré spĺňajú príslušné technické a obchodné požiadavky uvedené v CP a/alebo CPS CA;
- zaznamenať aktivity generovania kľúčového páru CA; a
- udržiavať účinné kontroly s cieľom poskytnúť primeranú istotu, že súkromný kľúč bol vygenerovaný a chránený v súlade s postupmi opísanými v jeho CP a/alebo CPS a (ak je to vhodné) jeho skripte na generovanie 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

RA Poskytovateľa musí zamietnuť žiadosť o vydanie certifikátu, ak je splnená jedna alebo viac z týchto podmienok:

- Kľúčový pár nespĺňa požiadavky dané v sekcii 6.1.5 a/alebo v sekcii 6.1.6;
- Existuje jasná dôkaz, že metóda použitá na generovanie kľúčového páru je chybná;
- Poskytovateľ bol informovaný, že súkromný kľúč bol kompromitovaný ako napr. v zmysle sekcie 4.9.1.1.

RA Poskytovateľa negeneruje kľúčový pár v mene držiteľa.

6.1.2 Doručenie súkromného kľúča Držiteľovi certifikátu

Ine strany ako držiteľ nesmú archivovať súkromný kľúč Držiteľa bez autorizácie zo strany Držiteľa.

V prípade, že sa Poskytovateľ dozvie o skutočnosti, že súkromný kľuč Držiteľa má k dispozícii osoba alebo organizácia, ktoré neboli autorizované Držiteľom, zruší všetky certifikáty obsahujúce verejný kľúč zodpovedajúci danému súkromnému kľúču.

6.1.3 Doručenie verejného kľúča vydavateľovi certifikátu

Žiadne ustanovenia.

6.1.4 Doručenie verejného kľúča CA spoliehajúcim sa stranám

Žiadne ustanovenia.

6.1.5 Dĺžky kľúčov

Pre RSA kľúčový pár sa musí Poskytovateľ uistiť, že:

- veľkosť modulu pri kódovaní je minimálne 2048 bitov;
- veľkosť modulu v bitoch je bez zvyšku deliteľná číslom 8.

6.1.6 Parametre a kvalita verejného kľúča

Pre RSA kľúčový pár musí Poskytovateľ potvrdiť, že hodnota verejného exponentu je nepárne číslo rovné 3 alebo viac. Okrem toho, verejný exponent by mal byť v rozsahu medzi 2^16 + 1 a 2^256 - 1. Modul by mal mať aj nasledujúce charakteristiky: nepárne číslo, nie mocnina prvočísla, a žiadne faktory menšie ako 752 (Pozri NIST SP 800-89, časť 5.3.3.).

6.1.7 Použitie kľúčov

Súkromný kľúč zodpovedajúci koreňovej certifikačnej autorite nesmie byť použitý na podpisovanie certifikátov s výnimkou:

- Vlastného self-signed podpisu koreňovej CA;
- Podpisu podriadených certifikačných autorít a krížových certifikátov;
- Certifikáty pre potreby internej infraštruktúry ako napr. certifikáty správcovských roli, interné prevádzkové certifikáty;
- Certifikáty OCSP responderov.

6.2 Ochrana súkromného kľúča a technické opatrenia pre kryptografický modul

6.2.1 Štandardy a opatrenia pre kryptografický modul

Poskytovateľ musí mať implementované fyzické a logické bezpečnostné opatrenia, aby zabránil neoprávnenému vydaniu certifikátu. Ochrana súkromného kľúča mimo overeného systému alebo HSM zariadenia musí pozostávať s fyzickej bezpečnosti, šifrovania, alebo ich kombinácie, implementovaných takým spôsobom, ktorý zabraňuje prezradeniu súkromného kľúča.

Poskytovateľ musí zašifrovať svoj súkromný kľúč pomocou algoritmu a dĺžky kľúča, ktoré sú podľa súčasného stavu techniky schopné odolať kryptoanalytickým útokom počas zvyškovej životnosti zašifrovaného kľúča alebo časti kľúča.

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

Žiadne ustanovenia.

6.2.3 „Key escrow“ súkromného kľúča

Žiadne ustanovenia.

6.2.4 Zálohovanie súkromného kľúča

Žiadne ustanovenia.

6.2.5 Archivácia súkromného kľúča

Iné strany ako Poskytovateľ nesmú archivovať súkromné kľúče podriadených CA bez autorizácie Poskytovateľom.

6.2.6 Prenos súkromných kľúčov z a do HSM modulu

Ak Poskytovateľ prevádzkovaná vydávajúca CA generuje súkromný kľúč v mene podriadenej CA, potom vydávajúca CA musí zašifrovať súkromný kľúč za účelom jeho transportu k podriadenej CA.

Ak sa vydávajúca CA dozvie, že súkromný kľúč podriadenej CA bol oznámený neoprávnenej osobe alebo organizácii, ktorá nie je pridružená k podriadenej CA, potom CA, ktorá vydala, zruší všetky certifikáty, ktoré obsahujú verejný kľúč zodpovedajúci oznámenému súkromnému kľúču.

6.2.7 Uchovávanie súkromných kľúčov v HSM module

Poskytovateľ musí chrániť svoj súkromný kľúč v systéme alebo zariadení, ktoré bolo overené ako spĺňajúce aspoň FIPS 140-2 úroveň 3, FIPS 140-3 úroveň 3 alebo príslušný Common Criteria Protection Profile or Security Target, EAL 4 (alebo vyšší), ktorý zahŕňa požiadavky na ochranu súkromného kľúča a iných aktív pred známymi hrozbami.

6.2.8 Spôsob aktivácie súkromných kľúčov

Žiadne ustanovenia.

6.2.9 Spôsob deaktivácie súkromného kľúča

Žiadne ustanovenia.

6.2.10 Spôsob zničenia súkromného kľúča

Žiadne ustanovenia.

6.2.11 Charakteristika HSM modulu

Žiadne ustanovenia.

6.3 Ďalšie aspekty manažmentu kľúčového páru

6.3.1 Archivácia verejných kľúčov

Žiadne ustanovenia.

6.3.2 Dĺžka platnosti certifikátov a použiteľnosť kľúčového páru

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

Typ certifikátu	Platnosť (maximálne)
Koreňová CA	30 rokov
Podriadená CA	15 rokov
Certifikát pre koncového používateľa	5 rokov

6.4 Aktivačné údaje

6.4.1 Vytváranie a inštalácia aktivačných údajov

Žiadne ustanovenia.

6.4.2 Ochrana aktivačných údajov

Žiadne ustanovenia.

6.4.3 Ostatné aspekty aktivačných údajov

Žiadne ustanovenia.

6.5 Riadenie bezpečnosti počítačov

6.5.1 Špecifické požiadavky na bezpečnosť počítačov

Poskytovateľ musí zaviesť viacfaktorovú autentifikáciu pre všetky účty, ktoré sú schopné priamo spôsobiť vydanie certifikátu.

6.5.2 Hodnotenie bezpečnosti informácií

Žiadne ustanovenia.

6.6 Opatrenia v životnom cykle

6.6.1 Opatrenia pri vývoji systémov

Žiadne ustanovenia.

6.6.2 Opatrenia na riadenie bezpečnosti

Žiadne ustanovenia.

6.6.3 Bezpečnostné opatrenia v životnom cykle

Žiadne ustanovenia.

6.7 Sieťové bezpečnostné opatrenia

Musia byť dodržané všetky požiadavky dané v dokumente „ Network and Certificate System Security Requirements“ [16]

6.8 Využívanie časovej pečiatky

Žiadne ustanovenie

7. Profily certifikátov a zoznamov zrušených certifikátov

7.1 Profily certifikátov

Poskytovateľ musí spĺňať technické požiadavky uvedené v článkoch 6.1.5 a 6.1.6.

Poskytovateľ musí generovať nesekvenčné sériové čísla certifikátov väčšie ako 0 a menšie ako 2^159 obsahujúce aspoň 64 bitov z výstupu.

7.1.1 Verzia

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

7.1.2 Obsah a rozšírenia certifikátu

7.1.2.1 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. 6: 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 (nepovinná položka)
O	2.5.4.10	organizationName	**Disig a.s.**
CN	2.5.4.3	commonName	*v závislosti od typu CA* [1)]

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

Tabuľka č. 7: 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

7.1.2.2 Podriadené certifikačné autority Poskytovateľa

Algoritmy a dĺžky kľúčov uplatňované v certifikátoch podriadených CA Poskytovateľa:

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

Tabuľka č. 8: 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**
O	2.5.4.10	organizationName	**Disig a.s.**
CN	2.5.4.3	commonName	*v závislosti od typu CA*[1)]

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

Tabuľka č. 9: 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

7.1.2.3 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

Tabuľka č. 10 obsahuje použité rozšírenia nachádzajúce sa vo všetkých typoch vydávaných certifikátov

Tabuľka č. 10: Základné rozšírenia (certificate extensions) vo vydávaných certifikátoch

Názov rozšírenia	ASN.1 názov a OID / Popis	Prítomnosť	Kritickosť
Certificate Policies	{id-ce-certificatePolicies} {2.5.29.32} Identifikuje certifikačné politiky, pod ktorými bol certifikát vydaný.	ÁNO	NIE
CRL Distribution Points	{id-ce-CRLDistributionPoints} {2.5.29.31} Určuje, akým spôsobom a odkiaľ je možné získať CRL.	ÁNO	NIE
AuthorityInfoAccess	{id-pe-authorityInfoAccess} {1.3.6.1.5.5.7.1.1} Určuje (http:// … p7c, certifikát alebo aj ldap://...) adresu na získanie certifikátov vydaných pre vydavateľa tohto certifikátu a adresu na OCSP.	ÁNO	NIE
basicConstraints {id-ce-basicConstraints} [2.5.29.19]	Toto rozšírenie smie byť prítomné. Pole cA nesmi byť nastavene na „true“ a pole pathLenConstraint nesmie byť uvedené.	SMIE	NIE
Key Usage	{id-ce-keyUsage} {2.5.29.15} Definuje účel použitia súkromného kľúča, ktorého verejný kľúč je súčasťou tohto certifikátu.	ÁNO	NIE
Extended Key Usage	{id-ce-extKeyUsage} [2.5.29.37] Rozširuje účel použitia súkromného kľúča definovaný v rozšírení „Key Usage“	ÁNO	NIE
Authority Key Identifier	{id-ce-authorityKeyIdentifier} {2.5.29.35}	ÁNO	NIE

	Identifikátor verejného kľúča certifikačnej autority CA, ktorá vydala tento certifikát.		
Subject Key Identifier	{id-ce-subjectKeyIdentifier} {2.5.29.14} Identifikátor verejného kľúča Držiteľa certifikátu.	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

Hodnoty atribútov musia byť kódované v zmysle RFC 5280 [2].

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 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)

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

Žiadne ustanovenia.

7.1.8 Syntax a sémantika politiky

Žiadne ustanovenia.

7.1.9 Sémantika spracovania kritických certifikačných politík

Žiadne ustanovenia.

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“ [17]

7.2.2 Použité rozšírenia (CRL extensions) v CRL vydávanom Poskytovateľom

Tabuľka č. 11 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. 11: 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

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“ [18]. 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).

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. 12: 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

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 všetkých relevantných programov koreňových certifikačných autorít [3], [4], [5], [6] a požiadaviek Nariadenia eIDAS [7]. 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.

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 [8], pričom musí zahŕňať aj normatívne odkazy z ETSI EN 319 401 [19].

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 relevantných programoch koreňových certifikačných autorít [3], [4], [5], [6] a kontrolovať poskytované služby vykonávaním interných auditov minimálne na štvrťročnej báze na náhodne vybranej reprezentatívnej vzorke 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. [15]

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 [15].

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 [15] 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 [15].

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 [10] 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 [10].

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 [10].

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 [10], 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 [10] 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. 18. 7. 2024 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 1.1, 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.