Pravidlá na výkon certifikačných činností certifikačnej autority CA Disig Časť - Registračná autorita

Pravidlá
verzia 4.4
platné od 01.07.2012

DISIG, a.s.

Záhradnícka 151

821 08 Bratislava 2

História zmien

Verzia	Dátum revízie	Popis revízie; revidoval
1.0	25.03.2006	Prvá verzia dokumentu; Miškovič
1.5	20.12.2006	Formálne úpravy textu dokumentu – formátovanie, opravy odkazov, úpravy textu v kapitole 4 „Prevádzkové požiadavky“; Miškovič
3.0	19.03.2008	Celková revízia CP vzhľadom k jednotlivým typom certifikátov; Ďurišová, Miškovič.
3.1	24.06.2008	Pridanie nového typu certifikátu; Miškovič
3.2	10.11.2008	Zrušenie prevádzky na Záhradníckej 153.
3.3	25.11.2008	Úprava znenia: ods. 3.1.9 - overovanie vlastníctva domény ods. 4.1.1, 4.1.2, - overovanie platnosti e-mail adresy žiadateľa
3.4	02.06.2009	Úprava v súvislosti s požiadavkou na minimálnu dĺžku verejného kľúča, na ktorý CA Disig vydá certifikát (ods.5.1.3; 6.1.2); Zmena umiestnenia e-mail adresy v profile certifikátu (ods. 3.1.2; 6.1.2); Miškovič
4.0	14.10.2009	Úprava v súvislosti s požiadavkami Mozilla Foundation pri uchádzaní sa o umiestnenie certifikátu CA Disig do Mozilla Root Certificate Store
4.1	11.05.2010	Zapracovanie navrhnutých nápravných opatrení z auditu zo dňa 13.11.2009 (audit podľa ETSI TS 102042 V1.3.4); Miškovič
4.2	11.03.2011	Zmena dĺžky platnosti certifikátov; zapracovanie požiadaviek novej bezpečnostnej politiky Mozilla Foundation a požiadaviek Microsoft (code signing); formálne úpravy tabuliek a textov; Miškovič
4.3	25.01.2012	Doplnenie možnosti vydávania podriadených CA a pravidelná ročná revízia obsahu; Miškovič
4.4	22.06.2012	Zapracovanie požiadaviek dokumentu „Baseline Requirements for the Issuance and Management of Publicly-Trusted Certificates, v.1.0, ktorý vydala CA/Browser Forum

Obsah

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

Tento dokument neprešiel jazykovou úpravou.

Ochranné známky

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

Zoznam použitých pojmov a skratiek

Pojmy

Zmluvný partner – právnická osoba, s ktorou ma spoločnosť Disig uzatvorenú písomnú zmluvu o vydaní a používaní certifikátu a služieb CA Disig.

Skratky

CP	–	Certifikačný poriadok (Certificate Policy)
CA	–	Certifikačná autorita (Certification Authority)
OID	–	Identifikátor objektu (Object Identifier)
PKI		Infraštruktúra verejných kľúčov (Public Key Infrastructure)
PMA	–	Autorita pre správu CP (Policy Management Authority)
CPS	–	Pravidlá na výkon certifikačných činností (Certificate Practice Statement)
RA	–	Registračná autorita (Registration Authority)
EFTA	–	Európska zóna voľného obchodu (European Free Trade Association) – členovia Island, Lichtenštajnsko, Nórsko a Švajčiarsko
CRL	–	Zoznam zrušených certifikátov (Certification Revocation List)
HSM	–	Hardware Security Modul
NBÚ	–	Národný bezpečnostný úrad
CMA	–	Autorita pre správu certifikátov (Certificate Management Authority)
IČO	–	Identifikačné číslo organizácie

1. Úvod

Tento dokument definuje pravidlá na výkon certifikačných činností (Certificate Practice Statement, ďalej len „Pravidlá“) pre registračnú autoritu (ďalej len „RA“) CA Disig (ďalej len „CA Disig“). Pravidlá vychádzajú z certifikačného poriadku CA Disig, ktorý sa uplatňuje pri implementovaní infraštruktúry verejných kľúčov (ďalej len „PKI“) pozostávajúcej z produktov a služieb, ktoré poskytujú a spravujú certifikáty podľa štandardu X.509 pre kryptografiu verejných kľúčov.

Certifikát jednoznačne identifikuje entitu, ktorej je vydávaný a túto entitu zväzuje s príslušným párom kľúčov pričom certifikát je vydávaný na ich verejnú časť.

1.1 Prehľad

Tieto pravidlá predstavujú pravidlá na výkon certifikačných činností na základe ktorých je spoločnosťou Disig, a.s., (ďalej len „Disig“), zriadená a prevádzkovaná CA Disig a popisujú činnosť RA.

Pravidlá boli vytvorené v súlade s vyhláškou NBÚ č. 133/2009 Z. z. o obsahu a rozsahu prevádzkovej dokumentácie vedenej certifikačnou autoritou a o bezpečnostných pravidlách a pravidlách na výkon certifikačných činností a na základe materiálov Internet X.509 Public Key Infrastructure - Certificate Policy and Certification Practices Framework (RFC3647) a Internet X.509 Public Key Infrastructure - Certificate and Certificate Revocation List (CRL) Profile (RFC5280).

Tieto pravidlá definujú vytváranie a správu certifikátov s verejnými kľúčmi podľa štandardu X.509 verzie 3 pre ich použitie v aplikáciách, ktoré si vyžadujú bezpečnú komunikáciu medzi počítačovými systémami pripojenými na počítačovú sieť.

Kostrová časť takejto počítačovej siete môže byť pritom nechránenou sieťou ako napr. internet.

1.2 Identifikácia

Názov:	**Pravidlá na výkon certifikačných činností certifikačnej autority CA Disig Časť - Registračná autorita**
Skratka názvu:	**CPS RA CA Disig**
Verzia:	**4.4**
Schválené dňa:	**22.06.2012**
Platnosť od:	**01.07.2012**
Tomuto dokumentu je priradený identifikátor objektu (OID):	**1.3.158.35975946.0.0.0.1.3.4.4**

Popis použitého identifikátora objektu (OID):

1. – ISO assigned OIDs

1.**3**. – ISO Identified Organization

1.3.**158**. – Identifikačné číslo subjektu (IČO)

1.3.158.35975946. – Disig, a.s.

1.3.158.35975946.**0.0.0.1.**– **CA Disig**

1.3.158.35975946.0.0.0.1.**3.** – **CPS RA CA Disig**

1.3.158.35975946.0.0.0.1.1.3.**4.4** - CPS RA CA Disig **verzia 4.4**

Tieto CPS sa týkajú osobných certifikátov, certifikátov pre právnickú osobu, certifikátov pre server a certifikátov pre softvérový komponent vydávaných CA Disig. Ostatné typy certifikátov sú popísané v samostatných CPS.

Pojmom certifikát resp. certifikát CA Disig sa v tomto dokumente označuje ľubovoľný z vyššie uvedených certifikátov vydaný CA Disig.

1.3 Komunita a použiteľnosť

1.3.1 Autority

Autorita pre správu politiky (Policy Management Authority (ďalej len „PMA“) je zložka ustanovená za účelom:

- dohľadu na vytváranie a aktualizáciu certifikačných politík, vrátane vyhodnocovania zmien a plánov na implementovanie ľubovoľných prijatých zmien
- revízie pravidiel CA Disig, aby sa zaručilo, že prax CA vyhovuje príslušnej certifikačnej politike

- revízie výsledkov auditov zhody, aby sa určilo, či CA adekvátne dodržuje ustanovenia tohto dokumentu, ďalej potom dávanie odporúčaní pre CA ohľadne nápravných akcií a iných vhodných opatrení
- riadenia a usmerňovania činnosti certifikačnej autority a registračných autorít
- na požiadanie robí výklad ustanovení týchto pravidiel a svojich pokynov pre RA a CA
- vykonávania auditu CA Disig
- vykonávania revízie týchto pravidiel prostredníctvom ich analýzy, aby sa zaručilo, že prax CA vyhovuje príslušnej certifikačnej politike
- zabezpečenia, že tieto pravidlá na výkon certifikačných činnosti (CPS) sú riadne a náležite realizované.

PMA predstavuje vrcholovú zložku, ktorá rozhoduje s konečnou platnosťou vo všetkých záležitostiach a aspektoch týkajúcich sa CA Disig a jej činnosti.

1.3.1.1 Certifikačná autorita

Certifikačná autorita (Certification Authority - CA) je entita autorizovaná PMA na vytváranie, podpisovanie a vydávanie certifikátov s verejným kľúčom.

CA je zodpovedná za všetky aspekty vydávania a správy certifikátov, vrátane kontroly nad procesom registrácie, procesom identifikácie a autentizácie, procesom vytvárania certifikátov, publikácie certifikátov, zrušovania certifikátov. CA zaručuje, že všetky aspekty jej služieb a operácií a infraštruktúry zviazanej s certifikátmi vydanými podľa týchto pravidiel sa vykonávajú v súlade s ich požiadavkami a ustanoveniami.

1.3.1.2 Registračné autority

Zložkou CA Disig, o ktorej detailne pojednávajú tieto pravidlá sú:

- Komerčná registračná autorita
- Interná registračná autorita

Pokiaľ sú vytvárané registračné autority na základe písomnej zmluvy s obchodným partnerom a tento bude prevádzkovať vlastné registračné autority, pre takýto typ budú vydávané samostatné pravidlá na výkon certifikačných činností danej registračnej autority.

Spoločný termín pre CA a RA je autority na správu certifikátov (Certificate Management Authority, ďalej len „CMA“). Termín CMA sa bude používať, keď funkciu možno priradiť buď CA alebo RA, prípadne keď sa požiadavka týka súčasne CA aj RA.

1.3.2 Koncové entity

1.3.2.1 Žiadatelia o certifikát CA Disig a držitelia certifikátov CA Disig

Žiadateľom o certifikát sa rozumie fyzická osoba, ktorá je oprávnená žiadať o certifikát v mene entity, ktorej meno sa objaví ako subjekt v certifikáte.

Entitou, ktorej meno sa objaví ako subjekt v certifikáte, môže byť:

- fyzická osoba,
- právnická osoba,
- komponent.

Žiadateľ o certifikát sa prevzatím certifikátu stáva držiteľom daného certifikátu.

Podmienky, ktoré musí žiadateľ o certifikát CA Disig splniť, definuje dokument CP CA Disig.

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

1.3.2.2 Strany spoliehajúce sa na certifikáty

Stranou spoliehajúcou sa na certifikát je entita, ktorá tým, že používa cudzí certifikát na overenie integrity elektronicky podpísanej správy, alebo na ustanovenie bezpečnej komunikácie s držiteľom certifikátu, sa spolieha na platnosť väzby držiteľa certifikátu s daným verejným kľúčom.

Strana spoliehajúca sa na certifikát by mala použiť informáciu z certifikátu na určenie vhodnosti certifikátu na dané použitie.

Synonymom pojmu strana spoliehajúca sa na certifikát je pojem používateľ certifikátu. Tento koná na základe dôvery v daný certifikát a/alebo na základe elektronického podpisu overeného daným certifikátom.

1.3.3 Použiteľnosť

Certifikáty CA Disig sú vo všeobecnosti určené na zabezpečenie komunikácie pomocou softvéru resp. hardvéru, ktorý podporuje využitie certifikátov vyhovujúcich špecifikácii X.509 verzie 3.

Účelom vydávania certifikátov CA Disig je vo všeobecnosti poskytnúť používateľovi certifikátu také prostriedky (certifikáty) na zabezpečenie komunikácie, aby mohol využívať výhody bezpečnej komunikácie s minimálnymi nákladmi, napr. vhodným používaním bežne dostupného softvéru ako je napr. prehliadač Microsoft Explorer, poštoví klienti Microsoft Outlook Express, Microsoft Outlook, softvér na strane servera typu Apache, Microsoft IIS a podobne.

Certifikáty vydané CA Disig môžu byť vo všeobecnosti použité pre potreby:

- zabezpečenia elektronickej pošty (podpisovanie a/alebo šifrovanie správ posielaných elektronickou poštou, neodmietnuteľnosť zodpovednosti za odoslanú správu elektronickej pošty),
- podpisovanie elektronických dokumentov,
- zabezpečenia WWW komunikácie (dôveryhodná identifikácia web servera resp. klienta),
- zabezpečovacích mechanizmov pracovných staníc používateľov,
- interných procesov PKI (bezpečná komunikácia medzi komponentmi PKI a pod.),

- podpisovanie softvérových komponentov.

CA Disig vydáva zákazníkom tieto typy certifikátov:

- osobné certifikáty – určené v prvom rade pre potreby zabezpečenia elektronickej pošty pre fyzickú osobu (ďalej len „osobný certifikát“) resp. fyzickú osobu konajúcu v mene právnickej osoby (ďalej len „certifikát pre právnickú osobu“),
- certifikáty pre server – určené v prvom rade pre potreby zabezpečenia komunikácie s web servermi,
- osobné certifikáty pre doménového používateľa – určené pre potreby prihlasovania sa do domény resp. vzájomnej komunikácie medzi užívateľmi príslušnej domény,
- certifikáty pre doménový radič – určené výhradne na zabezpečenie komunikácie pre doménové radiče danej domény,
- osobné certifikáty firemných zákazníkov – určené pre potreby vzájomnej komunikácie v rámci danej organizácie a na zabezpečenie vzájomnej komunikácie aplikácií používaných danou organizáciou a jej klientmi,
- certifikáty na podpisovanie softvérových komponentov.

CA Disig potvrdzuje, že v tomto CPS sú zohľadnené všetky požiadavky aktuálnej verzie dokumentu „Baseline Requirements for the Issuance and Management of Publicly-Trusted Certificates“, ktorá je publikovaná na stránke http://www.cabforum.org. V prípade akýchkoľvek rozporuplností medzi týmito požiadavkami a týmto CP, majú prednosť požiadavky dané aktuálnou verziou dokumentu „Baseline Requirements for the Issuance and Management of Publicly-Trusted Certificates“.

1.4 Kontaktné údaje

Registračná autorita CA Disig	
Adresa:	**Záhradnícka 151, 821 08 Bratislava 2**
e-mail:	**radisig@disig.sk**
telefón	**+421 2 20850140**
fax:	**+421 2 20850141**
www:	**http://www.disig.sk**

Zriaďovateľ, prevádzkovateľ a majiteľ CA Disig	
Spoločnosť:	**Disig, a.s.**
Adresa sídla:	**Záhradnícka 151, 821 08 Bratislava 2**
IČO:	**359 75 946**
telefón	**+421 2 20850140**
fax:	**+421 2 20828141**
e-mail:	**disig@disig.sk**
www:	**http://www.disig.sk** (slovenská verzia) **http://www.disig.eu** (anglická verzia)

2. Všeobecné ustanovenia

2.1 Povinnosti

2.1.1 Povinnosti RA

Registračné autority zriadené spoločnosťou Disig a vykonávajúce činnosti v mene CA Disig zabezpečuje funkciu podateľne pre CA Disig – konkrétne najmä zhromažďovanie a overovanie informácií od zákazníkov – žiadateľov o certifikát, ktoré majú byť uvedené v certifikátoch.

Na RA sa realizuje priamy kontakt medzi zákazníkmi a CA Disig.

RA prijíma žiadosti o certifikáty, preveruje totožnosť žiadateľov o certifikáty, odovzdáva vydané certifikáty ich držiteľom alebo nimi splnomocneným subjektom, sprostredkuje odovzdanie certifikátov a zoznamu zrušených certifikátov zákazníkom, prijíma a vybavuje ich reklamácie a sťažnosti, vyberá od zákazníkov stanovené poplatky za služby CA.

Pri svojej činnosti sa RA riadi týmto pravidlami.

RA zodpovedá za to, že ňou zbierané informácie RA overila a teda že tieto informácie sú v danom čase pravdivé.

Pracovníci RA sú povinní najmä:

- riadiť sa ustanoveniami certifikačného poriadku CA Disig, týchto pravidiel a pokynmi PMA,
- uchovávať v utajení súkromný kľúč RA – kompromitáciu súkromného kľúča, stratu svojej čipovej karty prípadne zabudnutie hesla na prístup k svojmu súkromnému kľúču bezodkladne hlásiť PMA,
- uchovávať korešpondenciu pracoviska RA realizovanú v písomnej alebo elektronickej forme a podľa pokynov odosielať písomné dokumenty RA na archiváciu,
- viesť záznamy o činnosti pracoviska RA v knihe „Záznamy registračnej autority CA Disig“,
- do „Záznamy registračnej autority CA Disig“ zaznamenávať všetky ostatné udalosti na RA, hlavne udalosti týkajúce sa súkromného kľúča RA (jeho kompromitácia, prijatie alebo strata čipovej karty, zabudnutie hesla), bezpečnosti pracoviska RA, prijatie (a spôsob vybavenia) podnetu, pripomienky alebo žiadosti o výklad CP a CPS,
- email komunikáciu robiť výlučne podpísanými a podľa možnosti aj šifrovanými správami,
- vykonávať registráciu zákazníkov – žiadateľov o certifikát, v rámci nej overovať ich identitu, hodnoty položiek rozlišovacieho mena nachádzajúce sa v žiadosti o certifikát, formát žiadostí o certifikát,

zhromažďovať dokumenty použité v procese registrácie, ktoré nevyhovujú ustanoveniam tohto dokumentu, odmietnuť,

- prijaté žiadosti o certifikát postúpiť na vybavenie tým, že ich vloží spolu s potrebnými údajmi do informačného systému CA Disig.
- niesť zodpovednosť za to, že ňou zbierané informácie overila a teda že tieto informácie sú v danom čase pravdivé.
- prijímať, protokolovať a postupovať na vybavenie podnety, pripomienky alebo žiadosti o výklad CP a CPS a ak ich riešenie na základe tohto dokumentu alebo iných pokynov záväzných pre RA nie je jasné, postúpiť ich na vybavenie PMA
- prijímať žiadosti o zrušenie certifikátu – oprávnené postúpiť na vybavenie, ostatné odmietnuť
- vyberať od zákazníkov stanovené poplatky za služby CA Disig

RA je oprávnená z naliehavých technických alebo prevádzkových dôvodov pozastaviť svoju činnosť na nevyhnutne potrebnú dobu.

Túto skutočnosť je povinná bezodkladne hlásiť PMA.

Špeciálnym prípadom RA je tzv. mobilná registračná autorita. Mobilná RA plní funkciu mobilnej podateľne, hlavne na báze zmluvy s konkrétnym zákazníkom CA Disig. Pokiaľ nie je stanovené osobitnou zmluvou so zákazníkom CA Disig inak, mobilná RA koná ako obyčajná RA.

RA, ktorá vykonáva registračné funkcie popísané v tejto CPS, musí vyhovovať ustanoveniam tohto dokumentu a konať podľa neho. Ak sa zistí, že RA nekoná v súlade s týmito povinnosťami, uplatnia sa na ňu príslušné opatrenia vrátane zastavenia jej činnosti ako RA.

2.1.2 Povinnosti držiteľa certifikátu

Povinnosťou držiteľa certifikátu je:

- neustále chrániť svoje súkromné kľúče v súlade s týmito pravidlami a tiež ako je stanovené v jeho zmluve o vydaní a používaní certifikátu CA Disig,
- bezodkladne upovedomiť CMA, ktorá vydala jeho certifikát, o podozrení, že jeho súkromný kľúč bol kompromitovaný alebo stratený a toto upovedomenie musí byť urobené prostredníctvom mechanizmu, ktorý je v súlade s týmto dokumentom,
- dodržovať všetky lehoty, podmienky a obmedzenia uložené na používanie svojich súkromných kľúčov a certifikátov,
- precízne sa identifikovať a vyjadrovať pri ľubovoľnej komunikácii s RA resp. CA,
- používať poskytnuté certifikáty len na patričné účely

Povinnosti držiteľa certifikátu sa týkajú aj osoby, ktorá prevzala certifikáty pre ňou spravované komponenty. (pozri časť 5.2)

Držiteľ certifikátu, ktorý nedodržuje resp. nedodržoval svoje povinnosti, stráca nárok na náhradu prípadnej škody.

2.1.3 Povinnosti strán spoliehajúcich sa na certifikáty

Strany spoliehajúce sa na certifikáty vydané podľa tejto CPS sú povinné:

- používať certifikát na účel, na ktorý bol vydaný, ako je to dané informáciami v certifikáte,
- predtým, ako sa na certifikát spoľahnú, overovať každý certifikát na jeho platnosť (tzn. overovať, že certifikát je v danom čase platný a že sa nenachádza na aktuálnom zozname zrušených certifikátov vydanom CA Disig)
- vytvoriť vzťah dôvery k CA, ktorá vydala daný certifikát, verifikovaním certifikačnej cesty v súlade so štandardom X.509 verzie 3 (tzn. napr. zabezpečiť, aby používaný softvér resp. hardvér mal pre svoju správnu funkciu vhodným spôsobom k dispozícii certifikát CA Disig, aby bolo možné overiť digitálny podpis CA na danom certifikáte),
- uchovávať originálne podpísané dáta, aplikácie potrebné na čítanie a spracovanie týchto dát a kryptografické aplikácie potrebné na overovanie digitálnych podpisov týchto dát, pokiaľ môže byť potrebné overovať podpis týchto dát

2.1.4 Povinnosti správy repozitára

Správa repozitára, ktorý podporuje CA pri publikovaní informácií podľa týchto pravidiel, je povinná

- udržovať prístupnosť informácií podľa ustanovení týchto pravidiel pre publikovanie informácií o certifikátoch
- poskytovať mechanizmus riadenia prístupu dostatočný na ochranu informácií uložených v repozitári podľa časti 2.6.3

2.2 Právne záruky

Tieto pravidlá sa riadia platnými zákonmi Slovenskej republiky, najmä zákonom č. 215/2002 Z. z. o elektronickom podpise a o zmene a doplnení niektorých zákonov a súvisiacimi vyhláškami Národného bezpečnostného úradu.

CA Disig garantuje jednoznačnosť čísla (Serial Number) každého ňou vydaného certifikátu, tzn. garantuje, že neexistujú a nikdy nebudú existovať žiadne dva certifikáty, ktoré by mali rovnaké číslo.

CA Disig poskytuje záruku, že ňou vydaný certifikát bude vyhovovať štandardu X.509 verzie 3 a bude v súlade s týmto dokumentom.

2.3 Finančná zodpovednosť

CA Disig zodpovedá za škody vzniknuté používaním ňou vydaného certifikátu v zmysle platnej legislatívy (napr. Obchodný zákonník, Občiansky zákonník). Predpokladom pritom je, že boli dodržané príslušné ustanovenia CP CA Disig.

Zodpovednosť za škodu a z nej vyplývajúce plnenie je možné uznať len za predpokladov, že zákazník neporušil svoje povinnosti (hlavne ochranu svojho súkromného kľúča), a že každý, kto sa v danom prípade spoliehal na certifikát vydaný CA Disig, urobil všetko, aby prípadnej škode zabránil a to , hlavne že si overil aktuálny stav predmetného certifikátu (t.j. či daný certifikát nebol v rozhodujúcom čase, keď sa na neho spoliehalo, na zozname zrušených certifikátov).

Neoverenie stavu certifikátu pomocou zoznamu zrušených certifikátov sa kvalifikuje ako hrubé porušenie povinností vyplývajúcich z CP CA Disig, dôsledkom čoho zanikajú akékoľvek nároky na prípadné uplatňovanie si záruky. CA Disig a ani zriaďovateľ CA Disig nemajú žiadnu finančnú zodpovednosť za prípadné škody, ktoré by vznikli držiteľovi certifikátu, alebo strane spoliehajúcej sa na certifikát, v súvislosti s používaním certifikátu CA Disig s nejakou konkrétnou aplikáciou resp. hardvérom, alebo v súvislosti s tým, že certifikát CA Disig nie je možné používať s nejakou konkrétnou aplikáciou resp. hardvérom.
Akákoľvek žiadosť o náhradu škody musí byť podaná písomne.

2.4 Rozhodcovské konanie a riešenie sporov

Pre potreby interpretácie ustanovení politiky alebo tohto dokumentu alebo riešenia sporov sa možno obrátiť na RA a v prípade nesúhlasu s jej rozhodnutím na najbližšiu vyššiu inštanciu. Inštancie sú usporiadané vzostupne v poradí:

- RA
- PMA (vybavuje len písomne podané žiadosti a podnety)

V prípade akýchkoľvek sporov o interpretácii ustanovení týchto pravidiel alebo ich použiteľnosti rozhoduje s konečnou platnosťou PMA.

Povinnosťou každej inštancie je prípad zaprotokolovať a dať žiadateľovi resp. sťažovateľovi vysvetlenie resp. návrh na riešenie sporu a v prípade jeho nesúhlasu prípad postúpiť na vyššiu inštanciu.

Žiadnym rozhodnutím niektorej z tu definovaných inštancií nie je dotknuté právo sťažovateľa postúpiť sťažnosť nezávislému súdu.

2.5 Poplatky

CA Disig bude vhodným spôsobom zverejňovať platný cenník svojich služieb. Cenník je zverejnený prostredníctvom web stránky CA Disig (pozri časť 1.4).

V prípade poskytovania svojich služieb len zmluvným partnerom cenník služieb nie je zverejňovaný.

2.6 Zverejňovanie informácií a repozitár

2.6.1 Zverejňovanie informácií o CA

CA zverejňuje informácie na Internete v on-line režime prostredníctvom svojho webu - repozitár, ktorý je prístupný držiteľom certifikátov a stranám spoliehajúcim sa na certifikáty a ktorý obsahuje:

- všetky certifikáty, ktoré CA vydala, pričom sa tieto zverejňujú prostredníctvom služby na vyhľadávanie certifikátov.,
- aktuálne CRL ako aj všetky CRL vydané od začiatku činnosti vydávania certifikátov,
- certifikát CA Disig (patriaci k jej podpisovému kľúču),
- v elektronickej forme kópiu platného Certifikačného poriadku CA Disig a Pravidiel na výkon certifikačných činnosti, časť Registračná autorita.

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

2.6.2 Frekvencia zverejňovania informácií

Certifikát sa publikuje ihneď po jeho vydaní a okamžite je možné jeho prevzatie držiteľom certifikátu. Informácie o vydanom certifikáte možno nájsť na web stránke spoločnosti Disig (www.disig.sk), ktorý slúži ako repozitár certifikačnej autority CA Disig.

CRL sa publikuje ako je špecifikované v časti 4.4.3.1. Informácie o zrušenom certifikáte možno nájsť na web stránke spoločnosti Disig (www.disig.sk), ktorý slúži ako repozitár certifikačnej autority CA Disig.

Všetky informácie, ktoré majú byť publikované v repozitári, sú publikované podľa možnosti čo najskôr.

Certifikáty vydávané pre uzatvorené systémy resp. pre interné účely CA Disig nie sú verejne dostupné a informácie o ich vydaní nie sú publikované v repozitári CA Disig.

2.6.3 Kontroly prístupu

CA Disig zodpovedajúcimi prostriedkami chráni ľubovoľnú informáciu uloženú v repozitári, ktorá nie je určená na verejné rozšírenie.

2.6.4 Repozitáre

Funkciu repozitára CA Disig zastáva webová stránka spoločnosti Disig, a.s., ktorej domovská stránka má URL uvedenú v časti 0. Repozitár je takto prostredníctvom Internetu verejne prístupný držiteľom certifikátov, stranám spoliehajúcim sa na certifikáty a verejnosti vôbec.

Verejne dostupné informácie uvedené na webovej stránke spoločnosti Disig majú charakter riadeného prístupu. Spoločnosť Disig vynakladá maximálne úsilie na to, aby zaistila integritu, dôvernosť a dostupnosť dát vyplývajúcich s poskytovaním certifikačných služieb. Taktiež boli vykonané logické a bezpečnostné opatrenia, aby zabránili neautorizovanému prístupu osobám, ktoré by mohli akýmkoľvek spôsobom zmeniť, poškodiť, pridať resp. vymazať údaje uložené v repozitári.

2.7 Audit zhody

2.7.1 Frekvencia auditu zhody pre danú entitu

CA sa podrobuje každoročnému auditu zhody.

2.7.2 Identita audítora a kvalifikačné požiadavky na neho

Audítor musí byť kompetentný v oblasti auditov zhody a musí byť dôkladne oboznámený s týmto dokumentom. Audítora menuje PMA.

Audit zhody môže vykonávať len osoba, ktorá spĺňa nasledovné požiadavky:

Ako osoba je:

a) etický, pravdovravný, úprimný, poctivý a diskrétny;

b) otvorený t.j. ochotný brať do úvahy alternatívne návrhy alebo pohľady;

c) diplomatický t.j. taktný pri jednaní s ľuďmi

d) samostatný t.j. pôsobí a jedná samostatne pri komunikácií s ostatnými partnermi

e) vlastní certifikát oprávňujúci ho k výkonu auditov informačných systémov

Ako audítor musí mať všeobecné znalosti v:

a) princípoch, postupoch a technikách vykonávania auditu, aby bolo zabezpečené , že audit nude prebiehať dôsledne a systematicky

b) legislatívnych požiadavkách kladených na systém, ktorý bude podrobovaný auditu,

Audítor musí dokumentovať svoju kompetenciu referenciami na vykonané audity obdobných IS.

2.7.3 Témy pokrývané auditom zhody

Účelom auditu zhody je záruka, že CA Disig má vyhovujúci systém práce RA, ktorý garantuje kvalitu služieb, ktoré CA Disig poskytuje a ktorý garantuje, že RA koná v súlade so všetkými požiadavkami týchto pravidiel. Predmetom auditu zhody sú všetky aspekty prevádzky CA Disig vzťahujúce sa k týmto pravidlám.

2.7.4 Akcie vykonané na odstránenie nedostatkov

Keď audítor zistí rozpor medzi prevádzkou RA CA Disig a ustanoveniami týchto pravidiel, musia sa uskutočniť nasledujúce akcie:

- audítor zaznamená rozpor,
- audítor upovedomí o rozpore subjekty definované v časti 2.7.5,
- CA Disig navrhne PMA zodpovedajúce opatrenie na nápravu vrátane očakávaného času potrebného na jeho realizáciu

PMA určí vhodné opatrenie na nápravu a to prípadne až po zrušenie certifikátu CA Disig. Po náprave nedostatkov PMA obnoví činnosť CA Disig resp. RA.

2.7.5 Zaobchádzanie s výsledkami auditu

Audítor zhody urobí pre PMA zápis o výsledkoch auditu zhody. Výsledky sú oznámené auditovanému subjektu (CA Disig resp. RA) a v prípade RA aj jej nadriadenej CA Disig.

Vykonanie opatrení na nápravu je dané na vedomie príslušnej autorite. Na potvrdenie vykonania a účinnosti opatrení na nápravu sa môže požadovať špeciálny audit zhody alebo čiastkový audit zhody zameraný na daný aspekt činnosti auditovaného subjektu.

2.8 Utajenie

2.8.1 Typy informácií, ktoré sa majú chrániť

Dôvernými informáciami podliehajúcimi zodpovedajúcej ochrane sú:

- súkromný kľúč CA Disig používaný na vytváranie elektronického podpisu pri vydávaní certifikátov CA Disig a certifikátov podriadených CA Disig,
- súkromné kľúče podriadených CA a poskytovaných služieb (TS resp. OCSP)
- súkromné kľúče patriace zložkám CA (AdmCA, RA),
- infraštruktúra (napr. dokumenty, procedúry, postupy, súbory, skripty, heslá, pass frázy a pod.) slúžiaca na prevádzku CA Disig, vrátane jej RA,
- informačný systém CA Disig a údaje uložené v ňom, z týchto údajov špeciálne osobné údaje držiteľov certifikátov podliehajúce ochrane v zmysle zákona č. 428/2002 Z. z. o ochrane osobných údajov v znení neskorších predpisov (ďalej len. Zákon č. 428/2002 Z. z.)

2.8.2 Okolnosti uvoľnenia dôverných informácií

CA Disig nezverejní žiadne informácie týkajúce sa žiadateľa o certifikát alebo držiteľa certifikátu žiadnej tretej strane, ak dané informácie nie sú považované za verejné, alebo ak to nie je požadované zákonom alebo príkazom

kompetentného štátneho orgánu, ako je polícia, súd, prokuratúra resp. je to predmetom zmluvy medzi CA Disig a jej partnerom.

Každá požiadavka na uvoľnenie informácií, ktoré nie sú považované za verejné, musí byť autentizovaná a zadokumentovaná.

CA Disig musí s osobnými údajmi zákazníka zaobchádzať v súlade s platnými zákonmi a nesmie ich poskytnúť žiadnej tretej strane s výnimkou subjektov, ktoré v zmysle zákona č 215/2002 Z. z. o elektronickom podpise a o zmene a doplnení niektorých zákonov v znení neskorších predpisov (ďalej len „zákon č. 215/2002 Z. z.“) majú právo kontrolovať činnosť CA Disig resp. v zmysle zákona č.428/2002 Z. z. môžu byť oprávnenými osobami.

2.9 Práva vyplývajúce z intelektuálneho vlastníctva

Vlastník CA Disig je vlastníkom všetkých autorských práv na všetky dokumenty, dáta, procedúry, politiky, certifikáty a súkromné kľúče, ktoré sú súčasťou infraštruktúry CA Disig a ktoré boli ňou vytvorené.

3. Identifikácia a autentizácia

3.1 Prvotná registrácia

Prijímané žiadosti o certifikát CA Disig musia vyhovovať štandardu PKCS #10 alebo SPKAC a musia byť vo formáte PEM, ak nebolo so zákazníkom vopred dohodnuté inak.

3.1.1 Typy mien

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

Žiadatelia o certifikát si sami zvolia rozlišovacie meno, ktoré má byť v ich certifikáte.

3.1.2 Potreba zmysluplnosti mien

Používané mená majú čo najjednoznačnejšie identifikovať osoby alebo iné subjekty resp. objekty, ktorým sú priradené. CMA má zaručovať, že existuje vzťah patričnosti (príslušnosti, členstva) medzi držiteľom certifikátu a ľubovoľnou organizáciou alebo organizačnou jednotkou, ktorá je identifikovaná ľubovoľnou časťou ľubovoľného mena v certifikáte daného držiteľa.

Dôraz sa pritom kladie na položku commonName, ktorá má jednoznačne reprezentovať držiteľa certifikátu spôsobom, ktorý je pre človeka ľahko pochopiteľný. V prípade osoby to bude typicky jej právoplatné meno a priezvisko. V prípade právnickej osoby to bude jej obchodné meno alebo názov. V prípade komponentu to môže byť napr. úplné doménové meno, názov modelu a sériové číslo alebo názov procesu a aplikácie, ap.

Pojem „zmysluplnosť“ znamená, že forma mena má bežne používanú sémantiku na určenie identity osoby, organizácie alebo jej časti, zariadenia a podobne.

Používanie pseudonymov, prezývok, krycích mien, aliasov a podobne (tzv. nicknames) v certifikátoch sa nepovoľuje – RA odmietne prijať žiadosť o certifikát, ktorá by obsahovala v rozlišovacom mene položku s takouto hodnotou.

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

Požiadavka na zmysluplnosť sa pritom vzťahuje na hodnotu ľubovoľnej položky v rozlišovacom mene. Porušenie tohto princípu môže byť príčinou odmietnutia vytvoriť certifikát z danej žiadosti o certifikát.

Pri zadávaní hodnôt do položiek žiadosti o certifikát musí žiadateľ o certifikát mať na zreteli, že na RA bude musieť uspokojivým spôsobom preukázať oprávnenosť všetkých údajov, ktoré zadal do jednotlivých položiek žiadosti o certifikát.

Rozlišovacie mená používané v certifikátoch CA Disig sú popísané v dokumente „Certifikačný poriadok CA Disig“ v časti 3.1.2.

3.1.3 Jedinečnosť mien

CA Disig nevynucuje jedinečnosť mien v rámci komunity držiteľov certifikátov, avšak samozrejme garantuje jednoznačnosť sériového čísla (Serial number) každého ňou vydaného certifikátu, tzn. garantuje, že neexistujú a nikdy nebudú existovať žiadne dva ňou vydané certifikáty, ktoré by mali rovnaké sériové číslo.

Okrem toho sa tiež vynucuje jednoznačnosť páru kľúčov certifikovaných daným certifikátom – v praxi to konkrétne znamená, že sa odmietne vydať certifikát verejného kľúča na žiadosť o certifikát obsahujúcej verejný kľúč, ku ktorému už bol zo strany CA Disig vydaný certifikát.

3.1.4 Procedúra riešenia sporov pri kolízii mien

V prípade sporov týkajúcich sa kolízie mien a mien vo všeobecnosti sa bude postupovať podľa ustanovení časti 2.4.

3.1.5 Rozpoznanie, autentizácia a rola obchodných značiek

Žiadnej entite sa negarantuje, že jej meno v certifikáte bude obsahovať jej obchodnú značku (trademark) a to ani na jej výslovnú žiadosť.

V certifikáte môžu byť použité len tie obchodné značky, ktorých vlastníctvo alebo prenájom žiadateľ o certifikát dôveryhodne doložil. Žiadnu inú autentizáciu obchodných značiek CMA nevykonáva.

CMA nevydá vedome certifikát obsahujúci meno, o ktorom kompetentný súd rozhodol, že porušuje obchodnú značku iného. CMA nebude povinné skúmať obchodné značky ani riešiť spory týkajúce sa obchodných značiek.

3.1.6 Preukazovanie vlastníctva súkromného kľúča

RA musí požadovať, aby žiadateľ o certifikát potvrdil, že vlastní súkromný kľúč, ktorý zodpovedá verejnému kľúču nachádzajúcemu sa v žiadosti o certifikát.

V prípade žiadosti o nový (následný) certifikát, ktorá bola vygenerované na nové kryptografické kľúče v softvérovom úložisku je prípustné, aby žiadateľ o certifikát potvrdil vlastníctvo svojho nového súkromného kľúča tak, že svoju novú žiadosť o certifikát zašle na RA podpísaným e-mailom. Pri podpise e-mailu so žiadosťou

musí žiadateľ použiť súkromný kľúč, na ktorý bol certifikačnou autoritou CA Disig vydaný certifikát, a tento je v čase overovania prijatého e-mailu platný.

V prípade doručenia žiadosti o certifikát elektronickou cestou, od žiadateľa, ktorý už vlastnil certifikát vydaný CA Disig, ktorá nemôže byť podpísaná súkromným kľúčom takéhoto certifikátu (certifikát neobsahuje rozšírenie na podpisovanie elektronickej pošty), bude vlastníctvo súkromného kľúča preverené kontaktovaním žiadateľa zo strany CA Disig a overením, že je pôvodcom danej žiadosti.

V prípade, keď si sám žiadateľ o certifikát generuje kľúč priamo do zariadenia na bezpečné vytváranie elektronického podpisu (Secure Signature Creation Device - SSCD), potom automaticky vlastní súkromný kľúč v čase jeho generovania.

Ak držiteľ certifikátu nevlastní SSCD v čase, keď sa jeho kľúč generuje na SSCD na RA, potom mu SSCD musí byť doručené dôveryhodným spôsobom.

Za dôveryhodný spôsob sa považuje doručenie zásielky do vlastných rúk.

CMA negeneruje páry kľúčov pre cudzie subjekty. Výnimkou môže byť len generovanie kľúčov na CMA priamo na SSCD zákazníka. Môže sa tak urobiť len v špeciálnych prípadoch na základe osobitnej písomnej zmluvy s daným zákazníkom, ktorá potvrdzuje výslovnú vôľu zákazníka, že CA Disig má pre neho generovať pár kľúčov na SSCD.

Žiadna zložka CA Disig v nijakom prípade nearchivuje žiadne súkromné kľúče patriace zákazníkom - cudzím subjektom.

3.1.7 Autentizácia identity právnickej osoby (organizácie)

Žiadateľ o certifikát konajúci v mene právnickej osoby musí predložiť názov právnickej osoby, iný identifikačný údaj, ak taký existuje (spravidla je to napr. IČO), adresu a dôkaz existencie danej právnickej osoby (spravidla výpisom z obchodného registra).

RA overuje tieto údaje a okrem identity oprávnenej osoby používateľa (žiadajúcej osoby) overuje, že daná osoba má právo jednať v mene danej právnickej osoby vo veci príslušného certifikátu.

Právnická osoba so sídlom v Slovenskej republike preukazuje svoju totožnosť výpisom z obchodného registra príp. iného platného registra právnických osôb. Bude vyžadovaný/á originál alebo úradne overená kópia originálu, nie starší/ia ako tri mesiace. Doklad musí obsahovať úplné obchodné meno alebo názov, identifikačný údaj (spravidla IČO), sídlo, meno/á osoby/osôb konajúcej/ich za právnickú osobu a spôsob konania a podpisovania za danú právnickú osobu.

V prípade, že právnická osoba nemá sídlo na území Slovenskej republiky, jej totožnosť sa overuje rovnakým spôsobom ako je uvedené vyššie. Výpis z platného registra právnických osôb musí byť úradne preložený do slovenského jazyka (okrem organizácií so sídlom v Českej republike).

Fyzické osoby, ktoré na základe predloženého výpisu z obchodného registra konajú na RA za danú právnickú osobu vo veci získania certifikátu, musia preukázať svoju totožnosť podľa časti 3.1.8.

V mene právnickej osoby môže na RA konať len oprávnená osoba používateľa t.j. osoba, ktorá je jej štatutárom (alebo viac takýchto osôb súčasne, ak to vyžaduje predložený výpis z obchodného registra), prípadne sa právnická osoba môže nechať zastupovať fyzickou alebo inou právnickou osobou.

Ak sa právnická osoba nechá zastupovať na RA, zastupujúca fyzická alebo právnická osoba musí vždy predložiť k nahliadnutiu overený výpis z obchodného registra zastupovanej právnickej osoby nie starší ako tri mesiace.

Ak sa právnická osoba nechá zastupovať na RA fyzickou osobou, táto zastupujúca fyzická osoba musí preukázať svoju totožnosť podľa časti 3.1.8 a navyše sa musí preukázať úradne overenou (notárom alebo matrikou) plnou mocou, z textu ktorej je jednoznačne jasné, že zastupujúca fyzická osoba bola splnomocnená splnomocňujúcou právnickou osobou konať v danej veci v jej mene.

Ak sa právnická osoba nechá zastupovať na RA inou právnickou osobou, táto zastupujúca právnická osoba okrem príslušnej plnej moci (viď predošlý odsek) musí preukázať svoju totožnosť rovnakým spôsobom ako zastupovaná právnická osoba, ako je to požadované vyššie.

Subjekt (fyzická alebo právnická osoba), ktorý zastupuje právnickú osobu, sa vo veci právnickej osoby, ktorú zastupuje, v žiadnom prípade nemôže nechať zastupovať iným subjektom.

V prípade, že právnická osoba nemôže preukázať svoju totožnosť výpisom z obchodného registra (platí pre nepodnikateľské subjekty ako sú napr. obec, cirkev, občianske združenie, nadácia, štátny orgán a podobne), musí takáto právnická osoba písomne preukázať okrem svojej totožnosti aj legálnosť (resp. „dôvod“) svojej existencie (s využitím a poukázaním na zákon alebo iný predpis, ktorý o subjekte daného typu pojednáva, zriaďovaciu listinu ap.).

3.1.8 Autentizácia identity fyzickej osoby

Fyzickou osobou môže byť plnoletý občan Slovenskej republiky alebo cudzí štátny príslušník.

Fyzická osoba musí preukázať svoju totožnosť dvomi z týchto osobných dokladov:

- občiansky preukaz,
- cestovný pas,
- vodičský preukaz,
- rodný list,
- povolenie na prechodný pobyt (resp. trvalý pobyt) v prípade cudzinca
- zbrojný preukaz
- služobný preukaz

Požaduje sa pritom, aby aspoň jeden z predkladaných dokladov bol dokladom, ktorého súčasťou je fotografia danej osoby. V prípade predloženia rodného listu, zbrojného preukazu alebo služobného preukazu sa musí predložiť aj jeden z týchto dokladov: občiansky preukaz alebo cestovný pas.

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

Ak právnická osoba zastupuje fyzickú osobu, okrem plnej moci (viď predošlý odsek) musí splnomocnená právnická osoba preukázať svoju totožnosť podľa časti 3.1.7.

Subjekt (fyzická alebo právnická osoba), ktorý zastupuje fyzickú osobu, sa vo veci fyzickej osoby, ktorú zastupuje, v žiadnom prípade nemôže nechať zastupovať iným subjektom.

3.1.9 Autentizácia identity komponentu

CMA musí garantovať aj v takomto prípade, že identita komponentu a jeho verejný kľúč sú zodpovedajúco previazané.

Hardvérový alebo softvérový komponent, ktorý bude používať certifikáty, bude predmetom certifikácie a je možné vytvoriť preň SSL certifikát resp. certifikát pre softvérový komponent. (t.j. nie osobný certifikát). V takom prípade komponent musí byť priradený fyzickej alebo právnickej osobe (organizácii), ktorá ho spravuje (viď časť 5.2).

Táto osoba alebo organizácia je povinná poskytnúť RA nasledujúce informácie, ako je to popísané v častiach 3.1.8 a 5.2:

- identifikáciu zariadenia (názov softvérového komponentu),
- verejný kľúč zariadenia (obsiahnutý v žiadosti o certifikát),
- autorizáciu zariadenia a jeho atribúty (ak nejaké majú byť uvedené v certifikáte),
- kontaktné údaje, aby CMA mohla v prípade potreby komunikovať s touto osobou,

RA musí autentizovať správnosť ľubovoľnej autorizácie (hodnoty položky rozlišovacieho mena), ktorá má byť uvedená v certifikáte a overuje predložené údaje.

Metódy na vykonanie tejto autentizácie a kontroly údajov zahrňujú:

- overenie identity danej osoby v súlade s požiadavkami časti 3.1.8,
- overenie identity organizácie, ktorej patrí daný komponent, v súlade s požiadavkami časti 3.1.7,
- overenie oprávnenosti použitia údajov, ktoré majú byť uvedené v jednotlivých položkách certifikátu, s dôrazom na obsah položky commonName.

Typickou hodnotou tejto položky bude úplné doménové meno.

Existencia domény a jej vlastník sa overí prostredníctvom služby WHOIS poskytovanej správcom internetovej domény najvyššej úrovne (napr. pre doménu „.sk“ je správcom SK-NIC – www.sk-nic.sk; pre doménu „.eu“ je správcom EURid

vzw/asbl so sídlom v Belgicku; pre doménu „.com“ je správcom VeriSign Global Registry Services so sídlom v USA).

Plné doménové meno sa overí zaslaním e-mailu, ktorý bude obsahovať tajnú nepredvídateľnú informáciu na niektoré e-mail účtov pre danú doménu uvedených v zázname získanom zo služby WHOIS resp. na e-mail pochádzajúci z danej domény na niektorý z týchto e-mail účtov: admin, administrator, webmaster, hostmaster alebo postmaster.

Žiadateľ o certifikát pre doménu musí zaslať späť overovaciu informáciu ako dôkaz vlastníctva domény v stanovenom časovom úseku.

V prípade, že nie je k dispozícii žiadna e-mailová adresa resp. z predpokladanej e-mail adresy nedostane RA späť overovaciu informáciu nakoľko táto neexistuje, musí RA vykonať ďalšie kroky na overenie vlastníctva domény napr. využiť publikované kontaktné údaje registrátora domény.

Pokiaľ z údajov získaných z vyššie uvedených zdrojov nie je možné dôveryhodne zistiť, že žiadateľ je vlastníkom resp. osobou vystupujúcou v mene vlastníka domény, RA odmietne vydanie certifikátu na danú žiadosť.

RA vykoná overenie všetkých položiek nachádzajúcich sa v DN certifikátu, s výnimkou položky organizationUnitName (Názov útvaru v organizácii). V prípade tejto položky sa vykoná len kontrola, či neobsahuje názov právnickej osoby, obchodné meno, obchodnú značku, adresu, lokalitu, alebo iný text poukazujúci na určiteľnú fyzickú alebo právnickú osobu.

3.1.10 Autentizácia identity u zmluvných partnerov

Autentizácia identity fyzickej osoby resp. komponentu u zmluvných partnerov spoločnosti Disig, a.s. (obchodní partneri), sa vykonáva v spolupráci so zodpovednými osobami tejto spoločnosti.

Niektoré postupy sú v tomto prípade zjednodušené a nemusia sa vykonávať napr. overovanie vlastníctva domény, overovanie kontroly e-mail konta ap.

3.1.11 Predkladané doklady

Všetky doklady predkladané na RA žiadateľmi o služby musia byť buď originály alebo úradne overené kópie originálov. Nesmie v nich byť žiaden údaj doplňovaný, pozmeňovaný, prečiarknutý a podobne. Doklady, na ktorých je vyznačená doba ich platnosti, musia byť platné.

Ak má pracovník RA pochybnosti o totožnosti potenciálneho zákazníka (napr. zjavný nesúlad medzi fotografiou v predloženom osobnom doklade a vzhľadom zákazníka, rozpornosť dvoch predložených dokladov a podobne), môže odmietnuť jeho registráciu.

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

Na žiadosť potenciálneho zákazníka alebo RA sa prípadné sporné prípady pri preukazovaní totožnosti riešia postupom podľa 2.4.

Pri predkladaní dokladov sa vyžaduje, aby na pobočke RA boli predložené originály týchto dokladov slúžiace k nahliadnutiu a kópie originálov (nemusia byť overené), okrem osobných dokladov identifikujúcich totožnosť žiadateľa resp. splnomocnenej osoby, slúžiace na archiváciu pre potreby CA. Predloženie výpisu z obchodného registra resp. živnostenského registra získaného z Internetu, zo strany žiadateľa, nie je postačujúce, nakoľko tento má len informatívny charakter a nie je použiteľný na právne úkony.

3.1.11.1 Fyzická osoba

Fyzická osoba predkladá dva doklady identifikujúce jej totožnosť. Primárnym dokladom je:

- Občan SR - platný občiansky preukaz
- Občan krajiny EÚ a EFTA – preukaz totožnosti, t.j. identifikačná karta
- Občan tretích krajín – povolenie na pobyt na území SR a ďalší doklad s fotografiou potvrdzujúci jeho totožnosť

Sekundárnym dokladom môže byť:

- cestovný pas
- vodičský preukaz
- preukaz poistenca zdravotného poistenia
- rodný list
- osobný preukaz vojaka z povolania alebo vojenská knižka
- povolenie na prechodný pobyt (resp. trvalý pobyt) v prípade cudzinca
- zbrojný preukaz vydaný príslušným policajným útvarom
- služobný preukaz

Požaduje sa pritom, aby aspoň jeden z predkladaných dokladov bol dokladom, ktorého súčasťou je fotografia danej osoby.

V prípade žiadosti o vydanie certifikátu pre potreby zmluvného partnera alebo žiadosti o jeho zrušenie postačuje, aby daná fyzická osoba preukázala svoju totožnosť jedným z nasledovných osobných dokladov – občiansky preukaz resp. pas. Žiadateľ o certifikát vydávaný pre potreby zmluvného partnera musí splniť aj ďalšie podmienky pre vydanie certifikátu tohto typu, ktoré si stanoví zmluvný partner.

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

Pokiaľ je žiadateľom o certifikát zákonný zástupca (spravidla rodič), musí navyše predložiť rodný list dieťaťa, osvojiteľ musí navyše predložiť rozhodnutie zo súdu alebo výpis z matriky. Postačujúcim dokladom je aj občiansky preukaz, v ktorom je dieťa zapísané.

3.1.11.2 Fyzická osoba - zamestnanec

Pokiaľ je žiadateľom o certifikát fyzická osoba, ktorá má v žiadosti uvedený aj názov organizácie, predkladá doklady podľa kapitoly 3.1.11.1. Zároveň musí predložiť súhlas s vydaním certifikátu od zamestnávateľa.

Pokiaľ je žiadateľom zamestnanec zmluvného partnera táto požiadavka je nahradená súhlasom na vydanie zo strany zmluvne stanovenej kontaktnej osoby.

3.1.11.3 Právnická osoba

V tomto prípade žiadateľ o certifikát predkladá doklady uvedené v kapitole 3.1.11.1. Súčasne musí predložiť doklad podľa kapitoly 3.1.7.

Pokiaľ za právnickú osobu konajú viaceré osoby spoločne, je potrebné predložiť úradne overenú (notárom) plnú moc, z textu ktorej je jednoznačne jasné, že zastupujúca fyzická osoba bola splnomocnená splnomocňujúcimi fyzickými osobami konať v danej veci v ich mene.

3.1.11.4 Komponent alebo softvér

Viď kapitola 3.1.9.

Všetky doklady predkladané na RA žiadateľmi o služby musia byť buď originály alebo úradne overené kópie originálov. Nesmie v nich byť žiaden údaj doplňovaný, pozmeňovaný, prečiarknutý a podobne. Doklady, na ktorých je vyznačená doba ich platnosti, musia byť platné.

Ak má pracovník RA pochybnosti o totožnosti potenciálneho zákazníka (napr. zjavný nesúlad medzi fotografiou v predloženom osobnom doklade a vzhľadom zákazníka, rozpornosť dvoch predložených dokladov a podobne), môže odmietnuť jeho registráciu.

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

Na žiadosť potenciálneho zákazníka alebo RA sa prípadné sporné prípady pri preukazovaní totožnosti riešia postupom podľa bodu 2.4.

Pri predkladaní dokladov sa vyžaduje, aby na pobočke RA boli predložené originály týchto dokladov slúžiace k nahliadnutiu a kópie originálov (nemusia byť overené), okrem osobných dokladov identifikujúcich totožnosť žiadateľa resp. splnomocnenej osoby, slúžiace na archiváciu pre potreby CA. Preloženie výpisu z obchodného registra resp. živnostenského registra získaného z Internetu, zo strany žiadateľa, nie je postačujúce, nakoľko tento má len informatívny charakter a nie je použiteľný na právne úkony.

3.1.12 Kontrola údajov na predložených dokladoch

V prípade ľubovoľných odôvodnených pochybností o totožnosti potenciálneho zákazníka môže RA jeho registráciu odmietnuť. Pracovník RA kontroluje na predložených dokladoch najmä nasledovné:

- Osobné doklady fyzickej osoby:

- platnosť predloženého dokladu - v prípade neplatného osobného dokladu sa postupuje ako pri chýbajúcom osobnom doklade - RA registráciu odmietne
- plnoletosť fyzickej osoby (t.j. vek 18 rokov) - RA odmietne registráciu neplnoletých osôb pričom za neplnoleté osoby má právo konať ich zákonný zástupca (obvykle rodič).
- či nie je zjavný nesúlad medzi fotografiou v osobnom doklade a vzhľadom držiteľa osobného dokladu – v prípade, že áno, RA môže odmietnuť registráciu.
- rozpornosť predložených dokladov, t.j. či údaje na jednom doklade neodporujú údajom na inom doklade

- Výpisy z obchodného registra:
  - či výpis nie je starší ako 3 mesiace
  - či majú fyzické osoby (stačí jedna fyzická osoba, ak na výpise nie je uvedené inak), ktoré predložili daný výpis, právo konať (podpisovať) za danú právnickú osobu (t.j. či sú jej štatutárnymi zástupcami)
  - či je výpis úradne overený (notárom alebo matrikou), ak sa nejedná o originál
- Plné moci:
  - či je plná moc úradne overená (notárom alebo matrikou)
  - či sa údaje, uvedené v plnej moci, ktoré definujú zastupujúcu fyzickú resp. právnickú osobu, zhodujú s údajmi uvedenými na osobných dokladoch zastupujúcej fyzickej osoby resp. s údajmi uvedenými na výpise z obchodného registra zastupujúcej právnickej osoby
  - rozsah plnej moci - t.j. či plná moc oprávňuje splnomocnenú fyzickú alebo právnickú osobu k požadovanému úkonu na RA v mene splnomocňujúcej fyzickej alebo právnickej osoby
  - či plná moc nie je časovo obmedzená alebo ak obsahuje inú podmienku, či je táto splnená
- Čestné prehlásenia:
  - oprávnenie na podpis – či osoba podpisujúca prehlásenie je oprávnená zastupovať právnickú osobu. Oprávnenosť sa kontroluje podľa výpisu z OR resp. iného registra právnických osôb. Pokiaľ podpisujúca osoba nie je zapísaná v tomto výpise, musí predložiť iný doklad, na základe ktorého môže konať za spoločnosť (spravidla notárom overená plná moc)

Druh predložených dokladov (napr. občiansky preukaz, pas) a príslušné údaje z nich zaznamená pracovník RA elektronicky do informačného systému CA.

V prípade zistených nedostatkoch na predložených dokladoch, resp. predložení neúplných dokladov, musí pracovník RA registráciu žiadateľa odmietnuť. Služba vydania certifikátu bude v tomto prípade zamietnutá.

Pracovník RA musí akceptovať aj dokumenty predkladané žiadateľom v elektronickej podobe podpísané platným ZEP (výpis s obchodného registra, plná moc, prehlásenie, poverenie ap.)

3.1.13 Prvotná registrácia RA

Prvotná registrácia osoby v role RA sa vykoná za rovnakých, vyššie popísaných podmienok ako v prípade zákazníka - žiadateľa o osobný certifikát. Vlastné overenie identity pracovníkov RA vykonajú pracovníci spoločnosti Disig pokiaľ nie je zmluvne dohodnutý iný mechanizmus.

3.2 Vydanie následného certifikátu

Podmienky vydania následného certifikátu sú podrobne popísané v aktuálnom CP v časti 3.2.

RA vykoná vydanie certifikátu bez osobnej návštevy držiteľa len v prípade osobného certifikátu resp. certifikátu pre právnickú osobu po splnení podmienok uvedených v časti 3.2 písm. a) aktuálneho CP. Overovanie zaslanej žiadosti, v prípade nepodpísaného e-mailu z e-mail adresy zhodnej z adresou uvedenou v prijatej žiadosti resp. zaslanej z iného e-mailu ako je v prijatej žiadosti, vykoná RA tak, že na danú e-mail adresu zašle elektronickú správu ktorá bude obsahovať tajnú nepredvídateľnú informáciu (overovacia informácia). Žiadateľ o certifikát musí zaslať späť overovaciu informáciu ako dôkaz kontroly zaslania žiadosti o vydanie následného certifikátu. Odpoveď musí byť zaslaná v stanovenom časovom úseku, dostatočnom na odoslanie elektronickej pošty. V prípade, že overenie zaslania žiadosti prebehne neúspešne, CA Disig odmietne vydanie certifikátu.

3.3 Vydanie následného certifikátu po zrušení starého

Po zrušení certifikátu musí žiadateľ o následný certifikát podrobiť všetkým požiadavkám prvotnej registrácie.

3.4 Žiadosť o zrušenie certifikátu

Žiadosť o zrušenie certifikátu musí byť autentizovaná, pozri časť 4.4. Žiadosť o zrušenie certifikátu môže byť autentizovaná použitím súkromného kľúča patriaceho k certifikátu bez ohľadu na to, či daný súkromný kľúč bol alebo nebol kompromitovaný.

4. Prevádzkové požiadavky

4.1 Žiadanie o certifikát

Keď žiadateľ o certifikát požiada o certifikát, žiadateľ a RA musia vykonať nasledovné kroky:

- RA musí overiť a zaznamenať identitu žiadateľa (podľa časti 3.1), ako aj overiť všetky ostatné údaje, ktoré sú v certifikáte, za použitia nezávislých zdrojov a alternatívnych komunikačných kanálov,
- žiadateľ musí preukázať, že verejný kľúč tvorí pár kľúčov so súkromným kľúčom vlastneným žiadateľom o certifikát (podľa časti 3.1.6),
- žiadateľ musí poskytnúť dostatočné podklady na overenie ľubovoľných identifikačných údajov, ktoré sa majú dostať do certifikátu.

Všetka komunikácia medzi jednotlivými zložkami CA týkajúca sa žiadosti o certifikát a procesu vydania certifikátu má byť autentizovaná a chránená pred modifikáciou pomocou mechanizmov primeraných požiadavkám dát, ktoré sa majú chrániť použitím predtým vydaných certifikátov. Ľubovoľný elektronický prenos delených tajomstiev musí byť uskutočnený šifrovane.

4.1.1 Detailný postup na získanie osobného certifikátu a certifikátu pre právnickú osobu

4.1.1.1 Príprava na návštevu RA

Zákazník (žiadateľ o certifikát) vykoná tieto kroky:

- Oboznámi sa s týmto postupom, prípadne s princípmi a návodmi na získanie certifikátu.
- Vygeneruje si na svojom počítači pomocou vyhovujúceho prehliadača novú žiadosť o certifikát prostredníctvom web stránky spoločnosti Disig (viď URL adresu v časti 1.4) a uloží si ju na vhodné médium (HDD, USB disk, disketa ap.).

Upozorňujeme, že 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 bude na RA odmietnutá! Žiadosť musí povinne obsahovať vhodne vyplnené položky "Meno a Priezvisko" resp. „Organizácia“ a "E-mail". Jednotlivé položky pritom vyplní tak, aby zadané hodnoty boli v súlade s týmito pravidlami s dôrazom na jeho časť 3.1.2. Pri zadávaní hodnôt do položiek žiadosti o certifikát by mal žiadateľ o certifikát mať na zreteli, že RA bude musieť uspokojivým spôsobom preukázať oprávnenosť všetkých údajov, ktoré zadal do jednotlivých položiek žiadosti o certifikát.
Všetky údaje sa musia zadávať bez diakritiky (mäkčene, dĺžne a pod.).
Použitie špeciálnych znakov (napr. čiarka, pomlčka, =, / a iné) treba obmedziť na minimálnu nutnú mieru, odporúčame prípadne tieto znaky použiť až po dohode s CA Disig, v opačnom prípade si CA Disig vyhradzuje právo odmietnuť takúto žiadosť o certifikát.
V poli „Organizácia“ sa nesmie použiť znak čiarka.

- Pripraví si zvolené doklady totožnosti resp. iné potrebné doklady, napr. výpis z obchodného registra (odporúčame overiť platnosť dokladov) podľa ustanovení časti 3.

Poznámky: Je potrebné, aby si zákazník pripravil kópie (nemusia byt overené) všetkých dokladov (okrem osobných dokladov fyzických osôb), ktoré mieni predložiť na RA (napr. výpis z obchodného registra a iné doklady o právnickej osobe, splnomocnenie, ak sa dá zastupovať na RA), aby ich mohol odovzdať na RA. Predloženie výpisu z obchodného registra získaného z Internetu, zo strany žiadateľa, nie je postačujúce, nakoľko tento výpis má len informatívny charakter a nie je použiteľný na právne úkony. Odporúča sa, aby si zákazník na RA ešte pred návštevou RA overil a vyjasnil prípadné pochybnosti a problémy, najmä tie, ktoré týkajú vhodnosti hodnôt jednotlivých položiek v žiadosti o certifikát.

- Dohodne si termín návštevy RA (telefonicky, e-mailom).
- Zašle elektronicky žiadosť o vydanie certifikátu na príslušnú RA - elektronické adresy RA sú k dispozícii na web stránke spoločnosti Disig. (pozri 1.4). Žiadosť o certifikát určený na podpisovanie a šifrovanie elektronickej pošty musí byť zaslaná z e-mail adresy, ktorá je uvedená v žiadosti o certifikát v položke E-mail.

4.1.1.2 Návšteva RA

Zákazník v dohodnutom termíne príde na RA, pričom vezme so sebou a identifikuje resp. predloží:

- Žiadosť o certifikát v elektronickej forme (vygenerovanú prehliadačom)

Poznámka: Zákazník musí byť schopný identifikovať na RA hodnotu údaja RequestId (je to číselný reťazec, pred ktorým je reťazec „disigweb„ , ktorý jednoznačne identifikuje vygenerovanú žiadosť o certifikát) z tej žiadosti o certifikát, z ktorej sa má vyhotoviť certifikát. Žiadosť o certifikát určený na podpisovanie a šifrovanie elektronickej pošty musí byť zaslaná na registračnú autoritu vopred elektronicky (pozri 4.1.1.1).

- Zvolené doklady totožnosti resp. iné potrebné doklady, napr. výpis z obchodného registra, plná moc atď. podľa ustanovení časti 3.

Poznámka: Zákazník odovzdá na RA kópie (nemusia byt overené) všetkých dokladov (okrem osobných dokladov fyzických osôb), ktoré predkladá na RA pri registrácii (napr. výpis z obchodného registra a iné doklady o právnickej osobe, splnomocnenie, v prípade zastupovania iného subjektu).

- Príslušnú peňažnú čiastku, ak nebola vopred dohodnutá iná forma platby za certifikát.

4.1.1.3 Postup RA pri zaslaní žiadosti elektronicky

1. Pracovník RA overí, či elektronicky zaslaná žiadosť o vydanie certifikátu daného žiadateľa (povinné pri certifikátoch s rozšírením „Secure Email (1.3.6.1.5.5.7.3.4)“), bola zaslaná z rovnakej e-mail adresy, aká sa nachádza v žiadosti o vydanie certifikátu. V prípade zistených rozdielov odmietne vydanie certifikátu.
2. V prípade, že vopred zaslaná žiadosť o vydanie certifikátu obsahuje rovnakú e-mail adresu z akej bola zaslaná, vykoná pracovník RA overenie kontroly tejto e-mailovej adresy. Overenie sa vykoná tak, že na danú e-mail adresu zašle elektronickú správu ktorá bude obsahovať tajnú nepredvídateľnú

informáciu (overovacia informácia). Žiadateľ o certifikát musí zaslať späť overovaciu informáciu ako dôkaz kontroly danej e-mail adresy. Odpoveď musí byť zaslaná v stanovenom časovom úseku, dostatočnom na odoslanie elektronickej pošty. V prípade, že overenie e-mail adresy prebehne neúspešne, CA Disig odmietne vydanie certifikátu. Detailný postup je popísaný v príslušných príručkách pre pracovníkov RA a rovnako je predmetom úvodného školenia pracovníkov RA. Overovanie e-mailovej adresy nie je potrebné v prípade, že je zaslaná žiadosť o následný certifikát elektronicky e-mailom, ktorý je podpísaný platným certifikátom žiadateľa, vydaným certifikačnou autoritou CA Disig a e-mailová adresa, z ktorej bola žiadosť zaslaná je zhodná s e-mailovou adresou nachádzajúcou sa v žiadosti.

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

4.1.1.4 Postup pri registrácii zákazníka na RA

1. Pracovník RA overí totožnosť žiadateľa o certifikát resp. subjektu, ktorý ho zastupuje, podľa ustanovení častí 3.1.7 a 3.1.8.
2. Pracovník RA vyberie vopred zaslanú žiadosť o certifikát identifikovanú žiadateľom. Žiadosť o vydanie osobného certifikátu určeného na podpisovanie a šifrovanie elektronickej pošty musí byť zaslaná na príslušnú RA elektronicky z adresy, ktorá bude uvedená v DN žiadosti v položke E-mail.
3. Pracovník RA skontroluje úplnosť a správnosť prijatej žiadosti o certifikát (napr. či niektoré položky neobsahujú zjavne chybné údaje).

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

Žiadateľ o certifikát musí na RA uspokojivým spôsobom preukázať všetky údaje, ktoré zadal do jednotlivých položiek žiadosti o certifikát. Ak žiadateľ predloží aj iné doklady (okrem osobných dokladov fyzických osôb, napr. výpis z obchodného registra alebo iný doklad o právnickej osobe, plná moc v prípade zastupovania iného subjektu), pracovník RA prevezme a uschová kópie (nemusia byt overené) všetkých predložených dokladov, porovná ich s originálmi a na každú kópiu napíše text „Potvrdzujem zhodu s originálom“ a doplní dátum a svoj podpis. Predloženie výpisu z obchodného registra získaného z Internetu, zo strany žiadateľa, nie je postačujúce, nakoľko tento výpis má len informatívny charakter a nie je použiteľný na právne úkony.

4. Prostredníctvom informačného systému CA Disig sa automatizovane overí, či pre verejný kľúč nachádzajúci sa v predloženej žiadosti o certifikát už nebol v minulosti vydaný certifikát. Ak bol, RA žiadosť o certifikát odmietne z bezpečnostných dôvodov prijať, nakoľko už raz certifikovaný verejný kľúč nemôže byť použitý v inom certifikáte.
5. Pracovník RA predloží žiadateľovi o certifikát na podpis Zmluvu o vydaní a používaní certifikátu a služieb CA Disig v dvoch exemplároch – jeden pre CA Disig a jeden pre zákazníka. Súhlas žiadateľa s textom tejto zmluvy je podmienkou na prijatie žiadosti o certifikát a vytvorenie certifikátu.

6. Zákazník zaplatí za certifikát sumu podľa platného Cenníka služieb CA Disig v zmysle príslušného odseku Zmluvy, pokiaľ nie je dohodnutý iný spôsob platby.

7. Pracovník RA vloží do informačného systému CA Disig žiadosť o certifikát a ostatné požadované údaje.

Poznámka: V prípade, že z danej žiadosti o certifikát z nejakého dôvodu nie je možné urobiť certifikát, CA Disig o tom upovedomí príslušnú RA vrátane uvedenia dôvodu, ktorá potom vyrozumie žiadateľa o certifikát. Žiadateľ o certifikát môže v takom prípade buď podať novú žiadosť o certifikát alebo mu budú vrátené zaplatené peniaze.

8. Bezprostredne po vydaní certifikátu bude môcť žiadateľ o certifikát prevziať svoj certifikát. Pritom podpíšu žiadateľ o certifikát a pracovník RA „Potvrdenie o vydaní osobného certifikátu a jeho odovzdaní žiadateľovi o certifikát“, ktoré tvorí prílohu „Zmluvy o vydaní a používaní certifikátu a služieb CA Disig“. Toto potvrdenie sa vyhotoví v dvoch exemplároch – jeden pre žiadateľa a jeden zostane RA, ktorá ho potom postúpi vydávajúcej CA Disig. V prípade zmluvných partnerov, ktorých zamestnancom sú vydávané certifikáty na zmluvnom základe je podpisované len „Potvrdenie o vydaní osobného certifikátu a jeho odovzdaní žiadateľovi o certifikát“.

4.1.2 Detailný postup na získanie SSL certifikátu

4.1.2.1 Príprava na návštevu na RA

Zákazník (žiadateľ o certifikát) vykoná nasledovné kroky:

- oboznámi sa s týmto postupom, prípadne s princípmi a návodmi na získanie certifikátu,
- pomocou svojho softvéru (typicky napr. Microsoft IIS alebo Apache/Openssl) si vygeneruje žiadosť o SSL certifikát a túto odošle elektronicky na príslušnú RA a zároveň si ju uloží z dôvodov zálohy na vhodné prenosné médium,

Poznámky a upozornenia: Upozorňujeme, že žiadosť o SSL certifikát resp. v nej sa nachádzajúci verejný kľúč, na ktorý už bol vydaný certifikát, nemôže byť z bezpečnostných dôvodov použitá opakovane na vydanie iného SSL certifikátu a bude na RA odmietnutá! Žiadosť o SSL certifikát musí povinne obsahovať vhodne vyplnenú položku subject:commonName (tzv. názov entity). Jednotlivé položky je potrebné vyplniť tak, aby zadané hodnoty boli v súlade s týmto dokumentom s dôrazom na jeho časť 3.1.2, a aby jednoznačne identifikovali entitu, ktorá bude používať daný SSL certifikát (typicky úplné doménové meno). Pokiaľ je v žiadosti vyplnená položka O (subject:organizationName), tak musí byť vyplnená aj položka L (subject:localityName). Pokiaľ položka O (subject:organizationName) nie je vyplnená, tak nesmie byť vyplnená položka L (subject:localityName).

Použitie špeciálnych znakov (napr. čiarka, pomlčka, =, / a iné) treba obmedziť na minimálnu nutnú mieru, odporúčame prípadne tieto znaky použiť až po dohode s CA Disig, v opačnom prípade si CA Disig vyhradzuje právo odmietnuť takúto žiadosť o SSL certifikát. Všetky údaje sa musia zadávať bez diakritiky (mäkčene, dĺžne a pod.). V poli Organizácia sa nesmie použiť znak čiarka. Žiadateľom o SSL certifikát môže byť len štatutár organizácie resp. ním splnomocnená osoba, ktorej patrí entita, pre ktorú je SSL certifikát vydávaný. Všetky údaje v žiadosti musia byť zo strany žiadateľa hodnoverne preukázané, okrem položky subject:organizationUnitName (OU). Položka OU nesmie obsahovať názov právnickej osoby, obchodné meno, obchodnú značku, adresu, lokalitu,

alebo iný text poukazujúci na určiteľnú fyzickú alebo právnickú osobu, pokiaľ použitie týchto informácií nie je žiadateľ schopný hodnoverne doložiť.

- pripraví si zvolené doklady totožnosti resp. iné potrebné doklady, napr. výpis z obchodného registra (odporúčame overiť platnosť dokladov) podľa ustanovení časti 3.

Poznámka: Je potrebné, aby si zákazník pripravil kópie (nemusia byt overené) všetkých dokladov (okrem osobných dokladov fyzických osôb), ktoré mieni predložiť na RA (napr. výpis z obchodného registra a iné doklady o právnickej osobe, splnomocnenie, ak sa dá zastupovať na RA), aby ich mohol odovzdať na RA. Predloženie výpisu z obchodného registra získaného z Internetu, zo strany žiadateľa, nie je postačujúce, nakoľko tento výpis má len informatívny charakter a nie je použiteľný na právne úkony.

Odporúča sa, aby si zákazník na RA ešte pred návštevou RA overil a vyjasnil prípadné pochybnosti a problémy, najmä tie, ktoré týkajú vhodnosti hodnôt jednotlivých položiek v žiadosti o SSL certifikát.

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

4.1.2.2 Postup RA pred vydaním SSL certifikátu

1. SSL certifikáty zásadne vydáva spoločnosť Disig svojimi pracovníkmi v centrále spoločnosti v Bratislave.
2. Na základe vopred zaslanej žiadosti RA vykoná overenie vlastníctva domény v zmysle ods. 3.1.9 a zároveň skontroluje úplnosť a správnosť prijatej žiadosti o SSL certifikát v zmysle požiadaviek CP časť 3.1.2.3 Tabuľka č. 3, týkajúcich sa položiek subject:organizationName a subject:localityName. Ak má pracovník RA vážne podozrenie na neoprávnené použitie danej domény druhej úrovne žiadateľom o certifikát, má právo požadovať, aby žiadateľ dôveryhodným spôsobom dokladoval oprávnenosť použitia danej domény druhej úrovne, v opačnom prípade môže RA odmietnuť prijať danú žiadosť o SSL certifikát. Overenie vlastníctva domény sa netýka žiadateľov o SSL certifikát, ktorí sú zmluvným partnerom CA Disig.

Upozornenia a poznámky: Všetky položky musia byť vyplnené bez diakritiky. Malé a veľké písmená sa rozlišujú.
Položky „Názov organizácie“ "Útvar vo firme:" „Lokalita“ a „Email:“ sú nepovinné.
Žiadosť musí povinne obsahovať vhodne vyplnenú položku commonName (tzn. názov entity). Jednotlivé položky pritom musia byť vyplnené tak, aby zadané hodnoty boli v súlade s týmto dokumentom s dôrazom na jeho časť 3.1.2. Pri posudzovaní hodnôt všetkých položiek berie pracovník RA do úvahy zmysluplnosť týchto hodnôt (bližšie pozri časť 3.1.2) – porušenie princípu zmysluplnosti môže byť dôvodom na odmietnutie vydania certifikátu.
Plné doménové meno nesmie byť obsiahnuté v žiadnej inej položke okrem položky subject:CommonName (CN) a rozšírenia certifikátu SubjectAlternativeName. Pokiaľ je v žiadosti vyplnená položka O (subject:organizationName), tak musí byť vyplnená aj položka L (subject:localityName). Pokiaľ položka O (subject:organizationName) nie je vyplnená, tak nesmie byť vyplnená položka L (subject:localityName). Položka OU nesmie obsahovať názov právnickej osoby, obchodné meno, obchodnú značku, adresu, lokalitu, alebo iný text poukazujúci na určiteľnú fyzickú alebo právnickú osobu, pokiaľ tieto informácie neboli hodnoverne overené a zároveň takáto žiadosť obsahuje položky subject:organizationName, subject:localityName, and subject:countryName, ktoré boli rovnako hodnoverne overené. Ak žiadateľ predloží aj iné doklady (okrem osobných dokladov fyzických osôb, napr. výpis z obchodného registra alebo iný doklad o právnickej osobe, plná moc v prípade zastupovania iného subjektu), pracovník RA prevezme a uschová kópie (nemusia byt overené) všetkých predložených dokladov, porovná ich s originálmi a na každú kópiu napíše

text „Potvrdzujem zhodu s originálom“ a doplní dátum a svoj podpis. Predloženie výpisu z obchodného registra získaného z Internetu, zo strany žiadateľa, nie je postačujúce, nakoľko tento výpis má len informatívny charakter a nie je použiteľný na právne úkony.
Pracovník RA overí, či by vydaním certifikátu nedošlo k duplicite certifikátov resp. či daný subjekt už nemá platný osobný certifikát – dôraz sa pritom kladie na hodnotu uvedenú v položke subject:commonName.
Nesplnenie podmienok uvedených vyššie je závažným dôvodom na odmietnutie prijatia žiadosti o certifikát.

3. Vydanie SSL certifikátu externou RA je možné len po predchádzajúcom písomnom súhlase s vydaním takéhoto certifikátu zo strany PMA CA Disig. Súhlas sa dáva vo forme podpísanej elektronickej správy od člena PMA CA Disig (viď CP CA Disig ods.1.3.1.1).
4. Skôr ako si dohodne externá RA stretnutie s klientom požiada PMA CA Disig o súhlas s vydaním SSL certifikátu. Súhlas sa žiada formou elektronicky podpísanej správy, ktorá bude v prílohe obsahovať informácie o žiadateľovi a doméne, pre ktorú sa vydanie certifikátu žiada. Podrobnosti o rozsahu zasielaných informácií budú zaslané na jednotlivé RA formou metodického usmernenia zo strany CA Disig.

4.1.2.3 Návšteva RA

Zákazník v dohodnutom termíne príde na RA, pričom vezme so sebou a predloží:

- zvolené doklady totožnosti resp. iné potrebné doklady, napr. výpis z obchodného registra, plná moc atď. podľa ustanovení časti 3. Zákazník odovzdá na RA kópie (nemusia byt overené) všetkých dokladov (okrem osobných dokladov fyzických osôb), ktoré predkladá na RA pri registrácii (napr. výpis z obchodného registra a iné doklady o právnickej osobe, splnomocnenie, v prípade zastupovania iného subjektu).
- príslušnú peňažnú čiastku, ak nebola vopred dohodnutá iná forma platby za certifikát

4.1.2.4 Postup pri registrácii zákazníka na RA

1. Pracovník RA overí totožnosť žiadateľa o certifikát resp. subjektu, ktorý ho zastupuje, podľa ustanovení častí 3.1.7 a 3.1.8.
2. Pracovník RA požiada zákazníka o identifikáciu zaslanej žiadosti o certifikát.
3. Prostredníctvom informačného systému CA sa automatizovane overí, či na verejný kľúč nachádzajúci sa v predloženej žiadosti o certifikát už nebol v minulosti vydaný certifikát. Ak bol, RA žiadosť o certifikát odmietne z bezpečnostných dôvodov prijať, lebo už raz certifikovaný verejný kľúč nemôže byť použitý v inom certifikáte.
4. Pracovník RA predloží žiadateľovi o certifikát na podpis „Zmluvu o vydaní a používaní certifikátu a služieb CA Disig“ v dvoch exemplároch – jeden pre CA Disig a jeden pre zákazníka. Súhlas žiadateľa s textom tejto zmluvy je podmienkou na prijatie žiadosti o certifikát a vytvorenie certifikátu.

5. Zákazník zaplatí za certifikát sumu podľa platného Cenníka služieb CA Disig v zmysle príslušného odseku Zmluvy, ak nebol dohodnutý iný spôsob úhrady ceny.
6. Pracovník RA vloží do informačného systému CA žiadosť o certifikát a ostatné požadované údaje.

Poznámka: V prípade, že z danej žiadosti o certifikát z nejakého dôvodu nie je možné urobiť certifikát, CA o tom upovedomí príslušnú RA vrátane uvedenia dôvodu, ktorá potom vyrozumie žiadateľa o certifikát. Žiadateľ o certifikát môže v takom prípade buď podať novú žiadosť o certifikát alebo mu budú vrátené zaplatené peniaze.

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

4.2 Vydanie certifikátu

CA Disig nevytvorí certifikát, kým sa k spokojnosti CA Disig nedokončia všetky verifikácie a prípadné zmeny, ak sú potrebné. CA Disig nezodpovedá za prípadné dodatočné náklady žiadateľa o certifikát, ktoré vzniknú v priebehu registrácie, napr. kvôli potrebe opakovanej návštevy RA napr. v dôsledku neúplných alebo chýbajúcich dokladov alebo iných nedostatkov.

Hoci žiadateľ pripravuje väčšinu dátových položiek certifikátu, na RA zostáva zodpovednosť overiť, že informácie sú správne a precízne.

Za preverenie údajov žiadateľa zodpovedá RA.

CA Disig má právo nevytvoriť certifikát, hoci žiadateľ o certifikát úspešne prešiel procesom registrácie na RA, ak sa dodatočne zistí závažná skutočnosť, ktorá bráni vydaniu certifikátu (napr. chyba vo formáte žiadosti o certifikát).

4.2.1 Doručenie súkromného kľúča držiteľovi certifikátu

Súkromný kľúč bude generovať sám žiadateľ o certifikát.

4.2.2 Doručenie verejného kľúča CA používateľom

CMA a strany spoliehajúce sa na certifikáty musia konať v súčinnosti, aby sa zaručilo autentizované a integrálne doručenie certifikátu CA Disig.

Prijateľné metódy na doručenie certifikátu CA Disig a jeho autentizovanie sú:

- nahranie certifikátu z web stránky CA Disig,
- osobné prevzatie certifikátu na RA,
- RA na požiadanie poskytne strane spoliehajúcej sa na certifikáty alebo inému ľubovoľnému záujemcovi fingerprint certifikátu CA Disig a to konkrétne telefonicky, e-mailom alebo osobne pri návšteve záujemcu

na RA, pričom konkrétna voľba spôsobu poskytnutia fingerprintu závisí na dohode so záujemcom.

4.3 Prevzatie certifikátu

Nakoľko CA Disig pracuje v on-line režime t.j. certifikáty sa vytvárajú a vydávajú automatizovane a priebežne, žiadateľ bude spravidla môcť prevziať vydaný certifikát v priebehu tej istej návštevy RA, kedy podal žiadosť o daný certifikát.

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

Žiadateľ o certifikát sa pri preberaní svojho certifikátu môže dať zastupovať na RA inou fyzickou alebo právnickou osobou za rovnakých podmienok ako pri podávaní žiadosti o certifikát (pozri časti 3.1.7 resp. 3.1.8). Prevzatie certifikátu sa štandardne uskutoční na tej istej RA, kde bola podaná žiadosť o daný certifikát.

Oznam o vydaní certifikátu bude zaslaný na emailovú adresu uvedenú v certifikáte a odovzdaný držiteľovi certifikátu alebo subjektu, ktorý ho zastupuje, spolu s certifikátom CA Disig a CP CA Disig. V prípade certifikátu CA Disig a CP CA Disig postačuje odkaz na web stránku CA Disig, kde sú tieto k dispozícii.

CA Disig môže osobitnou zmluvou so žiadateľom dohodnúť aj iný postup na prevzatie certifikátu.

4.3.1 Prvotné nahratie novovytvoreného certifikátu:

4.3.1.1 Osobný certifikát

Vo všeobecnosti existujú dve možnosti ako nahrať novovytvorený osobný certifikát do prehliadača, aby mohol byť prehliadačom priradený k príslušnému súkromnému kľúču, ktorý sa vytvoril a uschoval na danom osobnom počítači, v danom užívateľskom profile a v použitom prehliadači, v priebehu generovania žiadosti o certifikát:

- Použitím linky, ktorú žiadateľ o certifikát dostane v odoslanom e-maily.
- Otvorením súboru, ktorý obsahuje certifikát vo DER formáte (súbor musí mať vhodnú príponu, napr. .der) a jeho inštaláciou.

Podmienky na správnu prvotnú inštaláciu certifikátu sú, že musí byť vykonaná

- na tom istom počítač,
- v tom istom užívateľskom profile a
- v tom istý prehliadač

na ktorom bola predtým vygenerovaná žiadosť o certifikát o daný certifikát.

4.3.1.2 SSL certifikát

Postup pri nahrávaní novovytvoreného SSL certifikátu závisí od konkrétneho softvéru resp. hardvéru, kde sa má daný certifikát použiť.

4.4 Suspendovanie certifikátu a zrušenie certifikátu

4.4.1 Zrušenie certifikátu

4.4.1.1 Okolnosti zrušenia certifikátu

Certifikát sa má zrušiť, keď sa väzba medzi subjektom a jeho verejným kľúčom definovaným v certifikáte už nepovažuje za platnú. Príklady okolností, ktoré rušia túto väzbu, sú:

- držiteľ certifikátu alebo iná oprávnená strana požiada o zrušenie certifikátu,
- je podozrenie, že bol kompromitovaný súkromný kľúč (zodpovedajúci verejnému kľúču v certifikáte), alebo certifikát bol iným spôsobom zneužitý
- ukázalo sa, že držiteľ certifikátu nedodržuje svoje povinnosti držiteľa certifikátu, ktoré ho zmluvne viažu,
- identifikačné informácie alebo pričlenené prvky ľubovoľných mien v certifikáte sa stanú neplatnými,
- je podozrenie, že certifikát nebol vydaný v súlade s týmto CP resp. zodpovedajúcimi CPS pre RA a CA,
- zistilo sa, že niektorá z informácií uvedených v certifikáte je chybná alebo nesprávna,
- CA Disig ukončí z akéhokoľvek dôvodu svoju činnosť a zmluvne nezaisti u inej CA, aby poskytovala informácie o zrušených certifikátoch v mene CA Disig,
- skončili okolnosti, ktoré vyžadovali vydanie certifikátu (testovanie, overovanie aplikácií ap.),
- došlo ku strate súkromného kľúča,
- technické parametre alebo formát certifikátu by mohli viesť k neakceptovateľnému riziku z pohľadu dodávateľov softvéru alebo spoliehajúcich sa strán (zmena kryptografických algoritmov na podpisovanie, dĺžka kryptografických kľúčov ap.),
- smrť držiteľa certifikátu,
- došlo ku kompromitácii súkromného kľúča vydávajúcej CA Disig,
- právoplatný rozsudok alebo predbežné opatrenie súdu.

Vždy, keď sa CA dozvie o niektorej z vyššie uvedených okolností, daný certifikát sa zruší a dá sa na zoznam zrušených certifikátov (ďalej len „CRL“).

Zrušené certifikáty sa budú vyskytovať vo všetkých nových vydaniach CRL, minimálne dovtedy, kým dané certifikáty nestratia platnosť..

4.4.1.2 Kto môže žiadať o zrušenie certifikátu

Držiteľ certifikátu (alebo ním poverená fyzická alebo právnická osoba) môže kedykoľvek požiadať spôsobom stanoveným týmto dokumentom (najmä časť 4.4.1.3) o zrušenie svojho vlastného certifikátu a to aj bez udania dôvodu žiadosti o zrušenie certifikátu.

RA dá CA Disig návrh na zrušenie certifikátu daného držiteľa, ak sa dozvie, že nastala niektorá z okolností uvedených v časti 4.4.1.1.

Ak bol certifikát vydaný na zamestnancovi zmluvného partnera, v príslušnej zmluve je možné dohodnúť, kto okrem držiteľa certifikátu má právo požiadať o jeho zrušenie, akým spôsobom a za akých okolností.

O zrušenie certifikátu môže tiež požiadať:

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

V prípade certifikátu RA môže o zrušenie certifikátu okrem jeho držiteľa (danej RA) požiadať tiež PMA, ak sa zistí závažná okolnosť (pozri časť 4.4.1.1) na zrušenie daného certifikátu.

4.4.1.3 Procedúra žiadosti o zrušenie certifikátu

Žiadosť o zrušenie certifikátu podáva oprávnená osoba na RA prostredníctvom dvoch exemplárov vyplneného formulára „Žiadosť o zrušenie certifikátu“, ktorý je k dispozícii na webe CA Disig alebo na RA – jeden výtlačok zostáva na RA, jeden výtlačok pracovník RA potvrdí s uvedením aktuálneho dátumu a času a vráti žiadateľovi.

RA poskytne v prípade potreby žiadateľovi o zrušenie pomoc pri zistení čísla (serial number) predmetného certifikátu, aby bolo možné jednoznačne identifikovať certifikát, ktorý sa má zrušiť.

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

Osoba požadujúca zrušenie certifikátu sa buď musí na RA podrobiť rovnakému procesu autentizácie, aký je požadovaný pri prvotnej registrácii žiadateľa o certifikát alebo musí hodnoverným spôsobom preukázať, že je oprávnenou osobou, ktorá môže žiadať o zrušenie daného certifikátu.

Autentizácia požiadavky na zrušenie certifikátu je dôležitá, aby sa predišlo svojvoľnému zrušeniu certifikátu neautorizovanou stranou.

Ak sa držiteľ certifikátu nechá na RA zastupovať vo veci zrušenia certifikátu, zastupujúci subjekt sa musí preukázať overenou plnou mocou (notárom alebo matrikou), z textu ktorej je jednoznačne zrejmá vôľa držiteľa certifikátu zrušiť svoj certifikát. Zastupujúci subjekt je povinný nechať na RA doklad potvrdzujúci jeho plnú moc alebo jeho kópiu (nemusí byť overená). Pracovník RA prevezme a uschová tento doklad, v prípade neoverenej kópie túto porovná s originálom a napíše na ňu text „Potvrdzujem zhodu s originálom“ a doplní dátum a svoj podpis.

RA posúdi oprávnenosť žiadosti o zrušenie certifikátu, v prípade, že je zrejmé, že žiadateľ o zrušenie nie je oprávnenou osobou, RA môže danú žiadosť o zrušenie odmietnuť.

RA tiež odmietne žiadosť, ak žiadateľ nesplní podmienky autentizácie svojej identity (pozri časti 3.1.7 resp. 3.1.8).

Po prijatí žiadosti o zrušenie certifikátu, ktorú RA považuje za oprávnenú (t.j. ktorá vyhovuje príslušným ustanoveniam týchto pravidiel), RA bezodkladne vloží prijatú žiadosť o zrušenie certifikátu do informačného systému RA, aby sa daný certifikát mohol automatizovane zrušiť.

Držiteľ platného certifikátu CA Disig môže požiadať o zrušenie svojho certifikátu tiež tak, že pošle na kontaktnú email adresu príslušnej RA email podpísaný svojím osobným certifikátom CA Disig, ktorý obsahuje správu s jednoznačne vyjadrenou vôľou zrušiť certifikát, konkrétne vetu "Žiadam týmto o zrušenie svojho certifikátu CA Disig so sériovým číslo xxxxxxx".

Takýmto spôsobom možno požiadať o zrušenie certifikátu aj z dôvodu kompromitácie súkromného kľúča, na podpis žiadosti o zrušenie certifikátu pritom možno použiť certifikát, ktorého zrušenie požaduje samotná žiadosť.

Držiteľ platného certifikátu CA Disig môže požiadať o zrušenie svojho certifikátu tiež tak, že pošle na kontaktnú email adresu príslušnej RA obyčajný mail (t.j. nemusí byť podpísaný).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

Žiadosť o zrušenie certifikátu je možné podať aj telefonicky, písomne alebo faxom. Žiadateľ sa pri tom autentizuje pomocou hesla na zrušenie certifikátu.

Po zrušení certifikátu systém CA Disig zašle držiteľovi certifikátu automaticky e-mail notifikáciu, na e-mail adresu uvedenú v certifikáte, o zrušení jeho certifikátu aj s informáciou o dôvodoch jeho zrušenia.

4.4.1.4 Čas na zrušenie certifikátu

CA bude zrušovať certifikáty tak rýchlo, ako je to len možné po prevzatí náležitej žiadosti o zrušenie a zruší certifikáty v rámci časových obmedzení popísaných v časti 4.4.3.1.

4.4.2 Suspendovanie certifikátov

Pod termínom „suspendovanie certifikátov“ sa myslí dočasné pozastavenie ich platnosti.

CA Disig túto črtu nepodporuje.

4.4.3 Zoznamy zrušených certifikátov

4.4.3.1 4.4.3.1 Frekvencia vydávania CRL

CRL sa:

- vydáva bez zbytočného odkladu po zrušení certifikátu.
- vydáva automatizovane každých 24 hodín (a to aj v prípade, keď za posledných 24 hodín sa nezrušil žiaden certifikát)
- zverejňuje prostredníctvom repozitára.

CA Disig:

- zruší certifikát bezodkladne po prijatí náležitej žiadosti o zrušenie certifikátu na RA, najneskoršie však do 24 hodín od prijatia žiadosti,
- zverejňuje okrem aktuálneho, najnovšieho CRL všetky vydané CR
- archivuje všetky CRL, ktoré vydala.

RA na požiadanie cez email, telefón alebo fax zašle aktuálne CRL prostredníctvom mailu na dohodnutú email adresu čo najskôr.

4.4.3.2 Požiadavky na overovanie CRL

Použitie zrušeného certifikátu môže spôsobiť škodu alebo mať fatálne následky pre isté aplikácie. Odpoveď na otázku, ako často by sa mali získavať nové údaje o zrušených certifikátoch, má byť určená stranou spoliehajúcou sa na certifikáty alebo správcom daného systému. Ak dočasne nie je možné získať informácie o zrušených certifikátoch, potom strana spoliehajúca sa na certifikáty musí buď odmietnuť použitie certifikátu alebo urobiť kvalifikované rozhodnutie, ktorým akceptuje riziko, zodpovednosť a dôsledky použitia certifikátu, ktorého autenticita nemôže byť zaručená podľa štandardov tohto dokumentu. Takéto použitie certifikátu môže byť príležitostne nevyhnutné, aby sa vyhovelo urgentným operačným požiadavkám.

V čase medzi podaním oprávnenej žiadosti o zrušenie certifikátu a zverejnením zrušeného certifikátu na CRL nesie 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.

4.4.4 Overenie aktuálneho stavu certifikátu

Overenie aktuálneho stavu certifikátu sa robí prostredníctvom aktuálneho CRL publikovaného CA Disig.

Softvér využívaný CA Disig a softvér klientov, strany spoliehajúce sa na certifikáty, môže voliteľne podporovať (automatizované) overovanie aktuálneho stavu certifikátu v režime on-line. Pretože však táto on-line komunikácia sa vo všeobecnosti nemôže garantovať, strana spoliehajúca sa na certifikát má byť pripravená na manuálne (neautomatizované) overovanie aktuálneho stavu certifikátov, na ktoré sa spolieha.

Ak daný softvér nepodporuje overovanie aktuálneho stavu certifikátu v režime on-line, strana spoliehajúca sa na certifikát je povinná manuálne (tzn. v režime off-line) overiť aktuálny stav certifikátu, na ktorý sa spolieha.

4.4.5 Iné použiteľné spôsoby oznamovania o zrušení certifikátu

RA odpovie na dopyt týkajúci sa stavu konkrétneho certifikátu, ak bol tento dopyt urobený telefonicky, faxom alebo emailom.

4.5 Audit bezpečnosti

4.5.1 Typy zaznamenávaných udalostí

Zaznamenávajú sa všetky udalosti na RA a tiež interakcie žiadateľov o certifikát a držiteľov certifikátov s RA. Záznamy môžu byť buď v elektronickej alebo v písomnej forme.

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

Záznamy sa pravidelne archivujú.

Každé pracovisko RA písomne vedie záznamy o činnosti daného pracoviska RA prostredníctvom knihy „Záznamy registračnej autority CA Disig“ (ďalej len „kniha RA“).

Do knihy RA sa zaznamenáva prijatie žiadosti o zrušenie certifikátu a odovzdanie certifikátu resp. SSCD zákazníkovi.

Do knihy RA sa zaznamenávajú všetky ostatné udalosti na RA - hlavne udalosti týkajúce sa súkromného kľúča RA (jeho kompromitácia, prijatie alebo strata čipovej karty, zabudnutie hesla), bezpečnosti pracoviska RA, prijatie (a spôsob vybavenia) podnetu, pripomienky alebo žiadosti o výklad CP a CPS, odmietnuté žiadosti o certifikát, došlé požiadavky, sťažnosti a pod. a ich vybavenie, požiadavky na zaslanie CRL a certifikátu CA Disig. Zaznamenáva sa tu tiež vykonanie kontroly alebo auditu na danej RA.

RA tu môže urobiť ľubovoľný zápis týkajúci sa CA Disig, ktorý považuje za potrebný alebo užitočný.

Pracovisko RA uchováva všetku email korešpondenciu týkajúcu sa CA Disig s inými zložkami CA Disig aj externým prostredím (zákazníci, záujemca o služby ap.).

Pracovisko RA uchováva tiež všetku svoju písomnú korešpondenciu týkajúcu sa CA Disig.

4.6 Archívne záznamy

Archivácia záznamov sa vykonáva vhodným spôsobom v pravidelných intervaloch, aby sa zabezpečilo dlhodobé uloženie záznamov v zmysle požiadaviek zákona č. 215/2002 Z. z.

Prezeranie archivovaných záznamov sa umožní v celom rozsahu PMA a osobám vykonávajúcim audit zhody.

Modifikovanie alebo odstraňovanie archivovaných informácií nie je prípustné.

4.7 Zmena kľúča

Nevykonáva sa – v prípade potreby zmeny kľúča je nutné postupovať rovnako ako v prípade potreby vydania nového certifikátu (resp. následného certifikátu).

Ak má predmetný certifikát platnosť viac ako 30 dní, pred podaním žiadosti o nový certifikát (alebo najneskôr súčasne s ňou) je nevyhnutné požiadať o zrušenie predmetného certifikátu.

4.8 Havarijný plán pre mimoriadne udalosti

V prípade kompromitácie kľúča koreňovej CA Disig resp. podriadených CA sa tieto zrušia. Informácia o ich zrušení sa musí publikovať okamžite najrýchlejším možným spôsobom.

CA Disig upozorní držiteľov certifikátov, ktoré boli podpísané zrušeným certifikátom CA Disig ako aj strany spoliehajúce sa na dané certifikáty, že zrušený certifikát CA Disig sa má odstrániť z každej aplikácie, ktorú používajú strany spoliehajúce sa na certifikáty, a má byť nahradený novým certifikátom CA Disig. Tento sa musí distribuovať spoľahlivým spôsobom a v súlade s časťou 2.6.

V prípade havárie, pri ktorej je vybavenie CA Disig poškodené a neschopné prevádzky, ale nie je zničený jej podpisový kľúč, je potrebné obnoviť funkčnosť CA Disig ,podľa možnosti čo najrýchlejšie, pričom treba dať prioritu schopnosti zrušovať certifikáty a zverejňovať aktuálne CRL.

V prípade havárie, pri ktorej je inštalácia CA Disig fyzicky poškodená a jej podpisový kľúč je v dôsledku toho zničený, certifikát CA Disig sa zruší. Potom sa kompletne zopakuje inštalácia CA Disig s obnovením vybavenia CA Disig, vygenerovaním nových kľúčov CA Disig, vytvorením nového certifikátu CA Disig a nových certifikátov RA. Nakoniec sa nanovo vydajú všetky užívateľské certifikáty za použitia nového certifikátu CA Disig. Náklady na vytvorenie nových certifikátov subjektom, ktoré boli dotknuté vytvorením nového certifikátu CA Disig, nesie v takomto prípade CA Disig.

Strany spoliehajúce sa na certifikáty môžu na vlastné riziko urobiť rozhodnutie pokračovať v používaní certifikátov podpísaných použitím zničeného súkromného kľúča, aby sa splnili ich urgentné operačné požiadavky.

V prípade straty alebo poškodenia čipovej karty, na ktorej je uložený certifikát RA alebo v prípade zabudnutia hesla na prístup ku súkromnému kľúču uloženému

na danej čipovej karte alebo v prípade nefunkčnosti čítačky čipových kariet je RA povinné na nevyhnutnú mieru obmedziť alebo pozastaviť výkon svojej činnosti a udalosť okamžite oznámiť PMA.

Fungovanie RA sa obnoví tak, že sa certifikát RA zruší a vytvorí sa nový certifikát RA. O tomto sa urýchlene oboznámia všetky zložky CA Disig a zabezpečí im doručenie nového certifikátu danej RA (prostredníctvom email správy podpísanej novým certifikátom RA).

4.9 Ukončenie činnosti CA Disig

Pri ukončení činnosti CA Disig z iných dôvodov ako sú udalosti spôsobené vyššou mocou (napr. prírodná katastrofa, vojnový stav, rozhodnutie štátnej moci a pod.) sa postupuje v súlade s časťou 4.8.

CA Disig pritom vhodným spôsobom sprístupní informácie o ukončení svojej činnosti držiteľom všetkých ňou vydaných platných certifikátov a stranám spoliehajúcim sa na certifikáty.

Po ukončení svojej činnosti CA Disig nevydá žiaden certifikát a zabezpečí preukázateľné zničenie podpisových dát (súkromného kľúča) CA Disig.

Ak je dôvodom ukončenia činnosti CA Disig nejaký dôvod bez vzťahu k bezpečnosti, potom ani certifikát CA Disig, ktorá končí činnosť, ani certifikáty podpísané touto CA Disig nemusia byť zrušené.

Pred ukončením svojej činnosti RA poskytne archivované dáta zložke CA Disig podľa pokynu PMA.

5. Fyzické, procedurálne a personálne bezpečnostné opatrenia

5.1 Fyzické bezpečnostné opatrenia

Prístup RA k vybaveniu CA Disig, ktoré RA využíva pri svojej činnosti, bude chránený pred neautorizovaným prístupom tým, že RA bude na svoju autentizáciu používať vlastný certifikát RA, prostredníctvom ktorého sa bude identifikovať.

Dôležitým bezpečnostným opatrením, ktoré podstatným spôsobom obmedzuje možnosť zneužitia elektronickej identity RA (certifikátu RA a najmä k nemu patriaceho súkromného kľúča), je to, že daný pár kľúčov RA bude uložený na čipovej karte. Prístup k súkromnému kľúču uloženému na karte je navyše chránený pomocou hesla (pass phrase).

Na ochranu vybavenia RA sa použijú aj ďalšie bezpečnostné mechanizmy primerané úrovni hrozby v prostredí vybavenia RA.

5.2 Procedurálne bezpečnostné opatrenia

Osoby vybrané na zastávanie roly RA musia byť zodpovedné a dôveryhodné, lebo táto rola si vyžaduje dôveryhodnosť. Funkcie vykonávané touto rolou patria k funkciám, ktoré formujú v personálnej rovine základ dôvery v celú CA Disig.

Každá RA, ktorá funguje podľa tohto dokumentu, je predmetom jeho ustanovení. Zodpovednosťou RA je v prvom rade:

- overovanie identity buď prostredníctvom osobného kontaktu alebo prostredníctvom zastupujúceho subjektu,
- zaznamenávanie informácií od žiadateľov o certifikát a overovanie ich správnosti,
- bezpečná komunikácia s CA Disig,
- distribuovanie certifikátov pre server prijatých od CA Disig,
- komunikácia so žiadateľmi o certifikát a držiteľmi certifikátov a dokumentovanie tejto komunikácie.

Osoba spravujúca daný komponent zastáva rolu žiadateľa o certifikát a držiteľa certifikátu v prípade hardvérových alebo softvérových komponentov (t.j. neživých systémov), pre ktoré sa vydáva certifikát. Osoba spravujúca daný komponent koná v súčinnosti s CMA pri registrovaní komponentov (routre, firewally atď.) v súlade s časťou 3.1.9 a zodpovedá za plnenie povinností držiteľov certifikátov ako sú definované v tomto dokumente.

5.3 Personálne bezpečnostné opatrenia

Personálne bezpečnostné opatrenia sú zabezpečované internými mechanizmami subjektu – zriaďovateľa.

Personál pre ľubovoľnú rolu sa musí vyberať na základe spoľahlivosti, lojality a dôveryhodnosti. Všetky osoby zastávajúce rolu RA musia byť občanmi Slovenskej republiky.

Všetky osoby zastávajúce rolu RA musia byť náležite poučené a zaškolené.

Témy majú obsahovať fungovanie softvéru a hardvéru používaného RA, prevádzkové a bezpečnostné procedúry, ustanovenia tohto dokumentu.

6. Technické bezpečnostné opatrenia

6.1 Generovanie páru kľúčov a inštalácia

6.1.1 Generovanie páru kľúčov

Tieto CPS nevylučujú žiadny zdroj kľúčov, ktoré boli vygenerované v súlade s ustanoveniami týchto pravidiel a lokálnymi bezpečnostnými požiadavkami. Predpokladá sa, že súkromný kľúč bude vygenerovaný subjektom, ktorý sa stane jeho vlastníkom: napr. žiadateľom o certifikát alebo RA a na zariadení (napr. počítač, čipová karta alebo iný token, HSM modul a pod.), ktoré je v počas generovania kľúča pod bezprostrednou kontrolou subjektu, ktorý sa stane vlastníkom generovaného kľúča.

Súkromný kľúč sa nesmie dostať von z modulu, v ktorom bol vygenerovaný, s výnimkou, že je zašifrovaný kvôli jeho lokálnemu prenosu alebo spracovaniu alebo úschove.

CA Disig zásadne neposkytuje službu generovania páru kľúčov pre cudzí subjekt na zariadeniach patriacich CA Disig.

Dôležitým bezpečnostným aspektom, ktorý podstatným spôsobom obmedzuje možnosť zneužitia privátneho kľúča patriaceho RA, je to, že daný pár kľúčov RA bude generovaný a uložený na čipovej karte.

Proces generovania páru kľúčov na čipovú kartu sa iniciuje prostredníctvom pripojenia sa na web CA Disig vhodným prehliadačom, otvorenia stránky, cez ktorú sa generuje žiadosť o osobný certifikát a príslušnej voľby typu kľúča.

6.1.2 Doručenie súkromného kľúča držiteľovi certifikátu

Predpokladá sa, že súkromný kľúč bude vygenerovaný samotným subjektom (žiadateľom o certifikát), ktorý sa stane jeho vlastníkom a na zariadení, ktorého držiteľom je daný subjekt – týmto odpadá potreba doručenia súkromného kľúča držiteľovi certifikátu.

6.1.3 Dĺžky kľúčov

Algoritmy a dĺžky kľúčov uplatňované v certifikátoch AdmCA:

Algoritmus podpisu (Signature Algorithm)
sha1RSA
Verejný kľúč
RSA, dĺžka je 2048 bitov
Algoritmus odtlačku (fingerprint, hash) (Thumbprint Algorithm)
SHA1

Algoritmy a dĺžky kľúčov uplatňované v certifikáte koreňovej CA Disig:

Algoritmus podpisu (Signature Algorithm)
sha1RSA
Verejný kľúč
RSA, dĺžka je 2 048 bitov
Algoritmus odtlačku (fingerprint, hash) (Thumbprint Algorithm)
SHA1

Algoritmy a dĺžky kľúčov uplatňované v certifikáte podriadených CA Disig:

Algoritmus podpisu (Signature Algorithm)
sha1RSA resp. sha256RSA
Verejný kľúč
RSA, dĺžka je minimálne 2 048 bitov
Algoritmus odtlačku (fingerprint, hash) (Thumbprint Algorithm)
SHA1
Doba platnosti certifikátu
V závislosti na platnosti certifikátu koreňovej CA Disig*

* - hodnota „Valid to“ certifikátu podriadenej CA nesmie prekročiť hodnotu poľa „Valid to“ nadriadenej (koreňovej) CA.

6.2 Ochrana súkromného kľúča

Držiteľ certifikátu musí zabezpečiť, aby sa jeho súkromný kľúč nikdy nedostal v nezašifrovanej forme mimo modul, kde je uložený.

Základným princípom je, že nikto nemá mať prístup k súkromnému kľúču okrem jeho držiteľa.

Držiteľom kľúčov je dovolené zálohovať ich vlastné páry kľúčov. Počas zálohovania a prenosu majú byť kľúče zašifrované. Držiteľ kľúča zodpovedá za garanciu, že všetky kópie súkromných kľúčov sú chránené, vrátane ochrany všetkých pracovných staníc, na ktorých sa nachádza ľubovoľný z jeho súkromných kľúčov.

Pass-frázy, PINy, biometrické dáta alebo iné mechanizmy ekvivalentnej autentizačnej robustnosti sa musia použiť na ochranu prístupu k použitiu súkromného kľúča.

Kryptografické moduly, ktoré sa aktivovali, nesmú byť ponechané bez dozoru alebo inak otvorené pre neautorizovaný prístup. Hardvérové kryptografické moduly sa majú vyňať a uschovať, keď sa nepoužívajú.

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

Aktivačné dáta pre súkromné kľúče patriace k certifikátom potvrdzujúcim individuálnu identitu nemajú byť nikdy využívané spoločne viacerými osobami.

Aktivačné dáta pre súkromné kľúče patriace k certifikátom potvrdzujúcim identitu organizácie resp. jej organizačnej zložky majú byť známe len tým osobám, ktoré sú v organizácii autorizované na použitie daných súkromných kľúčov.

Súkromný kľúč RA uložený na čipovej karte sa nikdy nedostane mimo čipovú kartu, na ktorej bol vygenerovaný, dokonca sa ani nedá zálohovať. Prístup k súkromnému kľúču uloženému na karte je navyše chránený pomocou hesla (pass phrase).

Čipová karta ako odpojiteľný prvok vybavenia RA nesmie byť ponechaná bez dozoru v čítačke kariet, ale vždy, keď sa nepoužíva, sa musí inaktivovať vybraním z čítačky.

Čipovú kartu musí osoba, ktorá ju používa, uložiť čo najbezpečnejšie, podľa možnosti v uzamykateľnom zariadení (bezpečnostná skriňa, trezor a pod.).

Aktivačné dáta patriace k čipovej karte (t.j. heslo na prístup k súkromnému kľúču uloženému na karte) v žiadnom prípade nesmú byť zaznamenané a uložené spolu s čipovou kartou, aby sa predišlo zneužitiu súkromného kľúča uloženého na karte v prípade straty alebo krádeže karty.

6.3 Manažment páru kľúčov

Všetky certifikáty, ktoré vydá CA Disig, budú archivované ďalších 10 rokov po ukončení ich platnosti resp. ukončení činnosti CA Disig.

Archivovanie súkromných kľúčov je plne vecou držiteľov týchto kľúčov, CA Disig ich nemôže archivovať, keďže ich nemá k dispozícii a ani ich negeneruje pre externé subjekty.

7. Profily certifikátov a zoznamov zrušených certifikátov

Profily certifikátov a zoznamov zrušených certifikátov sú stanovené centrálne – zákazník ani RA nemôžu meniť štruktúru certifikátov.

7.1 Profily certifikátov

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

7.2 Profily zoznamov zrušených certifikátov

CRL vydávané CA Disig sú CRL verzie 2.

Algoritmus podpisu (Signature Algorithm):	**sha1RSA**

CRL obsahuje všetky zrušené certifikáty vrátane tých, ktoré už v čase vydania daného CRL nie sú platné.

8. Administrácia špecifikácií

8.1 Procedúry na zmenu špecifikácie

PMA môže posúdiť a prípadne revidovať tento dokument.

Chyby, požiadavky na aktualizáciu, alebo navrhované zmeny tohto dokumentu sa majú oznámiť kontaktu uvedenému v časti 0. Takáto komunikácia musí obsahovať popis zmeny, zdôvodnenie zmeny a kontaktné údaje osoby, ktorá zmenu požaduje.

Všetky zmeny motivované PMA musia byť dané na vedomie subjektom, ktorých sa týkajú (viď časť 8.2) v priebehu jedného mesiaca.

Po uplynutí doby určenej na posúdenie návrhu na zmenu musí PMA navrhovanú zmenu prijať, prijať s úpravou alebo odmietnuť.

8.2 Publikačná a oznamovacia politika

PMA publikuje verejne informácie, ktoré sú obsahom tohto dokumentu. V prípade schválenia novej verzie CPS RA sú tieto publikované najneskoršie pred dňom účinnosti prostredníctvom repozitára (pozri 2.6), tak aby bola dostupná všetkým spoliehajúcim sa stranám v čase nadobudnutia účinnosti. Schválená verzia CPS RA je zaslaná v elektronickej forme všetkým externým RA v dostatočne dlhom čase pred nadobudnutím ich účinnosti, tak aby sa mohli tieto pripraviť na ich implementáciu. Za zaslanie je zodpovedný vedúci oddelenia služieb CA.

8.3 Procedúry zverejňovania

Tento dokument bude plne k dispozícii pre PMA, CA Disig a RA a audítora vykonávajúceho audit CA Disig resp. RA.

Pre verejnosť sa bude dokument zverejňovať prostredníctvom web stránky CA Disig a prípadne aj iným vhodným spôsobom.

8.4 Úľavy

PMA má právo rozhodnúť, či je odchýlka v praxi CMA prijateľná podľa tohto dokumentu, alebo či má CA navrhnúť zmenu tohto dokumentu.

PMA môže povoliť úľavu od niektorej požiadavky tohto dokumentu, aby sa vyhovelo urgentným, nepredvídateľným prevádzkovým požiadavkám.

Keď sa povolí úľava, má sa to zverejniť pomocou webu CA Disig, aby sa o úľave dozvedeli strany spoliehajúce sa na certifikáty a má sa, buď iniciovať zmena do tohto dokumentu, alebo sa má pre platnosť danej úľavy stanoviť konkrétny časový limit. Každá úľava musí byť zaznamenaná knihe CA Disig.