POLITIKA

poskytovania dôveryhodnej služby vyhotovovania a overovania S/MIME certifikátov

Disig, a.s.

Vypracoval	**Ing. Peter Miškovič**
Dátum platnosti	**2.1.2024**
Verzia	**1.1**
Typ	**POLITIKA**
Schválil	**Ing. Ľuboš Batěk**

Obsah

Obchodné meno	Disig, a.s.
Sídlo	Záhradnícka 151, 821 08 Bratislava
Zapísaná v OR	OR Mestského súdu Bratislava III, odd. Sa 3794/B
Telefón	+ 421 2 208 50 140
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 Záhradnícka 151, 821 08 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 všetky koreňové certifikačné autority a k nim podriadené certifikačné autority, prevádzkované Poskytovateľom, prostredníctvom ktorých poskytuje dôveryhodnú službu vyhotovovania S/MIME certifikátov v zmysle požiadaviek Baseline Requirements for the Issuance and Management of Publicly-Trusted S/MIME Certificates [1] (ďalej aj „certifikát“).

Certifikát vyhotovovaný pre koncového používateľa (ďalej aj „Držiteľ“) jednoznačne identifikuje entitu, ktorej je certifikát vydávaný a túto entitu zväzuje 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 v súlade s požiadavkami RFC 5280 „Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile“ [2], požiadavkami Baseline Requirements for the Issuance and Management of Publicly-Trusted S/MIME Certificates [1] 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“) [3] a ETSI TS 119 411-6 „Electronic Signatures and Infrastructures (ESI); Policy and security requirements for Trust Service Providers issuing certificates; Part 6: Requirements for Trust Service Providers issuing publicly trusted S/MIME certificates“ [4]. S/MIME certifikáty sú vydávané v súlade s požiadavkami pre NCP a NCP+ politikami v zmysle ETSI EN 319 411-1 „Electronic Signatures and Infrastructures (ESI); Policy and security requirements for Trust Service Providers issuing certificates; Part 1: General requirements“ [5].

Táto politika je štruktúrovaná v súlade s RFC 3647 [6].

1.2 Názov dokumentu a jeho identifikácia

Názov	POLITIKA poskytovania dôveryhodnej služby vyhotovovania a overovania S/MIME certifikátov
Skratka názvu:	**CP SMIME CA Disig***
Verzia:	**1.1**
Schválené dňa:	**25.1.2024**
Platnosť od:	**2.1.2024**
Tomuto dokumentu je priradený identifikátor objektu (OID):	**1.3.158.35975946.0.0.0.1.11**

* - 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.**11** – **CP S/MIME CA Disig**

1.2.1 História zmien

Verzia	Dátum revízie	Popis revízie; revidoval
1.0	1.9.2023	Prvá verzia dokumentu; Miškovič
1.1	2.1.2024	Doplnenie možnosti online zrušenia certifikátu (4.9.3); 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“) [7].

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.

Pokiaľ sa v texte použije výraz „RA Poskytovateľa“, tak sa to týka všetkých vyššie uvedených typov RA.

1.3.2.1 Firemná RA

Poskytovateľ môže delegovať na firemnú RA overenie žiadostí o certifikát pre fyzické osoby v rámci ich vlastnej organizácie. Poskytovateľ nebude akceptovať žiadosti o certifikát autorizované firemnou RA, pokiaľ nie sú splnené tieto požiadavky:

- Ak sa žiadosť o certifikát týka S/MIME profilu typu „*organization-validated*“ alebo „*sponsor-validated*“ Poskytovateľ potvrdí, že firemná RA má autorizáciu alebo kontrolu nad požadovanými e-mailovými adresami v súlade s časťami 3.2.2.1 alebo 3.2.2.3.
- Poskytovateľ musí potvrdiť, že obsah „*subject:organizationName* je buď názov spoločnosti, ktorá prevádzkuje firemnú RA, alebo pridruženej spoločnosti firemnej RA, alebo že firemná RA je zástupcom uvedeného subjektu. Poskytovateľ musí zaviesť tieto obmedzenia ako zmluvnú

požiadavku pre firemnú RA a monitorovať súlad zo strany firemnej RA v súlade s časťou 8.8.

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 – vydáva sa S/MIME certifikát pre podpis,
- fyzická osoba identifikovaná v spojení s právnickou osobou - vydáva sa S/MIME certifikát pre podpis,
- právnická osoba, ktorou môže byť organizácia alebo jej jednotka resp. oddelenie – vydáva sa S/MIME certifikát pre pečať,

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“) [8] zverejnené na webovom sídle Poskytovateľa (pozri sekcia 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 S/MIME certifikát pre podpis , ktorý je vydávaný 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 S/MIME certifikát pre pečať 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 RA 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 RA Poskytovateľa môžu byť vo všeobecnosti použité bežným spôsobom, výhradne v súlade s ich účelovým určením, a to v závislosti od konkrétneho certifikátu najmä pre potreby:

- zabezpečenia elektronickej pošty (podpisovanie a/alebo šifrovanie správ posielaných elektronickou poštou),
- podpisovania elektronických dokumentov zdokonaleným elektronickým podpisom,
- opatrovania elektronických dokumentov zdokonalenou elektronickou pečaťou,
- autentifikácia fyzickej resp. právnickej osoby

Certifikačné autority Poskytovateľa (ďalej „CA Poskytovateľa“) vyhotovujú pre Zákazníkov tieto typy certifikátov:

- **SMIME certifikát pre podpis resp. S/MIME certifikát pre pečať** - obsahuje verejný kľúč viazaný na e-mailovú adresu a môže tiež obsahovať totožnosť fyzickej osoby alebo právnickej osoby, ktorá má takúto e-mailovú adresu pod kontrolou. Kľúčový pár potom môže byť použitý na podpisovanie, overovanie, šifrovanie a dešifrovanie e-mailov; vydaný certifikát bude okrem iného obsahovať aj niektorý z týchto identifikátory certifikačnej politiky v tvare:
  - {joint-iso-itu-t(2)international-organizations(23)ca-browser-forum(140) certificate-policies(1)smime-baseline(5)organization-validated(2) multipurpose (2)} (2.23.140.1.5.2.2);
  - {joint-iso-itu-t(2)international-organizations(23)ca-browser-forum(140) certificate-policies(1)smime-baseline(5)organization-validated (2) strict (3)} (2.23.140.1.5.2.3);
  - {joint-iso-itu-t(2)international-organizations(23)ca-browser-forum(140) certificate-policies(1)smime-baseline(5)sponsor-validated(3) multipurpose (2)} (2.23.140.1.5.3.2);
  - {joint-iso-itu-t(2)international-organizations(23)ca-browser-forum(140) certificate-policies(1) smime-baseline(5) sponsor-validated (3) strict (3)} (2.23.140.1.5.3.3);
  - {joint-iso-itu-t(2)international-organizations(23)ca-browser-forum(140) certificate-policies(1) smime-baseline(5) individual-validated (4) multipurpose (2)} (2.23.140.1.5.4.2); a
  - {joint-iso-itu-t(2)international-organizations(23)ca-browser-forum(140) certificate-policies(1) smime-baseline(5) individual-validated (4) strict (3)} (2.23.140.1.5.4.3);

  v zmysle Baseline Requirements for S/MIME [1]

Poskytovateľ pre svoje potreby vydáva certifikáty na správu (certifikáty podriadených certifikačných autorít a certifikát pre on-line overovanie stavu certifikátov (OCSP)).

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

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

Názov	**CA Disig R2I5 Certification Service**
Sériové číslo certifikátu	081b06df4c7965509d0000000000000000e
Vydavateľ	CA Disig Root R2
Odtlačok (sha256)	90ba720b376fb9fdcf8a1037a5316fb493b5acf656ad79c6839008bd43343fdd
Poznámka	Vydáva SMIME certifikáty pre podpis/pečať pre koncových používateľov v zmysle požiadaviek uvedených v „Baseline Requirements for the Issuance and Management of Publicly-Trusted S/MIME Certificates [1]

1.4.2 Nedovolené použitie certifikátov

Certifikáty vydávané v zmysle tejto CP nie sú EÚ kvalifikované certifikáty v zmysle Nariadenia eIDAS [3] a nie je ich možné použiť tam, kde sú požadované EÚ kvalifikované certifikáty.

1.5 Správa politiky

1.5.1 Organizácia zodpovedná za správu dokumentu

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

Tabuľka č. 1: Kontaktné údaje Poskytovateľa

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

1.5.2 Kontaktná osoba

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

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

Tabuľka č. 2: Kontaktné údaje Poskytovateľa

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

1.5.3 Osoba rozhodujúca o súlade CPS s CP

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

1.5.4 Postupy schvaľovania CPS a externej politiky

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

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

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

1.6 Definície a skratky

1.6.1 Definície

CA Poskytovateľa – certifikačné autority Poskytovateľa určené na vydávanie S/MIME certifikátov

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;

RA Poskytovateľa – výraz, ktorý zahŕňa všetky typy RA Poskytovateľa (komerčná, firemná, interná)

S/MIME certifikát - obsahuje verejný kľúč viazaný na e-mailovú adresu a môže tiež obsahovať totožnosť fyzickej osoby alebo právnickej osoby, ktorá má takúto e-mailovú adresu pod kontrolou;

S/MIME STRICT profil - profil pre S/MIME certifikáty s „*extKeyUsage*“ obmedzeným na „*id-kp-emailProtection*“ a prísnejšie používanie atribútov DN subjektu a iných rozšírení.

S/MIME MULTIPURPOSE profil - profil zosúladený s presnejším profilom STRICT, ale s ďalšou možnosťou pre „*extKeyUsage*“ a ďalšie rozšírenia. Certifikát vydaný z tohto profilu umožňuje flexibilitu pre prípady krížového použitia medzi podpisovaním dokumentov a bezpečným e-mailom.

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 [3];

Zdokonalený elektronický podpis - elektronický podpis, ktorý spĺňa požiadavky stanovené v článku 26 Nariadenia eIDAS [3];

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

1.6.2 Skratky

ASCII	–	Americký štandardný kód pre výmenu informácií (American Standard Code for Information Interchange)
CA	–	Certifikačná autorita (Certification Authority)
CAA	-	DNS záznam definujúci CA, ktoré môžu vydať certifikát pre danú doménu
CMA	–	Autorita pre správu certifikátov (Certificate Management Authority)
CP	–	Certifikačná politika (Certificate Policy)
CPS	–	Pravidlá poskytovania dôveryhodnej služby vyhotovovania a overovania certifikátov (Certificate Practice Statement)
CRL	–	Zoznam zrušených certifikátov (Certification Revocation List)
FQDN	-	Presne stanovené meno domény (Fully Qualified Domain Name) je jednoznačné meno domény, ktoré absolútne udáva pozíciu uzla v stromovej hierarchii DNS.

HSM	–	Hardware Security Modul
HTTP	-	Hypertext Transfer Protocol
IČO	–	Identifikačné číslo organizácie
LEI	-	Identifikátor právnickej osoby (Legal Entity Identifier)
OCSP	-	Online Certificate Status Protocol
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)
RFC	-	Request for Comments
S/MIME	-	Secure MIME (Multipurpose Internet Mail Extensions)
TSA	-	Time Stamp Authority
URL	-	Internetový ekvivalent pre web adresu (Uniform Resource Locator)
UTC	-	Coordinated Universal Time

1.6.3 Odkazy

[1] Baseline Requirements for the Issuance and Management of Publicly-Trusted S/MIME Certificates. s.l. : CA/BROWSER FORUM. version 1.0.1.

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

[3] 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 .

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

[5] Pravidlá poskytovania dôveryhodnej služby vyhotovovania a overovania certifikátov-časť RA . 1.0.

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

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

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

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

[10] RFC5322 "Internet Message Format".

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

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

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

[14] RFC 5019 The Lightweight Online Certificate Status Protocol (OCSP) Profile.

[15] Recommendation for ObtainingAssurances for Digital SignatureApplications.

[16] Forum, CA/Browser. Network and Certificate System Security Requirements. 1.7.

[17] RFC5280, Request for Comments: 5280, Internet X.509 Public Key Infrastructure: Certificate and Certificate Revocation List (CRL) Profile.

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

[19] Recommendation ITU-T X.509; Information technology – Open Systems Interconnection – The Directory: Public-key and attribute certificate frameworks.

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

[21] ETSI EN 319 412-3 Electronic Signatures and Infrastructures (ESI); Certificate Profiles;Part 3: Certificate profile for certificates issued to legal persons.

[22] ETSI EN 319 412-2 Electronic Signatures and Infrastructures (ESI);Certificate Profiles;Part 2: Certificate profile for certificates issued to natural persons.

[23] Mozilla Root Store Policy version 2.9

2. Zverejňovanie informácií a úložiská

Poskytovateľ musí vyhotoviť, implementovať, vynucovať a minimálne jedenkrát ročne aktualizovať svoju CP/CPS, ktoré popisujú podrobnosti ako sú implementované legislatívne požiadavky a požiadavky dokumentu. [1]

2.1 Úložiská

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

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

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

2.2 Zverejňovanie informácií o CA

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

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

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

Poskytovateľ potvrdzuje, že v tejto CP sú zohľadnené všetky požiadavky aktuálnej verzie dokumentu [1], ktorý je publikovaný na stránke https://cabforum.org/smime-br/. V prípade akýchkoľvek rozporuplností medzi týmito požiadavkami a touto CP, majú prednosť požiadavky dané aktuálnou verziou dokumentu [1].

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“) [9], konkrétne s X.501 [10] resp. X.520 [11] a mená v zmysle RFC5322 Internet Message Format [12].

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 (organizácie)).

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 S/MIME certifikátoch nie je povolené.

3.1.4 Pravidlá na interpretáciu rôznych foriem mien

3.1.4.1 Náhrada znakov, ktoré nie sú ASCII

V S/MIME certifikátoch je možné používať diakritické znaky, ktoré nie sú súčasťou základnej tabuľky znakov ASCII.

V prípade potreby je možné nahradiť diakritické znaky ich ekvivalentom v základnej ASCII tabuľke takto:

Znak	ASCII ekvivalent
á, ä	a
č	c
ď	d
dž	dz
é	e
í	i
ľ, ĺ	l
ň	n

Znak	ASCII ekvivalent
ó, ô	o
ŕ	r
š	s
ť	t
ú	u
ý	y
ž	z

Znak	ASCII ekvivalent
Á, Ä	A
Č	C
Ď	D
DŽ	DZ
É	E
Í	I
Ľ,Ĺ	L
Ň	N

Znak	ASCII ekvivalent
Ó, Ô	O
Ŕ	R
Š	S
Ť	T
Ú	U
Ý	Y
Ž	Z

3.1.4.2 Geografické názvy

Žiadne ustanovenia.

3.1.5 Jedinečnosť mien

Žiadne ustanovenia.

3.1.6 Rozpoznanie, autentizácia a rola obchodných značiek

Žiadne ustanovenia.

3.2 Počiatočné overenie identity

CA Disig musí autentifikovať všetky atribúty identity subjektu, ktoré budú zahrnuté v S/MIME certifikáte a kontrolu subjektu nad e-mailovou adresou podľa týchto požiadaviek:

Typ S/MIME certifikátu	Kontrola na e-mailovou adresou	Identita právnickej osoby (organizácie)	Identita fyzickej osoby
S/MIME pre podpis fyzická osoba [Individual-validated]	sekcia 3.2.2	NA	sekcia 3.2.4
S/MIME pre podpis zamestnanec PO [Sponsor-validated]	sekcia 3.2.2	sekcia 3.2.3	sekcia 3.2.4
S/MIME certifikát pre pečať [Organization-validated]	sekcia 3.2.2	sekcia 3.2.3	NA

3.2.1 Preukazovanie vlastníctva súkromného kľúča

Žiadne ustanovenia.

3.2.2 Overenie kontroly nad e-mailovou adresou

Táto časť definuje procesy a postupy na potvrdenie kontroly žiadateľa nad e-mailovou adresou, ktorá má byť zahrnutá vo vydávanom certifikáte.

RA Poskytovateľa musí overiť, že Žiadateľ kontroluje e-mailovú adresu, na ktorú sa odkazuje v žiadosti o certifikát.

Poskytovateľ nemôže delegovať overovanie kontroly nad e-mailovou adresou tretej strane. Toto sa netýka zmluvne viazaných RA, ktoré poskytujú dôveryhodné služby v mene Poskytovateľa.

RA Poskytovateľa musia viesť záznamy o tom, aká metóda bola použitá na overenie e-mailovej adresy vrátane verzie S/MIME Baseline requirements [1], ktorá bola pri overovaní použitá.

RA Poskytovateľa môže použiť vykonané overenie na vydanie viacerých certifikátov pri dodržaní časových intervalov daných v sekcii 4.2.1.

Poznámka: E-mailová adresa môže byť uvedená v certifikáte držiteľa ako „*rfc822Name*“ alebo „*otherName*“ typu „*id-on-SmtpUTF8Mailbox*“ v rozšírení „*subjectAltName*“.

3.2.2.1 Overenie kontroly nad e-mailovou adresou prostredníctvom domény

Pri vydávaní certifikátu pre zmluvného partnera typu „sponsor-validated“, kde nebude vykonávané overovanie e-mailovej adresy pre každého žiadateľa jednotlivo je možné vykonať overenie kontroly nad e-mailovou adresou overením, že zmluvný partner má kontrolu nad doménovou časťou e-mailovej adresy, ktorá sa má použiť v certifikáte.

Na vykonanie tohto overenia musí Poskytovateľ použiť iba schválené metódy uvedené v sekcii 3.2.2.4 dokumentu [13].

3.2.2.2 Overenie kontroly nad e-mailovou adresou prostredníctvom e-mailu

RA Poskytovateľa môže overiť kontrolu nad poštovou schránkou, pre každú e-mailovú adresu, ktorá má byť zahrnutá vo vydávanom S/MIME certifikáte odoslaním náhodnej hodnoty e-mailom a následným prijatím potvrdzujúcej odpovede s použitím náhodnej hodnoty.

Kontrola nad každou e-mailovou adresou musí byť potvrdená za použitia jedinečnej náhodnej hodnoty. Náhodná hodnota musí byť zaslaná iba na overovanú e-mailovú adresu a nesmie byť zdieľaná žiadnym iným spôsobom.

Náhodná hodnota musí byť v každom zasielanom e-maile jedinečná a môže zostať v platnosti na použitie v potvrdzujúcej odpovedi najviac 24 hodín od jej vytvorenia.

Náhodná hodnota sa musí zmeniť po každom výskyte e-mailu zaslaného CA na adresu poštovej schránky, avšak všetky relevantné náhodné hodnoty zaslané na rovnakú adresu poštovej schránky môžu zostať platné na použitie v potvrdzujúcej odpovedi počas doby platnosti uvedenej v tejto časti.

3.2.2.3 Overenie žiadateľa ako prevádzkovateľa zodpovedajúcich poštových serverov

Poskytovateľ túto metódu nepodporuje.

3.2.2.4 CAA záznam

Žiadne ustanovenia.

3.2.3 Autentifikácia identity organizácie (právnickej osoby)

Pri overovaní identity organizácie (právnickej osoby) zahrnutej v profiloch S/MIME certifikát pre zamestnanca právnickej osoby a S/MIME certifikát pre pečať musia byť dodržané požiadavky definované v nasledujúcich podkapitolách.

3.2.3.1 Zoznam atribútov identity organizácie

RA Poskytovateľa musia získať a uchovávať tieto dôkazy o identite organizácie (právnickej osoby), ak sú zahrnuté v certifikáte:

- Formálny názov
- Predpokladaný názov
- Organizačná zložka
- Adresa sídla
- Jurisdikcia založenia alebo registrácie
- Jedinečný identifikátor a jeho typ

Jedinečný identifikátor musí byť uvedený v subjekte certifikátu „*organizationIdentifier*“ v súlade s článkom 7.1.4.2.2 a prílohou A dokumentu [1].

3.2.3.2 Validácia identity organizácie (právnickej osoby)

3.2.3.2.1 Overenie mena, adresy a jedinečného identifikátora

RA Poskytovateľa si overí celé meno a adresu (ak sú zhrnuté v subjekte certifikátu) žiadateľa, právnickej osoby, prostredníctvom poskytnutej dokumentácie alebo komunikáciou aspoň s jedným z týchto:

1. Vládna agentúra spadajúca do jurisdikcie zriadenia, existencie alebo uznania právnickej osoby;
2. Odkaz na údaje identifikátora právnickej osoby (LEI);
3. Overenie zo strany RA Poskytovateľa alebo jeho zástupcu v sídle žiadateľa;
4. Osvedčenie, ktoré obsahuje kópiu podpornej dokumentácie na preukázanie právnej existencie Žiadateľa ako napr. osvedčenie o registrácii, stanovy, prevádzková zmluva, štatút alebo regulačný akt.

RA Poskytovateľa môže použiť dokumentáciu alebo komunikáciu popísanú v bodoch 1 až 4 na overenie identity a adresy Žiadateľa.

Organizácia (právnická osoba) so sídlom v Slovenskej republike musí preukázať svoju totožnosť výpisom z Obchodného registra Slovenskej republiky (https://www.orsr.sk/) príp. iného platného registra právnických osôb napr. Registra právnických osôb, podnikateľov a orgánov verejnej moci, ktorý vedie Štatistický úrad Slovenskej republiky (https://rpo.statistics.sk/). Zo strany RA 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. RA Poskytovateľa akceptujú aj elektronickú formu výpisu z použitého registra, ktorá

bude autorizovaná kvalifikovanou elektronickou pečaťou štátneho orgánu zodpovedajúceho za vedenie registra.

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 alebo registra právnických osôb, 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.

3.2.3.2.2 Overenie predpokladaného mena

Poskytovateľ podporuje len vydávanie certifikátu na riadne zaregistrované meno.

3.2.3.2.3 Zverejňovanie zdrojov overenia

RA Poskytovateľ musí overiť jedinečný identifikátor použitý v certifikáte v registri, ktorý vedie alebo autorizuje príslušný štátny úrad. Poskytovateľ musí zverejniť tento autorizovaný zdroj prostredníctvom vhodných a ľahko dostupných online prostriedkov (pozri sekcia 3.2.3.2.1).

3.2.4 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 Poskytovateľa 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 RA Poskytovateľa 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),
- ďalšie údaje uvedené v sekcii 3.2.4.1

RA Poskytovateľa musí pri spracúvaní osobných údajov a ich uchovávaní postupovať v zmysle platných právnych predpisov v súlade s ustanoveniami uvedenými v sekcii 9.4.

3.2.4.1 Získavanie identity fyzickej osoby

Poskytovateľ musí dokumentovať a zverejniť metódy, ktoré využíva a zhromažďuje na overenie identity fyzickej osoby.

3.2.4.1.1 Fyzický doklad totožnosti

Pri overovaní identity RA Poskytovateľa v súčasnosti akceptuje nasledovné doklady predkladané Držiteľom za jeho fyzickej účasti:

- občiansky preukaz,
- cestovný pas.

Zákazník/Držiteľ musí zároveň predložiť aj ďalší doklad, ktorý obsahuje minimálne meno a priezvisko Držiteľa a ďalší jeho osobný údaj (dátum narodenia, rodné číslo):

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

RA Poskytovateľa musí zaznamenať aj tieto údaje z dokladov:

- meno a priezvisko
- rodné číslo príp. dátum narodenia
- trvalé bydlisko
- číslo preukazu totožnosti,
- vydavateľa preukazu totožnosti,
- dátum platnosti preukazu totožnosti, ak je vyznačený.

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.

3.2.4.1.2 Digitálny doklad o identite

Poskytovateľ momentálne nepodporuje tento spôsob prvotného overovania identity fyzickej osoby.

3.2.4.1.3 Schéma elektronickej identifikácie (eID)

Poskytovateľ momentálne nepodporuje tento spôsob prvotného overovania identity fyzickej osoby.

3.2.4.1.4 Certifikát elektronického podpisu vytvoreného Žiadateľom

Poskytovateľ momentálne nepodporuje tento spôsob prvotného overovania identity fyzickej osoby.

3.2.4.1.5 Záznamy firemnej RA

V prípade certifikátov vydávaných zamestnancom zmluvného partnera firemnou RA sú zdrojom identity zamestnanca záznamy vedené zmluvným partnerom. Zmluvný partner musí viesť záznamy v súlade s požiadavkami článkov 1.3.2 a 8.8.

3.2.4.1.6 Potvrdenie právnickej osoby o príslušnosti

V prípade certifikátov pre zamestnanca právnickej osoby, ktoré nie sú vydávané firemnou RA, môže RA overiť príslušnosť držiteľa k danej právnickej osobe, ktorá má byť zahrnutá v časti „*subject:organizationName*“, na základe potvrdenia poskytnutého touto právnickou osobou. RA však musí overiť identitu jednotlivca v súlade s článkom 3.2.4 a identitu organizácie v súlade s článkom 3.2.3.

3.2.4.1.7 Všeobecné potvrdenie

Dôkaz o atribútoch identity jednotlivca môže byť získaný pomocou osvedčenia od kvalifikovaného právnika alebo notára v jurisdikcii Žiadateľa.

3.2.4.1.8 Autorizované referenčné zdroje ako doplnkový dôkaz

Dôkaz pre atribúty individuálnej identity musí byť založený aspoň na jednom zo zdrojov ako autoritatívny dôkaz: fyzický alebo digitálny doklad totožnosti, digitálny podpis podporovaný certifikátom, záznamy Enterprise RA alebo vhodné osvedčenie.

RA Poskytovateľa môže dodatočne zhromažďovať a overovať dodatočné dôkazy pomocou autorizovaných zdrojov, ako sú dodatočné úradné dokumenty, vládne alebo regulačné registre alebo národné registre obyvateľstva.

RA Poskytovateľa musí interne dokumentovať akceptované referenčné zdroje vrátane popisu dokumentov alebo atestácií akceptovaných ako doplnkový dôkaz.

3.2.4.2 Overenie identity fyzickej osoby

RA Poskytovateľa musí overiť všetky atribúty fyzickej osoby, ktoré majú byť zahrnuté v certifikáte. Ak má použitý dôkaz explicitnú dobu platnosti, tak RA Poskytovateľa overí, že čas overenia identity je v rámci obdobia platnosti dôkazu napr. občianskeho preukazu, pasu ap. V kontexte to môže zahŕňať atribúty „*notBefore*“ a „*notAfter*“ položky v certifikáte elektronického podpisu alebo dátum skončenia platnosti dokladu totožnosti.

RA Poskytovateľa môže opätovne použiť existujúce dôkazy na overenie identity fyzickej osoby v súlade s časovými obmedzeniami uvedenými v sekcii 4.2.1.

3.2.4.2.1 Validácia predložených dokladov vo fyzickej podobe

Musí byť predložený originálny doklad. RA Poskytovateľa akceptuje len osobne predložený doklad a nepodporuje jeho vzdialené overovanie napr. cez kameru.

Pracovník RA Poskytovateľa musí vykonať vizuálne porovnanie fyzického vzhľadu žiadateľa s fotografiou tváre a/alebo inými informáciami uvedenými v doklade totožnosti.

Pracovník RA Poskytovateľa musí byť oboznámený, kde sú dostupné hodnoverné informácie o vzhľade dokladu.

Poskytovateľ resp. RA Poskytovateľa si uchovávajú všetky informácie dostatočné na preukázanie splnenia procesu overenia identity a overených atribútov. Okrem osobných údajov si Poskytovateľ uchováva aj typ identifikačného dokladu, sériové číslo, jeho vydavateľa a dobu platnosti.

3.2.4.2.2 Validácia digitálneho dokladu o identite

Poskytovateľ momentálne nepodporuje tento spôsob prvotného overovania identity fyzickej osoby.

3.2.4.2.3 Validácia schémy elektronickej identifikácie (eID)

Poskytovateľ momentálne nepodporuje tento spôsob prvotného overovania identity fyzickej osoby.

3.2.4.2.4 Validácia certifikátu elektronického podpisu vytvoreného Žiadateľom

Poskytovateľ momentálne nepodporuje tento spôsob prvotného overovania identity fyzickej osoby.

3.2.4.2.5 Validácia potvrdenia

Pokiaľ sa na potvrdenie používa ako dôkaz na validáciu atribútov identity fyzickej osoby, potom je jeho spoľahlivosť musí overiť v zmysle sekcie 3.2.8.

3.2.4.2.6 Validácia prostredníctvom záznamov firemnej RA

Firemná RA, ktorá vydáva certifikát pre podpis typu „sponsor-validated“, musí overiť všetky atribúty identity fyzickej osoby, ktoré majú byť zahrnuté v certifikáte. Firemná RA sa môže spoliehať pri overovaní identity jednotlivca na svoje existujúce interné záznamy.

3.2.5 Neoverované informácie o Držiteľovi

Informácie o žiadateľovi, ktoré neboli overené v súlade s touto CP nesmú byť uvedené v certifikátoch.

3.2.6 Potvrdenie autority

Pred začatím vydávania certifikátov pre zamestnanca právnickej osoby a certifikátov pre pečať musí Poskytovateľa použiť spoľahlivý spôsob komunikácie na overenie oprávnenia a schválenia zástupcu žiadateľa na vykonanie jedného alebo viacerých z nasledujúcich:

- pôsobiť ako Firemná RA;

- požiadať o vydanie alebo zrušenie Certifikátov; alebo
- prideliť povinnosti iným, aby konali v týchto rolách.

Poskytovateľ môže zaviesť proces, ktorý umožní Žiadateľovi určiť jednotlivcov, ktorí môžu priebežne pôsobiť ako zástupcovia žiadateľa. Rovnako Poskytovateľ poskytne Žiadateľovi zoznam svojich oprávnených Zástupcov Žiadateľa na základe overenej písomnej žiadosti Žiadateľa.

Poskytovateľ môže použiť zdroje uvedené v časti 3.2.3.2.1 na overenie spoľahlivej metódy komunikácie. Za predpokladu, že Poskytovateľ používa spoľahlivý spôsob komunikácie, môže overiť pravosť Žiadosti o certifikát priamo u zástupcu Žiadateľa alebo u dôveryhodného zdroja v rámci organizácie Žiadateľa, ako sú obchodné úseky žiadateľa, úseky ľudských zdrojov, úseky informačných technológií alebo iné oddelenie, ktoré Poskytovateľ považuje za vhodné.

3.2.7 Kritériá interoperability

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

3.2.8 Spoľahlivosť overovacích zdrojov

Predtým ako sa RA Poskytovateľa spoľahne na zdroj overovacích údajov pri overovaní žiadosti o certifikát musí overiť jeho vhodnosť ako spoľahlivého zdroja údajov.

Záznamy firemnej RA sú spoľahlivým zdrojom pre atribúty fyzickej osoby zahrnuté v certifikátoch pre podpis typu „sponsor-validated“ vydávaných v rámci organizácie, ktorá je firemnou RA Poskytovateľa.

RA Poskytovateľa sa spolieha na list potvrdzujúci, že informácie alebo iná skutočnosť sú správne v prípade, ak si overí, že list napísal účtovník, právnik, vládny úradník alebo iná spoľahlivá tretia strana v jurisdikcii Žiadateľa, na ktorých sa pri získavaní týchto informácií zvyčajne spolieha.

Potvrdenie musí obsahovať kópiu dokumentu potvrdzujúcu skutočnosť, ktorá sa má osvedčiť.

RA Poskytovateľa bude na kontaktovanie odosielateľa a na potvrdenie pravosti osvedčenia používať spoľahlivý spôsob komunikácie.

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

Žiadne ustanovenia.

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:

- S/MIME certifikát pre podpis fyzická osoba [Individual validated]:
  - fyzická osoba
- S/MIME certifikát pre podpis zamestnanec PO [Sponsor-validated]:
  - fyzická osoba splnomocnená Zákazníkom,
  - akákoľvek entita, s ktorou je fyzická osoba spojená napr. jej zamestnávateľ, nezisková organizácia, ktorej je členom ap.
- S/MIME certifikátu pre pečať [Organization-validated]:
  - akákoľvek entita, ktorá v zmysle platnej národnej legislatívy koná v mene danej právnickej osoby (organizácie).

4.1.2 Proces registrácie a zodpovednosti

4.1.2.1 Príprava

Zákazník musí vykonať nasledovné kroky ako prípravu na návštevu RA Poskytovateľa:

- Oboznámiť sa so „Všeobecnými podmienkami poskytovania a používania dôveryhodnej služby vydávania a overovania certifikátov“ (ďalej len „Všeobecné podmienky“) [8] a Informáciou o spracúvaní osobných údajov [14], 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 žiadosť o vydanie certifikátu vo formáte PKCS#10, ktorú zašle vopred elektronickou poštou RA Poskytovateľa (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. 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.

Žiadosť o certifikát pre fyzickú osobu musí byť zaslaná príslušnej RA Poskytovateľa elektronickou poštou vopred a z e-mailovej adresy, ktorá je uvedená v žiadosti o certifikát v položke e-mail.

Žiadosť o certifikát pre právnickú osobu musí byť zaslaná príslušnej RA Poskytovateľa elektronickou poštou vopred a z e-mailovej adresy, ktorá je uvedená v žiadosti o certifikát v položke e-mail. E-mailová adresa v žiadosti o certifikát pre právnickú osobu nesmie byť adresa fyzickej osoby. RA Poskytovateľa akceptuje len všeobecnú e-mailovú adresu právnickej osoby ako napr. obchod@disig.sk, faktury@disig.ak ap.

RA Poskytovateľa si vyhradzuje právo odmietnuť žiadosť o vydanie certifikátu pre právnickú osoby, kde táto požiadavka nebude splnená.

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 príslušnú RA Poskytovateľa (https://eidas.disig.sk/sk/kontakt/registracne-autority/), ktorá musí vykonať všetky procedúry súvisiace s procesom vydávania certifikátu.

4.2 Spracovanie žiadosti o certifikát

4.2.1 Vykonanie identifikácie a autentifikácie

Pred vydaním certifikátu musí RA Poskytovateľa:

- informovať prítomnú fyzickú osobu o Všeobecných podmienkach [8],
- skontrolovať úplnosť a správnosť údajov v prijatej žiadosti o certifikát,
- overiť totožnosť budúceho Držiteľa certifikátu a vložiť jeho osobné údaje do IS Poskytovateľa, pričom je povinný vyplniť všetky povinné položky vyžadované systémom Poskytovateľa,

- overiť ďalšie doklady na overenie ľubovoľných identifikačných údajov, ktoré sa majú dostať do certifikátu.

V prípade certifikátu pre fyzickú osobu alebo právnickú osobu, kde kryptografické kľúče nie sú v QSCD musí pracovník RA Poskytovateľa, pred overením totožnosti Držiteľa, skontrolovať doručenú žiadosť, ktorá môže byť vo formáte PKCS#10. Obsah položiek žiadosti a povinnosť ich vyplnenia pozri 7.

Pracovník RA Poskytovateľa musí overiť, či elektronicky zaslaná žiadosť o vydanie certifikátu daného Zákazníka obsahuje vyplnenú položku s e-mailovou adresou, a či bola zaslaná z rovnakej e-mailovej adresy, aká sa nachádza v žiadosti o vydanie certifikátu. V prípade zistených rozdielov môže odmietnuť vydanie certifikátu.

4.2.1.1 Overenie vlastníctva a kontroly e-mailovej adresy

Overenie vlastníctva a kontroly e-mailovej adresy prostredníctvom domény resp. overenie žiadateľa ako prevádzkovateľa zodpovedajúcich poštových serverov, ktoré bolo úspešne dokončené v súlade s požiadavkami sekcie 3.2.2.1 alebo sekcie 3.2.2.3 je možné získať najneskoršie 398 dní pred vydaním certifikátu.

Overenie vlastníctva a kontroly e-mailovej adresy, ktoré bolo úspešne ukončené v súlade s požiadavkami sekcie 3.2.2 je možné získať najneskoršie 30 dní pred vydaním certifikátu.

4.2.1.2 Overenie identity organizácie

Overenie kontroly, ktoré bolo úspešne dokončené v súlade s požiadavkami sekcie 3.2.3 je možné získať najneskoršie 825 dní pred vydaním certifikátu.

Potvrdenie autority v súlade s požiadavkami sekcie 3.2.6 je možné získať najneskôr 825 dní pred vydaním certifikátu, pokiaľ zmluva medzi Poskytovateľom a Žiadateľom/Zákazníkom neurčuje iný termín.

4.2.1.3 Overenie identity fyzickej osoby

Úplné overenie identity fyzickej osoby v súlade s článkom 3.2.4 je možné získať najneskôr 825 dní pred vydaním certifikátu. Predchádzajúca validácia sa nesmie opätovne použiť, ak boli akékoľvek údaje alebo dokumenty použité pri predchádzajúcej validácii získané skôr ako je povolený čas na ich opätovné použitie.

4.2.2 Schválenie alebo zamietnutie žiadosti o certifikát

Žiadne ustanovenia.

4.2.3 Čas na spracovanie žiadosti o certifikát

Žiadne ustanovenia.

4.3 Vydanie certifikátu

4.3.1 Činnosť CA pri vydávaní certifikátu

Vydanie certifikátu koreňovou CA si vyžaduje prítomnosť minimálne dvoch osôb v dôveryhodných roliach (napr. systémový administrátor CA, administrátor CA,

manažér CA), z ktorých jedna zadá jednoznačný príkaz, že koreňová CA Disig Root R2 má vykonať podpis certifikátu.

4.3.2 Informovanie Držiteľa o vydaní certifikátu

Žiadne ustanovenia.

4.4 Prevzatie certifikátu

4.4.1 Spôsob prevzatia certifikátu

Žiadne ustanovenia.

4.4.2 Zverejňovanie certifikátu

Žiadne ustanovenia.

4.4.3 Oznámenie o vydaní certifikátu iným subjektom

Žiadne ustanovenia.

4.5 Kľúčový pár a používanie certifikátu

4.5.1 Použitie súkromného kľúča a certifikátu držiteľa

Pozri sekcia 9.6.3, ustanovenia 2 a 4.

4.5.2 Použitie verejného kľúča a certifikátu spoliehajúcu sa stranou

Žiadne ustanovenia.

4.6 Obnova certifikátu

Pri vydávaní S/MIME certifikátu ide vždy o vydanie nového certifikátu na novo vygenerované kľúče, kde sa postupuje v zmysle ustanovení uvedených v sekcii 4.1 až 4.5.

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

Pri vydávaní S/MIME certifikátu ide vždy o vydanie nového certifikátu na novo vygenerované kľúče, kde sa postupuje v zmysle ustanovení uvedených v sekcii 4.1 až 4.5.

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 Spracovanie žiadosti 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 získa dôkaz prostredníctvom preukázateľnej alebo osvedčenej metódy, že je možné jednoducho vypočítať súkromný kľúč na základe znalosti verejného kľúča certifikátu napr. Debian week key (https://wiki.debian.org/SSLkeys)
- Poskytovateľ získa dôkaz, že sa nemôže spoľahnúť na overenie vlastníctva a kontroly nad e-mailovou adresou uvedenou 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 článkov 6.1.5 a 6.1.6,
- Poskytovateľ získa dôkaz, že došlo k jeho zneužitiu,
- Poskytovateľ zistí, že Držiteľ certifikátu nedodržuje svoje povinnosti Držiteľa certifikátu, ktorými je zmluvne viazaný,

- Poskytovateľ je informovaný o okolnostiach, ktoré naznačujú, že používanie e-mailovej adresy alebo plne kvalifikovaného názvu domény (FQDN) v certifikáte už nie je zo zákona povolené napr. súd alebo rozhodca zrušil právo používať e-mailovú adresu alebo doménové meno, príslušná licenčná alebo služobná zmluva medzi odberateľom bola ukončená, alebo držiteľ účtu nesplnil podmienky na udržanie aktívneho stavu e-mailovej adresy alebo doménového mena
- 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,
- zaniklo právo Poskytovateľa vydávať certifikáty v zmysle tejto CP, alebo bolo zrušené alebo došlo k ukončeniu vydávania, pokiaľ Poskytovateľ neprijal opatrenia na zaistenie kontinuity poskytovania CRL/OCSP repozitárov,
- zrušenie je vyžadované ustanoveniami CP a/alebo príslušnými CPS,
- Poskytovateľ je informovaný na základe preukázateľnej alebo overenej metódy, že súkromný kľúč Držiteľa je vystavený kompromitácii, alebo existuje jasný dôkaz, že konkrétna metóda použitá na generovania kľúča bola chybná.

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 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 články 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,
- zaniklo právo vydávajúcej CA alebo podriadenej CA Poskytovateľa vydávať certifikáty v zmysle tejto CP, alebo bolo zrušené alebo došlo k ukončeniu vydávania, pokiaľ Poskytovateľ neprijal opatrenia na zaistenie kontinuity poskytovania CRL/OCSP repozitárov,
- 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.

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),

Zákazníci, spoliehajúce sa strany, dodávatelia aplikačného softvéru a iné tretie strany môžu predkladať správy o problémoch s certifikátom, ktoré informujú vydávajúcu CA o primeranom dôvode na zrušenie certifikátu.

4.9.3 Postup žiadosti o zrušenie certifikátu

V prípade splnenia podmienok autentifikácie Držiteľa certifikátu, ktorý žiada o jeho zrušenie, je možné žiadosť o zrušenie certifikátu podať:

- Osobne na pobočke RA prostredníctvom formulára „Žiadosť o zrušenie certifikátu“ dostupnom na RA – pracovník RA môže vyžiadať heslo na zrušenie certifikátu v prípade, ak osobou, ktorá žiada o zrušenie certifikátu nie je Držiteľ certifikátu, ale ním poverená osoba;
- Prostredníctvom elektronickej pošty – zaslaním elektronickej poštovej správy, podpísanej s využitím súkromného kľúča, tvoriaceho kľúčový pár s certifikátom, o zrušenie ktorého sa žiada. Obsahom správy musí byť jednoznačná vôľa na zrušenie certifikátu vyjadrená vetou „Žiadam týmto o zrušenie môjho certifikátu so sériovým číslom XXXXXX“;
- Prostredníctvom elektronickej pošty – zaslaním elektronickej poštovej správy (nemusí byť podpísaná). Obsahom správy musí byť jednoznačná vôľa na zrušenie certifikátu vyjadrená vetou „Žiadam týmto o zrušenie môjho certifikátu so sériovým číslom XXXXXX“. Pri takto zaslanej správe musí byť súčasťou mailu aj heslo na zrušenie certifikátu;
- Prostredníctvom poštovej zásielky spolu so zadaním hesla na zrušenie certifikátu zaslanej na adresu Poskytovateľa resp. príslušnej RA

Poskytovateľa, 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 Poskytovateľa, 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 sekcii 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 je povinný v priebehu 24 hodín od oznámenia problému s certifikátom 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 sekcii 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.

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 [8].

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. 3 obsahuje informácie o maximálnych požiadavkách na vydávanie.

Tabuľka č. 3: 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 nie viac ako 10 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

Ak je poskytovaná služba OCSP, tak musí byť v súlade s požiadavkami RFC 6960 [15] a/alebo RFC 5019 [16]. OCSP odpoveď musí byť podpísaná:

- CA, ktorá vydala certifikát, ktorého stav zrušenia sa kontroluje, alebo
- OCSP responderom, ktorého certifikát je podpísaný CA, ktorá vydala certifikát, ktorého stav zrušenia sa overuje.

V prípade použitia OCSP respondera musí podpisový certifikát obsahovať „*ocspSigning EKU (1.3.6.1.5.5.7.3.9)*“ a rozšírenie typu „*id-pkix-ocsp-nocheck*“, tak ako sú definované v RFC 6960 [15].

4.9.10 Požiadavky na OCSP overovanie

OSCP respondery Poskytovateľa musia podporovať metódu HTTP GET v súlade s RFC 6960 [15] a/alebo RFC 5019 [16].

Čas platnosti OCSP odpovede je rozdiel medzi položkami „*thisUpdate*“ a „*nexUpdate*“ vrátane. Na účely výpočtu sa 3600 sekúnd rovná jednej hodine

a rozdiel 86400 sekúnd sa rovná jednému dňu, pričom prestupné sekundy sa ignorujú.

Odpovede k stavu vydaných SMIME certifikátov:

- OCSP odpoveď musí mať interval platnosti väčší alebo rovný 8 hodín
- OCSP odpoveď musí mať interval platnosti menší alebo rovný 8 dní
- Pre OCSP odpovede platné menej ako šestnásť (16) hodín musí Poskytovateľ aktualizovať informácie poskytované prostredníctvom OCSP pred uplynutím polovice doby platnosti pred časom uvedeným v položke nextUpdate
- Pre OCSP odpovede platné šestnásť (16) alebo viac hodín musí Poskytovateľ aktualizovať informácie poskytované prostredníctvom OCSP najneskôr osem (8) hodín pred časom uvedeným v položke nextUpdate a nie neskôr ako štyri (4) dni po čase uvedenom v položke thisUpdate.

Pre stav certifikátov podriadených CA musí informácie poskytované prostredníctvom OCSP aktualizovať:

- minimálne každých dvanásť (12) mesiacov
- do dvadsaťštyri (24) hodín po zrušení certifikátu podriadenej CA

Ak OCSP responder dostane požiadavku na overenie stavu certifikátu so sériovým číslom, ktoré príslušná vydávajúca CA nevydala, tak OCSP responder nesmie odpovedať stavom „*good*“. Poskytovateľ by mal monitorovať OCSP responder na žiadosti obsahujúce sériové čísla, ktoré daná CA nevydala ako súčasť svojich bezpečnostných procesov týkajúcich sa OCSP.

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.

Zrušené certifikáty nesmú byť vynechané s CRL resp. OCSP minimálne do času exspirácie certifikátu.

4.10.2 Dostupnosť služieb

Poskytovateľ musí prevádzkovať udržiavať svoj systém poskytovania CRL a OCSP s takými zdrojmi, ktoré zabezpečia čas odozvy do desiatich (10) sekúnd alebo menej za normálnych prevádzkových podmienok.

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 minimálne nasledovné dôležité udalosti:

5.4.1.1 Udalosti týkajúce sa generovania a životného cyklu kľúčov vydávajúcich CA Poskytovateľa:

- generovanie, zálohovanie, uchovávanie, obnova, archivácia a likvidácia;
- žiadosť o vydanie, obnovu a zmenu kľúčov a ich zrušenie;

- schválenie a zamietnutie žiadosti na vydanie;
- udalosti riadenia životného cyklu kryptografických zariadení;
- vytváranie CRL;
- podpisovania OCSP odpovedí v zmysle požiadaviek článkov 4.9 a 4.10;
- 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;
- všetky overovacie činnosti dané v tejto politike a v CPS RA SMIME CA Disig;
- schválenie a odmietnutie žiadosti o vydanie;
- vydanie certifikátu;
- vytvorenie CRL;
- podpisovania OCSP odpovedí v zmysle požiadaviek článkov 4.9 a 4.10.

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*“ a „*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

Program týkajúci sa bezpečnosti Poskytovateľa musí zahŕňať každoročné hodnotenie rizika, ktoré:

- Identifikuje predvídateľné interné a externé hrozby, ktoré by mohli viesť k neoprávnenému prístupu, zverejneniu, zneužitiu, zmene alebo zničeniu akýchkoľvek údajov certifikátu alebo procesov správy certifikátov;
- Posúdi pravdepodobnosť a potenciálne škody z týchto hrozieb, berúc do úvahy citlivosť údajov certifikátu a procesov správy certifikátov;
- Posúdi dostatočnosť politík, postupov, informačných systémov, technológií a iných opatrení, ktoré má Poskytovateľ k dispozícii na boj proti takýmto hrozbám.

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 pri posudzovaní súladu s požiadavkami SMIME BR [1]. 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 páru kľúčov

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

Žiadne ustanovenia.

6.1.1.3 Generovanie kľúčových párov pre Držiteľov

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.) [17].

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

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.

6.2.1 Štandardy a opatrenia pre kryptografický modul

Žiadne ustanovenia.

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

Pozri sekcia 5.2.2.

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)
STRICT a MULTIPURPOSE	825 dní rokov

Na účely výpočtov sa deň meria ako 86 400 sekúnd. Akýkoľvek čas dlhší ako tento, vrátane zlomkových sekúnd a/alebo prestupných sekúnd, predstavuje ďalší deň.

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“ [18].

6.8 Využívanie časovej pečiatky

Žiadne ustanovenia.

7. Profily certifikátov a zoznamov zrušených certifikátov

7.1 Profily certifikátov

Poskytovateľ musí spĺňať technické požiadavky uvedené v článkoch 2.2; 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 certifikátu a rozšírenia; aplikácia RFC 6818

V tejto časti sú špecifikované požiadavky na obsah certifikátu a jeho rozšírenia.

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. 4: 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 R1, Root R2 ap.

Tabuľka č. 5: Použité rozšírenia (certificate extensions) v certifikáte koreňových CA Poskytovateľa

Rozšírenie / OID	Prítomnosť	Kritickosť
basicConstraints / 2.5.29.19	MUSÍ	**ÁNO**
keyUsage / 2.5.29.15	MUSÍ	**ÁNO**
subjectKeyIdentifier / 2.5.29.14	MUSÍ	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. 6: 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 napr. R2I2 Certification Service, R2I3 Certification Service ap.

Tabuľka č. 7: Použité rozšírenia (certificate extensions) v certifikáte podriadených CA Poskytovateľa

Rozšírenie / OID	Prítomnosť	Kritickosť
certificatePolicies / 2.5.29.32	MUSÍ	NIE
crlDistributionPoints / 2.5.29.31	MUSÍ	NIE
authorityInfoAccess / 1.3.6.1.5.5.7.1.1	MALO BY BYŤ	NIE
basicConstraints / 2.5.29.19	MUSÍ	**ÁNO**
keyUsage / 2.5.29.15	MUSÍ	**ÁNO**
extKeyUsage/ 2.5.29.37	MUSÍ	NIE
Authority Key Identifier / 2.5.29.35	MUSÍ	NIE
subjectKeyIdentifier / 2.5.29.14	MUSÍ	NIE

7.1.2.3 Rozšírenia v certifikátoch 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. 8 obsahuje použité rozšírenia nachádzajúce sa v jednotlivých typoch vydávaných certifikátov

Tabuľka č. 8: 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}	Musí obsahovať jeden rezervovaný identifikátor politiky uvedený v sekcii 7.1.6	MUSÍ	NIE
CRL Distribution Points {id-ce-CRLDistributionPoints} {2.5.29.31}	Profily úrovne „Strict“ a „Multipurpose“ musia obsahovať aspoň jeden distribučný bod s uvedením plnej URI adresy. Všetky uvedené URI musia mať URI schému HTTP. Ine schémy nie sú povolené.	MUSÍ	NIE
AuthorityInfoAccess {id-pe-authorityInfoAccess} {1.3.6.1.5.5.7.1.1}	1. id-ad-ocsp: Rozšírenie MÔŽE obsahovať jednu alebo viacero hodnôt accessMethod typu id-ad-ocsp, ktoré špecifikujú URI OCSP respondera vydávajúcej CA. Profily úrovne „Strict“ a „Multipurpose“ musia obsahovať pre každú uvedenú metódu URI schému HTTP. Ine schémy nie sú povolené. 2. id-ad-calssuers:	MALO BY BYŤ	NIE

	Mal by obsahovať aspoň jednu hodnotu accessMethod typu id-ad-calssuers, ktorá špecifikuje URI certifikátu vydávajúcej CA. Profily úrovne „Strict“ a „Multipurpose“ musia obsahovať pre každú uvedenú metódu URI schému HTTP. Ine schémy nie sú povolené.		
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}	Profil úrovne „STRICT“: len pre podpisovanie, MUSÍ byť prítomná bitová pozícia pre „digitalSignature“. SMIE byť uvedená bitová pozícia pre „nonRepudiation“. Len pre správu kľúčov MUSIÍ byť bitová pozícia nastavené na „keyEncipherment“. Pri duálnom použití BY sa bitové pozície MALI nastaviť pre „digitalSignature“ a „keyEncipherment“a SMÚ byť nastavené pre „nonRepudiation“. Profil úrovne „MULTIPURPOSE“: platí to isté ako pre „STRICT“ s tým, že pre duálne použitie môže byť ešte nastavená bitová pozícia pre „dataEncipherment“ Iné bitové pozície NESMÚ byť uvedené.	MUSÍ	MAL BY BYŤ
Extended Key Usage {id-ce-extKeyUsage} [2.5.29.37]	Profil úrovne „STRICT“: MUSÍ byť prítomné id-kp-emailProtection. Iné hodnoty NESMÚ byť prítomné. Profil úrovne „MULTIPURPOSE“: MUSÍ byť prítomné id-kp-emailProtection. MÔŽU byť prítomné aj iné hodnoty. Hodnoty id-kp-serverAuth, id-kp-codeSigning, id-kp-timeStamping a anyExtendedKeyUsage NESMIE byť prítomné v žiadnom profile	MUSÍ	NIE
Authority Key Identifier {id-ce-authorityKeyIdentifier} {2.5.29.35}	MUSÍ byť prítomné pole keyIdentifier. Polia AuthorityCertIssuer a AuthorityCertSerialNumber NESMÚ byť prítomné.	MUSÍ	NIE
subjectAltName id-ce-subjectAltName [2.5.29.17]	Hodnota tohto rozšírenia MUSÍ byť zakódovaná tak, ako je špecifikované v časti 7.1.4.	MUSÍ	NIE
Subject Key Identifier {id-ce-subjectKeyIdentifier} {2.5.29.14}	MAL by obsahovať hodnotu, ktorá je odvodená od verejného kľúča zahrnutého v účastníckom certifikáte.	MALO BY BYŤ	NIE

7.1.2.4 Všetky certifikáty

Všetky polia a rozšírenia v certifikáte by mali byť nastavené v súlade s RFC 5280 [19]. Poskytovateľ nesmie vydať certifikát, ktorý obsahuje iné hodnoty použité v keyUsage a extKeyUsage a rozšírenia (Cerificate extensions), alebo iné údaje, ktoré nie sú špecifikované v článkoch 7.1.2.1 alebo 7.1.2.3 pokiaľ si Poskytovateľ nie je vedomý zaradenia týchto údajov do certifikátu. Ak Poskytovateľ zahŕňa polia alebo rozšírenia v certifikáte, ktoré nie sú špecifikované, ale sú inak povolené týmito požiadavkami, potom musí dokumentovať procesy a postupy, ktoré CA používa na validáciu informácií obsiahnutých v takýchto poliach a rozšíreniach v tomto CP alebo zodpovedajúcom CPS.

Poskytovateľ nesmie vydať certifikát s:

- Obsahujúci rozšírenia, ktoré sa neuplatňujú v kontexte verejného internetu
- Obsahujúci hodnoty poľa a rozšírenia, ktoré neboli overené v zmysle procesov a postupov popísaných v tejto CP alebo zodpovedajúcich CPS.

7.1.3 Identifikátory použitých algoritmov

7.1.3.1 SubjectPublicKeyInfo

Tieto požiadavky sa vzťahujú na položku „*subjectPublicKeyInfo*“ v certifikáte. Nie je povolené žiadne iné kódovanie.

7.1.3.1.1 RSA

RSA kľúčový pár musí byť označený prostredníctvom identifikátora algoritmu „*rsaEncryption* (OID: 1.2.840.113549.1.1.1)“. Parametre musia byť prítomné a musia mať explicitnú hodnotu „*NULL*“.

Poskytovateľ nesmie používať iný identifikátor algoritmu na označenie RSA kľúčového páru ako napr. *id-RSASSA-PSS* (OID: 1.2.840.113549.1.1.10).

Zakódovaný identifikátor algoritmu pre RSA kľúčový pár musí byť byte po byte identická s týmto hex-kódovaným zápisom: *300d06092a864886f70d0101010500*.

7.1.3.1.2 ECDSA

Poskytovateľ nevydáva certifikáty na takýto typ kľúčov.

7.1.3.1.3 EdDSA

Poskytovateľ nevydáva certifikáty na takýto typ kľúčov.

7.1.3.2 Identifikátor algoritmu podpisu

Všetky objekty podpísané súkromným kľúčom CA Poskytovateľa musia vyhovovať týmto požiadavkám na použitie „*AlgorithmIdentifier*“ alebo odvodené typy „*AlgorithmIdentifier*“ odvodené v kontexte podpisov. Platí to najmä pre všetky tieto objekty a polia:

- Pole „*signatureAlgorithm*“ certifikátu.
- Pole podpisu „*TBSCertifikátu*“ (napríklad ako ho používa certifikát).
- Pole „*signatureAlgorithm*“ zoznamu „*CertificateList*“

- Pole podpisu „*TBSCertList*“
- Pole „*signatureAlgorithm*“ v BasicOCSPResponse.

Pre tieto polia nie sú povolené žiadne iné kódovania.

7.1.3.2.1 RSA

CA Poskytovateľa musí použiť jeden z týchto podpisových algoritmov a kódovaní. Zakódovaný „*AlgorithmIdentifier*“ musí byť bajt za bajtom identický so špecifikovanými hex-kódovanými bajtmi.

AlgorithmIdentifier	Encoding:
RSASSA-PKCS1-v1_5 with SHA-256	300d06092a864886f70d01010b0500
RSASSA-PKCS1-v1_5 with SHA-384	300d06092a864886f70d01010c0500
RSASSA-PKCS1-v1_5 with SHA-512	300d06092a864886f70d01010d0500
RSASSA-PSS with SHA-256, MGF-1 with SHA-256, and a salt length of 32 byt	304106092a864886f70d01010a3034 a00f300d06096086480165030402010500a11c301a06092a864886f70d010108300d06096086480165030402010500a203020120
RSASSA-PSS with SHA-384, MGF-1 with SHA-384, and a salt length of 48 bytes	304106092a864886f70d01010a3034 a00f300d06096086480165030402020500a11c301a06092a864886f70d010108300d06096086480165030402020500a203020130
RSASSA-PSS with SHA-512, MGF-1 with SHA-512, and a salt length of 64 bytes:	304106092a864886f70d01010a3034 a00f300d06096086480165030402030500a11c301a06092a864886f70d010108300d06096086480165030402030500a203020140

7.1.3.2.2 ECDSA

Poskytovateľ nepoužíva tento podpisový algoritmus.

7.1.3.2.3 EdDSA

Poskytovateľ nepoužíva tento podpisový algoritmus.

7.1.4 Formy mien

Hodnoty atribútov musia byť kódované v zmysle RFC 5280 [19].

7.1.4.1 Kódovanie názvu

Pre každú platnú certifikačnú cestu (ako je definovaná v RFC 5280, sekcia 6):

- Pre každý certifikát v certifikačnej ceste musí byť obsah poľa „*Issuer Distinguished Name*“ zakódovaný bajt po bajte identicky so zakódovanou formou poľa „*Subject Distinguished Name*“ certifikátu vydávajúcej CA.
- Pre každý certifikát CA v certifikačnej ceste musí byť obsah poľa „*Subject Distinguished Name*“ certifikátu zakódovaný bajt po bajte identicky medzi všetkými certifikátmi, ktorých „*Subject Distinguished Names*“ možno

považovať za rovnocenné podľa RFC5280 [19], časť 7.1, vrátane certifikátov s ukončenou platnosťou a zrušených certifikátov.

7.1.4.2 Informácie o subjekte – certifikáty koncových držiteľov

CA Poskytovateľa vydaním certifikátu prehlasuje, že dodržala postupy uvedené v tejto CP alebo príslušných CPS, aby overila, že všetky údaje o subjekte certifikátu boli v čase vydania presné.

Poskytovateľ nesmie vložiť e-mailovú adresu do položky pre e-mail pokiaľ nebola overená v zmysle sekcie 3.2.2.

Atribúty subjektu certifikátu nesmú obsahovať iba samotné metadáta ako sú napr. znaky „.“ (bodka), „-„(pomlčka) a „ „ (medzera) a alebo akékoľvek iné označenie, že hodnota chýba, je neúplná alebo sa nedá použiť.

7.1.4.2.1 Rozšírenie „*Subject alternative name*“

Položka certifikátu	Vyžadovaná/ Voliteľná	Obsah
extensions:subjectAltName	Musí byť Prítomná	Toto rozšírenie musí obsahovať aspoň jednu položku *GeneralName* z týchto typov: ▪ Rfc822Name a/alebo ▪ otherName typu id-on-SmtpUTF8Mailbox, zakódované v súlade s RFC 8398

7.1.4.2.2 Položky rozlišovacieho mena subjektu (Distinguished Name)

Poskytovateľ vydáva tieto typy SMIME certifikátov:

- SMIME certifikát pre podpis
  - Individual-validated (STRICT a MULTIPURPOSE)
  - Sponsor-validated (STRICT a MULTIPURPOSE)
- S/MIME certifikát pre pečať (STRICT a MULTIPURPOSE)

V jednotlivých typoch SMIME certifikátov sú uvádzané tieto položky:

Položka	SMIME certifikát pre podpis				S/MIME certifikát pre pečať	
	Individual-validated		Sponsor-validated		Organization-validated	
	Multipurpose	Strict	Multipurpose	Strict	Multipurpose	Strict
commonName	**ÁNO**	**ÁNO**	**ÁNO**	**ÁNO**	**ÁNO**	**ÁNO**
givenName	**ÁNO**	**ÁNO**	**ÁNO**	**ÁNO**		
surname	**ÁNO**	**ÁNO**	**ÁNO**	**ÁNO**		
serialNumber	**ÁNO**	**ÁNO**	**ÁNO**	**ÁNO**		
countryName	**ÁNO**	**ÁNO**	**ÁNO**	**ÁNO**	**ÁNO**	**ÁNO**
organizationName			**ÁNO**	**ÁNO**	**ÁNO**	**ÁNO**
organizationIdentifier			**ÁNO**	**ÁNO**	**ÁNO**	**ÁNO**
localityName			**ÁNO**	**ÁNO**	**ÁNO**	**ÁNO**
emailAddress	**ÁNO**	**ÁNO**	**ÁNO**	**ÁNO**	**ÁNO**	**ÁNO**

a) Položka certifikátu „*subject:commonName* (OID 2.5.4.3)“

Položka musí obsahovať niektorú z nižšie uvedených hodnôt overených v zmysle sekcie 3.2

Typ certifikátu	Obsah
Organization-validated	*subject:organizationName* alebo E-mailová adresa
Sponsor-validated	Meno osoby, Pseudonym, alebo E-mailová adresa
Individual-validated	Meno osoby, Pseudonym, alebo E-mailová adresa

Meno osoby by malo byť uvedené ako „*subject:givenName*“ a/alebo „*subject:surname*“. Meno osoby môže byť uvedené vo forme ako preferuje držiteľ alebo vo forme preferovanom Poskytovateľom, ale musí byť zmysluplnou reprezentáciou mena subjektu, ako je overené v časti 3.2.4.

Ak sa uvádza E-mailová adresa, tak musí obsahovať hodnotu *rfc822Name* alebo *otherName* typu *id-on-SmtpUTF8Mailbox* z *extensions:subjectAltName*.

Rovnako ako všetky ostatné atribúty certifikátu, „*subject:commonName*“ musí spĺňať horné hranice atribútov definované v RFC 5280 [19].

b) Položka certifikátu „*subject:organizationName* (OID 2.5.4.10)“

Musí obsahovať úplný názov organizácie (právnickej osoby) overený v zmysle 3.2.3. RA Poskytovateľa môže povoliť uvádzať v tejto položke aj názov organizácie, ktorý sa mierne líši napr. za použitia bežne používaných skratiek resp. vynechanie znaku „,“(čiarka) v názve resp. nahradenie diakritických znakov v názve v zmysle 3.1.4.1.

c) Položka certifikátu „*subject:organizationalUnitName* (OID: 2.5.4.11)“

Poskytovateľ uvádzanie tejto položky v certifikátoch nepodporuje.

d) Položka certifikátu „*subject:organizationIdentifier* (2.5.4.97)“

Položka musí obsahovať identifikátor právnickej osoby uvedený v identifikovanej registračnej schéme.

Položka „*subject:organizationIdentifier*“ musí byť zakódovaná ako PrintableString alebo UTF8String.

Použitá registračná schéma uvedená v certifikáte musí byť výsledkom overenia vykonaného v zmysle sekcie 3.2.3.

Registračná schéma bude uvádzaná v certifikáte pomocou tejto štruktúry:

- trojznakový identifikátor registračnej schémy (napr. NTR)
- dvojznakový identifikačný kód krajiny v zmysle ISO 3166, pre krajinu ku ktorej registračná schéma prináleží

Tieto registračné schémy sú považované za platné v zmysle požiadaviek [1] na použitie v položke *subject:organizationIdentifier*:

- NTR: Pre identifikátor pridelený národným alebo štátnym obchodným registrom právnickej osobe uvedenej „*subject:organizationName*“;
- DPH: Pre identifikátor pridelený vnútroštátnymi daňovými úradmi právnickej osobe uvedenej *v „subject:organizationName*“.
- PSD: Pre národné autorizačné číslo pridelené poskytovateľovi platobných služieb uvedenému v „*subject:organizationName*“ podľa smernice

o platobných službách (EÚ) 2015/2366; Používa sa rozšírená štruktúra definovaná v ETSI TS 119 495, sekcia 5.2.1.

- LEI: Pre identifikátor právnickej osoby, ako je špecifikovaný v ISO 17442 pre subjekt uvedený v „*subject:organizationName*“. Dvojmiestny kód krajiny ISO 3166 musí byť nastavený na „XG“.

Kód krajiny použitý v identifikátore registračnej schémy sa musí zhodovať s kódom „*subject:countryName*“ v certifikáte, ako je uvedené v časti 7.1.4.2.2.

e) Položka certifikátu „*subject:givenName* (2.5.4.42)“ a/alebo „*subject:surname* (2.5.4.4)“

Musí obsahovať meno fyzickej osoby overené podľa sekcie 3.2.4. Ak má osoba len jedno právne meno, tak sa musí uviesť v položke „*subject:surname*“. Ak je použitý „*subject:pseudonym*“, tak sa položky „*subject:givenName*“ a/alebo „*subject:surname*“ nesmú uvádzať.

f) Položka certifikátu „*subject:pseudonym* (2.5.4.65)“

Poskytovateľ nevydáva SMIME certifikáty obsahujúce položku „*subject:pseudonym*“.

g) Položka certifikátu „*subject:serialNumber* (2.5.4.5)“

Môže byť uvedená na rozlíšenie jedinečnosti Držiteľa certifikátu.

V certifikátoch pre podpis sa môže použiť identifikátor fyzickej osoby v súlade s ustanoveniami sekcie 5.1.3 ETSI EN 319412-1 [20].

Poskytovateľ musí potvrdiť, že fyzická osoba, ktorej identifikátor je uvedený zodpovedá osobe, ktorá je držiteľom certifikátu.

h) Položka certifikátu „*subject:emailAddress* (1.2.840.113549.1.9.1)“

Musí obsahovať jednu e-mailovú adresu overenú v zmysle sekcie 3.2.2.

i) Položka certifikátu „*subject:title* (2.5.4.12)“

Poskytovateľ uvádzanie tejto položky v certifikátoch nepodporuje.

j) Položka certifikátu „*subject:streetAddress* (OID: 2.5.4.9)“

Poskytovateľ uvádzanie tejto položky v certifikátoch nepodporuje.

k) Položka certifikátu „*subject:localityName* (OID: 2.5.4.7)“

Musí obsahovať informácie o lokalite subjektu overené v zmysle sekcie 3.2.3 pre certifikáty pre podpis typu „*sponsor-validated*“ alebo certifikáty pre pečať resp. v zmysle sekcie 3.2.4 pre certifikát pre podpis typu „*individual-validated*“.

l) Položka certifikátu „*subject:stateOrProvinceName* (OID: 2.5.4.8)“

Poskytovateľ uvádzanie tejto položky v certifikátoch nepodporuje.

m) Položka certifikátu „*subject:postalCode* (OID: 2.5.4.17)“

Poskytovateľ uvádzanie tejto položky v certifikátoch nepodporuje.

n) Položka certifikátu „*subject:countryName* (OID: 2.5.4.6)“

Položka musí obsahovať dvojpísmenový kód krajiny v zmysle ISO 3166-1 spojený so sídlom subjektu overeného podľa časti 3.2.3 pre certifikáty pre podpis typu

„sponsor-validated“ alebo certifikáty pre pečať resp. v zmysle sekcie 3.2.4 pre certifikát pre podpis typu „individual-validated“.

7.1.4.3 Informácie o subjekte – certifikát koreňovej CA a certifikát podriadenej CA

Vydaním certifikátu podriadenej CA Poskytovateľ prehlasuje, že postupoval podľa postupu uvedeného v tejto CP a/alebo príslušných CPS, aby overil, že ku dňu vydania certifikátu boli všetky informácie o subjekte uvedené v certifikáte presné.

7.1.4.3.1 Polia rozlišovacieho mena subjektu

a) Položka certifikátu „*subject:commonName* (OID 2.5.4.3)“

Táto položka musí byť uvedená a mala by obsahovať jedinečný názov certifikátu v rámci všetkých certifikátov vydaných vydávajúcou CA.

b) Položka certifikátu „*subject:organizationName* (OID 2.5.4.10)“

Táto položka musí byť uvedená a musí obsahovať buď názov certifikačnej alebo DBA meno, ktoré boli overené podľa sekcie 3.2.3.2.2. Poskytovateľ môže v tomto poli uviesť informáciu, ktorá sa mierne líšia od overeného názvu, ako sú bežné variácie alebo skratky.

c) Položka certifikátu „subject:countryName (OID: 2.5.4.6)“

Položka musí obsahovať dvojpísmenový kód krajiny v zmysle ISO 3166-1 pre krajinu, v ktorej sa nachádza miesto podnikania Poskytovateľa.

d) Ďalšie položky

V subjekte certifikátu sa môžu nachádzať aj iné atribúty. Ak sú prítomné, musia obsahovať informácie, ktoré Poskytovateľ overil.

7.1.5 Obmedzenia týkajúce sa mien

Certifikát podriadenej CA sa považuje za technicky obmedzený, keď obsahuje rozšírenie *Extended key Usage (EKU)*, ktoré špecifikuje všetky rozšírenia možnosti použitia kľúčov, pre ktoré je certifikát podriadenej autority oprávnený vydávať certifikáty.

EKU pre použitie kľúča v tvare *anyExtendedKeyUsage* sa nesmie použiť.

7.1.6 Identifikátor certifikačnej politiky

Tento článok popisuje požiadavky na identifikátory koreňovej CA, podriadenej CA a certifikátov pre koncových používateľov tuľkajúce sa identifikácie certifikačnej politiky.

7.1.6.1 Vyhradené identifikátory certifikačnej politiky

Tieto identifikátory certifikačnej politiky definované CA/Browser Forum sú vyhradené na použitie pre Poskytovateľa, aby potvrdili, že certifikát je v súlade s týmito požiadavkami.

Typ certifikátu	Subtyp	Identifikátor politiky
Certifikát pre podpis typ „Individual-validated“	STRICT	2.23.140.1.5.4.3
	MULTIPURPOSE	2.23.140.1.5.4.2
Certifikát pre podpis typ “Sponsor-validated“	STRICT	2.23.140.1.5.3.3
	MULTIPURPOSE	2.23.140.1.5.3.2
Certifikát pre pečať	STRICT	2.23.140.1.5.2.3
	MULTIPURPOSE	2.23.140.1.5.2.2

7.1.6.2 Certifikát koreňovej certifikačnej autority

Certifikát koreňovej certifikačnej autority by nemal obsahovať rozšírenie *certificatePolicies*. Ak obsahuje, tak rozšírenie musí spĺňať požiadavky stanovené pre certifikáty vydané podriadeným CA v súlade s článkom 7.1.6.3.

7.1.6.3 Certifikát podriadenej CA

Certifikát vydaný podriadenej CA, ktorá je pridruženou súčasťou Poskytovateľa, musí obsahovať niektorý z týchto dvoch identifikátorov politiky:

- Jeden alebo viacero explicitných identifikátorov politiky definovaných v časti 7.1.6.1, ktoré označujú dodržiavanie a súlad s požiadavkami danými v dokumente [1] zo strany podriadenej CA Poskytovateľa a môžu obsahovať jeden alebo viacero identifikátorov zdokumentovaných v tejto CP a/alebo CPS; alebo
- Identifikátor *„anyPolicy (2.5.29.32.0)“* - Podriadená CA a vydávajúca CA musia vo svojich CP a/alebo CPS vyhlásiť, že všetky certifikáty obsahujúce identifikátor politiky indikujúci súlad s požiadavkami danými v dokumente [1] sú vydané a spravované v súlade s nimi.

7.1.6.4 Certifikát koncového používateľa

Certifikát vydaný koncovému používateľovi musí obsahovať v rozšírení *certificatePolicies* jeden z identifikátorov politiky, ktoré sú uvedené v časti 7.1.6.1.

Certifikát môže obsahovať aj ďalšie identifikátory politiky definované Poskytovateľom. Poskytovateľ prehlasuje, že certifikáty, ktoré vydáva, obsahujúce špecifikované identifikátory politiky, sú spravované v súlade s požiadavkami tejto CP

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

Žiadne ustanovenia.

7.2.2 Použité rozšírenia (CRL extensions) v CRL vydávanom Poskytovateľom

Tabuľka č. 9 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. 9: Rozšírenia vydávaného CRL

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

* Ak sa CRL záznam týka koreňovej CA alebo certifikátu podriadenej CA, vrátane krížových certifikátov, toto rozšírenie v CRL musí byť prítomné. Ak sa záznam CRL týka certifikátu, ktorý nie je technicky schopný spôsobiť vydanie ďalšieho certifikátu, toto rozšírenie v CRL by mohlo byť prítomné, ale môže byť vynechané, ak sú dodržané nasledujúce požiadavky.

CRLreason of *certificateHold (6)* sa nesmie používať pre certifikáty koreňovej CA alebo podriadenej CA.

Uvedený dôvod v CRL nesmie byť *unspecified (0)*. Ak dôvod odvolania nie je špecifikovaný, CA vynechajú rozšírenie zadávania kódu dôvodu.

Úložisko môže obsahovať položky CRL, ktoré majú *CRLReason* typu *CertificateHold (6)* pre certifikáty, ktoré zahŕňajú identifikátory certifikačnej politiky pre typy S/MIME certifikátov *LEGACY* resp. *MULTIPURPOSE*. Úložisko nebude obsahovať CRL položky, ktoré majú CRLreason typu *certificateHold (6)* pre certifikáty, ktoré obsahujú identifikátory certifikačnej politiky pre typy S/MIME certifikátov *STRICT*.

Ak je prítomné rozšírenie záznamu *CRL ReasonCode*, *CRLReason* musí uvádzať najvhodnejší dôvod na zrušenie certifikátu, ako je definovaný v tejto CP SMIME.

Ak je prítomné, rozšírenie *reasonCode (OID 2.5.29.21)*, tak sa neoznačuje ako kritické.

7.3 Profil OCSP

Ak sa odpoveď OCSP týka koreňovej certifikačnej autority alebo certifikátu podriadenej certifikačnej autority vrátane krížových certifikátov a tento certifikát bol zrušený, v rámci *RevokedInfo* v *CertStatus* musí byť prítomné pole *revocationReason*.

Uvedená CRLReason ba mal obsahovať hodnotu povolenú pre CRL, ako je uvedené v časti 7.2.2.

7.3.1 Verzia

Žiadne ustanovenia.

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. 10: 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

„*singleExtensions*“ OCSP odpovede nesmie obsahovať „*reasonCode (OID 2.5.29.21)*“ z CRL zoznamu.

8. Audit zhody

Účelom auditu o zhode má byť záruka, že Poskytovateľ má vyhovujúci systém práce, ktorý garantuje kvalitu dôveryhodných služieb, ktoré Poskytovateľ poskytuje a taktiež garantuje, že koná v súlade so všetkými požiadavkami tejto CP, svojho CPS, požiadaviek Nariadenia eIDAS [3] a CA/Browser fórum [13]. Všetky aspekty prevádzky CA vzťahujúce sa k tejto CP majú byť predmetom auditov zhody.

Poskytovateľ musí:

- vydávať certifikáty a prevádzkovať svoje PKI v súlade so všetkými právnymi predpismi, ktoré sa vzťahujú na jej podnikanie, a certifikáty, ktoré vydáva v každej jurisdikcii, v ktorej pôsobí,
- dodržiavať požiadavky tejto CP,
- dodržovať požiadavky auditu uvedené v tomto články a
- byť licencovaný ako poskytovateľ dôveryhodných služieb (CA) v každej jurisdikcii, v ktorej pôsobí, ak zákon tejto jurisdikcie vyžaduje licenciu na vydávanie certifikátov.

8.1 Frekvencia auditu zhody pre danú entitu

Certifikáty, ktoré je možné použiť na vydávanie nových certifikátov musia byť buď technicky obmedzené v súlade s článkom 7.1.5 a auditované iba v súlade s článkom 8.8, alebo neobmedzené a plne auditované v súlade so všetkými zostávajúcimi požiadavkami tejto sekcie. Certifikát sa považuje za použiteľný na vydávanie nových certifikátov, ak obsahuje rozšírenie X.509v3 „*basicConstraints*“, pričom „*boolean cA*“ je nastavený na hodnotu „*true*“, a preto je podľa definície certifikátom koreňovej CA alebo certifikátom podriadenej CA.

Obdobie, počas ktorého Poskytovateľ vydáva certifikáty musí byť rozdelené do neprerušenej postupnosti období auditu. Obdobie auditu nesmie trvať dlhšie ako jeden rok.

Ak má Poskytovateľ aktuálne platnú správu o audite, ktorá uvádza súlad so schémou auditu uvedenou v sekcii 8.4, potom nie je potrebné žiadne hodnotenie pripravenosti pred vydaním.

Ak Poskytovateľ nemá aktuálne platnú správu o audite, ktorá uvádza súlad s jednou zo schém auditu uvedených v sekcii 8.4, potom pred vydaním verejne dôveryhodných SMIME certifikátov Poskytovateľ úspešne dokončí hodnotenie pripravenosti v danom čase v súlade s platnými normami v rámci jednej zo schém auditu uvedených v sekcii 8.4. Posúdenie pripravenosti k určitému bodu musí byť ukončené najskôr dvanásť (12) mesiacov pred vydaním SMIME certifikátov a musí po ňom nasledovať úplný audit podľa takejto schémy do deväťdesiatich (90) dní od vydania prvého SMIME certifikátu v zmysle tejto CP.

8.2 Identita audítora a kvalifikačné požiadavky na neho

Audit Poskytovateľa vykonáva kvalifikovaný audítor. Kvalifikovaný audítor znamená fyzickú osobu, právnickú osobu alebo skupinu fyzických alebo právnických osôb, ktoré spoločne majú tieto kvalifikácie a zručnosti:

- Nezávislosť od predmetu auditu;
- Schopnosť vykonať audit, ktorý sa zaoberá kritériami špecifikovanými v oprávnenej schéme auditu (pozri sekcia 8.4);
- Zamestnáva jednotlivcov, ktorí majú odbornosť v skúmaní technológie infraštruktúry verejného kľúča, nástrojov a techník informačnej bezpečnosti, informačnej technológie a bezpečnostného auditu a funkcie overovania treťou stranou;
- Pre audity vykonávané v súlade s ktoroukoľvek z noriem ETSI je akreditovaný v súlade s ISO 17065 uplatňujúcou požiadavky špecifikované v ETSI EN 319 403 alebo ETSI EN 319 403-1;
- Viazaný zákonom, nariadením vlády alebo profesijným etickým kódexom;
- Okrem prípadu internej vládnej audítorskej agentúry má poistenie profesijnej zodpovednosti/chyby a opomenutia s poistnými limitmi na krytie minimálne jeden milión amerických dolárov

8.3 Vzťah audítora k auditovanému subjektu

Pozri časť 8.2.

8.4 Témy pokryté audiom

Pre Obdobia auditu začínajúce po dátume účinnosti definovanom v sekcii 1.2.1 dokumentu [1] Poskytovateľ podstúpi audit v súlade s touto schémou:

- ETSI EN 319 411-1 v1.3.1 alebo novšia, ktorá zahŕňa normatívne odkazy na ETSI EN 319 401 (mala by sa použiť najnovšia verzia odkazovaných dokumentov ETSI);

Audit vykonáva kvalifikovaný audítor, ako je uvedené v časti 8.2.

8.5 Akcie vykonané na odstránenie nedostatkov

Žiadne ustanovenia.

8.6 Zaobchádzanie s výsledkami auditu

V audítorskej správe musí byť výslovne uvedené, že pokrýva príslušné systémy a procesy používané pri vydávaní všetkých certifikátov, ktoré uvádzajú jeden alebo viacero identifikátorov politiky uvedených v časti 7.1.6.1.

Poskytovateľ musí auditnú správu poskytnúť verejne, a to najneskôr do troch mesiacov po skončení obdobia auditu. V prípade omeškania dlhšieho ako tri

mesiace, Poskytovateľ musí poskytnúť vysvetľujúci list podpísaný kvalifikovaným audítorom.

Správa o audite MUSÍ obsahovať aspoň tieto jasne označené informácie:

- Názov organizácie, ktorá je predmetom auditu;
- Názov a adresa organizácie vykonávajúcej audit;
- SHA-256 odtlačok všetkých koreňových a podriadených certifikátov CA, vrátane krížových certifikátov, ktoré boli v rozsahu auditu;
- Kritériá auditu s číslom verzie (číslami), ktoré sa použili na audit každého z certifikátov (a súvisiacich kľúčov);
- Zoznam dokumentov politík Poskytovateľa s číslami verzií, na ktoré sa odkazuje počas auditu;
- Či audit hodnotil časové obdobie alebo časový bod;
- Začiatok a dátum ukončenia obdobia auditu pre tie, ktoré pokrývajú určité časové obdobie;
- Časový dátum pre tie, ktoré sú pre určitý čas;
- Dátum vydania správy, ktorý bude nevyhnutne po dátume ukončenia alebo časovom dátume;
- Pri auditoch vykonaných v súlade s ktoroukoľvek z noriem ETSI) vyhlásenie, v ktorom sa uvedie, či bol audit úplným auditom alebo dozorným auditom a ktoré časti kritérií boli aplikované a hodnotené, napr. ETSI EN 319 401, ETSI EN 319 411-1 politika LCP, NCP alebo NCP+, ETSI EN 319 411-2 politika QCP-n, QCP-n-qscd, QCP-l alebo QCP-l-qscd; a
- Pre audity vykonávané v súlade s ktoroukoľvek normou ETSI) vyhlásenie, ktoré uvádza, že audítor sa odvolal na príslušné kritériá CA/Browser Forum, ako je tento dokument, a na použitú verziu.

Kvalifikovaný audítor poskytuje oficiálnu anglickú verziu verejne dostupných informácií o audite a Poskytovateľ zabezpečí, aby boli verejne dostupné.

Správa o audite musí byť k dispozícii vo formáte PDF a musí byť v texte možné vyhľadávať všetky požadované informácie. Každý odtlačok SHA-256 v správe o audite musí byť veľkými písmenami a nesmie obsahovať dvojbodky, medzery ani posuny riadkov.

8.7 Interný audit

Počas obdobia, v ktorom Poskytovateľ vydáva certifikáty bude monitorovať dodržiavanie tejto CP a/alebo príslušných CPS a kontrolovať kvalitu svojich služieb vykonávaním vlastných auditov aspoň štvrťročne na náhodne vybranej vzorke zodpovedajúce väčšiemu počtu z tridsať (30) certifikátov alebo tri percentá (3 %) ním vydaných certifikátov v období, ktoré sa začína bezprostredne po odobratí predchádzajúcej vzorky na interný audit.

8.8 Preskúmanie externých a firemných RA

Žiadne ustanovenia.

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

Žiadne ustanovenia.

9.1.3 Poplatky za služby vydávania CRL a OCSP

Žiadne ustanovenia.

9.1.4 Poplatky za ostatné služby

Žiadne ustanovenia.

9.1.5 Vrátenie platby

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

9.2 Finančná zodpovednosť

9.2.1 Poistenie

Žiadne ustanovenia.

9.2.2 Iné aktíva

Žiadne ustanovenia

9.2.3 Poistenie a záruky pre Zákazníkov

Žiadne ustanovenia;

9.3 Dôvernosť

Žiadne ustanovenia.

9.3.1 Nechránené informácie

Žiadne ustanovenia.

9.3.2 Zodpovednosť za ochranu dôverných informácií

Žiadne ustanovenia.

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 [14].

Poskytovateľ zverejní zásady ochrany osobných údajov, ktoré poskytujú informácie o postupoch Poskytovateľa na ochranu údajov. Zásady ochrany osobných údajov by mali obsahovať informácie o tom, ako Poskytovateľ zhromažďuje, používa, zdieľa, ukladá a vymazáva alebo uchováva údaje, ako aj kontaktné údaje na uplatnenie práv na ochranu osobných údajov.

Zásady ochrany osobných údajov sú dostupné na:

https://eidas.disig.sk/pdf/info_oou_gdpr.pdf

9.4.2 Informácie považované za osobné údaje

Poskytovateľ zaobchádza so všetkými osobnými údajmi o fyzickej osobe, ktoré nie sú verejne dostupné v obsahu certifikátu, ako so súkromnými informáciami. Patria sem aj informácie, ktoré spájajú položku „*subject:pseudonym*„ so skutočnou identitou Držiteľa.

9.4.3 Informácie, ktoré nie sú považované za osobné údaje

Žiadne ustanovenia.

9.4.4 Zodpovednosť za ochranu osobných údajov

Poskytovateľ bude chrániť osobné údaje pomocou vhodných bezpečnostných opatrení a primeranej starostlivosti. Poskytovateľ bude vyžadovať to isté od všetkých poskytovateľov služieb, ktorí spracúvajú osobné údaje v mene Poskytovateľa.

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 [14].

9.4.6 Zverejnenie na základe súdneho alebo správneho procesu

Žiadne ustanovenia.

9.4.7 Ďalšie okolnosti zverejňovania informácií

Žiadne ustanovenia.

9.5 Práva duševného vlastníctva

Žiadne ustanovenia.

9.6 Vyhlásenie a záruky

9.6.1 Vyhlásenia a záruky Poskytovateľa

Vydaním certifikátu Poskytovateľ poskytuje záruky uvedené v tomto dokumente na nasledujúci príjemcom certifikátu:

- Držiteľ, ktorý je zmluvnou stranou zmluvy o poskytovaní dôveryhodných služieb;
- Všetci dodávatelia aplikačného softvéru, s ktorými Poskytovateľ uzatvoril zmluvu o zahrnutí jej certifikátu koreňovej CA do softvéru distribuovaného týmto dodávateľom aplikačného softvéru; a
- Všetky spoliehajúce sa strany, ktoré sa primerane spoliehajú na platný certifikát.

Poskytovateľ vyhlasuje a zaručuje príjemcom certifikátu, že počas doby platnosti certifikátu dodržiavala tieto svoju CP a príslušné CPS pri vydávaní a správe certifikátu.

Záruky týkajúce sa certifikátu konkrétne zahŕňajú, ale nie sú obmedzené na:

1. Právo používať e-mailovú adresu - Poskytovateľ v čase vydania:
   i. implementoval postup na overenie toho, že žiadateľ má právo používať alebo kontrolovať e-mailovú adresu uvedenú v subjekte certifikátu a rozšírení „subjectAltName“, alebo mu takéto právo alebo kontrolu udelil niekto, kto mal takéto právo používať alebo kontrolovať;
   ii. dodržal postup pri vydávaní certifikátu;
   iii. má presne popísaný postup v tejto CP a príslušných CPS;
2. Autorizáciu pre vydanie certifikátu – Poskytovateľ v čase vydania:
   i. zaviedol postup na overenie, či Žiadateľ autorizoval vydanie certifikátu, a či zástupca Žiadateľa je oprávnený v mene Žiadateľa žiadať o vydanie certifikátu;
   ii. dodržal postup pri vydávaní certifikátu;
   iii. má presne popísaný postup v tejto CP a príslušných CPS;
3. Presnosť informácií – Poskytovateľ v čase vydania:
   i. implementoval postup na overenie správnosti všetkých informácií obsiahnutých v certifikáte (s výnimkou atribútu „*subject:serialNumber*“);

ii. dodržal postup pri vydávaní certifikátu; a

iii. má presne popísaný postup v tejto CP a príslušných CPS;

4. Identitu žiadateľa - Poskytovateľ, ak certifikát obsahuje informácie o identite subjektu, tak:

i. implementoval postup na overenie totožnosti Žiadateľa v súlade s článkom 3.2 a článkom 7.1.4.2.2;

ii. dodržal postup pri vydávaní Certifikátu; a

iii. má presne popísaný postup v tejto CP a príslušných CPS;

5. Zmluva s Držiteľom - Ak Poskytovateľ a Držiteľ nie sú z tej istej organizácie, tak Držiteľ a Poskytovateľ sú zmluvnými stranami právoplatnej a vykonateľnej zmluvy o dôveryhodných službách (Ďalej len „Zmluva“), ktorá spĺňa požiadavky tejto CP, alebo ak sú Poskytovateľ a Držiteľ rovnaký subjekt, zástupca žiadateľa vzal na vedomie podmienky používania;

6. Stav certifikátu - Poskytovateľ udržiava 24 x 7 verejne prístupné úložisko s aktuálnymi informáciami o stave (platný alebo zrušený) všetkých certifikátov, ktorým neuplynula platnosť; a

7. Zrušenie certifikátu - Poskytovateľ zruší certifikát z akéhokoľvek dôvodu uvedeného v týchto požiadavkách.

9.6.2 Vyhlásenia a záruky RA

Žiadne ustanovenia.

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 [8].

Pred vydaním certifikátu Poskytovateľ na svoj výslovný prospech a prospech spoliehajúcich sa strán ako aj Žiadateľa získa:

1. Súhlas s Žiadateľa so zmluvou o poskytovaní dôveryhodných služieb, alebo

2. Potvrdenie o súhlase s Všeobecnými podmienkami [8].

Poskytovateľ musí implementovať proces, ktorý zabezpečí, že každá Zmluva alebo Všeobecné podmienky budú voči Žiadateľovi právne vymáhateľné. V oboch prípadoch sa Zmluva vzťahuje na Certifikát, ktorý sa má vydať na základe žiadosti o certifikát. Pre každú žiadosť o certifikát môže byť použitá samostatná Zmluva alebo jedna Zmluva môže byť použitá na pokrytie viacerých budúcich žiadostí o certifikát a výsledných certifikátov, pokiaľ sa na každý certifikát, ktorý CA vydá žiadateľovi, jasne vzťahuje táto Zmluva alebo Všeobecné podmienky [8].

Zmluva alebo Všeobecné podmienky musia obsahovať ustanovenia ukladajúce samotnému Žiadateľovi tieto povinnosti a záruky:

1. **Presnosť informácií** - Povinnosť a záruka poskytovať Poskytovateľovi vždy presné a úplné informácie, a to tak v žiadosti o certifikát, ako aj inak, ako to Poskytovateľ požaduje v súvislosti s vydaním certifikátu (certifikátov), ktorý má poskytnúť;

2. **Ochrana súkromného kľúča** - Povinnosť a záruka Žiadateľa prijať všetky primerané opatrenia na zabezpečenie kontroly, utajenia a náležitej ochrany súkromného kľúča, ktorý zodpovedá verejnému kľúču, ktorý má byť zahrnutý do požadovaného certifikátu a akékoľvek súvisiace aktivačné údaje alebo zariadenie, ako je heslo alebo token;

3. **Akceptácia certifikátu** - Záväzok a záruka, že Držiteľ skontroluje a overí správnosť obsahu certifikátu;

4. **Používanie Certifikátu** - Povinnosť a záruka používať certifikát len s e-mailovou adresou uvedenou v certifikáte a používať certifikát výlučne v súlade so všetkými platnými zákonmi a výlučne v súlade so Zmluvou alebo Všeobecnými podmienkami [8];

5. **Oznamovanie a zrušenie** - Povinnosť a záruka:

   i. okamžite požiadať o zrušenie certifikátu a prestať ho používať a jeho pridružený súkromný kľúč, ak dôjde k akémukoľvek skutočnému alebo podozreniu zo zneužitia alebo ohrozenia súkromného kľúča Držiteľa spojeného s verejným kľúčom zahrnutým v certifikáte, a

   ii. bezodkladne požiadať o zrušenie certifikátu a prestať ho používať, ak sú alebo sa stanú akékoľvek informácie v certifikáte nesprávne alebo nepresné;

6. **Ukončenie používania certifikátu** - Povinnosť a záruka okamžitého ukončenia používania súkromného kľúča zodpovedajúceho verejnému kľúču zahrnutému v certifikáte po zrušení tohto certifikátu z dôvodov ohrozenia kľúča.

7. **Schopnosť reagovať** - Povinnosť reagovať na pokyny Poskytovateľa týkajúce sa ohrozenia kľúča alebo zneužitia certifikátu v rámci stanoveného časového obdobia.

8. **Potvrdenie a akceptácia** - Potvrdenie a akceptovanie toho, že Poskytovateľ je oprávnený okamžite zrušiť certifikát, ak by Žiadateľ porušil podmienky Zmluvy alebo Všeobecných podmienok, alebo ak zrušenie vyžaduje táto CP a/alebo príslušná CPS Poskytovateľa.

9.6.4 Vyhlásenia a záruky spoliehajúcej sa strany

Žiadne ustanovenia.

9.6.5 Vyhlásenia a záruky iných strán

Žiadne ustanovenia.

9.7 Odmietnutie poskytnutia záruky

Žiadne ustanovenia.

9.8 Obmedzenie zodpovednosti

V prípade delegovaných úloh na RA si Poskytovateľ alebo RA môžu medzi sebou zmluvne rozdeliť zodpovednosť, ale Poskytovateľ bude naďalej plne zodpovedať za plnenie voči všetkým stranám v súlade s touto CP, ako keby úlohy neboli delegované.

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 [8] 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.

Bez ohľadu na akékoľvek obmedzenia svojej zodpovednosti voči predplatiteľom a závislým stranám Poskytovateľ chápe a uznáva, že dodávatelia aplikačného softvéru, ktorí súhlasili s distribúciou certifikátu koreňovej CA Poskytovateľa nepreberajú žiadnu povinnosť alebo potenciálnu zodpovednosť Poskytovateľa podľa tejto CP alebo ktorá by inak mohla existovať z dôvodu vydávania alebo udržiavania certifikátov alebo spoliehania sa na ne Spoliehajúcimi sa stranami alebo inými. Teda Poskytovateľ bude obhajovať, odškodňovať a chrániť každého dodávateľa aplikačného softvéru za všetky nároky, škody a straty, ktoré takýto dodávateľ aplikačného softvéru utrpel v súvislosti s certifikátom vydaným CA, bez ohľadu na dôvod konania alebo príslušnú právnu teóriu. To sa však nevzťahuje na žiadne nároky, škody alebo straty, ktoré utrpel takýto dodávateľ aplikačného softvéru v súvislosti s certifikátom vydaným CA, ak takýto nárok, škoda alebo strata bola priamo spôsobená softvérom dodávateľa aplikačného softvéru, ktorý sa javil ako nedôveryhodný certifikát, ktorý je však stále platný alebo sa zobrazuje ako dôveryhodný:

(1) certifikát ktorému skončila platnosť, resp.

(2) Certifikát, ktorý bol zrušený (ale iba v prípadoch, keď je stav zrušenia momentálne dostupný u Poskytovateľa online a aplikačný softvér buď zlyhal pri kontrole tohto stavu, alebo ignoroval indikáciu stavu zrušenia).

9.10 Doba platnosti, ukončenie platnosti

9.10.1 Doba platnosti

Tato verzia CP platí odo dňa nadobudnutia jej platnosti t. j. 2.1.2024 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

Žiadne ustanovenia.

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 sekcii 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 sekcia 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.