PRAVIDLÁ

poskytovania dôveryhodnej služby vyhotovovania a overovania S/MIME certifikátov - **časť RA**

Disig, a.s.

Vypracoval	**Ing. Peter Miškovič**
Dátum platnosti	1.9.2023
Verzia	1.0
Typ	PRAVIDLÁ
Schválil	**Ing. Ľuboš Batěk**

Obsah

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

Tento dokument neprešiel jazykovou úpravou.

1. Úvod

Tento dokument definuje pravidlá poskytovania dôveryhodnej služby vyhotovovania a overovania S/MIME certifikátov - časť: RA (Certificate Practice Statement, ďalej len „CPS“) pre registračné autority (ďalej len „RA“) spoločnosti Disig ako poskytovateľa dôveryhodných služieb (ďalej len „Poskytovateľ“). CPS vychádzajú z dokumentu „Politika poskytovania dôveryhodnej služby vyhotovovania a overovania S/MIME certifikátov“ (OID=1.3.158.35975946.0.0.0.1.11) [1] Poskytovateľa (ďalej len „CP SMIME“). Aktuálna verzia CP SMIME, na ktorú sa viažu tieto CPS je verzia 1.0 s platnosťou od 1.9.2023.).

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

https://eidas.disig.sk

1.1 Prehľad

Táto CPS 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 [3] a požiadavkami Nariadenia Európskeho parlamentu a Rady (EÚ) č. 910/2014 z 23. júla 2014 o elektronickej identifikácii a dôveryhodných službách pre elektronické transakcie na vnútornom trhu a o zrušení smernice 1999/93/ES (ďalej len „Nariadenie eIDAS“) [4] a je

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

1.2 Názov dokumentu a jeho identifikácia

Názov	PRAVIDLÁ **poskytovania dôveryhodnej služby** vyhotovovania a overovania S/MIME certifikátov - **časť RA**
Skratka názvu:	CPS RA SMIME CA Disig*
Verzia:	1.0
Schválené dňa:	25.8.2023
Platnosť od:	1.9.2023
Tomuto dokumentu je priradený identifikátor objektu (OID):	1.3.158.35975946.0.0.0.1.12

* - 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

1.3.158.35975946.0.0.0.1.12 – CPS RA SMIME CA Disig

1.2.1 História zmien

Verzia	Dátum revízie	Popis revízie; revidoval
1.0	1.9.2023	Prvá verzia dokumentu; Miškovič

1.3 Účastníci PKI

1.3.1 Certifikačné autority

Pozri sekcia 1.3.1 CP SMIME.

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 CPS MIME v aktuálnom znení.

Poskytovateľ má zriadené RA nasledovných typov:

- K**omerčná RA** – je určená na sprostredkovanie vybraných dôveryhodných služieb Poskytovateľa širokej verejnosti a je prevádzkovaná treťou stranou, na základe písomnej zmluvy s Poskytovateľom – zoznam pozri . https://eidas.disig.sk/sk/kontakt/registracne-autority/
- 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 ďalej texte použije skratka „RA“, tak sa to týka všetkých vyššie uvedených existujúcich RA.

1.3.2.1 Firemná RA

Poskytovateľ zmluvne delegoval 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 dané v časti 1.3.2.1 CP SMIME.

1.3.3 Zákazník a Držiteľ certifikátu

Pozri sekcia 1.3.3 CP SMIME.

1.3.4 Spoliehajúca sa strana

Pozri sekcia 1.3.4 CP SMIME.

1.3.5 Iní účastníci

Pozri sekcia 1.3.5 CP SMIME.

1.4 Použiteľnosť certifikátov

1.4.1 Vhodné použitie certifikátov

Pozri sekcia 1.4.1 CP SMIME.

1.4.2 Nedovolené použitie certifikátov

Pozri sekcia 1.4.2 CP SMIME.

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:	https://www.disig.sk

1.5.2 Kontaktná osoba

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

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:	https://eidas.disig.sk
Oznamovanie incidentov	tspnotify@disig.sk viac pozri: https://eidas.disig.sk/pdf/incident_reporting.pdf

1.5.3 Osoba rozhodujúca o súlade CPS s CP

Osobou, ktorá je zodpovedná za rozhodovanie o súlade postupov Poskytovateľa, ktoré sú uvedené v CPS s CP SMIME je PMA (pozri sekcia 1.3.5 CP SMIME).

1.5.4 Postupy **schvaľovania CPS a externej politiky**

Ešte pred začiatkom prevádzky má Poskytovateľ schválený svoj CP a tieto CPS a spĺňať všetky ich požiadavky. Obsah CPS je schválený osobami menovanými do roly PMA.

Tieto CPS sú sprístupnené Spoliehajúcim sa stranám na webovom sídle Poskytovateľa (https://eidas.disig.sk/sk/poskytovatel/politiky-a-dokumenty/).

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 [4];

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

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

1.6.2 Skratky

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)
HSM	-	Hardware Security Modul
IČO	-	Identifikačné číslo organizácie
OID	-	Identifikátor objektu (Object Identifier)
PKCS#10	-	Formát žiadosti o certifikát podľa štandardu Public Key Cryptographic Standards (RFC 2986)
PKI		Infraštruktúra verejných kľúčov (Public Key Infrastructure)
PMA	-	Autorita pre správu CP (Policy Management Authority)
RA	-	Registračná autorita (Registration Authority)
RFC	-	Request for Comments
SAN	-	Rozšírenie definované štandardom X.509 [6], ktoré umožňuje uviesť v certifikáte rôzne hodnoty (e-mail, URI, FQDN, IP adresa), ktorú budú umiestnené v položke subjAltName.
S/MIME	-	Secure MIME (Multipurpose Internet Mail Extensions)

1.6.3 Odkazy

[1] Politika poskytovania dôveryhodnej služby vyhotovovania a overovania S/MIME certifikátov. 1.0.

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

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

[4] Nariadenie Európskeho parlamentu a Rady (EÚ) č. 910/2014 z 23. júla 2014 o elektronickej identifikácii a dôveryhodných službách pre elektronické transakcie na vnútornom trhu a o zrušení smernice 1999/93/ES .

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

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

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

[8] CA/Browser Forum Baseline Requirements for the Issuance and Management of Publicly-Trusted Certificates v. 1.8.4.

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

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

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

2. Zverejňovanie informácií a úložiská

2.1 Úložiská

Funkciu úložiska Poskytovateľa zastávať webové sídlo https://eidas.disig.sk, ktoré je prostredníctvom Internetu verejne prístupné Zákazníkom, Držiteľom certifikátov, Spoliehajúcim sa stranám a verejnosti vôbec.

2.2 Zverejňovanie informácií o CA

Poskytovateľ vo svojom úložisku poskytuje v on-line režime (24x7), tieto informácie:

- certifikáty vydané v súlade s CP SMIME a týmito CPS,
- 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 S/MIME certifikátov a CRL
- aktuálnu verziu CP SMIME a týchto CPS,
- informáciu o výsledku pravidelného auditu výkonu poskytovaných dôveryhodných služieb

2.3 Frekvencia zverejňovania informácií

Pozri sekcia 2.3 CP SMIME.

2.4 Kontroly prístupu

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

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

3. Identifikácia a autentizácia

3.1 Mená

3.1.1 Typy mien

Poskytovateľ prijíma len tie žiadosti o certifikát, ktoré vyhovujú štandardu PKCS #10 alebo SPKAC, ak nebolo so zákazníkom vopred dohodnuté inak.

3.1.2 Potreba zmysluplnosti mien

Vo všeobecnosti Poskytovateľ neprirađuje pre certifikáty zákazníkov rozlišovacie mená v zmysle X.500 [7] (X.500 Distinguished Name, ďalej len „rozlišovacie meno“).

Žiadatelia o certifikát si sami zvolia rozlišovacie meno, ktoré má byť v ich certifikáte v súlade s požiadavkami uvedenými v sekcii 7.1.4.2.2 CP SMIME.

3.1.3 Anonymita a **používanie pseudonymov**

Používanie pseudonymov, prezývok, krycích mien, aliasov a podobne (tzv. nicknames) v S/MIME certifikátoch vydávaných Poskytovateľom nie je povolené.

3.1.4 Pravidlá na interpretáciu rôznych foriem mien

3.1.4.1 Náhrada znakov, ktoré nie sú ASCII

Pozri sekcia 3.1.4.1 CP SMIME.

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

Pracovník RA v mene Poskytovateľa vykoná autentifikáciu všetkých atribútov 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 sekcia definuje procesy a postupy na potvrdenie kontroly žiadateľa nad e-mailovou adresou, ktorá má byť zahrnutá vo vydávanom certifikáte.

Poznámka: E-mailová adresa bude uvedená v certifikáte držiteľa ako „*rfc822Name*“ v rozšírení „*subjectAltName*“.

3.2.2.1 Overenie kontroly nad e-mailovou adresou prostredníctvom domény

Pri vydávaní certifikátov typu „sponsor-validated“ pre zmluvného partnera, kde nebude vykonávané overovanie jednotlivých e-mailových adries žiadateľov si RA overí, že zmluvný partner má kontrolu nad doménovou časťou e-mailovej adresy, ktorá sa má použiť v certifikáte.

Overenie vykoná Pracovník RA, v zmysle sekcie 3.2.2.4.2 „Baseline Requirements for the Issuance and Management of Publicly-Trusted Certificates“ [8] v aktuálne verzii, zaslaním náhodného textového reťazca s minimálnou dĺžkou 20 znakov, ktorý bude obsahovať veľké a malé písmená, čísla a špeciálne znaky. Takto vygenerovanú hodnotu zašle prostredníctvom emailu na emailovú adresu identifikovanú ako oprávnený kontakt pre danú doménu v registri oprávneného registrátora pre danú doménu (napr. pre doménu najvyššej úrovne „.sk“ je to whois.sk-nic.sk). Náhodná hodnota musí byť pre každú odoslanú emailovú správu jedinečná. Overenie doménovej časti e-mailovej adresy bude úspešné, pokiaľ pracovník RA dostane spätne potvrdzujúci e-mail od oprávneného kontaktu, ktorý bude obsahovať zaslaný náhodný textový reťazec. Pracovník RA potom archivuje príslušnú emailovú komunikáciu z overenia v elektronickej podobe.

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

Pred vydaním certifikátu musí pracovník RA Poskytovateľa vykonať overenie vlastníctva a kontrolu e-mailovej adresy nachádzajúcej sa v žiadosti o vydanie certifikátu.

Overenie sa vykoná prostredníctvom aplikácie RA Client zaslaním náhodnej hodnoty na e-mailovú adresu nachádzajúcu sa v žiadosti o certifikát. Zaslanie je vykonané automatickým spôsobom po načítaní profilu pre S/MIME certifikát a zodpovedajúcej žiadosti na vydanie do aplikácie RA Client a voľbe možnosti overenia e-mailovej adresy (verify Email). Po zaslaní overovacieho e-mailu má Žiadateľ 24 hodín na potvrdenie zaslanej náhodnej hodnoty. Stav overenia si kontroluje Pracovník RA v aplikácii RA Client v menu „Vyhľadávanie“ a záložke „Overenie eMail“. Pokiaľ je overenie v stave „approved“, tak overenie e-mailovej adresy bolo úspešné.

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 pracovník RA byť dodržiava požiadavky uvedené v nasledujúcich sekciách.

3.2.3.1 Zoznam atribútov identity organizácie

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

- Formálny názov
- Jedinečný identifikátor a jeho typ

Jedinečný identifikátor je identifikátor uvedený v subjekte certifikátu „*organizationIdentifier*“ v súlade so sekciou 7.1.4.2.2 a prílohou A dokumentu [3].

3.2.3.2 Validácia identity organizácie (právnickej osoby)

3.2.3.2.1 Overenie mena, adresy a jedinečného identifikátora

RA Poskytovateľa overuje celé meno žiadateľa (právnickej osoby) so sídlom v Slovenskej republike a jedinečného identifikátora na základe:

- predloženého originálu výpisu z Obchodného registra Slovenskej republiky (https://www.orsr.sk/) (ďalej len „OR SR“).
- v prípade žiadateľa (organizácie), ktorá nie je vedená v OR SR si overuje meno na základe originálu výpisu z Registra právnických osôb, podnikateľov a orgánov verejnej moci, ktorý vedie Štatistický úrad Slovenskej republiky (https://rpo.statistics.sk/) (ďalej len „RPO SR“),

- V prípade, že právnická osoba nemá sídlo na území Slovenskej republiky, jej totožnosť sa overuje predložením výpisu z registra vládnej agentúry v jurisdikcii vytvorenia, existencie a lebo uznania právnickej osoby. RA Poskytovateľa si potom potvrdí existenciou prostredníctvom webovej stránky „Business registers – search for a company in the EU“

Originál alebo úradne overená kópia originálu predkladaných dokumentov nesmie byť staršia ako tri mesiace. Dokument musí obsahovať úplné obchodné meno alebo názov a identifikačný údaj.

RA Poskytovateľa akceptujú aj elektronickú formu výpisu z použitého registra, ktorá bude autorizovaná kvalifikovanou elektronickou pečaťou štátneho orgánu zodpovedajúceho za vedenie registra.

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

Pozri sekcia 3.2.3.2.1.

3.2.4 Autentizácia identity fyzickej osoby

3.2.4.1 Získavanie identity fyzickej osoby

RA Poskytovateľa overuje identitu fyzickej osoby na základe predloženého identifikačného dokladu, ktorý musí obsahovať 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),

3.2.4.1.1 Fyzicky predložený doklad totožnosti

Pri overovaní identity RA Poskytovateľa v súčasnosti akceptuje tieto doklady, ktoré obsahujú fotografiu tváre a sú predkladané Držiteľom, za jeho fyzickej účasti:

- občiansky preukaz,
- cestovný pas.

3.2.4.1.2 Digitálny doklad o identite

Žiadne ustanovenia.

3.2.4.1.3 Schéma elektronickej identifikácie (eID)

Žiadne ustanovenia.

3.2.4.1.4 Certifikát elektronického podpisu vytvoreného Žiadateľom

Žiadne ustanovenia.

3.2.4.1.5 Záznamy firemnej RA

V prípade certifikátov vydávaných zamestnancom zmluvného partnera firemnou RA, zriadenou Poskytovateľom na základe zmluvy o spolupráci, môžu byť zdrojom identity zamestnanca aj záznamy vedené zmluvným partnerom. Zmluvný partner potom vedie 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, RA overuje príslušnosť držiteľa k danej právnickej osobe, ktorá má byť zahrnutá v časti „*subject:organizationName*“, na základe potvrdenia poskytnutého touto právnickou osobou. RA však overuje 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 napr. ak fyzická osoba zastupuje pri vydávaní certifikátu inú fyzickú osobu, musí preukázať identitu zastupovanej osoby 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, a ktorá obsahuje všetky údaje uvedené v sekcii 3.2.4.1.

3.2.4.1.8 Autorizované referenčné zdroje ako doplnkový dôkaz

Žiadne ustanovenia.

3.2.4.2 Overenie identity fyzickej osoby

RA Poskytovateľa overuje všetky atribúty fyzickej osoby, ktoré majú byť zahrnuté v certifikáte. V prípade občianskeho preukazu resp. pasu RA Poskytovateľa overí, že čas overenia identity je v rámci obdobia platnosti predložených dokladov totožnosti t. j. dátum overenia identity nepresahuje dátum skončenia platnosti dokladu totožnosti.

RA Poskytovateľa môže opätovne použiť existujúce dôkazy overenia identity fyzickej osoby, ktoré bolo získané najneskôr 825 dní pred vydaním certifikátu.

3.2.4.2.1 Validácia predložených dokladov vo fyzickej podobe

Pri osobnej návšteve RA Poskytovateľa musí byť zo strany Žiadateľa predložený originálny doklad o identite fyzickej osoby. RA Poskytovateľa nepodporuje jeho vzdialené overovanie napr. cez kameru.

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

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

RA Poskytovateľa zadáva do informačného systému Poskytovateľa všetky informácie dostatočné na preukázanie splnenia procesu overenia identity a overených atribútov. Okrem osobných údajov si Poskytovateľ uchováva v informačnom

systéme aj typ identifikačného dokladu a jeho sériové číslo, vydavateľa a dátum ukončenia platnosti.

3.2.4.2.2 Validácia digitálneho dokladu o identite

Žiadne ustanovenia.

3.2.4.2.3 Validácia schémy elektronickej identifikácie (eID)

Žiadne ustanovenia.

3.2.4.2.4 Validácia certifikátu elektronického podpisu vytvoreného Žiadateľom

Žiadne ustanovenia.

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“, overuje všetky atribúty identity fyzickej osoby, ktoré majú byť zahrnuté v certifikáte. V rámci overovania sa firemná RA môže pri overovaní identity fyzickej osoby spoliehať na svoje existujúce interné záznamy a nemusí vyžadovať fyzické predloženie identifikačného dokladu. Podmienka je, že interné záznamy musia obsahovať všetky Poskytovateľom osobné údaje fyzickej osoby a údaje, ktoré budú zapísané v certifikáte.

3.2.5 Neoverované informácie o Držiteľovi

Informácie o žiadateľovi, ktoré neboli overené v súlade s CP SMIME a týmito CPS nesmú byť uvedené v certifikátoch.

3.2.6 Potvrdenie autority

Pred začatím vydávania certifikát pre zamestnanca právnickej osoby (sponsor-validated) a certifikátov pre pečať (organization-validated) Poskytovateľa používa spoľahlivý spôsob na overenie oprávnenia vydania takéhoto typu certifikátu pre danú fyzickú osobe resp. právnickú osobu.

3.2.7 Kritériá interoperability

Žiaden ustanovenia.

3.2.8 Spoľahlivosť overovacích zdrojov

RA Poskytovateľa sa spolieha na zdroj overovacích údajov pri overovaní žiadosti o certifikát len u 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 rovnako spolieha na zoznam údajov o Žiadateľoch, ktoré sú zasielané kontaktnou osobou zmluvného partnera, ktorá je uvedená v uzatvorenej zmluve o poskytovaní dôveryhodných služieb.

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

RA Poskytovateľ sa tiež spolieha na údaje, ktoré sú úradne overené v zmysle platnej legislatívy.

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 predchádzaj**úceho

Žiadne ustanovenia.

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

Žiadne ustanovenia.

4. Požiadavky na životný cyklus certifikátu

4.1 Žiadanie o certifikát

4.1.1 Kto môže žiadať o vydanie certifikátu

Pozri sekcia 4.1.1. CP SMIME.

4.1.2 Proces registrácie a zodpovednosti

4.1.2.1 Príprava

Pozri sekcia 4.1.2.1 CP SMIME.

4.1.2.2 Generovanie žiadosti

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

Pozri sekcia 4.1.2.2.1 CP SMIME.

4.1.2.3 Zaslanie žiadosti o certifikát

Pozri sekcia 4.1.2.3 CP SMIME.

4.2 Spracovanie žiadosti o certifikát

4.2.1 Vykonanie identifikácie a autentifikácie

Pred vydaním certifikátu RA Poskytovateľa vykoná prostredníctvom aplikácie RA Client:

- kontrolu, či e-mailová adresa uvedená v žiadosti zodpovedá e-mailovej adrese, z ktorej bola žiadosť zaslaná,
- kontrolu úplnosti a správnosti údajov v prijatej žiadosti o certifikát, či obsahuje len povolené položky v zmysle sekcie 7.1.4.2.2 CP SMIME [3],
- overenie vlastníctva a kontroly e-mailovej adresy Žiadateľa v zmysle sekcie 4.2.1.1,
- kontrolu, či overenie vlastníctva e-mailovej adresy Žiadateľa bolo úspešné a môže byť vydaný certifikát

Pri osobnej návšteve Žiadateľa alebo ním poverenej osoby na RA Poskytovateľa:

- informuje prítomnú fyzickú osobu o Všeobecných podmienkach [9],
- overuje totožnosť budúceho Držiteľa certifikátu v zmysle sekcie 3.2.4.2 a prostredníctvom klientskej aplikácie RA Client vkladá jeho osobné údaje do IS Poskytovateľa, pričom vypĺňa všetky povinné položky vyžadované systémom Poskytovateľa,

- overuje ďalšie doklady na overenie ľubovoľných identifikačných údajov, ktoré sa majú dostať do certifikátu napr. identita organizácie v zmysle sekcie 3.2.3.2.

V prípade zistených rozdielov môže odmietnuť vydanie certifikátu.

Pri overovaní identity fyzickej osoby resp. právnickej osoby je možné využiť existujúce overenie týchto identít pokiaľ tieto spĺňajú lehoty dané v sekcii 4.2.1.3 resp. 4.2.1.2.

4.2.1.1 Overenie vlastníctva a kontroly e-mailovej adresy

Overenie e-mailovej adresy, ktoré bolo úspešne dokončené v súlade s požiadavkami sekcie 3.2.2.2 je možné získať najneskoršie 30 dní pred vydaním certifikátu. Pokiaľ Pracovník RA zistí, že existujúce overenie je staršie ako 30 dní, tak musí vykonať nové overenie.

Overenie e-mailovej adresy, ktoré bolo úspešne dokončené v súlade s požiadavkami sekcie 3.2.2.1 je možné získať najneskoršie 398 dní pred vydaním certifikátu. Pokiaľ Pracovník RA zistí, že existujúce overenie je staršie ako 398 dní, tak musí vykonať nové overenie vlastníctva a kontroly e-mailovej adresy..

4.2.1.2 Overenie identity organizácie

Overenie identity organizácie, 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.

Pokiaľ Pracovník RA zistí, že existujúce overenie je staršie ako 825 dní, tak musí vykonať nové overenie identity organizácie.

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.

Pokiaľ Pracovník RA zistí, že existujúce overenie je staršie ako 825 dní, tak musí vykonať nové overenie identity fyzickej osoby.

4.2.2 Schválenie alebo zamietnutie žiadosti o certifikát

Žiadosť o vydanie certifikátu začne pracovník RA spracovávať ihneď po jej prijatí v zmysle postupov uvedených v časti 4.2.1. Certifikát vydá v prípade, že sú splnené všetky podmienky na vydanie.

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

4.2.3 Čas na spracovanie žiadosti o certifikát

Žiadne ustanovenia.

4.3 Vydanie certifikátu

4.3.1 Činnosť CA pri vydávaní certifikátu

Pozri sekcia 4.3.1 CP SMIME.

4.3.2 Informovanie **Držiteľa** o vydaní certifikátu

Držiteľ je upozornený o vydaní certifikátu okamžite po jeho vydaní zaslaním e-mailovej správy priamo zo systému CA Poskytovateľa na e-mailovú adresu uvedenú v certifikáte.

4.4 Prevzatie certifikátu

4.4.1 Spôsob prevzatia certifikátu

Vydaný certifikát je k dispozícii na prevzatie prostredníctvom úložiska Poskytovateľa na adrese https://eidas.disig.sk/sk/poskytovatel/certifikacna-autorita/vyhladavanie-certifikatov/ resp. v upozorňujúcom e-maile, ktorý sa zasiela priamo po vydaní je uvedená linka, kde si Držiteľ môže vydaný certifikát stiahnuť/nainštalovať.

4.4.2 Zverejňovanie certifikátu

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

4.4.3 Oznámenie o vydaní certifikátu iným subjektom

Žiadne ustanovenia.

4.5 Kľúčový pár a používanie certifikátu

4.5.1 Použitie súkromného kľúča a certifikátu držiteľa

Pozri sekcia 9.6.3 CP SMIME, ustanovenia 2 a 4.

4.5.2 Použitie verejného kľúča a certifikátu spoliehajúcu sa stranou

Žiadne ustanovenia.

4.6 Obnova certifikátu

Pozri sekcia 4.6 CP SMIME.

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**

Pozri sekcia 4.7 CP SMIME.

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**

RA Poskytovateľa zruší certifikát v prípade, že má k dispozícii relevantnú informáciu, že sa väzba medzi subjektom a jeho verejným kľúčom definovaným v certifikáte už nepovažuje za platnú.

4.9.1.1 Zrušenie certifikátu Zákazníka/Držiteľa

RA Poskytovateľ zruší do 24 hodín certifikát, ktorý spravuje v prípade, že nastal jeden z nasledujúcich prípadov:

- Zákazník/Držiteľ certifikátu alebo iná oprávnená strana písomne požiadala o zrušenie certifikátu,
- Zákazník/Držiteľ oznámil Poskytovateľovi, že pôvodná žiadosť o vydanie ním nebola autorizovaná a neposkytne spätnú autorizáciu vydania,
- Poskytovateľ získal dôkaz, že došlo ku kompromitácii súkromného kľúča, ktorý zodpovedá verejnému kľúču v certifikáte,
- Poskytovateľ získal 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 získal dôkaz, že sa nemôže spoľahnúť na overenie vlastníctva a kontroly nad e-mailovou adresou uvedenou v certifikáte

Poskytovateľ zruší certifikát v priebehu 24 hodín a najneskoršie do piatich (5) dní v prípade, keď nastal niektorý z týchto prípadov:

- certifikát už viac nespĺňa požiadavky v zmysle článkov 6.1.5 a 6.1.6,
- Poskytovateľ získal dôkaz, že došlo k jeho zneužitiu,
- Poskytovateľ zistil, že Držiteľ certifikátu nedodržuje svoje povinnosti Držiteľa certifikátu, ktorými je zmluvne viazaný,
- Poskytovateľ bol 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 bol oboznámený, že došlo k podstatným zmenám informácií uvedených v certifikáte,
- Poskytovateľ bol oboznámený s tým, že certifikát nebol vydaný v súlade s CP SMIME alebo týmito CPS,
- Poskytovateľ zistil, že niektorá z informácií uvedených v certifikáte je nepresná,
- Poskytovateľ ukončil z akéhokoľvek dôvodu svoju činnosť a zmluvne nezaistil u inej CA, aby poskytovala informácie o zrušených certifikátoch v jeho mene,
- zaniklo právo Poskytovateľa vydávať certifikáty v zmysle CP SMIME, alebo bolo zrušené alebo došlo k ukončeniu vydávania, pokiaľ Poskytovateľ neprijal opatrenia na zaistenie kontinuity poskytovania CRL/OCSP repozitárov,
- zrušenie je vyžadované ustanoveniami CP SMIME alebo týmito CPS,
- Poskytovateľ bol 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.

Certifikát bude zrušený vždy a zaradený na zoznam zrušených certifikátov (ďalej len „CRL“), keď sa Poskytovateľ dozvedel o niektorej z vyššie uvedených okolností.

4.9.1.2 Zrušenie certifikátu podriadenej CA

Poskytovateľ zruší certifikát podriadenej CA v priebehu 7 dní v prípade že:

- dostal písomnú požiadavku na zrušenie podriadenej CA,
- podriadená CA informovala vydávajúcu CA Poskytovateľa, že pôvodná požiadavka nebola autorizovaná a neposkytne dodatočnú autorizáciu,

- Poskytovateľ získal 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 získal dôkaz, že došlo k zneužitiu certifikátu podriadenej CA,
- Poskytovateľ bol oboznámený s tým, že certifikát podriadenej CA nebol vydaný v súlade s CP SMIME a príslušnými CPS (RA, CA),
- Poskytovateľ rozhodol, že niektorá z informácií uvedených v certifikáte podriadenej CA je nepresné alebo zavádzajúca,
- došlo 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 CP SMIME, alebo bolo zrušené alebo došlo k ukončeniu vydávania, pokiaľ Poskytovateľ neprijal opatrenia na zaistenie kontinuity poskytovania CRL/OCSP repozitárov,
- zrušenie bolo vyžadované CP SMIME alebo príslušnými CPS (RA, CA).

4.9.2 Kto môže žiadať o zrušenie certifikátu

Pozri sekcia 4.9.2 CP SMIME.

4.9.3 Postup **žiadosti o zrušenie certifikátu**

Pozri sekcia 4.9.3 CP SMIME.

4.9.4 Čas na podanie žiadosti o zrušenie certifikátu

Žiadne ustanovenia.

4.9.5 Čas na spracovanie žiadosti o zrušenie certifikátu

Poskytovateľ preskúma v priebehu 24 hodín od oznámenia problému s certifikátom skutočnosti týkajúce sa oznámeného problému a poskytne Zákazníkovi/Držiteľov a spoliehajúcim sa stranám predbežnú informáciu o svojich zisteniach,

Po preskúmaní faktov a okolností Poskytovateľ v súčinnosti so Zákazníkom/Držiteľom a koncovou entitou, ktorá oznámila problém rozhodne, 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 CP SMIME., pričom stanovený termín zohľadní 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

Pozri sekcia 4.9.6 CP SMIME.

4.9.7 Frekvencia vydávania CRL

Pozri sekcia 4.9.7 CP SMIME.

4.9.8 Doba publikovania CRL

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

4.9.9 Dostupnosť služby OCSP

Služba OCSP je poskytovaná v súlade s požiadavkami RFC 6960 [10] OCSP odpoveď je podpísaná:

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

Podpisový certifikát OCSP respondera obsahuje „*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 [10].

4.9.10 Požiadavky na OCSP overovanie

OSCP respondery Poskytovateľa podporujú metódu HTTP GET v súlade s RFC 6960 [10] a/alebo RFC 5019 [11].

Odpovede k stavu vydaných SMIME certifikátov:

- OCSP odpoveď má interval platnosti väčší alebo rovný 8 hodín
- OCSP odpoveď má interval platnosti menší alebo rovný 8 dní
- Poskytovateľ aktualizuje informácie poskytované prostredníctvom OCSP okamžite po zmene stavu certifikátu v jeho IS.

Pre stav certifikátov podriadených CA sú informácie poskytované prostredníctvom OCSP aktualizované:

- 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 nezasiela odpovedať so stavom „*good*“. Poskytovateľ monitoruje OCSP responder na žiadosti obsahujúce sériové čísla, ktoré daná CA nevydala ako súčasť svojich bezpečnostných procesov týkajúcich sa OCSP.

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

Žiadne ustanovenia.

4.9.12 Špeciálne požiadavky na zmenu kľúčov po ich kompromitácii

Pozri sekcia 4.9.12 CP SMIME.

4.9.13 Okolnosti pozastavenia platnosti certifikátu

Pozri sekcia 4.9.13 CP SMIME.

4.9.14 Kto môže žiadať o pozastavenie certifikátu

Pozri sekcia 4.9.14 CP SMIME.

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

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

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

Zrušené certifikáty nikdy nie sú s CRL resp. OCSP vynechané.

4.10.2 Dostupnosť služieb

Poskytovateľ prevádzkuje a udržiava svoj systém poskytovania CRL a OCSP s takými zdrojmi, ktoré zabezpečujú čas odozvy do desiatich (10) sekúnd za normálnych prevádzkových podmienok.

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

Služba OCSP je dostupná v režime 24x7.

4.10.3 Doplnkové funkcie

Žiadne ustanovenia.

4.11 Ukončenie poskytovanie služieb

Žiadne ustanovenia.

4.12 Uchovávanie a obnova kľúčov

4.12.1 Politika a postupy uchovávania a obnovy kľúčov

Pozri sekcia 4.12.1 CP SMIME.

4.12.2 Politika a postupy ochrany „session key“

Žiadne ustanovenia.

5. Fyzické, personálne a prevádzkové bezpečnostné opatrenia

5.1 Opatrenie týkajúce sa fyzickej bezpečnosti

5.1.1 Priestory

Žiadne ustanovenia.

5.1.2 Fyzický prístup

Žiadne ustanovenia.

5.1.3 Zásobovanie elektrickou energiou a klimatizácia

Žiadne ustanovenia.

5.1.4 Ochrana pre vodou

Žiadne ustanovenia.

5.1.5 Ochrana pred ohňom

Žiadne ustanovenia.

5.1.6 Úložisko médií

Médiá sú uskladnené v priestoroch, ktorú sú chránené pred náhodným, neúmyselným poškodením (vodou, ohňom, elektromagneticky). Médiá, ktoré obsahujú osobné údaje sú uložené, tak, že k nim nemajú prístup žiadne neoprávnené osoby.

5.1.7 Nakladanie s odpadom

Pozri sekcia 5.1.7 CP SMIME.

5.1.8 Zálohovanie off-site

Žiadne ustanovenia.

5.2 Procedurálne bezpečnostné opatrenia

5.2.1 Dôveryhodné role

V rámci RA je definovaná dôveryhodná role zodpovedné za aspekty poskytovaných dôveryhodných služieb týkajúcich sa povinností registračnej autority, tak ako sú definované v zmluve o RA.

5.2.2 Počet osôb v jednotlivých rolách

Žiadne ustanovenia.

5.2.3 Identifikácia a autentizácia pre každú rolu

Pracovník RA má prístup do IS Poskytovateľa len prostredníctvom aplikácie RA Client, ktorá je dodávaná Poskytovateľom. Autentifikácia v aplikácii RA Client pri prístupe do IS Poskytovateľa je vykonávaná na základe autentifikačného certifikátu, ktorý je uložený na čipovej karte, a ktorého vydavateľom je interná CA Poskytovateľa.

5.2.4 Role vyžadujúce oddelenie zodpovedností

Žiadne ustanovenia.

5.3 Personálne bezpečnostné opatrenia

Pracovníci RA sú poverení na výkon danej roly štatutárnym zástupcom právnickej osoby, ktor, na základe zmluvy, prevádzkuje RA. Pracovníci internej RA Poskytovateľa sú menovaný do roly výkonným manažmentom Poskytovateľa.

5.3.1 Požiadavky na kvalifikáciu, skúsenosti a previerky

Pozri sekcia 5.3.1 CP SMIME.

5.3.2 Požiadavky na previerky

Pozri sekcia 5.3.2 CP SMIME.

5.3.3 Požiadavky na školenia

Pracovník RA musí pred menovaním do roly pracovník RA absolvovať školenie, ktoré vykoná poverený člen úseku PMA/Legal Poskytovateľa.

5.3.4 Požiadavky na frekvenciu obnovy školení

Frekvencia školení pre pracovníkov RA je dané v internej smernici „Životný cyklus RA“.

5.3.5 Rotácia rolí

Žiadne ustanovenia.

5.3.6 Postihy za neoprávnenú činnosť

Pozri sekcia 5.3.6 CP SMIME.

5.3.7 Požiadavky na externých dodávateľov

Pozri sekcia 6.3.7 CP SMIME.

5.3.8 Dokumentácia dodávané pre personál

Pozri 5.3.8 sekcia CP SMIME.

5.4 Postupu získavania auditných záznamov

Žiadne ustanovenia.

5.4.1 Typy zaznamenávaných udalosti

Žiadne ustanovenia.

5.4.2 Frekvencia spracovávania auditných záznamov

Žiadne ustanovenia.

5.4.3 Doba uchovávanie auditných záznamov

Žiadne ustanovenia.

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 zraniteľnosti

Žiadne ustanovenia.

5.5 Uchovávanie záznamov

5.5.1 Typy archivovaných záznamov

Žiadne ustanovenia.

5.5.2 Doba uchovávania záznamov

Žiadne ustanovenia.

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 riešen**ia incidentov a kompromitácie

1. *Žiadne ustanovenia.*

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

6.1 Generovanie a inštalácia páru kľúčov

6.1.1 Generovanie páru kľúčov

6.1.1.1 Generovanie kľúčového páru certifikačnej autority

Žiadne ustanovenia.

6.1.1.2 Registračné autority

Žiadne ustanovenia.

6.1.1.3 Generovanie kľúčových párov pre Držiteľov

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

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

RA Poskytovateľa negeneruje kľúčový pár v mene držiteľa.

6.1.2 Doručenie súkromného kľúča Držiteľovi certifikátu

Žiadne ustanovenia.

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

Pozri sekcia 6.1.5 CP SMIME.

6.1.6 Parametre a kvalita verejného kľúča

Pozri sekcia 6.1.6 CP SMIME.

6.1.7 Použitie kľúčov

Žiadne ustanovenia.

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

6.2.1 **Štandardy** a opatrenia pre kryptografický modul

Žiadne ustanovenia.

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

Žiadne ustanovenia.

6.2.3 **„Key escrow“ súkromného kľúča**

Žiadne ustanovenia.

6.2.4 **Zálohovanie súkromného kľúča**

Žiadne ustanovenia.

6.2.5 **Archivácia súkromného kľúča**

Žiadne ustanovenia.

6.2.6 Prenos sú**kromných kľúčov z** a do HSM modulu

Žiadne ustanovenia.

6.2.7 **Uchovávanie súkromných kľúčov v** HSM module

Žiadne ustanovenia.

6.2.8 **Spôsob aktivácie súkromných kľúčov**

Žiadne ustanovenia.

6.2.9 **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**

Pozri sekcia 6.3.2 CP SMIME.

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 ma zavedenú viacfaktorovú autentifikáciu pre všetkých pracovníkov RA, ktorí sú schopní 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

Žiadne ustanovenia.

6.8 Využívanie časovej pečiatky

Žiadne ustanovenie

7. Profily certifikátov a zoznamov zrušených certifikátov

7.1 Profily certifikátov

7.1.1 Verzia

Žiadne ustanovenia.

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

Žiadne ustanovenia.

7.1.2.2 Podriadené certifikačné autority Poskytovateľa

Žiadne ustanovenia.

7.1.2.3 Rozšírenia v certifikátoch koncových používateľov

Žiadne ustanovenia.

7.1.2.4 Všetky certifikáty

Žiadne ustanovenia.

7.1.3 Identifikátory použitých algoritmov

7.1.3.1 SubjectPublicKeyInfo

Pozri sekcia 7.1.3.1 CP SMIME.

7.1.3.1.1 RSA

Pozri sekcia 7.1.3.1.1 CP SMIME.

7.1.3.1.2 ECDSA

Žiadne ustanovenia.

7.1.3.1.3 EdDSA

Žiadne ustanovenia.

7.1.3.2 Identifikátor algoritmu podpisu

Pozri sekcia 7.1.3.2 CP SMIME.

7.1.3.2.1 RSA

Pozri sekcia 7.1.3.2.1 CP SMIME.

7.1.3.2.2 ECDSA

Žiadne ustanovenia.

7.1.3.2.3 EdDSA

Žiadne ustanovenia.

7.1.4 Formy mien

Žiadne ustanovenia.

7.1.4.1 Kódovanie názvu

Žiadne ustanovenia.

7.1.4.2 Informácie o subjekte – certifikáty koncových držiteľov

Žiadne ustanovenia.

7.1.4.2.1 Rozšírenie „Subject alternative name“

Položka certifikátu	**Vyžadovaná/ Voliteľná**	Obsah
extensions:subjectAltName	Musí byť Prítomná	Toto rozšírenie bude obsahovať jednu položku *GeneralName* typu: ▪ Rfc822Name

7.1.4.2.2 Položky rozlišovacieho mena subjektu (Distinguished Name)

RA Poskytovateľa majú oprávnenie vydávať 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 budú uvádzané ako povinné 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 bude obsahovať niektorú z nižšie uvedených hodnôt overených v zmysle sekcie 0

Typ certifikátu	Obsah
Organization-validated	*subject:organizationName*
Sponsor-validated	Meno a priezvisko
Individual-validated	

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

Bude obsahovať úplný názov organizácie (právnickej osoby) overený v zmysle 3.2.3. RA Poskytovateľa umožní 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 sekcie 3.1.4.1 CP SMIME.

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

Žiadne ustanovenia.

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

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

Použitá registračná schéma uvedená v certifikáte bude 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 podporuje Poskytovateľ ako platné pre vydávanie S/MIME certifikátov za platné v zmysle požiadaviek [3] na použitie v položke *subject:organizationIdentifier*:

- NTR: Pre identifikátor pridelený národným alebo štátnym obchodným registrom právnickej osobe uvedenej „*subject:organizationName*“;
- VAT: Pre identifikátor pridelený vnútroštátnymi daňovými úradmi právnickej osobe uvedenej *v* „*subject:organizationName*“.

Kód krajiny použitý v identifikátore registračnej schémy sa bude 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 **„***subject:surname* (2.5.4.4)**“**

Bude obsahovať meno fyzickej osoby overené podľa sekcie 3.2.4 v bežne používanom tvare Meno a priezvisko, oddelené medzerou.

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

Žiadne ustanovenia.

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

Bude uvedená na rozlíšenie jedinečnosti Držiteľa certifikátu a bude obsahovať jedinečné číslo spojené s daným držiteľom certifikátu.

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

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

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

Žiadne ustanovenia.

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

Žiadne ustanovenia.

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

Bude obsahovať informáciu o lokalite subjektu overenú 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)**“**

Žiadne ustanovenia.

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

Žiadne ustanovenia.

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

Položka bude 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

Žiadne ustanovenia.

7.1.4.3.1 Polia rozlišovacieho mena subjektu

Žiadne ustanovenia.

7.1.5 Obmedzenia týkajúce sa mien

Žiadne ustanovenia.

7.1.6 Identifikátor certifikačnej politiky

Pozri sekcia 7.1.6 CP SMIME.

7.1.6.1 Vyhradené identifikátory certifikačnej politiky

Tieto vyhradené identifikátory certifikačnej politiky definované CA/Browser Forum budú uvádzané Poskytovateľom, aby potvrdili, že vydaný 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

Žiadne ustanovenia.

7.1.6.3 Certifikát podriadenej CA

Žiadne ustanovenia.

7.1.6.4 Certifikát koncového používateľa

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

Certifikát bude navyše obsahovať aj identifikátor CP SMIME definovaný Poskytovateľom v tvare OID=1.3.158.35975946.0.0.0.1.11 ako aj URI adresu, kde je predmetná politika dostupná.

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

Žiadne ustanovenia.

7.3 Profil OCSP

7.3.1 Verzia

Žiadne ustanovenia.

7.3.2 OCSP rozšírenia

Žiadne ustanovenia.

8. Audit zhody

Žiadne ustanovenia.

8.1 Frekvencia auditu zhody pre danú entitu

Žiadne ustanovenia.

8.2 Identita audítora a kvalifikačné požiadavky na neho

Žiadne ustanovenia.

8.3 Vzťah audítora k auditovanému subjektu

Žiadne ustanovenia.

8.4 Témy pokryté audiom

Žiadne ustanovenia.

8.5 Akcie vykonané na odstránenie nedostatkov

Žiadne ustanovenia.

8.6 Zaobchádzanie s výsledkami auditu

Žiadne ustanovenia.

8.7 Interný audit

Počas obdobia, v ktorom Poskytovateľ vydáva certifikáty monitoruje dodržiavanie CP SMIME a týchto CPS zo strany RA Poskytovateľa a kontroluje kvalitu ich služieb vykonávaním vlastných auditov aspoň 1x ročne 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

Žiadne ustanovenia.

9.1.1 Poplatky za vydanie certifikátu

Žiadne ustanovenia.

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

Žiadne ustanovenia.

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

Žiadne ustanovenia.

9.4.2 **Informácie považované za osobné údaje**

Žiadne ustanovenia.

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

Žiadne ustanovenia.

9.4.4 **Zodpovednosť za ochranu osobných údajov**

RA Poskytovateľa musia chrániť osobné údaje pomocou vhodných bezpečnostných opatrení a primeranej starostlivosti.

9.4.5 Súhlas so spracovaním osobných údajov

Žiadne ustanovenia.

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**

Pozri sekcia 9.6.1. CP SMIME.

9.6.2 Vyhlásenia a záruky RA

Žiadne ustanovenia.

9.6.3 Vyhlásenie a záruky **Držiteľa**

Pozri sekcia 9.6.3 CP SMIME.

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

Žiadne ustanovenia.

9.9 Náhrada škody

Žiadne ustanovenia.

9.10 Doba platnosti, ukončenie platnosti

9.10.1 Doba platnosti

Tato verzia CPS platí odo dňa nadobudnutia jej platnosti t. j. 1.9.2023 až do jej nahradenia novou verziou. Podrobnosti o histórii zmien tejto CPS sú uvedené v časti 1.2.1 „História zmien“.

9.10.2 Ukončenie platnosti

Platnosť tejto verzie CPS skončí dňom publikovania novej verzie s vyšším číslom ako je 1.0, 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 CPS 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 CPS 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 CPS 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 CPS 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 týchto CPS musí byť očíslovaná a evidovaná, tak že novšia verzia musí mať vyššie číslo verzie ako tá, ktorú nahradzuje .

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

9.12.2 Postup a periodicita oznamovania zmien

Poskytovateľ publikuje informácie týkajúce sa aktuálnej verzie CPS prostredníctvom svojho webového sídla

https://eidas.disig.sk/sk/poskytovatel/politiky-a-dokumenty/

Poverený zástupca Poskytovateľa informuje všetky zmluvne viazané RA Poskytovateľa o schválení novej verzie CPS, zaslaním jeho verzie elektronickou poštou ešte pred nadobudnutím jeho účinnosti v zmysle časti 9.12.1.

Aktuálna verzia CPS je k dispozícii na každej zmluvne viazanej RA Poskytovateľa minimálne v elektronickej forme. Interní zamestnanci sú informovaní o novej verzii týchto CPS.

9.12.3 Okolnosti zmeny OID

Žiadne ustanovenia.

9.13 Riešenie sporov

Žiadne ustanovenia.

9.14 Rozhodné právo

Žiadne ustanovenia.

9.15 Súlad s platnými právnymi predpismi

Žiadne ustanovenia.

9.16 Rôzne ustanovenia

9.16.1 Rámcová dohoda

Žiadne ustanovenia.

9.16.2 Postúpenie práv

Žiadne ustanovenia.

9.16.3 Salvatórska klauzula

Žiadne ustanovenia.

9.16.4 Uplatnenie práv

Žiadne ustanovenia.

9.16.5 **Vyššia moc**

Žiadne ustanovenia.

9.17 Iné ustanovenia

Žiadne ustanovenia.