Certifikačný poriadok CA Disig

verzia 4.6

platný od 1.7.2013

OID 1.3.158.35975946.0.0.0.1.1

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
2.0	23.01.2007	Rozšírenie CP v súvislosti s novým typom vydávaných certifikátov pre zmluvného klienta. Doplnenie kapitoly 7 „Profily certifikátov“; Miškovič.
2.1	29.03.2007	Opravy textu v kap. 2.8 a kap. 4.9 Úpravy textu v súvislosti s minoritnou zmenou v certifikáte pre zmluvného partnera; Miškovič
3.0	19.03.2008	Celková revízia CP vzhľadom k jednotlivým typom certifikátov; Ďurišová, Miškovič
3.1	24.06.2008	Pridanie nového typu certifikátu; Miškovič
3.2	10.11.2008	Zmena dĺžky platnosti certifikátov pre doménového používateľa PKI VšZP Zrušenie prevádzky na Záhradníckej 153.
3.3	25.11.2008	Úprava znenia: ods. 3.1.9 - overovanie vlastníctva domény ods. 4.1.1, 4.1.2, - overovanie platnosti e-mail adresy žiadateľa
3.4	02.06.2009	Úprava v súvislosti s požiadavkou na minimálnu dĺžku verejného kľúča, na ktorý CA Disig vydá certifikát (ods.5.1.3; 6.1.2); Zmena umiestnenia e-mail adresy v profile certifikátu (ods. 3.1.2; 6.1.2); Miškovič
4.0	14.10.2009	Úprava v súvislosti s požiadavkami Mozilla Foundation pri uchádzaní sa o umiestnenie certifikátu CA Disig do Mozilla Root Certificate Store; Miškovič
4.1	11.05.2010	Zapracovanie navrhnutých nápravných opatrení z auditu zo dňa 13.11.2009 (audit podľa ETSI TS 102042 V1.3.4); Miškovič
4.2	11.03.2011	Zmena dĺžky platnosti certifikátov; zapracovanie požiadaviek novej bezpečnostnej politiky Mozilla Foundation a požiadaviek Microsoft (code signing); formálne úpravy tabuliek a textov; Miškovič
4.3	25.01.2012	Doplnenie možnosti vydávania podriadených CA, doplnenie podpisových algoritmov a pravidelná ročná revízia obsahu; Miškovič
4.4	22.06.2012	Zapracovanie požiadaviek dokumentu „Baseline Requirements for the Issuance and Management of Publicly-Trusted Certificates, v.1.0, ktorý vydala CA/Browser Forum; Miškovič
4.5	15.08.2013	Spresnenie profilu certifikátov koreňových certifikačných autorít CA Disig a ostatných vydávaných typov certifikátov; Miškovič
4.6	21.6.2013	Spresnenie OID dokumentu – vypustenie verzie dokumentu z OID (kap. 1.2). Úprava profilov pre vydávanie podriadených CA – certificatePolicies Identifier (kap.7.1.2); Povolenie vydávania „wildcard“ SSL certifikátov na tretej úrovni doménového mena; (3.1.2 Miškovič

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

CA	–	Certifikačná autorita (Certification Authority)
CMA	–	Autorita pre správu certifikátov (Certificate Management Authority)
CP	–	Certifikačný poriadok (Certificate Policy)
CPS	–	Pravidlá na výkon certifikačných činností (Certificate Practice Statement)
CPS_CA	–	Pravidlá na výkon certifikačných činností – Časť Certifikačná autorita
CRL	–	Zoznam zrušených certifikátov (Certification Revocation List)
EFTA	–	Európska zóna voľného obchodu (European Free Trade Association) – členovia Island, Lichtenštajnsko, Nórsko a Švajčiarsko
HSM	–	Hardware Security Modul
IČO	–	Identifikačné číslo organizácie
NBÚ	–	Národný bezpečnostný úrad
OID	–	Identifikátor objektu (Object Identifier)
PEM	-	Formát umožňujúci ukladanie a distribúciu binárnych dát v čitateľnej podobe pomocou algoritmu Base64
PKCS#10	-	Formát žiadosti o certifikát podľa štandardu Public Key Cryptographic Standards (RFC 2986)
PKI		Infraštruktúra verejných kľúčov (Public Key Infrastructure)
PMA	–	Autorita pre správu CP (Policy Management Authority)
RA	–	Registračná autorita (Registration Authority)
SSCD	-	Zariadenie určené na bezpečné generovanie, uloženie a použitie páru kľúčov (súkromný aj verejný). Môže byť napr. vo forme čipovej karty, USB kľúča, HSM modulu.

Odkazy

1. Zákon č. 215/2002 Z. z. o elektronickom podpise a o zmene a doplnení niektorých zákonov v znení zákona č. 76/2009 Z. z.
2. RFC5280, Request for Comments: 5280, Internet X.509 Public Key Infrastructure: Certificate and Certificate Revocation List (CRL) Profile, Cooper et al, May 2008.
3. CA/Browser Forum Baseline Requirements for the Issuance and Management of Publicly-Trusted Certificates, v.1.1.3 (Current through adoption of Ballot 97 on 21 February 2013), CA / Browser Forum, 2011-2013
4. ETSI TS 102 042 V2.1.1, Electronic Signatures and Infrastructures (ESI); Policy requirements for certification authorities issuing public key certificates.
5. Zákon č. 122/2013 o ochrane osobných údajov a o zmene a doplnení niektorých zákonov.
6. RFC3647, Request for Comments: 3647, Internet X.509 Public Key Infrastructure Certificate Policy and Certification Practices Framework, S. Chokhani, Orion Security Solutions, Inc.; W. Ford, VeriSign, Inc.; R. Sabett, Cooley Godward LLP; C. Merrill, McCarter & English, LLP; S. Wu, Infoliance, Inc.; November 2003

1. Úvod

V tomto dokumente je popísaný certifikačný poriadok (ďalej len „CP“) certifikačnej autority CA Disig (ďalej len „CA Disig“), platný pre všetky koreňové certifikačné autority CA Disig a všetky podriadené certifikačné autority, prevádzkované spoločnosťou Disig, a. s., (ďalej len „Disig“).

CP je využívaný pri implementácii infraštruktúry verejných kľúčov (ďalej len PKI), ktorá pozostáva z produktov a služieb, ktoré poskytujú a spravujú certifikáty podľa štandardu X.509 (Internet X.509 Public Key Infrastructure – Infraštruktúra verejných kľúčov).

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

Niektoré určené aplikácie pri svojom používaní môžu vyžadovať aj vyššiu úroveň zabezpečenia ako je tá, ktorá je uvedená v tomto CP.

1.1 Prehľad

Cieľom CP nie je definovanie konkrétnej implementácie PKI ani plány na budúce implementácie alebo budúce certifikačné poriadky.

Tento CP definuje vytváranie a správu certifikátov s verejnými kľúčmi, podľa štandardu X.509 verzie 3 v súlade s požiadavkami zákona č. 215/2002 Z. z. o elektronickom podpise a o zmene a doplnení niektorých zákonov [1], požiadavkami RFC 5280 „Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile“ [2] a požiadavkami Baseline Requirements for the Issuance and Management of Publicly-Trusted Certificates [3].

1.2 Identifikácia

Názov:	**Certifikačný poriadok CA Disig**
Skratka názvu:	**CP CA Disig**
Verzia:	**4.6**
Schválené dňa:	**21.6.2013**
Platnosť od:	**1.7.2013**
Tomuto dokumentu je priradený identifikátor objektu (OID):	**1.3.158.35975946.0.0.0.1.1**

Popis použitého identifikátora objektu (OID):

1. – ISO assigned OIDs

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

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

1.3.158.35975946. – Disig, a. s.

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

1.3.158.35975946.0.0.0.1.**1** – **CP CA Disig**

Všetky certifikáty vydané do 1.6.2013 v zmysle tohto CP obsahujú základný OID v tvare **1.3.158.35975946.0.0.0.1.1,** ktorý navyše na posledných dvoch miestach obsahuje naviac presnú verziu platného CP v čase vydávania daného certifikátu t. j. napr. certifikáty vydané od 18.8.2012 do 1.6.2013 obsahujú OID politiky v tvare **1.3.158.35975946.0.0.0.1.1.4.5**.

Od tejto verzie CP bude používaný jednotný identifikátor tohto dokumentu v tvare ako je uvedený vyššie a všetky profily vydávaných certifikátov budú upravená tak aby obsahovali tento nový OID.

1.3 Komunita a použiteľnosť

1.3.1 Autority

1.3.1.1 Autorita pre správu CP

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

- dohľadu na vytváranie a aktualizáciu certifikačných poriadkov, vrátane vyhodnocovania zmien a plánov na implementovanie ľubovoľných prijatých zmien,
- revízie pravidiel na výkon certifikačných činností (Certificate Practice Statement ďalej len CPS) certifikačnej autority prostredníctvom analýzy CPS, aby sa zaručilo, že prax CA Disig vyhovuje príslušnému CP,

- revízie výsledkov auditov zhody, aby sa určilo, či CA Disig adekvátne dodržuje ustanovenia schváleného CPS,
- dávania odporúčaní pre CA Disig ohľadne nápravných akcií a iných vhodných opatrení,
- určenia vhodnosti používania cudzích poriadkov,
- dávania odporúčaní ohľadne vhodnosti certifikátov asociovaných s daným CP pre špecifické aplikácie riadenia a usmerňovania činnosti certifikačnej autority a registračných autorít,
- výkladu ustanovení CPS a svojich pokynov pre RA a CA,
- vykonávania auditu CA Disig,
- zabezpečenia, že prijatá a schválená certifikačná politika (CP) a 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.

1.3.1.2 Certifikačná autorita

Certifikačná autorita (Certification Authority - CA) je entita autorizovaná PMA na vytváranie, podpisovanie a vydávanie certifikátov s verejným kľúčom pre koreňové CA Disig, podriadené CA Disig a certifikáty koncových používateľov.

CA je zodpovedná za všetky aspekty vydávania a správy vyššie uvedených certifikátov, vrátane kontroly nad procesom registrácie, procesom identifikácie a autentizácie, procesom vytvárania certifikátov, publikácie certifikátov, zrušenia certifikátov, zmeny páru kľúčov certifikátu. CA zaručuje, že všetky aspekty jej služieb, operácií a infraštruktúry zviazanej s certifikátmi vydanými podľa tohto CP sa vykonávajú v súlade s požiadavkami a ustanoveniami tohto CP.

1.3.1.3 Registračná autorita

Registračná autorita (Registration Authority - RA) je entita, ktorá na základe rozhodnutia CA vykonáva činnosti, ktoré sú bližšie popísané v kapitole 2.1.2.

RA musí vykonávať svoje aktivity v súlade so schváleným CPS.

CA Disig môže zriadiť RA nasledovných typov:

- **komerčná RA** – bude slúžiť na poskytovanie služieb CA Disig pre záujemcov o certifikáty všetkých typov zo strany verejnosti resp. nezávislých tretích strán. Komerčná RA je prevádzkovaná, na základe písomnej zmluvy so spoločnosťou Disig ako prevádzkovateľom CA Disig, inou právnickou osobou a je splnomocnená podpisovať dokumenty vytvárané pri poskytovaní zmluvne dohodnutých služieb CA Disig.
- **firemná RA** – bude slúžiť na vydávanie certifikátov pre vlastné potreby danej spoločnosti resp. pre potreby ňou prevádzkovaných systémov vyžadujúcich použitie certifikátu. Firemná RA je prevádzkovaná na základe písomnej zmluvy so spoločnosťou Disig ako prevádzkovateľom CA Disig, inou

právnickou osobou a je splnomocnená podpisovať dokumenty vytvárané pri poskytovaní zmluvne dohodnutých služieb CA Disig.

- **interná RA** – bude prevádzkovaná spoločnosťou Disig a je určená na poskytovanie komplexných certifikačných služieb poskytovaných CA Disig pre všetkých záujemcov. Táto RA nie je samostatný právny subjekt.

CA a RA spolu tvoria Autoritu pre správu certifikátov (Certificate Management Authority, ďalej len „CMA“). Termín CMA sa bude používať, keď funkciu možno priradiť buď CA alebo RA alebo keď sa požiadavka týka súčasne CA aj RA. Rozdelenie zodpovednosti pri registrácii žiadateľa o certifikát medzi CA a RA sa môže líšiť pri viacerých implementáciách tohto CP. Toto rozdelenie zodpovednosti bude popísané v CPS pre danú RA.

CA Disig v súčasnej dobe zriaďuje len RA pôsobiace na území Slovenskej republiky, ktoré sú právnym subjektom so sídlom v Slovenskej republike.

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 splniť žiadateľ o certifikát, definuje tento CP.

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

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 držiteľovi certifikátu také bezpečnostné prostriedky (certifikáty) na zabezpečenie komunikácie, aby mohol využívať výhody bezpečnej komunikácie s minimálnymi nákladmi t. j. používaním bežne dostupného softvéru.

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

- zabezpečenia elektronickej pošty (podpisovanie a/alebo šifrovanie správ posielaných elektronickou poštou, nemožnosť popretia (non-repudiation) zodpovednosti za odoslanú správu elektronickej pošty),
- podpisovanie elektronických dokumentov,
- zabezpečenia SSL 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, v závislosti od typu CA (koreňová, podriadená) žiadateľom o certifikát tieto typy certifikátov:

- certifikáty na správu (certifikáty podriadených certifikačných autorít, služba časovej pečiatky (TS) resp. on-line overovanie stavu certifikátov (OCSP)),
- 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“) alebo podpisovanie elektronických dokumentov,
- SSL certifikáty – 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.

Certifikáty CA Disig, ktoré boli vydané pre zložky CMA, sa môžu používať výlučne na výkon činností týchto zložiek a to len na ich pracoviskách.

Dokument CPS môže presnejšie vymedziť:

- zoznam aplikácií, pre ktoré sú vydávané certifikáty vhodné,
- zoznam aplikácií, pre ktoré je použitie vydávaných certifikátov obmedzené,
- zoznam aplikácií, pre ktoré je použitie vydávaných certifikátov zakázané.

CA Disig potvrdzuje, že v tomto CP sú zohľadnené všetky požiadavky aktuálnej verzie dokumentu „Baseline Requirements for the Issuance and Management of Publicly-Trusted Certificates“ [3], 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 [3].

1.4 Kontaktné údaje

Certifikačná autorita CA Disig	
Adresa:	**Záhradnícka 151, 821 08 Bratislava 2**
e-mail:	**caoperator@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 CA

CA Disig, ktorá vydáva certifikáty založené na tomto CP, musí vyhovovať jeho ustanoveniam, vrátane nasledujúcich:

- poskytnúť PMA svoj dokument CPS, ako aj jeho ľubovoľné následné zmeny, na ohodnotenie jeho súladu s týmto CP,
- konať v súlade s ustanoveniami schváleného CPS,
- zaručiť, že sa akceptujú registračné informácie výlučne od RA, ktoré rozumejú tomuto CP a sú zaviazané konať v súlade s ním,
- uvádzať v certifikátoch len správne a náležité informácie a archivovať doklady dokazujúce správnosť údajov uvádzaných v certifikátoch,
- garantovať, že držiteľ certifikátu je viazaný povinnosťami v súlade s časťou 2.1.3 tohto CP a je informovaný o následkoch neplnenia týchto povinností,
- zrušiť certifikáty držiteľom, ak sa zistí, že títo konali v rozpore so svojimi povinnosťami,
- prevádzkovať v režime on-line repozitár, ktorý vyhovuje ustanoveniam uvedeným v časti 2.1.5.

Ak sa zistí, že CA Disig nekoná v súlade s týmito povinnosťami, uplatnia sa na ňu príslušné opatrenia.

CA Disig má výlučnú zodpovednosť za garancie, že certifikáty, ktoré podpisuje, sa vytvárajú a spravujú v súlade s týmto CP a že procesy vytvárania, správy a zrušenia certifikátov sú vykonávané len takými osobami, ktoré rozumejú príslušným požiadavkám CP a zaviazali sa ich dodržiavať.

CA Disig začne preskúmavanie oznámení podaných v súvislosti s možnou kompromitáciou súkromného kľúča resp. akýmkoľvek zneužitím certifikátu do 24 hodín od doručenia oznámenia. Pri rozhodovaní o možnom zrušení certifikátu príp. iných opatreniach bude brať do úvahy nasledovné:

1. Opodstatnenosť tvrdenia v oznámení;
2. Počet nahlásených problémov týkajúcich sa daného certifikátu resp. jeho držiteľa;
3. Postavenie oznamovateľa (napr. prijatie oznámenia od štátneho orgánu, že prostredníctvom web stránky sú vykonávané nelegálne aktivity bude mať vyššiu váhu ako oznámenie kupujúceho, že mu nebol doručený on-line objednaný tovar);
4. Zodpovedajúce legislatívne požiadavky;

CA Disig zabezpečí kontinuálnu schopnosť reakcie 24/7 pre súrne prípady bezpečnostných problémov s vydaným certifikátom a pokiaľ to bude nevyhnutné,

postúpi tieto zodpovedným autoritám a/alebo zruší certifikát, ktorý je predmetom oznámenia (sťažnosti).

2.1.2 Povinnosti RA

RA, ktorá vykonáva registračné funkcie popísané v tomto CP, musí vyhovovať jeho ustanoveniam a konať podľa príslušného schváleného CPS. Ak sa zistí, že RA nekoná v súlade s týmito povinnosťami, uplatnia sa na ňu príslušné opatrenia, vrátane zastavenia jej činnosti ako RA.

Rozdelenie zodpovednosti medzi CA a RA sa môže líšiť pri viacerých implementáciách tohto CP. Toto rozdelenie zodpovednosti bude popísané v CPS pre danú CA.

RA zabezpečuje funkciu podateľne pre certifikačnú autoritu CA Disig – konkrétne najmä zhromažďovanie a overovanie informácií od žiadateľov o certifikát, ktoré majú byť uvedené v certifikátoch.

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

RA prijíma žiadosti o certifikáty, preveruje totožnosť žiadateľov o certifikáty, sprostredkuje odovzdávanie certifikátov a zoznamu zrušených certifikátov držiteľom, za určitých okolností (pozri kapitolu 4.4.1.1.) inicializuje zrušenie certifikátu a vykonáva procesy spojené so žiadosťou o zrušenie certifikátu resp. žiadosťou o vydanie následného certifikátu, prijíma a vybavuje ich reklamácie a sťažnosti, vyberá od žiadateľov stanovené poplatky za služby CA Disig, pokiaľ nie je zmluvou dohodnuté inak.

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

2.1.3 Povinnosti oprávnenej osoby – držiteľa certifikátu

Pod pojmom oprávnená osoba sa myslí držiteľ certifikátu, tieto pojmy sú synonymami.

Povinnosťou držiteľa certifikátu je:

- neustále chrániť svoje súkromné kľúče v súlade s týmto CP a v súlade so znením ustanovení v 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,
- bezodkladne požiadať o zrušenie certifikátu v prípade, že akýkoľvek údaj uvedený v subjekte certifikátu sa stal neplatným (okrem e-mailovej adresy),
- dodržiavať všetky termíny, 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 príslušné účely,

- v prípade, používania certifikátu v inej krajine, pri jeho používaní dodržiavať legislatívne požiadavky na elektronický podpis platné pre danú krajinu.

Povinnosti držiteľa certifikátu sa týkajú aj fyzickej osoby, ktorá prevzala certifikáty pre ňou spravované komponenty.

Držiteľ certifikátu, ktorý nedodržuje resp. nedodržiaval svoje povinnosti, nemá nárok na náhradu prípadnej škody.

2.1.4 Povinnosti strán spoliehajúcich sa na certifikáty

Strany spoliehajúce sa na certifikáty vydané podľa tohto CP sú povinné:

- používať certifikát na účel, pre ktorý bol vydaný, ako je to dané informáciami v certifikáte,
- predtým, ako sa na certifikát spoľahnú, overovať každý certifikát na 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,
- uchovávať originálne podpísané údaje, aplikácie potrebné na čítanie a spracovanie týchto údajov a kryptografické aplikácie potrebné na overovanie elektronických podpisov týchto údajov, pokiaľ môže byť potrebné overovať podpis týchto údajov.

2.1.5 Povinnosti správy repozitára

Správa repozitára, ktorý podporuje CA Disig pri publikovaní informácií podľa tohto CP, je povinná:

- udržiavať prístupnosť informácií podľa ustanovení tohto CP pre publikovanie informácií o certifikátoch,
- poskytovať dostatočný ochranný mechanizmus riadenia prístupu k informáciám uloženým v repozitári podľa časti 2.6.3.

Prevádzkovanie a spravovanie repozitára patrí medzi povinnosti CA.

2.1.6 Povinnosti externých poskytovateľov služieb

Povinnosťou externého poskytovatelia služieb pre CA Disig je dodržiavanie zmluvne dojednaných podmienok poskytovanej služby.

2.1.7 Záruky CA pri vydávaní certifikátov

CA Disig zaručuje že pred a počas vydávania SSL certifikátu:

- overuje práva na použitie doménového mena, ktoré je uvedené v CN a v subjecAltName rozšírení, žiadateľom resp. či žiadateľ má toto pod jeho výhradnou kontrolou,

- overuje oprávnenie pracovníka RA na vydávanie SSL certifikátu a overuje, či prítomná osoba zastupujúca žiadateľa, je oprávnená na žiadanie SSL certifikátu v mene subjektu t. j. žiadateľa,
- overuje správnosť všetkých informácií obsiahnutých v žiadosti o certifikát s výnimkou poľa organizationalUnitName (OU),
- má stanovenú procedúru na zabezpečenie zníženia pravdepodobnosti, že informácia obsiahnutá v subjekte certifikátu v poli organizationalUnitName (OU) nebude zavádzajúca,
- vykonáva identifikáciu subjektu uvedeného v certifikáte v zmysle požiadaviek tohto CP časť 3 a CPS pre RA časť 3,
- uzatvorí s držiteľom certifikátu, ktorý nie je súčasťou spoločnosti Disig zmluvu vo forme dokumentu „Zmluva o vydaní a používaní certifikátu a služieb CA Disig“, ktorá spĺňa všetky požiadavky kladené na vydávané typy certifikátov (osobný – fyzická osoba, osobný - právnická osoba, SSL, code-signing),
- zruší certifikát na základe akéhokoľvek z dôvodov uvedených v tomto CP.

Všetky vyššie uvedené procesy sú vykonávané v zmysle prijatých postupov popísaných v tomto CP resp. v súvisiacom CPS pre RA.

2.2 Právne záruky

Tento CP sa riadi platnými zákonmi Slovenskej republiky, najmä zákonom č. 215/2002 Z. z. o elektronickom podpise a o zmene a doplnení niektorých zákonov v aktuálnom znení a súvisiacimi vyhláškami Národného bezpečnostného úradu.

CA Disig 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.

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

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 tohto CP.

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 tohto CP, 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 CP alebo riešenia sporov sa možno obrátiť na najbližšiu vyššiu inštanciu. Inštancie sú usporiadané vzostupne v poradí:

- RA
- CA

PMA rozhoduje s konečnou platnosťou v prípade akýchkoľvek sporov o interpretácii alebo použiteľnosti tohto CP.

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

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

2.5 Poplatky

Povinnosťou CA Disig je vhodným spôsobom zverejniť platný cenník svojich služieb resp. informáciu, za akých zmluvných podmienok je možné objednať certifikačné služby. Cenník je zverejnený prostredníctvom web stránky CA Disig (pozri časť 1.4).

Poplatky za certifikáty sa platia na RA spravidla v hotovosti, ak nie je vopred resp. zmluvne dohodnuté so žiadateľom inak.

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 Disig musí poskytovať v on-line režime repozitár, ktorý je prístupný držiteľom certifikátov a stranám spoliehajúcim sa na certifikáty, ktorý obsahuje minimálne nasledujúce informácie:

- certifikáty vydané v súlade s týmto CP,
- aktuálne CRL ako aj všetky CRL vydané od začiatku činnosti vydávania certifikátov,

- certifikát koreňových certifikačných autorít a podriadených certifikačných autorít patriacich k ich podpisovému kľúču,
- kópiu aktuálneho CP vrátane prípadných úľav pre CA schválených PMA.

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 čo najskôr po jeho vytvorení. Informácie o vydanom certifikáte možno nájsť na web stránke spoločnosti Disig (www.disig.sk), ktorý slúži ako repozitár certifikačnej autority CA Disig. 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.

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, musia byť publikované bezodkladne, hneď ako sa CA Disig takúto informáciu dozvie. CA Disig špecifikuje v CPS časové limity, v rámci ktorých bude publikovať rôzne typy informácií.

2.6.3 Kontroly prístupu

CA Disig musí chrániť ľubovoľnú informáciu uloženú v repozitári, ktorá nie je určená na verejné rozšírenie. Spoločnosť Disig vynaloží 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.

2.6.4 Repozitáre

Repozitáre musia byť lokalizované tak, aby boli prístupné držiteľom certifikátov a stranám spoliehajúcim sa na certifikáty a v súlade s celkovými bezpečnostnými požiadavkami.

Funkciu repozitára CA Disig bude zastávať web stránka certifikačnej autority CA Disig nachádzajúca sa na web stránke spoločnosti Disig. Presné URL adresy sú uvedené v časti 1.5. Stránka CA Disig je prostredníctvom Internetu verejne prístupná držiteľom certifikátov, stranám spoliehajúcim sa na certifikáty a verejnosti vôbec.

Verejne dostupné informácie uvedené na webovej stránke spoločnosti Disig majú charakter riadeného prístupu.

2.7 Audit zhody

2.7.1 Frekvencia auditu zhody pre danú entitu

CA Disig sa musí podrobiť auditu súladu poskytovaných služieb s požiadavkami medzinárodných štandardov (napr. ETSI TS 102 042 „Electronic Signatures and Infrastructures (ESI); Policy requirements for certification authorities issuing public key certificates“ [4]) minimálne jedenkrát ročne. Okrem toho každá CA má právo požadovať pravidelné a nepravidelné revízie činností jej podriadených CMA, aby sa potvrdilo, že podriadená CMA funguje v súlade s bezpečnostnými praktikami a procedúrami popísanými v príslušnom CPS.

2.7.2 Identita audítora a kvalifikačné požiadavky na neho

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

2.7.3 Témy pokrývané auditom zhody

Účelom auditu o zhode má byť záruka, že CA Disig má vyhovujúci systém práce, ktorý garantuje kvalitu služieb, ktoré CA Disig poskytuje a taktiež garantuje, že koná v súlade so všetkými požiadavkami tohto CP a svojho CPS. Všetky aspekty prevádzky CA vzťahujúce sa k tomto CP majú byť predmetom auditov zhody.

2.7.4 Akcie vykonané na odstránenie nedostatkov

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

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

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

2.7.5 Zaobchádzanie s výsledkami auditu

Audítor zhody urobí pre PMA zápis o výsledkoch auditu o zhode. Výsledky budú oznámené v súlade s časťou 2.6 auditovanej CA a jej nadradenej CA, ak táto existuje. Vykonanie opatrení na nápravu má byť 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 koreňových certifikačných autorít CA Disig používaný na vytváranie elektronického podpisu pri vydávaní certifikátov podriadených CA Disig, prípadne certifikátov koncových používateľov,
- súkromné kľúče podriadených CA a poskytovaných služieb (TS resp. OCSP)
- súkromné kľúče patriace zložkám CA Disig,
- infraštruktúra (napr. dokumenty, procedúry, postupy, súbory, skripty, heslá a pod.) slúžiaca na prevádzku CA Disig, vrátane všetkých jej RA,
- osobné údaje zákazníkov podliehajúce ochrane v zmysle zákona č. 122/2013 Z. z. o ochrane osobných a o zmene a doplnení niektorých zákonov. [5]

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

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

Ľubovoľná takáto informácia má byť explicitne definovaná v CPS. So všetkými informáciami uloženými v rámci CA Disig, ktoré nie sú v repozitári, sa má zaobchádzať ako s citlivými informáciami a prístup k nim má byť obmedzený len na osoby, ktoré tieto informácie nevyhnutne potrebujú na výkon svojich oficiálnych povinností.

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

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

2.8.2 Okolnosti uvoľnenia dôverných informácií

CA Disig nezverejní žiadne informácie týkajúce sa žiadateľa o certifikát alebo držiteľa certifikátu žiadnej tretej strane, pokiaľ to nie je povolené týmto CP, požadované zákonom alebo príkazom kompetentného súdu resp. je to predmetom zmluvy medzi CA Disig a jej partnerom. Každá požiadavka na uvoľnenie informácií má 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 zo zákona majú právo kontrolovať činnosť CA a kompetentných štátnych orgánov ako sú polícia, súdy, prokuratúra.

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 ním 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 žiadateľom vopred dohodnuté inak.

3.1.1 Typy mien

Každá CA má byť schopná vytvárať certifikáty, ktoré obsahujú rozlišovacie mená v zmysle X.500 (X.500 Distinguished Name, ďalej ako „rozlišovacie meno“).

Vo všeobecnosti CA Disig nemá priraďovať rozlišovacie mená.

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.

Keď sa používajú rozlišovacie mená, položka subject:CommonName má 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 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.

CA resp. RA má právo odmietnuť vydať certifikát, ktorý by obsahoval údaje porušujúce princíp zmysluplnosti mien. Zvláštny dôraz sa pritom kladie na údaj v položke CommonName.

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

Všetky informácie uvedené v položkách DN certifikátu, s výnimkou položky subject:organizationUnitName (Názov útvaru v organizácii), musia byť zo strany CA Disig overené.

Rozlišovacie meno používané v jednotlivých typoch certifikátov vydávaných CA Disig pozostáva z položiek, ktoré sú popísané v nasledovných častiach.

3.1.2.1 Osobný certifikát

V tabuľke sú uvedené štandardné položky nachádzajúce sa v DN osobného certifikátu s vyznačením minimálneho rozsahu povinných položiek.

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

Tabuľka č. 1: Položky osobného certifikátu a ich popis

Skratka názvu	Názov	Popis	Poznámka
C	countryName	Dvojznaková skratka štátu, **SK** pre Slovenskú republiku	**Údaj je povinný!!!**
L	localityName	Názov lokality	Údaj je nepovinný
O	organizationName	Názov organizácie	Údaj je nepovinný
OU	organizationUnitName	Názov útvaru v organizácii	Údaj je nepovinný
CN	commonName	Meno a priezvisko	**Údaj je povinný!!!**

Poznámka: 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 Názov organizácie sa nesmie použiť znak čiarka!!!

Dôležité upozornenie!!!: Pokiaľ bude osobný certifikát používaný na účely podpisovania a šifrovania elektronickej pošty je nevyhnutné, aby žiadosť vo formáte PKCS#10 obsahovala platnú **e-mailovú adresu** držiteľa certifikátu

3.1.2.2 Certifikát pre právnickú osobu

V nasledovnej tabuľke sú uvedené položky nachádzajúce sa v DN certifikátu pre právnickú osobu. Podľa potreby CA Disig môže byť certifikát pre právnickú osobu rozšírený aj o ďalšie položky v zmysle RFC 5280 časť 4.1.2.6 [2].

Tabuľka č. 2: Položky certifikátu pre právnickú osobu ich popis

Skratka názvu	Názov	Popis	Poznámka
C	countryName	Dvojznaková skratka štátu, **SK** pre Slovenskú republiku	**Údaj je povinný!!!**
L	localityName	Názov lokality	Údaj je nepovinný

O	organizationName	Názov organizácie	Údaj je nepovinný
OU	organizationUnitName	Názov útvaru v organizácii	Údaj je nepovinný
CN	commonName	Názov organizácie	**Údaj je povinný!!!**

Poznámka: 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 Názov organizácie sa nesmie použiť znak čiarka!!!

3.1.2.3 SSL certifikát a certifikát pre doménový radič

V nasledovnej tabuľke sú uvedené položky nachádzajúce sa v DN SSL certifikátov. Podľa potreby CA Disig môže byť SSL certifikát rozšírený aj o ďalšie položky v zmysle RFC 5280 časť 4.1.2.6 [2]. Každý SSL certifikát musí obsahovať rozšírenie „subjectAltName“, v ktorom bude uvedená minimálne jedna položka obsahujúca plné doménové meno domény, pre ktorú je certifikát určený.

Ako plné doménové meno bude akceptované aj meno obsahujúce znak hviezdička (*) na tretej a vyššej pozícii doménového mena (napr. *.disig.sk; *.mail.disig.sk ap.) a tento typ SSL certifikátu bude označovaný ako „wildcard“ SSL certifikát.

Plné doménové meno nesmie byť obsiahnuté v žiadnej inej položke okrem položky CommonName (CN) a rozšírenia certifikátu SubjectAlternativeName (pozri 7.1.2.3 tabuľka 12).

Tabuľka č. 3: Položky SSL certifikátu a ich popis

Skratka názvu	Názov	Popis	Poznámka
C	**countryName**	Dvojznaková skratka štátu, **SK** pre Slovenskú republiku	**Údaj je povinný!!!**
ST	stateOrProvinceName	Názov štátu –pre SR sa nepoužíva	Údaj je nepovinný
L[1)]	localityName	Názov lokality	Údaj je nepovinný[1)]
O[1)]	organizationName	Názov organizácie	Údaj je nepovinný[1)]
OU	organizationUnitName	Názov útvaru v organizácii	Údaj je nepovinný
CN	**commonName**	Názov komponentu, zariadenia	**Údaj je povinný!!!**

[1)] - **Pokiaľ je v žiadosti vyplnená položka O (organizationName), tak musí byť vyplnená aj položka L (localityName). Pokiaľ položka O (organizationName) nie je vyplnená, tak nesmie byť vyplnená položka L (localityName).**

Poznámka: 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 Názov organizácie sa nesmie použiť znak čiarka!!!

3.1.2.4 Certifikát na podpisovanie softvérových komponentov

V nasledovnej tabuľke sú uvedené položky nachádzajúce sa v DN certifikátu na podpisovanie softvérových komponentov (CodeSigning). Podľa potreby CA Disig môže byť certifikát na podpisovanie softvérových komponentov rozšírený aj o ďalšie položky v zmysle RFC 5280 časť 4.1.2.6 [2].

Tabuľka č. 4: položky certifikátu pre softvérový komponent a ich popis

Skratka názvu	Názov	Popis	Poznámka
C	countryName	Dvojznaková skratka štátu, SK pre Slovenskú republiku	**Údaj je povinný!!!**
L	localityName	Názov lokality	Údaj je nepovinný
O	organizationName	Názov organizácie	Údaj je nepovinný
OU	organizationUnitName	Názov útvaru v organizácii	Údaj je nepovinný
CN	commonName	Organizácia resp. meno a priezvisko	**Údaj je povinný!!!**

Dôležité upozornenie!!!: Žiadosť o vydanie certifikátu vo formáte PKCS#10 musí obsahovať platnú **e-mailovú adresu** držiteľa certifikátu (fyzickej osoby)

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.

CA Disig dokumentuje vo svojom CPS, aké formy mena budú používané a ako sa budú stanovovať mená v rámci komunity.

3.1.4 Procedúra riešenia sporov týkajúcich sa mien

V prípade sporov týkajúcich sa mien sa bude postupovať podľa ustanovení bodu 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 uspokojivo doloží. 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 bude 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 na SSCD zariadenie, 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 (pozri časť 6.1.2). Spôsob doručenia je podrobne opísaný v CPS.

CMA negeneruje páry kľúčov pre cudzie subjekty. Výnimkou môže byť len generovanie kľúčov na RA priamo na SSCD zariadenie žiadateľa.

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

3.1.7 Autentizácia identity právnickej osoby

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

V prípade, že právnická osoba nemá sídlo na území Slovenskej republiky, jej totožnosť sa 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).

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

3.1.8 Autentizácia identity fyzickej osoby

CMA musí garantovať, že identita žiadateľa o certifikát a jeho verejný kľúč sú zodpovedajúco previazané. Každá CMA má špecifikovať vo svojom CPS procedúry na autentizáciu identity žiadateľa o certifikát. CA bude zaznamenávať tento proces pre každý certifikát v písomnej alebo elektronickej forme. Dokumentácia o identifikácii musí minimálne obsahovať:

- identitu osoby, ktorá vykonáva identifikáciu,
- jednoznačné identifikačné čísla z predložených preukazov dokladujúcich identitu autentizovanej osoby,
- dátum a miesto vykonania identifikácie.

Súčasťou dokumentácie o identifikácii musí byť, dokument vlastnoručne podpísaný žiadateľom, v prítomnosti osoby vykonávajúcej autentizáciu identity, obsahujúci identifikačné údaje žiadateľa o certifikát. V prípade vydávania ďalšieho (následného) certifikátu zo strany CA Disig môže byť vlastnoručný podpis nahradený elektronickým za podmienok stanovených v príslušnom CPS. Žiadateľom o certifikát môže byť plnoletý občan Slovenskej republiky alebo cudzí štátny príslušník. Overenie identity vykonáva CMA na základe predloženia týchto údajov:

- celé meno a priezvisko,
- trvalý pobyt (v prípade, že je v doklade uvedený),
- rodné číslo (osoby, ktoré ho majú pridelené),
- dátum narodenia (osoby, ktoré nemajú pridelené rodné číslo),
- číslo preukazu totožnosti,
- vydavateľa preukazu totožnosti,
- dátum platnosti preukazu totožnosti.

Pokiaľ je vydávaný certifikát pre fyzickú osobu určený na podpisovanie elektronickej pošty (rozšírenie Secure Email – OID 1.3.6.1.5.5.7.3.4), tak CMA vykoná overenie vlastníctva príslušného e-mail konta postupom, ktorý je uvedený v kapitole 4.1.2.

Pokiaľ je vydávaný certifikát pre fyzickú osobu určený na podpisovanie softvérového kódu (rozšírenie Code Signing - OID1.3.6.1.5.5.7.3.3), tak zmluva musí obsahovať požiadavku na držiteľa certifikátu, že informácie k ním poskytovanej a podpísanej aplikácii určené tretím stranám budú pravdivé, správne a nezavádzajúce (názov aplikácie, informatívne URL a popis aplikácie).

Ďalšie požiadavky na prvotnú registráciu žiadateľa(držiteľa) sú podrobne popísané v kapitole 3.1.10 a 3.1.11.

3.1.9 Autentizácia identity komponentu

CMA musí garantovať aj v prípade, že certifikát je vydávaný pre hardvérový alebo softvérový komponent, ktorý môže používať certifikát, že identita komponentu a jeho verejný kľúč sú zodpovedajúco previazané.

Z uvedeného dôvodu musí byť komponent priradený fyzickej alebo fyzickej osobe konajúcej v mene právnickej osoby (organizácie), ktorá komponent spravuje (viď časť 5.2).

Táto fyzická osoba je povinná poskytnúť CMA nasledujúce informácie, ako je to popísané v častiach 3.1.10 a 5.2:

- identifikáciu zariadenia,
- verejné kľúče zariadenia (obsiahnuté 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,

CMA bude autentizovať správnosť ľubovoľnej autorizácie (hodnoty položky rozlišovacieho mena), ktorá má byť uvedená v certifikáte a bude overovať 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.

Poznámka:	Typickou hodnotou tejto položky bude úplné doménové meno.

V prípade použitia doménového mena je podmienkou, aby príslušná doména druhej úrovne patrila subjektu, ktorý je žiadateľom o daný SSL certifikát.

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.

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

Rovnaké pravidlá overovania platia aj pre „wildcard“ SSL certifikáty, ktoré obsahujú znak hviezdička (*) na tretej a vyššej pozícii úrovne domény.

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

3.1.10 Autentizácia identity u zmluvných partnerov

Autentizácia identity fyzickej osoby resp. komponentu u zmluvných partnerov spoločnosti Disig (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

3.1.11.1 Všeobecne

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 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.

3.1.11.2 Fyzická osoba

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

- občana SR - platný občiansky preukaz resp. cestovný pas
- cudzieho štátneho príslušníka – preukaz totožnosti, t. j. identifikačná karta, povolenie na pobyt na území SR, resp. cestovný pas.

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 certifikát pre potreby zmluvného partnera, alebo žiadosti o jeho zrušenie postačuje, aby daná fyzická osoba preukázala svoju totožnosť jedným z nasledovných osobných dokladov – občiansky preukaz resp. pas. 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.

3.1.11.3 Fyzická osoba - zamestnanec

Pokiaľ je žiadateľom o certifikát fyzická osoba, ktorá má v žiadosti uvedený aj názov organizácie, predkladá doklady podľa kapitoly 3.1.11.2. Zároveň musí predložiť súhlas s vydaním certifikátu od zamestnávateľa. Táto požiadavka sa netýka zamestnanca zmluvného partnera, kde je zmluvne dohodnutý iný mechanizmus overovania.

3.1.11.4 Právnická osoba

V tomto prípade žiadateľ o certifikát predkladá doklady uvedené v kapitole 3.1.11.2. 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.

3.1.11.5 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. 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.

3.1.12 Kontrola údajov na predložených dokladoch

Pracovník RA kontroluje na predložených dokladoch najmä nasledovné:

Osobné doklady fyzickej osoby:

a) súlad údajov uvedených v žiadosti s údajmi uvedenými v osobných dokladoch, najmä meno a priezvisko a trvalé bydlisko,

b) platnosť predloženého dokladu,

c) plnoletosť fyzickej osoby (t. j. vek 18 rokov),

d) súlad medzi fotografiou v osobnom doklade a vzhľadom majiteľa osobného dokladu,

e) zhodu v predložených dokladoch t. j. či údaje na jednom doklade neodporujú údajom na inom doklade.

Výpisy z obchodného registra príp. iného registra právnických osôb :

a) platnosť výpisu – nesmie byť starší ako 3 mesiace,

b) konanie za právnickú osobu - t. j., či má/majú fyzická/é osoba/y, ktoré predložili daný výpis, právo konať (podpisovať) za danú právnickú osobu,

c) forma výpisu – originál alebo úradne (notárom/matrikou) overená kópia výpisu.

Súhlas s vydaním certifikátu:

a) oprávnenie konať za spoločnosť – osoba podpisujúca súhlas musí byť oprávnená zastupovať zamestnávateľa. Oprávnenosť sa kontroluje podľa výpisu z OR resp. iného zákonom určeného registra (príp. zriaďovacej listiny, poverovacej listiny, menovacieho dekrétu). Pokiaľ podpisujúca osoba nie je zapísaná v tomto výpise, musí predložiť iný doklad, na základe ktorého môže konať za spoločnosť (spravidla notárom overená plná moc).

b) Platnosť – pokiaľ je v súhlase uvedená doba platnosti súhlasu, kontroluje sa aj tento údaj.

Plné moci:

a) overenie plnej moci (notárom/matrikou)

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

c) rozsah plnej moci - t. j. či plná moc oprávňuje splnomocnenú fyzickú alebo právnickú osobu k požadovanému úkonu na RA v mene splnomocňujúcej fyzickej, alebo právnickej osoby,

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

Čestné prehlásenia:

a) oprávnenie na podpis – osoba podpisujúca prehlásenie musí byť oprávnená zastupovať právnickú osobu. Oprávnenosť sa kontroluje podľa výpisu z OR resp. iného registra právnických osôb. Pokiaľ podpisujúca osoba nie je zapísaná v tomto výpise, musí predložiť iný doklad, na základe ktorého môže konať za spoločnosť (spravidla notárom overená plná moc)

V prípade ľubovoľných odôvodnených pochybností o totožnosti potenciálneho zákazníka, taktiež 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.

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

3.2 Vydanie následného certifikátu

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

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

O vydanie následného certifikátu (osobný certifikát, certifikát pre právnickú osobu) možno požiadať jedným z nasledovných spôsobov:

a) Žiadateľ o certifikát požiada o vydanie následného certifikátu tak, že svoju žiadosť o certifikát, s totožným obsahom (s výnimkou položiek Organizačný útvar a Mesto) ako mal predchádzajúci certifikát, zašle na kontaktnú adresu RA podpísaným mailom. Pri podpise e-mailu so žiadosťou použije súkromný kľúč prislúchajúci k platnému certifikátu, na základe ktorého sa má následný certifikát vydať. V zasielanej e-mailovej správe zároveň oznámi, že nedošlo k zmene jeho osobných údajov na základe, ktorých bol identifikovaný a autentifikovaný pri vydaní predchádzajúceho certifikátu. Pokiaľ nie je možné pri obnove certifikátu použiť podpísaný e-mail, je možné takúto žiadosť zaslať aj nepodpísaným e-mailom z rovnakej e-mail adresy aká sa nachádza v žiadosti. Súčasťou e-mailu je aj oznámenie o nezmenených osobných údajoch. V danom prípade bude zo strany RA spustený proces overenia zaslanej žiadosti. V prípade zaslania žiadosti o vydanie následného certifikátu nepodpísaným e-mailom z inej adresy ako je uvedená v zaslanej žiadosti bude táto akceptovaná len v prípade dodatočného overenia zaslania žiadosti zo strany RA.

b) Žiadateľ o následný certifikát sa podrobí požiadavkám prvotnej registrácie – osobne navštívi pobočku RA.

c) Žiadateľ o certifikát vytvorí novú žiadosť o vydanie následného certifikátu, elektronicky podpísanú súkromným kľúčom prislúchajúcim s vydaným certifikátom, na základe ktorého sa má tento následný certifikát vydať. Tento proces sa realizuje prostredníctvom webového rozhrania prístupného na web stránke CA Disig a je dostupný len vybraným zmluvným partnerom spoločnosti Disig. Držiteľ platného osobného certifikátu vydaného pre účely zmluvného partnera môže požiadať o vydanie následného certifikátu aj prostredníctvom iného mechanizmu, ktorý je dohodnutý s CA Disig.

V prípade, že došlo k zmene osobných údajov držiteľa osobného certifikátu resp. certifikátu pre právnickú osobu a držiteľ nie je zamestnancom vybraného zmluvného partnera spoločnosti Disig, následný certifikát je možné vydať len na základe vopred zaslanej žiadosti a za osobnej účasti držiteľa na príslušnej RA.

V prípade SSL certifikátov, certifikátov pre doménový radič a na podpisovanie softvérových komponentov sa následné certifikáty nevydávajú.

Všetky certifikáty CA Disig sa vydávajú s platnosťou maximálne na 36 mesiacov t. j. 3 roky.

3.3 Vydanie následného certifikátu po zrušení starého

CA Disig túto službu nepodporuje. V prípade, že po zrušení platnosti certifikátu chce mať žiadateľ nový platný certifikát vydaný CA Disig, musí požiadať o vydanie nového certifikátu podľa kapitoly 4.1. Pri tomto úkone sa podrobuje rovnakej autentizácii ako je uvedené v kapitole 3.1.7 – 3.1.9.

3.4 Žiadosť o zrušenie certifikátu

Žiadosť o zrušenie certifikátu musí byť autentizovaná, pozri časť 4.4.1.3. V prípade osobného certifikátu môže byť žiadosť o zrušenie certifikátu 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

Účelom tohto CP je

- identifikovať minimálne požiadavky a procedúry, ktoré sú nevyhnutné na podporu dôvery v certifikáty,
- minimalizovať špecifické implementačné požiadavky na CMA, žiadateľov o certifikát, držiteľov certifikátov a strany spoliehajúce sa na certifikáty.

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 a tento je vlastnený žiadateľom o certifikát (podľa časti 3.1.6),
- žiadateľ musí poskytnúť dostatočné podklady na overenie ľubovoľných identifikačných údajov, ktoré sa majú dostať do certifikátu.

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

Tieto kroky možno vykonať v ľubovoľnom poradí, ktoré je vyhovujúce pre CMA aj žiadateľov a ktoré nie je v rozpore s bezpečnosťou.

CA Disig implementujúca tento CP bude certifikovať inú CA (platí aj pre krížovú certifikáciu) len na základe autorizácie PMA.

Žiadosť CA o certifikát certifikačnej autority bude predložená PMA prostredníctvom kontaktu uvedeného v časti 1.4 a bude doplnená dokumentom CPS napísanom na základe materiálu Internet X.509 Public Key Infrastructure Certificate Policy and Certification Practices Framework (RFC3647)[6].

PMA ohodnotí prijateľnosť dodaného CPS. PMA môže požadovať prvotný audit o zhode, ktorý vykoná subjekt zvolený PMA, aby sa uistila, že CMA je pripravená implementovať všetky aspekty dodaného CPS ešte predtým, než PMA povolí CMA vydávať a spravovať certifikáty podľa tohto CP.

CA bude vydávať len certifikáty podľa tohto CP na základe písomnej autorizácie vydanej PMA a môže tak konať len v rámci obmedzení, ktoré PMA uložila.

Proces vydávania certifikátu pre podriadenú CA je podrobne popísaný v aktuálne platnom dokumente „Pravidlá na výkon certifikačných činností certifikačnej autority CA Disig Časť - Certifikačná autorita“.

4.1.1 Detailný postup na získanie osobného certifikátu (fyzická osoba, právnická osoba), SSL certifikátu a certifikát pre softvérový komponent

O osobný certifikát je možné požiadať len na základe elektronicky generovanej žiadosti. Žiadateľ o certifikát je povinný **na svojom počítači** pomocou vyhovujúceho prehliadača vygenerovať **novú** žiadosť o osobný certifikát prostredníctvom web stránky spoločnosti Disig (viď URL adresu v časti 0) a uložiť si ju na vhodné médium (HD, USB disk, disketa ap.).

Rovnaký postup platí aj pre žiadosť o certifikát na softvérový komponent.

Žiadosť o certifikát určený na podpisovanie a šifrovanie elektronickej pošty **musí byť zaslaná príslušnej RA** vopred elektronicky z e-mail adresy, ktorá je uvedená v žiadosti o certifikát v položke E-mail. E-mail adresy jednotlivých RA CA Disig sú k dispozícii na internetovej stránke spoločnosti Disig (pozri 1.4).

Pri žiadaní o SSL certifikát si zákazník pomocou svojho softvéru (typicky napr. Microsoft IIS alebo Apache/OpenSSL) vygeneruje **novú** žiadosť o SSL certifikát a túto si uloží na vhodné médium.

Žiadateľ o následný certifikát vytvorí žiadosť podľa postupu v kapitole 3.2.

- 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!
- Pri zadávaní hodnôt do položiek žiadosti o certifikát by mal 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.

Žiadosť o osobný certifikát vydávaný pre fyzickú osobu, ktorá je zamestnancom zmluvného partnera, je možné generovať aj iným spôsobom, ako prostredníctvom web stránky spoločnosti Disig napr. vlastný web portál zmluvného partnera ap. Tento spôsob je vopred dohodnutý so zmluvným partnerom a jednotlivý žiadatelia sú o spôsobe generovania a zasielania žiadosti informovaní ako zo strany zmluvného partnera, tak aj zo strany CA Disig.

4.1.2 Postup pri registrácii žiadateľa o certifikát na RA

1. Pracovník RA skontroluje úplnosť a správnosť údajov v prijatej žiadosti o certifikát. 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. 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 žiadosti o certifikát v položke E-mail.
2. Žiadateľ o certifikát musí na RA uspokojivým spôsobom preukázať všetky údaje, ktoré zadal do jednotlivých položiek žiadosti o certifikát.
3. RA musí overiť, či elektronicky zaslaná žiadosť o vydanie certifikátu daného žiadateľa bola zaslaná z rovnakej e-mail adresy, aká sa nachádza v žiadosti o vydanie certifikátu. V prípade zistených rozdielov môže odmietnuť vydanie

certifikátu. Toto sa nepoužije v prípade, že vydávaný certifikát neobsahuje rozšírenie „Secure Email (1.3.6.1.5.5.7.3.4)“.

4. V súvislosti s overovaním e-mailu, ktorý má byť použitý na podpisovanie elektronických správ (rozšírenie „Secure Email (1.3.6.1.5.5.7.3.4)“) vykoná pracovník RA overenie kontroly e-mailovej adresy nachádzajúcej sa v žiadosti o vydanie certifikátu, odpoveďou na e-mail, z ktorej bola žiadosť zaslaná. 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. V prípade, že overenie e-mail adresy prebehne neúspešne, CA Disig odmietne vydanie certifikátu. Overovanie e-mailovej adresy nie je potrebné v prípade, že je zaslaná žiadosť o následný certifikát elektronicky e-mailom, ktorý je podpísaný platným certifikátom 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.
5. 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.
6. Pracovník RA oboznámi žiadateľa o certifikát s textom „Zmluva o vydaní a používaní certifikátu a služieb CA Disig“. Súhlas žiadateľa s textom tejto zmluvy je podmienkou na vydanie certifikátu.
7. Pracovník RA vloží do informačného systému CA žiadosť o certifikát a ostatné požadované údaje. 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 musí v takom prípade podať novú žiadosť o certifikát.
8. V prípade žiadosti o následný certifikát sa postupuje podľa kapitoly 3.2.

4.1.3 Certifikáty pre interné účely zmluvného partnera

V prípadoch osobného certifikátu pre zmluvného partnera, osobného certifikátu pre doménového používateľa a certifikátu pre doménový radič, ktoré slúžia výhradne pre interné potreby zmluvného partnera, sú detailné postupy na získanie certifikátu týchto typov a postupy pri registrácii na RA pre daného zmluvného partnera, uvedené v príslušnom dokumente CPS alebo v interných dokumentoch zmluvného partnera.

4.1.4 Doručenie verejného kľúča žiadateľa o certifikát vydavateľovi certifikátu

Aby sa garantovala väzba overenej identity žiadateľa k verejnému kľúču na ktorý má byť vydaný certifikát, verejný kľúč (obsiahnutý v žiadostiach o certifikát) sa musí doručiť CA prostredníctvom RA. Doručiť sa môže buď osobne žiadateľom o certifikát (príp. splnomocnencom, ktorým sa žiadateľ nechá na RA zastupovať),

alebo na základe dohody s príslušnou RA sa môže zaslať aj elektronickou poštou. V prípade certifikátu, ktorý je určený na podpisovanie elektronickej pošty (rozšírenie „Secure Email (1.3.6.1.5.5.7.3.4)“) musí byť žiadosť zaslaná na príslušnú registračnú autoritu vopred elektronickým, aby mohlo byť vykonané overenie kontroly daného e-mail konta zo strany žiadateľa.

4.2 Vydanie certifikátu

CA Disig:

- nevytvorí certifikát, kým sa k spokojnosti nedokončia všetky verifikácie a prípadné zmeny, ak sú potrebné,
- 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.

4.2.1 Doručenie súkromného kľúča držiteľovi certifikátu

Súkromný kľúč si generuje sám žiadateľ o certifikát.

V prípade, že ako úložisko súkromného kľúča je určené SSCD zariadenie na základe zmluvy s držiteľom, potom sa SSCD musí doručiť držiteľovi spoľahlivým spôsobom, najlepšie osobne do rúk držiteľa prostredníctvom RA. V prípade doručenia SSCD iným spôsobom sa musia aktivačné dáta k SSCD (napr. heslo, PIN) doručiť držiteľovi oddelene od SSCD a to až po tom, ako držiteľ potvrdí prijatie SSCD. Zodpovednosť za uloženie a stav SSCD resp. modulu, až kým tento nebol odovzdaný jeho držiteľovi, má CMA.

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 (pozri 1.4),
- nahratie certifikátu priamo do Active Directory,
- pri použití SSCD RA môže nahrať dôveryhodné certifikáty na doručované SSCD,
- osobné prevzatie certifikátu CA Disig na RA.

RA na požiadanie poskytne strane spoliehajúcej sa na certifikáty alebo inému ľubovoľnému záujemcovi odtlačok (fingerprint, hash) certifikátu CA Disig a to konkrétne telefonicky, zabezpečeným mailom alebo osobne pri návšteve záujemcu na RA.

Konkrétna voľba spôsobu poskytnutia odtlačku (fingerprint, hash) závisí na dohode so záujemcom. Okrem toho bude CA Disig na Internete zverejňovať fingerprint certifikátu CA Disig prostredníctvom svojej web stránky.

Fingerprint (alebo hash) posielaný spolu s certifikátom nie je prijateľný ako autentizačný mechanizmus.

4.3 Prevzatie certifikátu

Certifikáty sa vytvárajú a vydávajú automatizovane a priebežne. Bezprostredne po vydaní certifikátu môže žiadateľ prevziať svoj certifikát. Po vydaný certifikátu podpíše pracovník RA so žiadateľom príslušnú dokumentáciu:

- Osobný certifikát, certifikát pre právnickú osobu, SSL certifikát, certifikát pre podpisovanie softvérových komponentov (komerčná RA):
  - Zmluva o vydaní a používaní certifikátu a služieb CA Disig
  - Potvrdenie o vydaní osobného certifikátu a jeho odovzdaní žiadateľovi o certifikát (v prípade osobného certifikátu)
- SSL certifikát (komerčná RA):
  - Zmluva o vydaní a používaní certifikátu a služieb CA Disig
  - Potvrdenie o vydaní certifikátu a jeho odovzdaní žiadateľovi o certifikát
- Osobný certifikát pre zmluvného partnera, doménového užívateľa, certifikát pre doménový radič
  - Potvrdenie o vydaní certifikátu a jeho odovzdaní žiadateľovi o certifikát
- Potvrdenia sa vyhotovujú v dvoch exemplároch – jeden originál je určený pre žiadateľa, jeden originál pre príslušnú RA.
- Žiadateľ o certifikát resp. splnomocnená osoba môže prevziať certifikát nasledovnými spôsobmi:
  - pracovník RA odovzdá certifikát žiadateľovi na podporovanom médiu (okrem prípadu, keď bola žiadosť vopred zaslaná mailom),
  - ihneď po vydaní certifikátu je držiteľovi mailom zaslaná linka na stiahnutie certifikátu z web stránky,
  - certifikát je možné prevziať prostredníctvom služby „Vyhľadávanie osobných certifikátov“ poskytovanej na web stránke CA Disig
  - iný postup – len na základe osobitnej zmluvy.
- V prípade podania žiadosti o následný certifikát elektronickou cestou, žiadateľovi bude certifikát doručený na e-mailovú adresu uvedenú v certifikáte.
- Po prevzatí certifikátu je zákazník povinný zaplatiť za poskytnutú službu v zmysle cenníka CA Disig vopred dohodnutým spôsobom.
- V prípade vydania následného certifikátu sa platba uskutočňuje na základe elektronicky doručenej faktúry, ak nie je v zmluve dohodnuté inak.

4.4 Zrušenie a suspendovanie certifikátu

4.4.1 Zrušenie certifikátu

4.4.1.1 Okolnosti zrušenia certifikátu

Certifikát sa musí 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 Disig dozvie o niektorej z vyššie uvedených okolností, daný certifikát sa zruší a dá sa na zoznam zrušených certifikátov (ďalej ako CRL).

Zrušené certifikáty sa budú vyskytovať na 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 o zrušenie svojho vlastného certifikátu a to aj bez udania dôvodu žiadosti o zrušenie certifikátu.

RA dá 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

V prípade splnenia podmienok autentifikácie žiadateľa o zrušenie certifikátu (kapitola 3.1.7 príp. 3.1.8), žiadosť o zrušenie certifikátu možno podať:

- Osobne na pobočke RA prostredníctvom formulára „Žiadosť o zrušenie certifikátu“ dostupnom na RA – pracovník RA môže od žiadateľa vyžiadať heslo na zrušenie certifikátu v prípade, ak žiadateľom o zrušenie certifikátu nie je držiteľ certifikátu, ale ním poverená osoba
- Prostredníctvom elektronickej pošty – zaslaním elektronickej poštovej správy, podpísanej súkromným kľúčom súvisiacim s certifikátom, o zrušenie ktorého sa žiada. Obsahom správy musí byť jednoznačná vôľa na zrušenie certifikátu vyjadrená vetou „Žiadam týmto o zrušenie môjho certifikátu so sériovým číslom XXXXXX“
- Prostredníctvom elektronickej pošty – zaslaním elektronickej poštovej správy (nemusí byť podpísaná). Obsahom správy musí byť jednoznačná vôľa na zrušenie certifikátu vyjadrená vetou „Žiadam týmto o zrušenie môjho certifikátu so sériovým číslom XXXXXX“. Pri takto zaslanej správe musí byť súčasťou mailu aj heslo na zrušenie certifikátu
- Prostredníctvom poštovej zásielky spolu so zadaním hesla na zrušenie certifikátu zaslanej na adresu príslušnej RA, ktorá vydala certifikát, o zrušenie ktorého sa žiada

- Telefonicky na telefónnom čísle patriacom príslušnej RA, ktorá vydala certifikát, ktorý sa má zrušiť. Telefónne číslo je zverejnené na webe CA Disig. Žiadateľ je povinný zadať heslo na zrušenie certifikátu.

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..

V prípade potreby poskytne RA žiadateľovi o zrušenie pomoc pri zistení čísla (Serial Number) predmetného certifikátu. 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).

V prípade, že sa zrušenie certifikátu vykonalo na základe súdneho rozhodnutia, pracovník RA musí k protokolu o zrušení priložiť fotokópiu súdneho rozhodnutia.

V prípade, že sa zrušenie certifikátu vykonalo na základe rozhodnutia pracovníka RA alebo CA Disig, pracovník RA musí k protokolu o zrušení certifikátu priložiť záznam, na základe ktorého sa zrušenie vykonalo.

Certifikát, ktorému uplynula platnosť, nie je možné zrušiť.

4.4.1.4 Čas na zrušenie certifikátu

Tento CP nestanovuje žiadny konkrétny čas na zrušenie certifikátu. CA Disig, po prevzatí náležitej žiadosti o zrušenie, bude rušiť certifikáty tak rýchlo ako je to len možné. CA Disig musí zrušiť certifikáty v rámci časových obmedzení popísaných v časti 4.4.3.1.

CA Disig automaticky informuje držiteľa certifikátu o zrušení jeho certifikátu, zaslaním e-mailu na e-mail adresu uvedenú v certifikáte, pričom uvedie informácie o dôvode zrušenia daného certifikátu.

4.4.2 Suspendovanie certifikátov

Suspendovanie certifikátov znamená dočasné pozastavenie ich platnosti.

CA Disig túto službu nevykonáva.

4.4.3 Zoznamy zrušených certifikátov

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 prevzatia žiadosti o zrušenie.
- zverejňuje okrem aktuálneho, najnovšieho CRL všetky vydané CRL, od začiatku svojej činnosti
- archivuje všetky CRL, ktoré vydala.

RA na požiadanie zašle aktuálne CRL prostredníctvom zabezpečeného mailu na dohodnutú email adresu čo najskôr.

4.4.3.2 Požiadavky na overovanie CRL

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.

Neoverenie certifikátu pomocou CRL je brané ako hrubé porušenie tohto CP.

4.4.4 Overenie aktuálneho stavu certifikátu

Overenie aktuálneho stavu certifikátu je možné vykonať manuálne prostredníctvom:

- Zoznamu vydaných certifikátov, ktorý je dostupný na adrese:
  - http://www.disig.sk/index.php?id=certsearch (SK verzia) resp.
  - http://www.disig.eu/index.php?id=certsearch&L=1 (EN verzia)
- Zoznamu zrušených certifikátov, ktorý je dostupný na adrese:
  - http://www.disig.sk/index.php?id=crl (SK verzia) resp.
  - http://www.disig.eu/index.php?id=crl&L=1 (EN verzia)

4.4.5 Iné použiteľné spôsoby oznamovania o zrušení certifikátu

RA odpovie telefonicky alebo emailom 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 CMA a tiež interakcie žiadateľov o certifikát a držiteľov certifikátov s CMA.

Záznamy môžu byť buď v elektronickej alebo v písomnej forme a môžu byť vytvárané buď automatizovane alebo manuálne.

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.

4.6 Archívne záznamy

Archivácia záznamov sa vykonáva 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.

Auditné záznamy sú uchovávané minimálne počas 7 rokov od ich vyhotovenia.

4.7 Zmena kľúča CA

CA Disig používa svoj podpisový (súkromný) kľúč pri vytváraní certifikátov používateľov. Strany spoliehajúce sa na certifikáty používajú certifikát CA Disig počas celej doby platnosti certifikátov. Z uvedeného dôvodu CA Disig nesmie vydávať užívateľom certifikáty, ktorých doba platnosti presahuje dobu platnosti certifikátov CA Disig (a verejných kľúčov CA) a doba platnosti certifikátu CA musí presahovať dobu platnosti všetkých vydaných užívateľských certifikátov.

Po vytvorení nového certifikátu CA Disig sa tento zverejní na webe CA Disig.

Celý proces musí prebehnúť bez negatívneho vplyvu na úroveň zabezpečenia.

4.8 Havarijný plán pre mimoriadne udalosti

V prípade kompromitácie kľúča CA Disig sa tento zruší.

Informácia o jeho zrušení sa musí publikovať okamžite najrýchlejším možným spôsobom. Následne sa musí vykonať nová inštalácia CA Disig.

CA Disig upozorní držiteľov certifikátov, ktoré boli podpísané jej zrušeným kľúčom, 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, fungovanie CA treba obnoviť 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, zruší sa certifikát CA Disig.

Následne sa kompletne zopakuje inštalácia CA Disig:

- obnovením jej vybavenia CA,
- vygenerovaním nových kľúčov CA,
- vytvorením nového certifikátu CA,
- vytvorením nových certifikátov RA,
- vydaním všetkých užívateľských certifikátov za použitia nového certifikátu CA Disig.

Poznámka: Náklady na vytvorenie nových certifikátov subjektom, ktoré boli dotknuté vytvorením nového certifikátu CA, 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.

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 znemožnenie opätovného použitia podpisových dát (súkromného kľúča) CA Disig. Podrobnosti sú popísane v ods. 4.9 CPS_CA CA Disig .

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

Vybavenie CA Disig má pozostávať len z vybavenia vyhradeného na funkcie certifikačnej autority, nemá slúžiť na žiadne účely, ktoré sa netýkajú tejto funkcie.

Neautorizované používanie vybavenia CA Disig je zakázané. Majú byť implementované opatrenia na fyzickú bezpečnosť, ktoré ochránia hardvér a softvér CMA pred neautorizovaným použitím. Kryptografické moduly CMA majú byť chránené pred krádežou, stratou a neautorizovaným použitím.

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

Vybavenie RA má byť chránené pred neautorizovaným prístupom, pokiaľ je nainštalovaný a aktivovaný kryptografický modul. RA má implementovať opatrenia na kontrolu fyzického prístupu, aby sa znížilo riziko zneužitia a falšovania. Tieto bezpečnostné mechanizmy majú byť primerané úrovni hrozby v prostredí vybavenia RA.

Odpojiteľné kryptografické moduly CMA sa majú pred uložením deaktivovať. Keď sa nepoužívajú, odpojiteľné kryptografické moduly a ľubovoľné aktivačné informácie používané na prístup alebo aktivovanie kryptografických modulov CMA alebo iného vybavenia CMA musia byť umiestnené v uzamknutých zariadeniach (bezpečnostné skrine, trezory a pod.). Aktivačné dáta sa majú zaznamenať a uložiť spôsobom primeraným bezpečnosti poskytnutej kryptografickému modulu a nemali by sa uložiť spolu s kryptografickým modulom.

Zariadenia a priestory, v ktorých je umiestnené vybavenie CA Disig, má byť postačujúco zásobované elektrickou energiou a klimatizované na vytvorenie spoľahlivého operačného prostredia.

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

Zálohy systému postačujúce na obnovu v prípade zlyhania systému sa majú vykonávať podľa periodického rozvrhu. Zálohy majú byť uložené na mieste s fyzickými a procedurálnymi opatreniami primeranými prevádzkovanej CA.

5.2 Procedurálne bezpečnostné opatrenia

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

Funkcie vykonávané týmito rolami formujú základ dôvery v celú PKI.

Aby sa zvýšila pravdepodobnosť, že tieto roly sa budú vykonávať úspešne, uplatňujú sa dva prístupy.

Prvým prístupom je zabezpečiť, aby osoba vykonávajúca rolu bola dôveryhodná a náležite vyškolená a poučená.

Druhým prístupom je podľa možnosti rozdeliť funkcie s rolami medzi niekoľko ľudí tak, aby si ľubovoľná škodlivá činnosť vyžadovala dohodu s inou osobou.

Primárne roly vyžadujúce si dôveryhodnosť definované týmto CP sú CA a RA.

Každá CA, ktorá funguje podľa tohto CP, je predmetom ustanovení tohto CP. Zodpovednosťou CA je zaručiť v prvom rade, že podľa tohto CP sa vykonávajú nasledovné funkcie:

- funkcie RA ako sú popísané v nasledujúcom odseku, ak sa neuplatní oddelená RA,
- vytváranie a zrušovanie certifikátov,
- zverejňovanie a doručovanie certifikátov a CRL,
- vykonávanie záloh,
- administratívne funkcie také ako záznam o kompromitácii a údržba údajovej základne,
- správa hardvérového kryptografického modulu.

Každá RA, ktorá funguje podľa tohto CP, je predmetom obmedzení tohto CP a CPS, podľa ktorého funguje.

Zodpovednosťou RA je v prvom rade:

- overovanie identity buď prostredníctvom osobného kontaktu, alebo prostredníctvom tretej strany, keď je to prípustné,
- zaznamenávanie informácií od žiadateľov o certifikát a overovanie ich správnosti,
- bezpečná komunikácia s CA,
- príjem a distribuovanie užívateľských certifikátov,
- komunikácia so žiadateľmi o certifikát a držiteľmi certifikátov.

Rola RA je veľmi závislá na implementácii PKI a lokálnych požiadavkách. Zodpovednosť RA a ich riadenie má byť podrobne popísané v dokumente CPS danej CA, ak táto CA používa RA.

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 RA 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 CP.

5.3 Personálne bezpečnostné opatrenia

Personálne bezpečnostné opatrenia sú zabezpečované internými mechanizmami subjektu – zriaďovateľa.

Personál pre ľubovoľnú CMA alebo inú rolu vyžadujúcu si dôveryhodnosť by sa mal vyberať na základe lojality, vernosti, dôveryhodnosti a integrity. Všetky osoby v CMA by mali byť občanmi Slovenskej republiky.

Všetok personál zahrnutý do prevádzky CMA má byť náležite vyškolený. Témy majú obsahovať fungovanie softvéru a hardvéru CMA, prevádzkové a bezpečnostné procedúry, ustanovenia tohto CP. Požadovaný špecifický výcvik bude závisieť na použitom vybavení a vybranom personáli.

6. Technické bezpečnostné opatrenia

6.1 Generovanie páru kľúčov a inštalácia

6.1.1 Generovanie páru kľúčov

Tento CP nevylučuje žiadny zdroj kľúčov, ktoré boli vygenerované v súlade s jeho ustanoveniami a lokálnymi bezpečnostnými požiadavkami. Predpokladá sa, že súkromný kľúč bude vygenerovaný subjektom, ktorý sa stane jeho držiteľom napr. žiadateľom o certifikát alebo RA a na SSCD zariadení (napr. počítač, čipová karta, HSM modul a pod.), ktoré je v čase generovania kľúča pod bezprostrednou kontrolou subjektu, ktorý sa stane držiteľom 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. Toto platí analogicky aj pre všetky RA.

6.1.2 Doručenie súkromného kľúča držiteľovi certifikátu

Ak súkromný kľúč generuje iná osoba ako jeho držiteľ, musí sa doručiť držiteľovi v SSCD, z ktorého sa nedá vybrať nezašifrovaný.

6.1.3 Dĺžky kľúčov

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

V prípade použitia algoritmu RSA stanovená minimálna dĺžka kľúča, na ktorý je vydávaný certifikát je 2 048 bitov.

V prípade použitia algoritmu RSA minimálna dĺžka kľúča certifikačnej autority je 2 048 bitov.

6.2 Ochrana súkromného kľúča

6.2.1 Súkromné kľúče CA

Súkromné kľúče používané CA Disig (koreňová CA, podriadené CA) sú uložený v špeciálnom zariadení – HSM module, ktorý je certifikovaný podľa štandardu FIPS 140-2 level 3.

Pri operáciách správy súkromných kľúčov CA Disig (napr. generovanie, zálohovanie, zničenie) bude vždy prítomný príslušný počet oprávnených osôb na princípe „k“ z „n“ určených oprávnených osôb. Manipulovať so súkromnými kľúčmi CA Disig môžu len na to oprávnené osoby.

Súkromné kľúče sa používa výlučne na podpisovanie certifikátov a CRL vydávaných CA Disig.

Pred ľubovoľnou operáciou so súkromnými kľúčmi CA sa bude musieť vykonať autentizáciu príslušného počtu oprávnených osôb na princípe „k“ z „n“ použitím kariet patriacich k HSM modulu, v ktorom je uložený súkromný kľúč CA.

Súkromné kľúče CA sú zálohované prostredníctvom softvéru na správu HSM modulu v zašifrovanej forme a tak, že k jeho dešifrovaniu je nevyhnutná autentizácia príslušného počtu oprávnených osôb na princípe „k“ z „n“ použitím administrátorských kariet patriacich k HSM modulu, v ktorom je príslušný súkromný kľúč CA uložený.

HSM modul uschovávajúci súkromný kľúč CA Disig spolu s počítačom na vytváranie certifikátov CA Disig sa bude nachádzať na režimovom pracovisku v miestnosti, ktorá má objektovú bezpečnosť minimálne na stupni „Dôverné“ v zmysle zákona 215/2004 Z. z. o ochrane utajovaných skutočností.

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

HSM modul spĺňa ochranu pred odchytávaním elektromagnetického vyžarovania.

Aby sa zabránilo odchytávaniu elektromagnetického vyžarovania vrátane zvuku mimo chráneného priestoru, budú použité špeciálne bezpečnostné zariadenia.

Miestnosť sa nachádza v budove, ktorá je nepretržite strážená strážnou službou a bezpečnostnou technikou.

6.2.2 Ostatné súkromné kľúče

Treba zabezpečiť, aby sa asymetrické súkromné kľúče nikdy nedostali v nezašifrovanej forme mimo modul, kde sú uložené.

Nikto nemá mať prístup k súkromnému podpisovému 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. Aktivačné dáta sa môžu držiteľom distribuovať osobne alebo poštou, ale len oddelene od kryptografického modulu, ktorý aktivujú.

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 zdieľané.

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

6.3 Manažment páru kľúčov

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

Súkromné kľúče uložené v SSCD zariadení sa spravidla nedajú archivovať mimo daného zariadenia.

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.

6.4 Počítačové bezpečnostné opatrenia

Počítačové vybavenie CA Disig je používané výhradne na účely výkonu činnosti certifikačnej autority. Bezpečnosť informačného systému je pravidelne podrobovaná kontrole na súlad s normami ISO 17799 a ISO 13335.

7. Profily certifikátov a zoznamov zrušených certifikátov

7.1 Profily certifikátov

Tento CP spravuje len certifikáty podľa štandardu X.509 verzie 3.

7.1.1 Certifikát koreňovej CA Disig

Algoritmy a dĺžky kľúčov uplatňované v certifikáte CA Disig:

Algoritmus podpisu (Signature Algorithm)
sha1RSA[1)] resp. **sha256RSA**
Verejný kľúč
RSA, dĺžka 2 048 bitov resp. 4 096 bitov
Doba platnosti certifikátu CA
maximálne 30 rokov

1) Algoritmus **SHA-1** sa bude používať len do doby pokiaľ nebude algoritmus **SHA-256** plne podporovaný prehliadačmi, ktoré sú využívané podstatnou časťou spoliehajúcich sa strán

Tabuľka č. 5: Obsah položiek v certifikáte koreňovej certifikačnej autority CA Disig

Skratka názvu	OID	Názov	Hodnota
C	2.5.4.6	countryName	**SK**
L	2.5.4.7	localityName	**Bratislava**
O	2.5.4.10	organizationName	**Disig a.s.**
CN	2.5.4.3	commonName	*v závislosti od typu CA*[1)]

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

Tabuľka č. 6: Použité rozšírenia (certificate extensions) v certifikáte koreňových CA Disig

Rozšírenie / OID Typ rozšírenia	Hodnota
basicConstraints / 2.5.29.19 kritické rozšírenie	CA:TRUE
keyUsage / 2.5.29.15 kritické rozšírenie	Certificate Signing, Off-line CRL Signing, CRL Signing (06)
subjectKeyIdentifier / 2.5.29.14 nekritické rozšírenie	*vygenerovaný systémom*
subjectAltName / 2.5.29.17* nekritické rozšírenie	RFC822 Name=caoperator@disig.sk URL=http://www.disig.sk/ca
crlDistributionPoints / 2.5.29.31[1)] nekritické rozšírenie	Distribution Point Name: Full Name: URL=http://www.disig.sk/ca/crl/ca_disig.crl Distribution Point Name: Full Name: URL=http://ca.disig.sk/ca/crl/ca_disig.crl
certificatePolicies / 2.5.29.32[1)] nekritické rozšírenie	Policy Identifier=1.3.158.35975946.0.0.0.1.1.1

[1)] Toto rozšírenie je len súčasťou koreňovej CA Disig vytvorenej dňa 22.6.2006. V koreňových CA Disig vytvorených po 1.7.2012 sa certificatePolicies rozšírenie nenachádza.

7.1.2 Podriadené certifikačné autority CA Disig

Algoritmy a dĺžky kľúčov uplatňované v certifikáte podriadenej CA Disig:

Algoritmus podpisu (Signature Algorithm)
sha1RSA[1)] resp. **sha256RSA**
Verejný kľúč
RSA, dĺžka 2 048 bitov
Doba platnosti certifikátu CA
maximálne 15 rokov

[1)] Algoritmus **SHA-1** sa bude používať len do doby pokiaľ nebude algoritmus **SHA-256** plne podporovaný prehliadačmi, ktoré sú využívané podstatnou časťou spoliehajúcich sa strán.

Tabuľka č. 7: Obsah položiek v certifikáte podriadenej certifikačnej autority CA Disig

Skratka názvu	OID	Názov	Hodnota
C	2.5.4.6	countryName	**SK**
L	2.5.4.7	localityName	**Bratislava**
O	2.5.4.10	organizationName	**Disig a.s.**
CN	2.5.4.3	commonName	*v závislosti od typu CA*[1)]

[1)] Súčasťou CN musí byť obchodné meno certifikačnej autority t. j. CA Disig doplnené podľa potreby o rozlišovacie meno typu podriadenej CA Disig napr. I1 Certification Service, R1I1 Certification Service ap.

Tabuľka č. 8: Použité rozšírenia (certificate extensions) v certifikáte podriadených CA Disig

Rozšírenie / OID Typ rozšírenia	Hodnota
authorityInfoAccess / 1.3.6.1.5.5.7.1.1	[1]Authority Info Access Access Method=On-line Certificate Status Protocol (1.3.6.1.5.5.7.48.1) Alternative Name: URL=http://ca-ocsp.disig.sk [2]Authority Info Access Access Method=Certification Authority Issuer (1.3.6.1.5.5.7.48.2) Alternative Name: URL=http://www.disig.sk/....[1)]
basicConstraints / 2.5.29.19 kritické rozšírenie	CA:TRUE Path Length Constraint=0
keyUsage / 2.5.29.15 kritické rozšírenie	Certificate Signing, Off-line CRL Signing, CRL Signing (06)
subjectKeyIdentifier / 2.5.29.14 nekritické rozšírenie	*vygenerovaný systémom*
subjectAltName / 2.5.29.17 nekritické rozšírenie	RFC822 Name=caoperator@disig.sk
crlDistributionPoints / 2.5.29.31 nekritické rozšírenie	[1]CRL Distribution Point Distribution Point Name: Full Name: URL=http://www.disig.sk/.....[2)] [2]CRL Distribution Point Distribution Point Name: Full Name: URL=http://ca.disig.sk/.....[2)]
certificatePolicies / 2.5.29.32 nekritické rozšírenie	Policy Identifier=2.5.29.32.0

1) Ďalšia cesta je špecifická pre vydávajúcu koreňovú CA napr. "../ca/cert/ca_disig.der"; "…/rootcar1/cert/rootcar1.der".

2) Ďalšia cesta k CRL je špecifická pre konkrétnu podriadenú CA napr. /subcar0i1/crl/subcar0i1.crl.

Podrobnosti o vydávaní podriadených CA sú popísané v dokumente „Pravidlá na výkon certifikačných činností certifikačnej autority CA Disig Časť - Certifikačná autorita".

7.1.3 Certifikáty vydávané CA Disig koncovým užívateľom

7.1.3.1 Osobný certifikát

Algoritmy a dĺžky kľúčov uplatňované v osobnom certifikáte vydávanom CA Disig:

Algoritmus podpisu (Signature Algorithm)
sha1RSA[1] resp. **sha256RSA**
Verejný kľúč
RSA, dĺžka je minimálne 2 048 bitov
Doba platnosti osobného certifikátu
Maximálne rok 36 mesiacov t. j. 3 roky (3*365 dní)

1) Algoritmus **SHA-1** sa bude používať len do doby pokiaľ nebude algoritmus **SHA-256** plne podporovaný prehliadačmi, ktoré sú využívané podstatnou časťou spoliehajúcich sa strán.

Tabuľka č. 9: Obsah štandardných položiek v osobnom certifikáte

Skratka názvu	OID	Názov	Hodnota
C	**2.5.4.6**	**countryName**	**SK** **Údaj je povinný!!!**
L	2.5.4.7	localityName	Názov lokality Údaj je nepovinný
O	2.5.4.10	organizationName	Názov organizácie Údaj je nepovinný
OU	2.5.4.11	organizationUnitName	Názov útvaru vo firme Údaj je nepovinný
CN	**2.5.4.3**	**commonName**	**Meno a priezvisko** **Údaj je povinný!!!**

Tabuľka č. 10: Základné rozšírenia (certificate extensions) v osobnom certifikáte

Rozšírenie / OID Typ rozšírenia	Hodnota
Subject Key Identifier / 2.5.29.14 nekritické rozšírenie	*Hodnota je automaticky vytváraná certifikačnou autoritou CA Disig*
Authority Key Identifier / 2.5.29.35 nekritické rozšírenie	KeyID= *Hodnota je automaticky pridávaná certifikačnou autoritou CA Disig*
Key Usage / 2.5.29.15 nekritické rozšírenie	Digital Signature, Non-Repudiation, Key Encipherment, Data Encipherment (f0)
CRL Distribution Points / 2.5.29.31 nekritické rozšírenie	[1]CRL Distribution Point Distribution Point Name: Full Name: URL=http://www.disig.sk/.....[1)] [2]CRL Distribution Point Distribution Point Name: Full Name: URL=http://ca.disig.sk/.....[1)]
Extended Key Usage / 2.5.29.37 nekritické rozšírenie	Client Authentication (1.3.6.1.5.5.7.3.2) Secure Email (1.3.6.1.5.5.7.3.4)
Certificate Policies / 2.5.29.32 nekritické rozšírenie	Policy Identifier=1.3.158.35975946.0.0.0.1.1
subjectAltName / 2.5.29.17 nekritické rozšírenie	E-mail adresa držiteľa certifikátu (rfc822Name)

1) Ďalšia cesta k CRL je špecifická pre konkrétnu podriadenú CA napr. /ca/crl/ca_disig.crl resp. /subcar0i1/crl/subcar0i1.crl ap.

7.1.3.2 Certifikát pre právnickú osobu

Algoritmy a dĺžky kľúčov uplatňované v certifikáte pre právnickú osobu sú rovnaké ako v prípade osobného certifikátu (pozri 7.1.3.1).

Tabuľka č. 11: Obsah základných položiek v certifikáte pre právnickú osobu

Skratka názvu	OID	Názov	Hodnota
C	**2.5.4.6**	**countryName**	**SK** **Údaj je povinný!!!**
L	2.5.4.7	localityName	Názov lokality Údaj je nepovinný
O	2.5.4.10	organizationName	Názov organizácie Údaj je nepovinný
OU	2.5.4.11	organizationUnitName	Názov útvaru vo firme Údaj je nepovinný
CN	**2.5.4.3**	**commonName**	Názov organizácia **Údaj je povinný!!!**

Tabuľka č. 12: Základné rozšírenia (certificate extensions) v certifikáte pre právnickú osobu

Rozšírenie / OID Typ rozšírenia	Hodnota
Subject Key Identifier / 2.5.29.14 nekritické rozšírenie	*Hodnota je automaticky vytváraná certifikačnou autoritou CA Disig*
Authority Key Identifier / 2.5.29.35 nekritické rozšírenie	KeyID= *Hodnota je automaticky pridávaná certifikačnou autoritou CA Disig*
Key Usage / 2.5.29.15 nekritické rozšírenie	Digital Signature, Non-Repudiation, Key Encipherment, Data Encipherment (f0)
CRL Distribution Points / 2.5.29.31 nekritické rozšírenie	[1]CRL Distribution Point Distribution Point Name: Full Name: URL=http://www.disig.sk/.....[1)] [2]CRL Distribution Point Distribution Point Name: Full Name: URL=http://ca.disig.sk/.....[1)]
Extended Key Usage / 2.5.29.37 nekritické rozšírenie	Client Authentication (1.3.6.1.5.5.7.3.2) Secure Email (1.3.6.1.5.5.7.3.4)[2)]
Certificate Policies / 2.5.29.32 nekritické rozšírenie	Policy Identifier=1.3.158.35975946.0.0.0.1.1
subjectAltName / 2.5.29.17 nekritické rozšírenie	E-mail adresa držiteľa certifikátu (rfc822Name)

[1)] Ďalšia cesta k CRL je špecifická pre konkrétnu podriadenú CA napr. /ca/crl/ca_disig.crl resp. /subcar0i1/crl/subcar0i1.crl ap.

[2] CA Disig môže vydávať certifikáty pre právnickú osobu, ktoré nebudú obsahovať toto rozšírenie.

7.1.3.3 SSL certifikát

Algoritmy a dĺžky kľúčov uplatňované v SSL certifikáte vydávanom CA Disig:

Algoritmus podpisu (Signature Algorithm)
sha1RSA[1] resp. sha256RSA
Verejný kľúč
RSA, dĺžka je minimálne 2 048 bitov
Doba platnosti SSL certifikátu
Maximálne 36 mesiacov t. j. 3 roky (3*365 dní)

[1] Algoritmus **SHA-1** sa bude používať len do doby pokiaľ nebude algoritmus **SHA-256** plne podporovaný prehliadačmi, ktoré sú využívané podstatnou časťou spoliehajúcich sa strán

Tabuľka č. 13: Obsah základných položiek v SSL certifikáte

Skratka názvu	OID	Názov	Hodnota
C	**2.5.4.6**	**countryName**	**SK** **Údaj je povinný!!!**
ST	2.5.4.8	stateOrProvinceName	Názov kraja Údaj je nepovinný
L*	2.5.4.7	localityName	Názov lokality Údaj je nepovinný[1]
O*	2.5.4.10	organizationName	Názov organizácie Údaj je nepovinný[1]
OU	2.5.4.11	organizationUnitName	Názov útvaru vo firme Údaj je nepovinný
CN	**2.5.4.3**	**commonName**	Názov komponentu **Údaj je povinný!!!**

[1] **Pokiaľ je v žiadosti vyplnená položka O (organizationName), tak musí byť vyplnená aj položka L (localityName). Pokiaľ položka O (organizationName) nie je vyplnená, tak nesmie byť vyplnená položka L (localityName).**

Tabuľka č. 14: Základné rozšírenia (certificate extensions) v SSL certifikáte

Rozšírenie / OID Typ rozšírenia	Hodnota
Subject Key Identifier / 2.5.29.14 nekritické rozšírenie	*Hodnota je automaticky vytváraná certifikačnou autoritou CA Disig*
Authority Key Identifier / 2.5.29.35 nekritické rozšírenie	KeyID= *Hodnota je automaticky pridávaná certifikačnou autoritou CA Disig*
Key Usage / 2.5.29.15 nekritické rozšírenie	Digital Signature, Key Encipherment, Data Encipherment (b0)
CRL Distribution Points / 2.5.29.31 nekritické rozšírenie	[1]CRL Distribution Point Distribution Point Name: Full Name: URL=http://www.disig.sk/.....[1)] [2]CRL Distribution Point Distribution Point Name: Full Name: URL=http://ca.disig.sk/.....[1)]
Extended Key Usage / 2.5.29.37 nekritické rozšírenie	Server Authentication (1.3.6.1.5.5.7.3.1), prípadne Client Authentication ((1.3.6.1.5.5.7.3.2)
Certificate Policies / 2.5.29.32 nekritické rozšírenie	[1]Certificate Policy: Policy Identifier=1.3.158.35975946.0.0.0.1.1 [2]Certificate Policy: Policy Identifier=2.23.140.1.2.1[2)] resp. 2.23.140.2.2[3)]
nsCertType / 2.16.840.1.113730.1.1 nekritické rozšírenie	SSL Server Authentication (40), prípadne SSL Client Authentication
subjectAltName[4)] / 2.5.29.17 nekritické rozšírenie	E-mail adresa držiteľa certifikátu (rfc822Name); DNS Name[4)]

[1)] - Ďalšia cesta k CRL je špecifická pre konkrétnu podriadenú CA napr. /subcar0i1/crl/subcar0i1.crl ap.

[2)] - Použije sa v prípade, že DN neobsahuje žiadnu z nasledovných položiek: organizationName, localityName, stateOrProvinceName

[3)] - Použije sa v prípade, že DN obsahuje všetky nasledovné položky: organizationName, localityName, stateOrProvinceName, countryName.

[4)] - V SSL certifikáte je možné zvoliť aj ďalšie alternatívne DNS mená, ktoré sa budú nachádzať v tomto rozšírení

7.1.3.4 Certifikát na podpisovanie softvérových komponentov

Algoritmy a dĺžky kľúčov uplatňované v certifikáte na podpisovanie softvérových komponentov (CodeSigning Certificate) vydávanom CA Disig:

Algoritmus podpisu (Signature Algorithm)
sha1RSA[1)] resp. **sha256RSA**
Verejný kľúč
RSA, dĺžka je minimálne 2 048 bitov
Doba platnosti certifikátu na podpisovanie softvérových komponentov
Maximálne 36 mesiacov t. j. 3 roky (3*365 dní)

1) Algoritmus **SHA-1** sa bude používať len do doby pokiaľ nebude algoritmus **SHA-256** plne podporovaný prehliadačmi, ktoré sú využívané podstatnou časťou spoliehajúcich sa strán

Tabuľka č. 15: Obsah položiek v certifikáte na podpisovanie softvérových komponentov

Skratka názvu	OID	Názov	Hodnota
C	**2.5.4.6**	**countryName**	**SK** **Údaj je povinný!!!**
L	2.5.4.7	localityName	Názov lokality Údaj je nepovinný
O	2.5.4.10	organizationName	Názov organizácie Údaj je nepovinný
OU	2.5.4.11	organizationUnitName	Názov útvaru v organizácii Údaj je nepovinný
CN	**2.5.4.3**	**commonName**	**Názov organizácie resp. meno a priezvisko držiteľa** **Údaj je povinný!!!**

Tabuľka č. 16: Základné rozšírenia (certificate extensions) v certifikáte na podpisovanie softvérových komponentov

Rozšírenie / OID Typ rozšírenia	Hodnota
Subject Key Identifier / 2.5.29.14 nekritické rozšírenie	*Hodnota je automaticky vytváraná certifikačnou autoritou CA Disig*
Authority Key Identifier / 2.5.29.35 nekritické rozšírenie	KeyID= *Hodnota je automaticky pridávaná certifikačnou autoritou CA Disig*
Key Usage / 2.5.29.15 nekritické rozšírenie	Digital Signature
CRL Distribution Points / 2.5.29.31	[1]CRL Distribution Point

nekritické rozšírenie	Distribution Point Name: Full Name: URL=http://www.disig.sk/.....[1)] [2]CRL Distribution Point Distribution Point Name: Full Name: URL=http://ca.disig.sk/.....[1)]
Extended Key Usage / 2.5.29.37 nekritické rozšírenie	Code Signing (1.3.6.1.5.5.7.3.3)
Certificate Policies / 2.5.29.32 nekritické rozšírenie	Policy Identifier=1.3.158.35975946.0.0.0.1.1
subjectAltName / 2.5.29.17 nekritické rozšírenie	E-mail adresa držiteľa certifikátu (rfc822Name) (2.5.29.17)

[1)] Ďalšia cesta k CRL je špecifická pre konkrétnu podriadenú CA napr. /ca/crl/ca_disig.crl resp. /subcar0i1/crl/subcar0i1.crl ap.

7.1.4 Ostatné ustanovenia

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

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

Použité základné rozšírenia (certificate extensions) u jednotlivých typov certifikátov môžu byť rozširované podľa aktuálnej potreby na základe rozhodnutia PMA. Takéto rozšírenie sa nepovažuje za zmenu profilu certifikátov tak ako sú definované v ods. 7.1.

Podľa potreby CA Disig môže byť všetky vydávané typy certifikátov (pozri bod 7.1.2 tohto CP) rozšírené aj o ďalšie položky v zmysle RFC 5280 časť 4.1.2.6.

7.2 Profil zoznamu zrušených certifikátov (CRL)

Profily zoznamov zrušených certifikátov CRL vydávané podľa tohto CP sú CRL verzie 2.

8. Administrácia špecifikácií

8.1 Procedúry na zmenu špecifikácie

PMA má právo posúdiť a prípadne revidovať tento CP. Chyby, požiadavky na aktualizáciu alebo navrhované zmeny tohto CP sa majú oznámiť kontaktu uvedenému v časti 1.4. Takáto komunikácia musí obsahovať popis zmeny, zdôvodnenie zmeny a kontaktné údaje osoby, ktorá zmenu požaduje.

Všetky zmeny CP motivované PMA majú byť dané na vedomie subjektom, ktorých sa týkajú (viď časť 8.2) v perióde aspoň jedného mesiaca.

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

CP a príslušné CPS musia byť revidované v pravidelnom intervale minimálne 1x ročne, bez ohľadu na to, či v danom časovom období sú navrhované ich zmeny, alebo nie. Za revíziu týchto dokumentov je zodpovedná Autorita pre správu CP (PMA) – pozri 1.3.1.1.

8.2 Publikačná a oznamovacia politika

PMA má publikovať informácie týkajúce sa tohto CP (vrátane tohto CP) prostredníctvom webu a v súlade s pravidlami organizácie týkajúcimi sa obsahu webu.

PMA bude udržiavať zoznam CA, ktoré implementujú tento CP. Navrhované zmeny CP a aktualizácie CP sa majú posielať týmto CA.

CMA má upovedomiť držiteľov certifikátov prostredníctvom mechanizmu popísaného v príslušnom CPS o každej zmene CP.

8.3 Procedúry schvaľovania CPS a externej politiky

PMA má urobiť rozhodnutie, či CPS je v súlade s týmto CP. Ešte pred začiatkom prevádzky má mať CMA schválený svoj CPS a musí spĺňať všetky jeho požiadavky. PMA má informovať o takýchto rozhodnutiach takým spôsobom, aby boli tieto informácie dobre prístupné stranám spoliehajúcim sa na certifikáty.

8.4 Úľavy

Za normálnych okolností PMA má rozhodnúť, či je odchýlka v praxi CMA podľa aktuálneho CP prijateľná alebo či má CMA požiadať PMA o zmenu CP. PMA môže povoliť úľavu od niektorej požiadavky CP, aby sa vyhovelo urgentným, nepredvídateľným prevádzkovým požiadavkám.

Keď sa povolí úľava, PMA má toto zverejniť pomocou webu prístupného stranám spoliehajúcim sa na certifikáty a má buď iniciovať trvalú zmenu do CP alebo má pre danú úľavu stanoviť konkrétny časový limit.