

D. Trust Certifikačná Autorita, a.s.



Certifikačný poriadok
pre vydávanie kvalifikovaných certifikátov

verzia 1.03

Obsah

| | | |
|-------|---|----|
| 1 | ÚVOD..... | 5 |
| 1.1 | Spolupráca DTCA a I.CA pri vydávaní kvalifikovaných certifikátov..... | 5 |
| 1.2 | Identifikácia dokumentu..... | 5 |
| 1.3 | Všeobecný prehľad..... | 6 |
| 1.3.1 | Normatívna opora a použitá dokumentácia | 6 |
| 1.3.2 | Definícia pojmov a skratiek..... | 7 |
| 1.4 | Prostredie a aplikovateľnosť..... | 9 |
| 1.4.1 | Nadväzujúce authority..... | 9 |
| 1.4.2 | Registračné authority..... | 9 |
| 1.4.3 | Klienti..... | 10 |
| 1.4.4 | Vydávané certifikáty | 10 |
| 1.4.5 | Použiteľnosť..... | 10 |
| 1.5 | Kontaktné informácie | 11 |
| 1.5.1 | Kontaktné adresy..... | 11 |
| 1.5.2 | Riadenie a špecifikácia CP | 11 |
| 1.5.3 | Osoba určujúca zhodu tohto CP so zodpovedajúcimi CPS | 11 |
| 2 | VŠEOBECNÉ USTANOVENIA | 11 |
| 2.1 | Povinnosti zúčastnených strán | 11 |
| 2.1.1 | Povinnosti DTCA..... | 12 |
| 2.1.2 | Povinnosti RA..... | 12 |
| 2.1.3 | Povinnosti subjektov | 12 |
| 2.1.4 | Povinnosti skladov kvalifikovaných certifikátov..... | 13 |
| 2.2 | Zodpovednosť a záruky..... | 14 |
| 2.2.1 | Zodpovednosť a záruky poskytované certifikačnou autoritou | 14 |
| 2.2.2 | Zodpovednosť RA..... | 14 |
| 2.3 | Náhrada škody | 14 |
| 2.4 | Výklad a výkonné mechanizmy | 15 |
| 2.5 | Poplatky..... | 15 |
| 2.6 | Zverejňovanie a uchovávanie informácií | 15 |
| 2.6.1 | Prístup k informáciám DTCA..... | 16 |
| 2.7 | Auditné činnosti | 16 |
| 2.8 | Dôvernosť | 17 |
| 2.8.1 | Chránené informácie | 17 |

| | | |
|-------|---|-----------|
| 2.8.2 | Sprístupnenie informácií o zrušení kvalifikovaných certifikátov | 17 |
| 2.8.3 | Sprístupnenie informácií orgánom činným v trestnom konaní a iným tretím stranám | 18 |
| 2.8.4 | Sprístupnenie informácií na základe občianskoprávneho konania | 18 |
| 2.8.5 | Sprístupnenie informácií na základe požiadavky držiteľa certifikátu..... | 18 |
| 2.8.6 | Ostatné okolnosti sprístupnenia informácií | 18 |
| 2.9 | Duševné vlastníctvo | 18 |
| 3 | IDENTIFIKÁCIA A AUTENTIZÁCIA | 19 |
| 3.1 | Prvotná registrácia..... | 19 |
| 3.1.1 | Typy podporovaných mien | 19 |
| 3.1.2 | Vecná správnosť mien | 19 |
| 3.1.3 | Pravidla interpretácie rôznych foriem mien | 23 |
| 3.1.4 | Jednoznačnosť mena | 24 |
| 3.1.5 | Preukazovanie totožnosti fyzickej osoby a splnomocnených osôb | 24 |
| 3.2 | Postup pri vydaní následného kvalifikovaného certifikátu..... | 25 |
| 3.3 | Žiadosť o zrušenie kvalifikovaného certifikátu | 25 |
| 3.3.1 | Osobné podanie žiadosti na RA | 26 |
| 3.3.2 | Podanie žiadosti elektronickou cestou | 26 |
| 3.3.3 | Podanie žiadosti listovou zásielkou | 27 |
| 3.3.4 | Okolnosti zrušenia certifikátu | 27 |
| 4 | OPERAČNÉ POŽIADAVKY | 28 |
| 4.1 | Vzor žiadosti o poskytnutie služby | 28 |
| 4.2 | Žiadosť o kvalifikovaný certifikát | 29 |
| 4.3 | Vydanie kvalifikovaného certifikátu..... | 30 |
| 4.4 | Akceptovanie kvalifikovaného certifikátu..... | 30 |
| 4.5 | Zrušenie kvalifikovaného certifikátu | 30 |
| 4.6 | Požiadavky na overovanie zoznamu zrušených kvalifikovaných certifikátov | 31 |
| 4.7 | Procedúry auditu vzhľadom k bezpečnosti..... | 31 |
| 4.8 | Výmena párových údajov CA..... | 32 |
| 4.9 | Odhalenie kompromitácií a nehôd | 32 |
| 4.10 | Ukončenie činnosti DTCA | 33 |
| 5 | FYZICKÉ, PROCEDURÁLNE A PERSONÁLNE BEZPEČNOSTNÉ MECHANIZMY 33 | |
| 6 | TECHNICKÁ BEZPEČNOSŤ | 34 |
| 6.1 | Generovanie párových údajov CA | 34 |
| 6.2 | Generovanie párových údajov klienta a inštalácia..... | 34 |

| | | |
|-----|--|----|
| 6.3 | Ochrana súkromného kľúča CA..... | 36 |
| 6.4 | Ďalšie požiadavky na správu párových údajov CA | 36 |
| 6.5 | Bezpečnosť počítačového vybavenia | 36 |
| 6.6 | Kontroly počítačovej bezpečnosti..... | 37 |
| 6.7 | Bezpečnostné kontroly v dobe životnosti..... | 37 |
| 6.8 | Kontroly bezpečnosti počítačovej siete..... | 37 |
| 6.9 | Kontroly bezpečnosti kryptografického modulu | 37 |
| 7 | CERTIFIKAČNÉ PROFILY A PROFILY QCRL..... | 38 |
| 7.1 | Profil kvalifikovaného certifikátu | 38 |
| 7.2 | Profil QCRL..... | 40 |
| 8 | RIADENIE ŠPECIFIKÁCIÍ..... | 40 |
| 8.1 | Procesy zmien špecifikácií | 40 |
| 8.2 | Politiky zverejňovania a ohlasovania..... | 40 |
| 8.3 | Proces schvaľovania základných materiálov | 41 |
| 8.4 | Platnosť a účinnosť | 41 |

1 ÚVOD

1.1 Spolupráca DTCA a I.CA pri vydávaní kvalifikovaných certifikátov

Spoločnosť D. Trust Certifikačná Autorita, a.s., (ďalej tiež „DTCA“) poskytuje akreditované certifikačné služby v spolupráci s českou spoločnosťou První certifikační autorita, a.s., (ďalej tiež „I.CA“), ktorá je akreditovaným poskytovateľom certifikačných služieb v Českej republike.

Správu kvalifikovaných certifikátov, t.j. vydávanie, overovanie platnosti, rušenie, archivovanie kvalifikovaných certifikátov a certifikačné činnosti s tým spojené, vykonáva pre DTCA na základe zmluvy uzatvorenej medzi DTCA a I.CA certifikačná autorita I.CA, pričom tieto certifikáty vydáva I.CA ako kvalifikované certifikáty v zmysle českého zákona č. 227/2000 Sb. o elektronickom podpise v platnom znení.

Identifikačné údaje I.CA:

První certifikační autorita, a.s.

Sídlo: Podvinný mlýn 2178/6, 190 00 Praha 9

IČ : 264 39 395

DIČ: 009 - 264 39 395

Registrácia: Obchodní rejstřík vedený Městským soudem v Praze,
oddíl B, vložka 7136

1.2 Identifikácia dokumentu

Názov: Certifikačný poriadok pre vydávanie kvalifikovaných certifikátov

Verzia: 1.03

Organizácia: D. Trust Certifikačná Autorita, a.s.

Schválil: predstavenstvo spoločnosti D. Trust Certifikačná Autorita, a.s.

Schválené dňa: 30.06.2005

OID dokumentu: 1.3.6.1.4.1.19725.1.2.2

Prehľad verzií dokumentu

| Verzia | Dátum vydania | Zhrnutie zmien |
|--------|---------------|--|
| 1.01 | 10.02.2004 | Prvá verzia dokumentu vytvorená pred podaním žiadosti o akreditáciu DTCA |
| 1.02 | 17.09.2004 | Zpracovanie pripomienok z procesu akreditácie |
| 1.03 | 30.06.2005 | Aktualizácia na základe vydania novej verzie |

| | | |
|--|--|--|
| | | certifikačnej politiky I.CA pre vydávanie kvalifikovaných certifikátov |
|--|--|--|

Tento dokument predstavuje certifikačný poriadok pre vydávanie kvalifikovaných certifikátov I.CA pre DTCA a je platný pre akreditovanú certifikačnú autoritu D. Trust Certifikačná Autorita, a.s.

Kvalifikované certifikáty vydávané podľa tohto certifikačného poriadku sú plne v súlade s kvalifikovanými certifikátmi vydávanými podľa „Certifikační politiky pro vydávání osobních kvalifikovaných certifikátů“ spoločnosti První certifikační autorita, a.s.

Tento Certifikačný poriadok sa zaoberá skutočnosťami, ktoré sa vzťahujú k DTCA, žiadateľom, držiteľom, používateľom a zmluvným partnerom, a ktoré súvisia s vydávaním kvalifikovaných certifikátov, s ich ďalšou správou, použitím, akceptovaním, zrušením a všetkými aspektmi súvisiacimi s nakladaním s párovými údajmi.

1.3 Všeobecný prehľad

1.3.1 Normatívna opora a použitá dokumentácia

Certifikačný poriadok pre vydávanie kvalifikovaných certifikátov (ďalej tiež „CP“) je vypracovaný v súlade s dokumentom „Certifikační politika pro vydávání osobních kvalifikovaných certifikátů“ I.CA.

CP zodpovedá požiadavkám stanoveným v RFC 3647, s prihliadnutím na doporučenia orgánov EÚ a na právo SR v danom odbore.

CP vychádza hlavne z nasledujúcich právnych predpisov, noriem, štandardov a doporučení:

- český zákon č. 227/2000 Sb. o elektronickém podpisu a o změně některých dalších zákonů, v platnom znení, s rešpektovaním slovenského zákona č. 215/2002 Z.z. o elektronickom podpise a o zmene a doplnení niektorých zákonov (ďalej tiež „ZoEP“) v platnom znení a vykonávacie vyhlášky č. 537 až 542/2002 Z.z.;
- RFC 3647 - Internet X.509 Public Key Infrastructure – Certificate Policy and Certification Practices Framework (ďalej tiež „RFC 3647“);
- RFC 3739 – Internet X.509 Public Key Infrastructure – Qualified Certificates Profile (ďalej tiež „RFC 3739“);
- RFC 3280 – Internet X.509 Public Key Infrastructure – Certificate and QCRL Profile;
- DRAFT REVISED ITU-T RECOMMENDATION X.509 | ISO/IEC 9594-8: „Information technology – open systems interconnection – the directory: public-key and attribute certificate frameworks“ (ďalej tiež „ISO/IEC 9594-8“);
- ETSI TS 101 456 V1.2.1 – Policy requirements for certification authorities issuing qualified certificates (ďalej tiež „ETSI TS 101 456“);
- ETSI TS 101 733 V1.5.1 – Electronic signature formats (ďalej tiež „ETSI TS 101 733“);
- ETSI TS 101 862 V1.3.1 – Qualified certificate profile (ďalej tiež „ETSI TS 101 862“);

- EESSI SG – V 1.44 Draft – Algorithms and Parameters for Secure Electronic Signatures.

1.3.2 Definícia pojmov a skratiek

Nižšie uvedené definície pojmov a skratiek sú platné pre tento dokument. Použité skratky majú alternatívny charakter, t.j. v texte môže byť použitý tak plný text, ako aj jeho skratka, pričom oba majú rovnakú obsahovú hodnotu.

CA – centrálné pracovisko certifikačnej autority;

certifikát – elektronický dokument vydaný certifikačnou autoritou, ktorý spája verejný kľúč s podpisujúcim subjektom a umožňuje overiť jeho totožnosť;

CP – Certifikačný poriadok (verejný dokument);

CPS (Certification Practice Statement) – Pravidlá na výkon certifikačných činností (neverejný dokument);

čas – svetový čas (UTC). Minimálnou časovou jednotkou pre účely tohto CP je jedna sekunda.

držiteľ certifikátu - klient, ktorý má párové údaje a ktorému DTCA na jeho verejný kľúč vydala kvalifikovaný certifikát;

DN – Distinguished Name – reťazce položky Subject certifikátu, naplnované dátami z žiadosti o certifikát, z ktorých niektoré sú overované DTCA podľa pravidiel uvedených v tomto CP;

Držiteľ certifikátu – fyzická osoba, ktorá požiadala o vydanie kvalifikovaného certifikátu a ktorej bol kvalifikovaný certifikát vydaný (ďalej tiež „držiteľ“);

DTCA – D. Trust Certifikačná Autorita, a.s., akreditovaná certifikačná autorita v zmysle zákona č. 215/2002 Z.z. o elektronickom podpise;

I.CA – První certifikační autorita, a.s., poskytovateľ certifikačných služieb podľa §2 písm. h), i), j) českého zákona č. 227/2000 Sb. o elektronickom podpise;

klient – fyzická alebo právnická osoba, ktorá uzavrela zmluvu o využívaní služieb DTCA s prevádzkovateľom jej služieb;

kvalifikovaný certifikát (QC) – elektronický dokument vydaný I.CA pre DTCA (na základe zmluvného zabezpečenia) v zmysle §7 ZoEP, ktorého vydanie, ďalšia správa, použitie, akceptácia, zrušenie a všetky aspekty súvisiace s nakladaním s párovými údajmi sa riadia týmto CP;

NBÚ – Národný bezpečnostný úrad Slovenskej republiky;

následný kvalifikovaný certifikát (následný QC) – kvalifikovaný certifikát, ktorý bol v súlade so zmluvou uzatvorenou medzi klientom a DTCA vydaný klientovi na základe novej žiadosti o vydanie certifikátu, podpísanej platným súkromným kľúčom súvisiacim s už vydaným QC, ku ktorému je vydávaný tento následný QC. Reťazce DN, ktoré sú overované DTCA, musia byť v pôvodne vydanom QC a následnom QC rovnaké, verejné kľúče v týchto certifikátoch musia byť rôzne Ostatné položky následného QC podliehajú aktuálnym pravidlám pre vydávanie kvalifikovaných certifikátov;

OID (Object Identifier) – číselná identifikácia objektu v rámci jednotnej klasifikácie objektov podľa ISO/ITU;

párové údaje – údaje pre vytváranie elektronického podpisu spolu so zodpovedajúcimi údajmi pre overovanie elektronického podpisu;

podpisovateľ – fyzická osoba, ktorá je držiteľom prostriedku na vytváranie elektronických podpisov a ktorá jedná v svojom mene alebo v mene inej fyzickej alebo právnickej osoby;

používateľ – subjekt spoliehajúci sa pri svojej činnosti na kvalifikované certifikáty DTCA;

QCRL (Qualified certificate revocation list) – zoznam kvalifikovaných certifikátov, ktoré boli zrušené;

RA – registračná autorita DTCA certifikačnej autority I.CA – súhrnný názov pre VSRA, VMRA, ZSRA. Používa sa v prípadoch, keď nie je podstatný majiteľ registračnej autority, ani jej forma;

subjekt – fyzická osoba, právnická osoba alebo softwarový modul s nepopierateľnou zodpovednosťou konkrétnej fyzickej osoby;

súkromný kľúč – jedinečné údaje na vytváranie elektronického podpisu;

verejný kľúč – jedinečné údaje na overovanie elektronického podpisu;

Status kvalifikovaného certifikátu – stav, v ktorom sa QC nachádza, t.j. platný, vypršaná platnosť, zrušený, zablokovaný.

VSRA – Vlastná stacionárna registračná autorita DTCA certifikačnej autority I.CA;

VMRA – Vlastná mobilná registračná autorita DTCA certifikačnej autority I.CA;

zablokovanie – stav, v ktorom sa QC nachádza od doby, kedy DTCA obdržala požiadavku na jeho zrušenie, do doby zaradenia tohto QC do QCRL. Certifikát je počas doby zablokovania stále platný;

zmluvný partner – subjekt, ktorý zabezpečuje na základe písomnej zmluvy pre DTCA certifikačné služby alebo ich časti. Najčastejšie ide o zmluvné registračné autority;

ZoEP – český zákon č. 227/2000 Sb. o elektronickom podpise a o zmene niektorých ďalších zákonov, v platnom znení, s rešpektovaním slovenského zákona č. 215/2002 Z.z. o elektronickom podpise a o zmene a doplnení niektorých zákonov, a naväzujúcich vyhlášok;

ZRA – Zmluvná registračná autorita Certifikačnej autority DTCA. Plní obdobné funkcie ako VSRA alebo VMRA na základe písomnej zmluvy medzi DTCA a prevádzkovateľom ZRA;

zrušený QC – QC, u ktorého bola predčasne ukončená platnosť bez možnosti obnovenia tejto platnosti.

žiadateľ – fyzická osoba alebo oprávnený konateľ právnickej osoby podávajúci na RA žiadosť o službu (certifikát);

žiadosť o službu (žiadosť) – formálny dokument žiadosti o niektorú zo služieb poskytovaných DTCA, napr. žiadosť o vydanie kvalifikovaného certifikátu, žiadosť o zrušenie kvalifikovaného certifikátu a pod.;

žiadosť o vydanie kvalifikovaného certifikátu – formálny, štandardný dokument elektronickej žiadosti o certifikát podľa prípustných noriem a smerníc definovaných v tomto Certifikačnom poriadku DTCA;

1.4 Prostredie a aplikovateľnosť

1.4.1 Nadväzujúce authority

I.CA prevádzkuje koreňovú certifikačnú autoritu vydávajúcu kvalifikované certifikáty.

I.CA prostredníctvom DTCA nezriaďuje, ani nepodporuje podriadené certifikačné authority vydávajúce kvalifikované certifikáty.

Zoznam podriadených autorít, poskytujúcich zvláštne služby, môže byť upravený v závislosti na službách poskytovaných I.CA prostredníctvom DTCA.

1.4.2 Registračné authority

Poskytovanie služieb DTCA sa realizuje prostredníctvom registračných autorít. RA sú buď vlastné alebo RA zmluvných partnerov. DTCA podporuje len nižšie uvedené typy registračných autorít.

Vlastné stacionárne registračné authority (VSRA)

- a) VSRA sú základnými decentralizovanými zložkami výkonného aparátu DTCA.
- b) VSRA je určená hlavne na to, aby plnila funkciu podateľne.
- c) VSRA prijíma žiadosti o služby podľa certifikačného poriadku DTCA a plní všetky ďalšie úlohy DTCA vyplývajúce z jej vzťahu ku klientom, hlavne prijíma žiadosti o vydanie kvalifikovaných certifikátov, sprostredkováva odovzdanie certifikátov a QCRL, poskytuje potrebné informácie klientom, vybavuje ich reklamácie a pod.
- d) VSRA je oprávnená z naliehavých prevádzkových alebo technických dôvodov pozastaviť úplne alebo čiastočne výkon svojej činnosti. Toto opatrenie je povinná neodkladne hlásiť generálnemu riaditeľovi DTCA, ktorý ho potvrdí, zruší alebo zmení.
- e) VSRA je splnomocnená v mene DTCA uzatvárať s klientmi DTCA zmluvy o vydaní a používaní kvalifikovaných certifikátov DTCA.
- f) VSRA zabezpečuje spoplatňovanie služieb DTCA, pokiaľ nie je stanovené zmluvou inak.

Vlastná mobilná registračná autorita (VMRA)

- a) VMRA sú zvláštnymi decentralizovanými mobilnými zložkami výkonného aparátu DTCA.
- b) VMRA je určená hlavne na to, aby plnila funkciu podateľne v mieste mimo umiestnenia VSRA, spravidla na základe individuálnej zmluvy medzi klientom a DTCA.
- c) VMRA prijíma žiadosti o služby podľa certifikačného poriadku DTCA a plní ďalšie úlohy DTCA vyplývajúce zo vzťahu ku klientom, hlavne prijíma žiadosti o vydanie kvalifikovaných certifikátov, sprostredkováva odovzdanie certifikátov a QCRL, poskytuje potrebné informácie klientom, vybavuje ich reklamácie a pod.

- d) VMRA je splnomocnená v mene DTCA uzatvárať s klientmi DTCA zmluvy o vydaní a používaní kvalifikovaných certifikátov DTCA.
- e) VMRA zabezpečuje spoplatňovanie služieb DTCA, pokiaľ nie je stanovené zmluvou inak.
- f) VMRA je oprávnená z naliehavých prevádzkových alebo technických dôvodov pozastaviť úplne alebo sčasti výkon svojej činnosti. Toto opatrenie je povinná neodkladne hlásiť generálnemu riaditeľovi DTCA, ktorý ho potvrdí, zruší alebo zmení.

Zmluvná registračná autorita (ZRA)

Plní v mene DTCA obdobné funkcie ako VMRA alebo VSRA na základe písomnej zmluvy medzi DTCA a prevádzkovateľom ZRA.

1.4.3 Klienti

Kvalifikované certifikáty DTCA sú komerčnou službou a sú prístupné každému, kto sa zmluvne zaviazal podľa tohto Certifikačného poriadku.

DTCA požaduje minimálny vek 15 rokov pre osobu, ktorá žiada o vydanie kvalifikovaného certifikátu. Žiadatelia vo veku od 15 do 18 rokov musia žiadať prostredníctvom ich zákonného zástupcu.

V prípade fyzickej osoby môže byť klientom iba osoba, ktorá je spôsobilá k právnym úkonom podľa príslušnej právnej normy. Pokiaľ žiadateľ nepožaduje služby priamo pre seba, ale pre inú osobu, musí mať oprávnenie túto osobu zastupovať.

1.4.4 Vydávané certifikáty

Týmto Certifikačným poriadkom sa riadi vydávanie **kvalifikovaných certifikátov** určených ako osobné certifikáty pre overovanie elektronického podpisu (napr. v rámci elektronickej pošty). Tieto kvalifikované certifikáty sú vydávané v súlade s nižšie uvedenými pravidlami.

Iné certifikáty podliehajúce tomuto Certifikačnému poriadku I.CA prostredníctvom DTCA nevydáva, ani neautorizuje (nepodpisuje).

1.4.5 Použitelnosť

Kvalifikované certifikáty môžu byť používané v aplikáciách pre nasledovné účely:

- pre overovanie elektronických podpisov,
- pre overovanie zaručených elektronických podpisov,
- zaistenie neodmietnuteľnosti zodpovednosti.

Kvalifikované certifikáty je možné používať v súlade so ZoEP..

1.5 Kontaktné informácie

1.5.1 Kontaktné adresy

Základné adresy, na ktorých je možné nájsť informácie o DTCA a jej CP (ďalej tiež **informačné adresy**) sú:

- a) sídlo spoločnosti;
- b) internetová adresa <http://www.dtca.sk> (ďalej tiež **internetová informačná adresa**);
- c) sídla registračných autorít.

Kontaktné adresy, ktoré slúžia pre kontakt klienta s DTCA, sú :

- a) sídlo registračnej autority, ktorá zmluvný vzťah klienta s DTCA sprostredkovala;
- b) adresa elektronickej pošty info@dtca.sk

Vyššie uvedené kontaktné a informačné adresy je povinná DTCA a jej zmluvní partneri zverejniť na svojich pracoviskách. Pracovníci DTCA a zmluvných partnerov sú taktiež povinní tieto informácie na požiadanie poskytnúť všetkým používateľom.

V prípade, že dôjde ku zmene kontaktných údajov, sú DTCA a jej zmluvní partneri povinní túto skutočnosť zverejniť prostredníctvom príslušných informačných adries.

1.5.2 Riadenie a špecifikácia CP

Použitie kvalifikovaných certifikátov vydávaných I.CA prostredníctvom DTCA sa riadi týmto Certifikačným poriadkom. Tento Certifikačný poriadok sa zverejňuje na internetových stránkach DTCA a je k dispozícii v tlačenej podobe na RA. Všetky otázky týkajúce sa výkladu CP je nutné smerovať na adresu elektronickej pošty, ktorá slúži pre kontakt klienta s DTCA.

1.5.3 Osoba určujúca zhodu tohto CP so zodpovedajúcimi CPS

Vedenie DTCA určuje osobu, ktorá je oprávnená meniť ustanovenia tohto Certifikačného poriadku a určuje zhodu Certifikačného poriadku a Pravidiel pre výkon certifikačných činností.

2 VŠEOBECNÉ USTANOVENIA

2.1 Povinnosti zúčastnených strán

Subjektami, ktoré podliehajú tomuto CP sú certifikačná autorita I.CA a DTCA. I.CA nezriaďuje ani nepodporuje podriadené certifikačné autority (viď. článok 1.4).

Všetky subjekty, ktoré pri svojej činnosti používajú alebo využívajú kvalifikované certifikáty, prípadne poskytujú, sprostredkovávajú, používajú alebo využívajú služby DTCA spojené so správou kvalifikovaných certifikátov, sú povinné dodržiavať právne normy platné v SR a tento Certifikačný poriadok.

2.1.1 Povinnosti DTCA

DTCA je povinná dodržiavať príslušné ustanovenia právnych noriem, ktoré upravujú oblasť poskytovania certifikačných služieb alebo obchodnú činnosť s týmto spojenú. Ďalej sa DTCA zaväzuje riadiť sa vlastnými normatívnymi dokumentmi. DTCA je povinná dohliadať na dodržiavanie zmluvných podmienok a ostatných predpisov upravujúcich činnosť jej zmluvných partnerov.

DTCA je povinná zaistiť, aby sa každý mohol uistiť o jej identite a musí zaistiť dostupnosť kvalifikovaného certifikátu akreditovanej certifikačnej autority DTCA.

Vzťah medzi DTCA ako poskytovateľom certifikačných služieb a jej klientmi je striktné daný zmluvou. DTCA v žiadnom prípade nevystupuje ako splnomocnenec alebo iný zástupca klientov. To isté platí aj pre zmluvných partnerov DTCA.

2.1.2 Povinnosti RA

Registračné authority sú povinné riadiť sa dokumentmi, normami a smernicami, ktoré vydáva DTCA, a ktoré upravujú ich činnosť (Certifikačný poriadok, smernice pre pracovníkov RA a pod.).

2.1.3 Povinnosti subjektov

2.1.3.1 Povinnosti držiteľov kvalifikovaných certifikátov

Držiteľia kvalifikovaných certifikátov sú povinní :

- bez zbytočného odkladu podávať presné, pravdivé a úplné informácie DTCA vzťahujúce sa ku kvalifikovanému certifikátu;
- dodržiavať všetky ustanovenia príslušnej zmluvy o vydaní a používaní QC.

2.1.3.2 Povinnosti podpisovateľov

Podpisovateľ je povinný :

- používať kvalifikované certifikáty výhradne v súlade s týmto Certifikačným poriadkom;
- dodržiavať všetky ustanovenia tohto Certifikačného poriadku;
- dodržiavať všetky ustanovenia príslušnej zmluvy o vydaní a používaní QC;
- dodržiavať príslušné ustanovenia ZoEP.

2.1.3.3 Povinnosti používateľov kvalifikovaných certifikátov

Používatelia kvalifikovaných certifikátov sú všetky subjekty, ktoré sa pri svojej činnosti spoliehajú na kvalifikované certifikáty. Používatelia sú povinní používať kvalifikované certifikáty v súlade s týmto Certifikačným poriadkom a s príslušnými právnymi normami (napr. ZoEP), hlavne kontrolovať platnosť kvalifikovaného certifikátu, predovšetkým:

- časové údaje o platnosti,
- podpis kvalifikovaného certifikátu certifikačnou autoritou,
- výskyt kvalifikovaného certifikátu na zozname zrušených kvalifikovaných certifikátov,
- dôveryhodnosť a platnosť príslušného kvalifikovaného certifikátu akreditovanej certifikačnej autority.

2.1.4 Povinnosti skladov kvalifikovaných certifikátov

DTCA za účelom poskytovania akreditovaných certifikačných služieb využíva sklady kvalifikovaných certifikátov, ktoré zriaďuje I.CA. DTCA prostredníctvom I.CA zverejňuje nasledujúce informácie o kvalifikovaných certifikátoch :

- informácie o vydaných kvalifikovaných certifikátoch vrátane odkazov, na ktorých je možné požadovaný kvalifikovaný certifikát získať. Priamo sa zverejňujú nasledovné informácie (ostatné informácie je možné získať priamo zo samotného certifikátu)
 - sériové číslo kvalifikovaného certifikátu;
 - obsah atribútu Všeobecné meno (Common name, vid' článok 3.1.2.1), prípadne len jeho prvých 32 znakov, ak je dlhší;
 - časové údaje o platnosti (začiatok a koniec platnosti);
 - odkazy na miesto, kde je možné získať kvalifikované certifikáty v rôznych formátoch.
- informácie o kvalifikovaných certifikátoch, ktoré boli zrušené, vrátane odkazov, na ktorých je možné získať aktuálne alebo archívne zoznamy zrušených kvalifikovaných certifikátov. Priamo sa zverejňujú nasledovné informácie (ostatné informácie je možné získať zo samotného QCRL):
 - dátum vydania QCRL;
 - číslo QCRL;
 - odkazy na miesto, kde je možné získať QCRL v určených formátoch (DER, PEM, TXT).

I.CA aktualizuje zoznam QC pri každom vydaní nového kvalifikovaného certifikátu. Odkazy, na ktorých je možné informácie o vydaných QC a požadované kvalifikované certifikáty získať, zverejňuje DTCA na svojej internetovej kontaktnej adrese.

I.CA postupne v čase aktualizuje QCRL. Pre tento účel I.CA vydáva aktuálny zoznam zrušených certifikátov tak, aby interval medzi prijatím žiadosti o zrušenie kvalifikovaného certifikátu a vydaním QCRL, na ktorom je tento certifikát po prvýkrát zverejnený, nepresiahol 12 hodín. Táto základná povinnosť je realizovaná periodickým vydávaním QCRL trikrát denne. Vydávanie QCRL je nepretržité – 7 dní v týždni. Internetové adresy, na ktorých je možné získať QCRL vzdialeným prístupom sú uvedené na internetovej informačnej adrese DTCA a sú rovnako uvedené v každom QC. DTCA garantuje funkčnosť najmenej jedného distribučného bodu, na ktorom možno vzdialeným prístupom získať platné QCRL.

2.2 Zodpovednosť a záruky

2.2.1 Zodpovednosť a záruky poskytované certifikačnou autoritou

I.CA ručí za to, že použije vlastné súkromné kľúče príslušné svojim kvalifikovaným certifikátom len pre podpisovanie ňou vydaných kvalifikovaných certifikátov a zoznamov zrušených kvalifikovaných certifikátov.

I.CA poskytuje záruky na jedinečnosť sériového čísla ňou vydaných kvalifikovaných certifikátov.

DTCA ručí za na zrušenie kvalifikovaného certifikátu, za predpokladu, že žiadosť o zrušenie kvalifikovaného certifikátu bola podaná spôsobom uvedeným v tomto Certifikačnom poriadku.

Všetky záruky a z nich plynúce plnenia je možné uznať len za predpokladu, že klient neporušil povinnosti vyplývajúce mu zo zmluvy s DTCA a z tohto Certifikačného poriadku.

Klient uplatňuje záruku vždy u RA, ktorá ho zaregistrovala.

Pokiaľ zmluvný partner nie je schopný vybaviť záručné nároky vo svojej právomoci, postúpi ich na vybavenie DTCA a o tejto skutočnosti vyrozumie klienta.

Na používanie certifikátu, ktorý DTCA nevydala, sa záruky nevzťahujú.

I.CA prehlasuje, že má k dispozícii dostatočné finančné zdroje alebo iné finančné zabezpečenie na prevádzku v súlade s požiadavkami uvedenými v ZoEP a s ohľadom na riziko zodpovednosti za škodu.

Platí vždy limit záruky, ktorý bol zmluvne dojednaný v písomnej forme. Ak by výška nárokovej straty presahovala dojednaný limit, poskytne DTCA plnenie maximálne do výšky limitu. Ak bolo zistené porušenie povinnosti klienta majúce súvis s uvádzanou škodou, nebude záručné plnenie poskytnuté. Táto skutočnosť musí byť klientovi oznámená a zaprotokolovaná.

2.2.2 Zodpovednosť RA

RA nesie zodpovednosť za správne vybavenie žiadostí o poskytovanie certifikačných služieb. RA nevybaví kladne žiadosť, pokiaľ klient hodnoverným spôsobom nepreukázal svoju totožnosť, odmietol poskytnúť potrebné údaje alebo odmietol podpísať príslušné dokumenty. Postup preukazovania totožnosti je popísaný v tomto Certifikačnom poriadku.

RA ďalej zodpovedá za včasné odovzdanie oprávnených žiadostí o zrušenie certifikátov na ich vybavenie na pracovisko CA.

RA rovnako zodpovedá za vysporiadanie pripomienok a sťažností klientov.

2.3 Náhrada škody

V prípade, že DTCA vznikne akákoľvek škoda, v priamej či nepriamej súvislosti s konaním držiteľov alebo používateľov kvalifikovaných certifikátov, DTCA si vyhradzuje právo podniknúť adekvátne opatrenia, napríklad zrušiť držiteľovi jeho QC.

2.4 Výklad a výkonné mechanizmy

Tento Certifikačný poriadok, jeho výklad a aplikácia sa riadia platným právnym poriadkom Slovenskej republiky.

V prípade, že klient alebo zmluvný partner nesúhlasí s predloženým výkladom, môže sa obrátiť na vyššiu inštanciu. Jednotlivé stupne vo všeobecnosti tvoria :

- zodpovedný pracovník RA;
- zodpovedný pracovník DTCA (nutné písomné podanie);
- vedenie DTCA (nutné písomné podanie).

Uvedený postup dáva nesúhlasiacej strane možnosť presadzovať svoj názor rýchlejším spôsobom, než je súdna cesta.

2.5 Poplatky

Poplatky za vydanie prvého alebo následného kvalifikovaného certifikátu sú uvedené v aktuálnom cenníku služieb DTCA. Aktuálny cenník je k dispozícii na:

- registračných autoritách DTCA;
- príslušných internetových stránkach DTCA, zahrnutých medzi informačné adresy.

DTCA si vyhradzuje právo na zmenu výšky poplatku za vydanie QC a následného QC.

Prístup ku kvalifikovaným certifikátom elektronickou cestou (prostredníctvom podporovaných protokolov, viď článok 2.6.1) DTCA nespoplatňuje. Poplatok za odovzdanie QC (s výnimkou prvotného odovzdania certifikátu, viď článok 4.2) prostredníctvom elektronického média je stanovený takto:

- dohodnutý poplatok podľa počtu požadovaných QC + cena média (podľa aktuálneho cenníku príslušnej RA).

Uvedené záznamy sa ukladajú výhradne na vlastné média RA. Z bezpečnostných dôvodov je prísne zakázané tieto záznamy nahrávať na média prinesené klientmi.

Zrušenie QC je bezplatné.

Certifikačný poriadok v listinnej forme je k dispozícii na registračných autoritách za poplatok uvedený v aktuálnom cenníku DTCA.

Stiahnutie aktuálneho QCRL z internetovej stránky alebo prostredníctvom protokolu FTP je bezplatné. V prípade požiadavky je možné dohodnúť poplatok za zasielanie aktuálneho zoznamu zrušených kvalifikovaných certifikátov elektronickou poštou.

Poplatky za iné služby sú stanovené zmluvne.

2.6 Zverejňovanie a uchovávanie informácií

DTCA umožňuje trvalý vzdialený prístup k tomuto CP na svojich internetových informačných adresách. Tento CP je možné získať aj prostredníctvom registračných autorít a je k dispozícii v elektronickej forme vo formáte PDF.

Na internetových informačných adresách sú uvedené presné podmienky pre používanie kvalifikovaných certifikátov, vrátane obmedzení pri ich používaní a reklamačných podmienok.

DTCA uverejňuje svoje vlastné kvalifikované certifikáty akreditovanej certifikačnej autority tak, aby boli k dispozícii všetkým používateľom a to najmenej dvoma nezávislými kanálmi. DTCA tieto kvalifikované certifikáty zverejňuje na svojich internetových stránkach bezodkladne po ich obdržaní od NBÚ. DTCA je taktiež povinná bezpečnou cestou odovzdať tieto certifikáty registračným autoritám a to bezodkladne po ich obdržaní od NBÚ. DTCA alternatívne zabezpečuje dostupnosť svojich kvalifikovaných certifikátov ich distribúciou na záznamových médiách, ktoré sú k dispozícii na všetkých RA. Kvalifikované certifikáty akreditovaných certifikačných autorít vydáva NBÚ, ktorý ich zároveň v zmysle zákona zverejňuje.

Zrušenie vlastných kvalifikovaných certifikátov je DTCA povinná bezodkladne oznámiť prostredníctvom svojich internetových stránok (ak nehrozí nebezpečenstvo oneskorenia, vid' článok 4.8), najneskôr však do 6 hodín od okamihu ich zrušenia.

2.6.1 Prístup k informáciám DTCA

Protokoly povolené pre prístup k informáciám o CP sú :

- HTTP.

Protokoly povolené pre prístup k informáciám o vydaných kvalifikovaných certifikátoch sú :

- HTTP;
- HTTPS.

Protokoly povolené pre prístup k informáciám o zrušených kvalifikovaných certifikátoch sú :

- HTTP;
- HTTPS.

Iné protokoly nie sú povolené. I.CA prostredníctvom DTCA môže bez udania dôvodu prístup prostredníctvom niektorých z vyššie uvedených protokolov zrušiť alebo pozastaviť, alebo môže rozšíriť prístup o ďalšie protokoly, pričom je povinná dodržať ustanovenia ZoEP. Tieto zmeny je DTCA povinná zverejniť prostredníctvom svojich informačných adries. Podrobnejšie informácie o možnostiach a príslušných parametroch uvedených protokolov zverejňuje DTCA tamtiež.

2.7 Auditné činnosti

Audit sa v DTCA alebo v jej podriadených subjektoch vykonáva na základe rozhodnutia DTCA alebo príslušného štátneho orgánu. Dotknuté subjekty sú povinné audítorom umožniť prístup ku všetkým skutočnostiam majúcim vzťah k službám poskytovania a správy kvalifikovaných certifikátov. Ak sa jedná o audit na základe rozhodnutia DTCA, táto menuje a odvoláva audítorov.

Audit má za úlohu vyhodnotiť zhodu reálneho stavu činnosti DTCA s požadovaným stavom vyplývajúcim zo schválených dokumentov DTCA. Ďalším cieľom auditu je kontrola bezpečnosti vykonávania certifikačných činností podľa ZoEP a vyhlášky 540/2002 Z.z.

U zmluvných partnerov je audit vykonávaný s rovnakými cieľmi ako u DTCA, s tým, že oprávnenie DTCA vykonávať audit musí byť konkrétne vyjadrené v príslušnej zmluve.

Frekvencie vykonávania auditov a kontrol sú najmenej:

- 1 x ročne hĺbkový audit;
- nepravidelná kontrola podľa rozhodnutia DTCA.

2.8 Dôvernosť

2.8.1 Chránené informácie

Chránenými informáciami DTCA a I.CA sú:

- súkromné kľúče prislúchajúce k verejným kľúčom obsiahnutým vo vlastných certifikátoch I.CA a DTCA;
- súkromné kľúče prislúchajúce k verejným kľúčom obsiahnutým v účelových kvalifikovaných certifikátoch DTCA a I.CA (napr. kľúče pre komunikáciu s RA);
- ostatné kryptograficky podstatné informácie slúžiace na prevádzku DTCA a I.CA;
- všetky osobné údaje klientov či používateľov, podliehajúce ochrane v zmysle príslušnej zákonnej normy (zákon č. 428/2002 Z.z. o ochrane osobných údajov).

Chránenými informáciami jednotlivých RA sú:

- súkromné kľúče prislúchajúce k verejným kľúčom obsiahnutým vo vlastných kvalifikovaných certifikátoch pracovníkov RA;
- súkromné kľúče prislúchajúce k verejným kľúčom obsiahnutým v účelových kvalifikovaných certifikátoch RA (napr. kľúče pre komunikáciu s CA);
- ostatné kryptograficky podstatné informácie slúžiace na prevádzku RA;
- všetky osobné údaje klientov či používateľov podliehajúce ochrane v zmysle príslušnej zákonnej normy (zákon 428/2002 Z.z.)

Za chránené informácie sa taktiež považujú všetky ďalšie informácie označené niektorým zo subjektov ako dôverné.

Za verejné sa považujú typy informácií, ktoré nepatria do žiadnej z vyššie uvedených skupín.

S chránenými informáciami je, bez ohľadu na typ nosiča, narábané tak, aby bola zabezpečená ich dôvernosť a integrita. Interne sú tieto informácie prístupne výlučne pracovníkom, ktorí ich pre výkon svojich povinností musia poznať a to len v nevyhnutne potrebnom rozsahu.

2.8.2 Sprístupnenie informácií o zrušení kvalifikovaných certifikátov

Informácie o zrušených kvalifikovaných certifikátoch smie obdržať ľubovoľný používateľ. DTCA je povinná tieto informácie uverejňovať včas, v súlade s článkom 4.4.

2.8.3 Sprístupnenie informácií orgánom činným v trestnom konaní a iným tretím stranám

DTCA poskytne tretej strane informácie označené ako dôverné iba na základe rozhodnutia súdu. Ďalej DTCA poskytne dôverné informácie orgánom činným v trestnom konaní iba na základe právoplatného rozhodnutia príslušného štátneho orgánu, a to iba na základe písomnej žiadosti vybavenej všetkými náležitosťami. Konkrétne hodnoty údajov pre vytváranie elektronických podpisov slúžiace k podpisovaniu kvalifikovaných certifikátov a QCRL sa neposkytujú.

2.8.4 Sprístupnenie informácií na základe občianskoprávneho konania

DTCA poskytne tretej strane informácie označené ako dôverné na základe ukončeného občianskoprávneho konania (napr. pozostalým po zomretom vlastníkovi kvalifikovaného certifikátu), ak je to v súlade s platnými právnymi normami a výsledkom predmetného občianskoprávneho konania. V týchto prípadoch sa DTCA riadi príslušnými ustanoveniami zákona. Konkrétne hodnoty údajov pre vytváranie elektronických podpisov slúžiace k podpisovaniu kvalifikovaných certifikátov a QCRL sa neposkytujú.

2.8.5 Sprístupnenie informácií na základe požiadavky držiteľa certifikátu

V prípade požiadavky držiteľa certifikátu na sprístupnenie určitých informácií súvisiacich s klientom a jeho kvalifikovaným certifikátom tretej strane tak DTCA vykoná po kontrole vlastníckeho práva k certifikátu a na jeho písomnú žiadosť. Táto skutočnosť musí byť zaprotokolovaná a musia byť dodržané právne normy týkajúce sa najmä ochrany osobných údajov.

2.8.6 Ostatné okolnosti sprístupnenia informácií

V ostatných prípadoch DTCA tretím stranám citlivé informácie neposkytuje.

2.9 Duševné vlastníctvo

Na základe zmluvného zabezpečenia medzi DTCA a I.CA je DTCA oprávnená vydať tento CP ako CP DTCA. Všetky práva duševného vlastníctva k tomuto Certifikačnému poriadku prináležia I.CA.

3 IDENTIFIKÁCIA A AUTENTIZÁCIA

3.1 Prvotná registrácia

3.1.1 Typy podporovaných mien

DTCA prijíma žiadosti o vydanie kvalifikovaného certifikátu v elektronickej podobe vo formáte podľa PKCS#10.

I.CA prostredníctvom DTCA podporuje v ňou vydávaných kvalifikovaných certifikátoch len nasledujúce atribúty položky *Subject*:

| | |
|-----------------------------|--|
| Common Name | Všeobecné meno |
| Surname | Priezvisko |
| Country | Štát podľa ISO 3166 (napr. SK=Slovensko, CZ=Česká republika) |
| Locality | Miesto (napr. mesto) |
| State or Province | Nižšia organizačná jednotka štátu, napr. kraj alebo okres |
| Organization | Názov firmy |
| Organization Unit | Názov časti firmy |
| Title | Titul (napr. postavenie vo firme) |
| Postal Address | Poštová adresa |
| Name | Celé meno subjektu |
| Given Name | Krstné meno |
| Initials | Iniciály |
| Generation Qualifier | Generačné rozlíšenie (napr. „Jr.“ alebo „IV“ pre Karol IV apod.) |
| E-mail Address | Adresa elektronickej pošty (podľa RFC-822) |
| Serial Number | Sériové číslo subjektu |

V súlade so ZoEP kvalifikovaný certifikát musí obsahovať:

- Meno a priezvisko podpisujúcej osoby alebo pseudonym s označením, že ide o pseudonym;
- Označenie, že ide o kvalifikovaný certifikát. Toto označenie generuje I.CA automaticky;
- Ostatné položky stanovené ZoEP. Ich uvedenie v kvalifikovanom certifikáte je zabezpečené automaticky.

3.1.2 Vecná správnosť mien

DTCA kontroluje predovšetkým prítomnosť nepovolených znakov (v závislosti na type atribútu). V prípade, že sa nepovolené znaky vyskytnú, žiadosť sa neprijme.

Ďalej sa kontroluje prítomnosť všetkých povinných položiek (meno spolu s priezviskom alebo pseudonym). Pokiaľ niektorá z povinných položiek nie je vyplnená, žiadosť sa neprijme.

V prípade atribútov tvorených reťazcami znakov sa úvodné a doprovodné znaky „medzera“ odstránia.

Ďalej sa kontroluje vecná správnosť mien. Rozsah kontroly je uvedený v nasledujúcich článkoch.

3.1.2.1 Všeobecné meno (Common Name)

Všeobecné meno (*Common Name*) žiadateľ nevyplňuje. I.CA prostredníctvom DTCA obsah tohto atribútu generuje podľa nasledujúcich pravidiel:

1. V prípade, že žiadateľ použil pseudonym, sa obsah atribútu **Pseudonym** preniesie do atribútu **Common Name** a doplní sa reťazcom „- PSEUDONYM“;
2. V prípade, že žiadateľ použil atribút Name, preniesie sa obsah atribútu Name do atribútu Common Name;
3. V prípade, že žiadateľ použil atribúty GivenName a Surname, naplní sa atribút CommonName najprv obsahom atribútu GivenName, za ktorý sa vloží jedna medzera a doplní sa obsahom atribútu Surname.

Položka môže obsahovať znaky s diakritikou.

3.1.2.2 Meno (Name)

Atribút **Meno** (*Name*) môže obsahovať len celé meno žiadateľa vrátane titulov tak, ako je uvedené v predloženom osobnom doklade, prípadne v ďalších dokumentoch, pokiaľ sa jedná o titul (doklad o získanom titule). RA prijímajúca predmetnú žiadosť obsah tohto atribútu, pokiaľ je uvedený, kontroluje, v prípade nezhody danú žiadosť odmietne. Pokiaľ žiadosť obsahuje titul, ktorý nie je uvedený, resp. nekorešponduje s titulom uvedeným v predloženom osobnom doklade, je žiadateľ povinný použitie uvedeného titulu doložiť nespochybniteľným spôsobom (napr. diplomom). Položka môže obsahovať znaky s diakritikou.

3.1.2.3 Krstné meno (Given Name)

Atribút **Krstné meno** (*Given Name*) môže obsahovať len nasledujúce:

- krstné meno,
- krstné meno a druhé krstné meno,
- krstné a rodné meno

žiadateľa tak, ako je uvedené v preukaze totožnosti. RA prijímajúca predmetnú žiadosť, obsah tohto atribútu, pokiaľ je vyplnený, kontroluje podľa preukazu totožnosti, v prípade nezhody danú žiadosť odmietne. Položka môže obsahovať znaky s diakritikou.

3.1.2.4 Priezvisko – (Surname)

Atribút **Priezvisko** (*Surname*) môže obsahovať len priezvisko žiadateľa, ktoré je v zhode s predloženým preukazom totožnosti. RA prijímajúca žiadosť, pokiaľ je atribút Priezvisko vyplnený, túto zhodu skontroluje oproti preukazu totožnosti, v prípade nezhody danú žiadosť odmietne. Položka môže obsahovať znaky s diakritikou.

3.1.2.5 Pseudonym – (Pseudonym)

Atribút **Pseudonym** (*Pseudonym*) môže obsahovať akúkoľvek sekvenciu povolených znakov. RA prijímajúca predmetnú žiadosť nevykonáva overenie obsahu tohto atribútu, nie sú však povolené výrazy vulgárne a výrazy propagujúce fašizmus, rasovú a triednu nenávisť a pod. O prípustnosti konkrétneho obsahu položky v prípade použitia pseudonymu rozhoduje pracovník registračnej autority, ktorý vykonáva vybavenie klientovej žiadosti na vydanie kvalifikovaného certifikátu. Taktiež nesmú byť dotknuté práva iných subjektov (registrované známky a pod.). Položka môže obsahovať znaky s diakritikou.

3.1.2.6 Iniciály (Initials)

Atribút **Iniciály** (*Initials*) môže obsahovať len iniciály celého mena žiadateľa. RA prijímajúca predmetnú žiadosť, pokiaľ je atribút Initials vyplnený, zhodu iniciál so žiadateľovým menom kontroluje, v prípade nezhody danú žiadosť odmietne. Položka môže obsahovať znaky s diakritikou.

3.1.2.7 Generačné rozlíšenie (Generation Qualifier)

Atribút **Generačné rozlíšenie** (*Generation Qualifier*) sa používa pre označenie umiestnenia v rodinnom strome. RA prijímajúca predmetnú žiadosť obsah nekontroluje, nie sú však povolené výrazy vulgárne, propagujúce fašizmus, rasovú a triednu nenávisť. Položka môže obsahovať znaky s diakritikou.

3.1.2.8 Štát (Country)

Atribút **Štát** (*Country*) môže obsahovať len kód štátu, v ktorom má žiadateľ trvalé bydlisko. RA kontroluje správnosť podľa preukazu totožnosti (pokiaľ nie je explicitne uvedený v preukaze totožnosti, uvedie sa štát, ktorý predkladaný preukaz totožnosti vydal), v prípade nezhody žiadosť odmietne. Kód štátu musí zodpovedať norme ISO 3166.

3.1.2.9 Miesto (Locality)

Atribút **Miesto** (*Locality*) môže obsahovať len miesto trvalého bydliska podľa preukazu totožnosti, teda ulicu a mesto, obec alebo inú správnu jednotku, ktorá je v preukaze totožnosti uvedená. RA prijímajúca predmetnú žiadosť správnosť tohto údajá v prípade, že bol uvedený, kontroluje, v prípade nezhody danú žiadosť odmietne. Položka môže obsahovať znaky s diakritikou.

3.1.2.10 Kraj (State or Province)

Atribút **Kraj** (*State or Province*) môže obsahovať len označenie územno-správneho celku, do ktorého spadá miesto trvalého bydliska podľa preukazu totožnosti, teda kraj,

prípadne okres. Z obsahu musí byť zrejmé, či sa jedná o kraj alebo iný celok. RA prijímajúca predmetnú žiadosť správnosť tohto údajá v prípade, že bol uvedený kontroluje a v prípade nezhody danú žiadosť odmietne. Položka môže obsahovať znaky s diakritikou.

3.1.2.11 Organizácia (Organization)

Atribút **Organizácia** (*Organization*) môže obsahovať len obchodný názov organizácie podľa obchodného registra, prípadne obchodné meno podľa živnostenského listu. Žiadateľ je povinný doložiť oprávnenosť použitia obsahu daného atribútu nespochybniteľným spôsobom¹.

RA prijímajúca predmetnú žiadosť správnosť tohto údajá v prípade, že bol uvedený kontroluje, v prípade nezhody danú žiadosť odmietne. Položka môže obsahovať znaky s diakritikou.

3.1.2.12 Organizačná jednotka (Organization Unit)

Atribút **Organizačná jednotka** (*Organization Unit*) môže obsahovať len názov organizačnej jednotky a to výhradne v tom prípade, že bol použitý atribút Organizácia. Žiadateľ je povinný doložiť oprávnenosť použitia obsahu daného atribútu nespochybniteľným spôsobom.

RA prijímajúca predmetnú žiadosť správnosť tohto údajá v prípade, že bol uvedený kontroluje, v prípade nezhody danú žiadosť odmietne. Položka môže obsahovať znaky s diakritikou a môže sa vyskytovať viackrát.

3.1.2.13 Titul (Title)

Obsahom atribútu **Titul** spravidla býva postavenie v určitej (spravidla firemnej) hierarchii. Obsah tohto atribútu sa kontroluje v závislosti na skutočnostiach, ktoré sú v ňom obsiahnuté. Položka môže obsahovať znaky s diakritikou a môže sa vyskytovať viackrát.

3.1.2.14 Poštová adresa (Postal Address)

Atribút **Poštová adresa** (*Postal Address*) môže obsahovať len poštovú adresu. Tento atribút sa, v prípade, že bol uvedený, kontroluje len z hľadiska vecnej správnosti, v prípade nejasností bude žiadateľ vyzvaný, aby existenciu poštovej adresy doložil. Položka môže obsahovať znaky s diakritikou.

3.1.2.15 Elektronická poštová adresa (E-mail Address)

Atribút **Elektronická poštová adresa** (*E-mail Address*) môže obsahovať len elektronickú poštovú adresu žiadateľa (podľa RFC 822). Vyžaduje sa hodnoverne doložené vlastníctvo tejto elektronickej poštovej adresy alebo čestné prehlásenie² žiadateľa, v ktorom

¹ Napr. v prípade obchodného mena živnostníka patričným živnostenským listom, alebo výpisom z obchodného registra v prípade, že žiadateľ je majiteľom firmy alebo spoločníkom.

² Čestné prehlásenie pre účely tohto Certifikačného poriadku je realizované formou potvrdenia pravdivosti údajov v zmluve o vydaní certifikátu.

žiadateľ toto vlastníctvo potvrdzuje. V prípade nesplnenia tejto podmienky má RA právo danú žiadosť odmietnuť. Položka nesmie obsahovať znaky s diakritikou.

3.1.2.16 Serial Number (serialNumber)

Sériové číslo subjektu, ktoré slúži k rozlíšeniu rôznych subjektov v rámci klientely DTCA a I.CA. Sériové číslo vyplňuje spravidla CA a je tvaru „ICA – IdNum“, kde IdNum je vlastné sériové číslo. Žiadateľ smie požiadať, aby si mohol sériové číslo zadať sám. V takom prípade mu predchádza reťazec „USER - “ (vo všeobecnom prípade).

3.1.2.17 Alternatívne meno

Pokiaľ je použité **Alternatívne meno**, je nutné overiť skutočnosti v ňom uvádzané, pokiaľ sa jedná o skutočnosti vyžadujúce overenie.

Ako súčasť alternatívneho mena sa pripúšťa:

- **elektronická adresa** – platí rovnaké ustanovenie ako v článku 3.1.2.15 pre elektronickú poštovú adresu;
- **meno doménového servera** – pokiaľ je doménové meno registrované, vyžaduje sa hodnoverne doložený súhlas vlastníka alebo čestné prehlásenie žiadateľa, v ktorom žiadateľ vlastníctvo doménového mena potvrdzuje;
- **identifikátor zdroja v internete (URI)** – pokiaľ je URI registrované, vyžaduje sa hodnoverne doložený súhlas vlastníka alebo čestné prehlásenie žiadateľa, v ktorom žiadateľ vlastníctvo URI potvrdzuje;
- **IP adresa** – pokiaľ je IP adresa registrovaná, vyžaduje sa hodnoverne doložený súhlas vlastníka alebo čestné prehlásenie žiadateľa, v ktorom žiadateľ vlastníctvo IP adresy potvrdzuje;
- **EDI meno** - pokiaľ je EDI meno registrované, vyžaduje sa hodnoverne doložený súhlas vlastníka alebo čestné prehlásenie žiadateľa, v ktorom žiadateľ vlastníctvo EDI mena potvrdzuje;
- **registrovaný identifikátor (OID)** - pokiaľ je OID registrované, vyžaduje sa hodnoverne doložený súhlas vlastníka alebo čestné prehlásenie žiadateľa, v ktorom žiadateľ vlastníctvo OID potvrdzuje;

Jednotlivé uvedené položky sa v rámci alternatívneho mena môžu vyskytovať raz alebo viackrát, prípadne sa nemusia vyskytnúť vôbec. DTCA môže bez udania dôvodu množinu povolených tvarov obmedziť, prípadne rozšíriť.

3.1.3 Pravidla interpretácie rôznych foriem mien

Pokiaľ sa jedná o mená alebo iné skutočnosti, ktoré sú uvedené v preukaze totožnosti fyzickej osoby alebo v iných dokumentoch, ktoré sú prípustné pre preukazovanie totožnosti prípadne vzťahu fyzickej osoby k právnickej osobe, prenášajú sa tieto mená v tej podobe, v akej sú v dokumente uvedené. Vlastné transkripcie sa zásadne pre účely vydávania osobných kvalifikovaných certifikátov nevykonávajú.

I.CA prostredníctvom DTCA akceptuje len nasledujúce znakové sady:

- UTF8;

- BMP_String.

3.1.4 Jednoznačnosť mena

Jednoznačnosť mena subjektu je zaručená použitím vyššie definovaného postupu pre tvorbu atribútu *SerialNumber*. V prípadoch, keď hodnotu *SerialNumber* určuje CA, je jednoznačnosť zaručená. V prípadoch, keď hodnotu *SerialNumber* určuje žiadateľ a dôjde ku kolízii s už zavedeným jednoznačným menom iného kvalifikovaného certifikátu, DTCA upozorní žiadateľa a požiada ho, aby niektorý z požadovaných údajov zmenil či doplnil. Pokiaľ žiadateľ toto neučiní, certifikát sa mu nevydá.

3.1.5 Preukazovanie totožnosti fyzickej osoby a splnomocnených osôb

Pre účely evidencie držiteľov osobných kvalifikovaných certifikátov vyžaduje DTCA od žiadateľa poskytnutie nasledujúcich údajov:

- celé občianske meno žiadateľa;
- dátum narodenia žiadateľa;
- číslo predloženého primárneho dokladu;
- adresa trvalého bydliska.

Pokiaľ dôjde behom trvania zmluvného vzťahu s DTCA ku zmenám vo vyššie uvedených vyžadovaných osobných údajov, je držiteľ osobného certifikátu povinný tieto zmeny ohlásiť DTCA.

Pri registrácii nového žiadateľa – fyzickej osoby sa vyžaduje:

- a) predloženie platného primárneho osobného dokladu žiadateľa a ďalšieho osobného dokladu (sekundárneho). Primárny osobný doklad pre občanov SR musí byť občiansky preukaz. Primárny osobný doklad pre cudzích štátnych príslušníkov je platný cestovný pas. Občania Českej republiky môžu použiť tiež občiansky preukaz ako primárny osobný doklad. Sekundárny osobný doklad musí byť vydaný orgánom verejnej moci alebo inou organizáciou, ktorej existenciu je možné doložiť. Sekundárny osobný doklad musí obsahovať celé občianske meno žiadateľa a ďalej najmenej jeden z nasledujúcich údajov:
 - dátum narodenia žiadateľa (alebo rodné číslo u občanov SR),
 - adresa trvalého bydliska žiadateľa,
 - fotografia tváre žiadateľa.

Údaje požadované v sekundárnom doklade musia byť zhodné s týmito údajmi v primárnom osobnom doklade. O zhodnosti rozhoduje pracovník RA. Pokiaľ žiadateľ nepredloží dva osobné doklady vyššie popísanej kvality, nebude mu kvalifikovaný certifikát vydaný. Príkladom akceptovateľného sekundárneho osobného dokladu je napr.: cestovný pas, vodičský preukaz, služobné preukazy štátnych úradov, preukaz poslanca, služobný preukaz polície, zbrojný preukaz, vojenská knižka, preukaz zdravotného poistenia, preukážka hromadnej dopravy, študentský preukaz atď.;

- b) spôsobilosť žiadateľa k právnym úkonom;

- c) doklady preukazujúce právo žiadateľa jednať za inú (fyzickú alebo právnickú) osobu ako zástupca na základe plnej moci s úradne overeným podpisom zastupovanej osoby.

Pracovník RA vykoná kontrolu predložených osobných dokladov. V prípade pochybností o pravosti predloženého primárneho osobného dokladu žiadateľa odmietne a proces vydávania kvalifikovaného certifikátu ukončí. V prípade pochybností o pravosti predloženého sekundárneho osobného dokladu, alebo v prípade nezahodných údajov s primárnym dokladom, požiada žiadateľa o predloženie iného osobného dokladu ako sekundárneho dokladu. Pokiaľ žiadateľ nepredloží sekundárny osobný doklad požadovaných vlastností, pracovník RA žiadateľa odmietne a proces vydávania kvalifikovaného certifikátu ukončí. Žiadateľ môže podať sťažnosť na postup pracovníka RA k riaditeľovi DTCA. Rozhodnutie riaditeľa DTCA je konečné. V prípade, že pracovník RA nepochybuje o totožnosti žiadateľa, okopíruje predložené osobné doklady (kompletne). Papierovú kópiu predložených osobných dokladov, kde je navyše na každom liste vytlačaná veta: „Súhlasím s tým, aby D. Trust Certifikačná Autorita, a.s., uchovávala túto kópiu mojich osobných dokladov v zmysle zákona č.215/2002 Z.z.“, nechá žiadateľovi podpísať. Pokiaľ žiadateľ odmietne tieto kópie svojich osobných dokladov podpísať, je pracovník RA povinný proces vydávania kvalifikovaného certifikátu ukončiť a kópie osobných dokladov zničiť. Pokiaľ žiadateľ o vydanie kvalifikovaného certifikátu požiada o publikovanie ďalších osobných údajov, musí byť táto skutočnosť explicitne uvedená v zmluve o vydaní kvalifikovaného certifikátu.

3.2 Postup pri vydaní následného kvalifikovaného certifikátu

DTCA nepodporuje žiadne vystavenie ďalšieho nového kvalifikovaného certifikátu na párové údaje, ktoré prislúchali už vydanému kvalifikovanému certifikátu, bez ohľadu na dôvod ukončenia jeho platnosti.

Jedinou formou následného kvalifikovaného certifikátu, ktorá je akceptovaná, je kvalifikovaný certifikát vydaný na základe novej žiadosti o vydanie kvalifikovaného certifikátu, podpísanej súkromným kľúčom súvisiacim s doposiaľ platným kvalifikovaným certifikátom, ku ktorému má byť následný QC vydaný. Údaje overované DTCA (viď článok 3.1.2) musia byť v žiadosti a pôvodnom QC zhodné. Ostatné položky následného QC podliehajú aktuálnym pravidlám pre vydávanie kvalifikovaných certifikátov.

Generovanie žiadosti o následný kvalifikovaný certifikát je obdobné ako u prvotného kvalifikovaného certifikátu. Klient má však možnosť túto žiadosť zaslať do DTCA elektronickou cestou. V takom prípade musí byť žiadosť podpísaná súkromným kľúčom súvisiacim s doposiaľ platným kvalifikovaným certifikátom klienta, ku ktorému sa žiada o následný kvalifikovaný certifikát. Táto žiadosť však musí byť obdobne ako prvá žiadosť podpísaná aj novým súkromným kľúčom, súvisiacim s verejným kľúčom uvedeným v následnom kvalifikovanom certifikáte. V prípade, že žiadosť nemá vyššie uvedené náležitosti, napr. je síce podpísaná, ale tieto podpisy nie je možné overiť verejnými kľúčmi uvedenými v pôvodnom a následnom kvalifikovanom certifikáte, I.CA prostredníctvom DTCA následný QC nevydá.

3.3 Žiadosť o zrušenie kvalifikovaného certifikátu

Akceptované spôsoby podania žiadosti o zrušenie kvalifikovaného certifikátu sú uvedené nižšie.

3.3.1 Osobné podanie žiadosti na RA

V tomto prípade musí žiadateľ o zrušenie kvalifikovaného certifikátu preukázať vlastníctvo tohto certifikátu. Žiadosť musí byť písomná a podpísaná žiadateľom. V tejto písomnej žiadosti musí byť uvedené sériové číslo QC (buď v dekadickom tvare alebo hexadecimálnom – v tomto prípade musí začínať reťazcom „0x“), celé občianske meno klienta, ktorému bol QC vydaný, a heslo pre zrušenie QC. Pokiaľ si žiadateľ heslo pre zrušenie certifikátu nepamätá, musí to explicitne uviesť do písomnej žiadosti o zrušenie QC. V takom prípade musí v žiadosti uviesť číslo primárneho osobného dokladu predloženého pri žiadosti o vydanie QC a týmto primárnym osobným dokladom sa preukázať pracovníkovi RA.

Pracovník RA okamžite odovzdá túto žiadosť (diaľkovým prístupom) na CA. Zodpovedný pracovník CA rozhodne, či je táto žiadosť oprávnená a toto rozhodnutie oznámi žiadateľovi prostredníctvom pracovníka RA. V prípade, že žiadosť o zrušenie QC je oprávnená, CA bezodkladne zruší tento QC. Pokiaľ z ľubovoľného dôvodu nebude možné žiadosť akceptovať (zlé zadané heslo pre zrušenie, nepreukázateľná identita žiadateľa), žiadosť o zrušenie QC bude zamietnutá.

3.3.2 Podanie žiadosti elektronickou cestou

Prípustné sú nasledujúce možnosti:

- **podpísaná elektronická správa**, podpis musí byť realizovaný údajmi pre vytváranie podpisu príslušnými k predmetnému certifikátu, ktorý má byť zrušený. Telo správy musí byť nasledujúceho tvaru:

Ziadam o zrusenie certifikatu cislo = xxxxxxx

alebo

Žiadam o zrušenie certifikátu číslo = xxxxxxx

kde „xxxxxxx“ je sériové číslo kvalifikovaného certifikátu.

Sériové číslo QC je buď v dekadickom tvare alebo hexadecimálnom (v tomto prípade musí začínať reťazcom „0x“);

- **nepodpísaná elektronická správa**. V tomto prípade telo správy musí byť nasledujúceho tvaru:

Ziadam o zrusenie certifikatu cislo = xxxxxxx

Heslo pre zrusenie = yyyyyy

alebo

Žiadam o zrušenie certifikátu číslo = xxxxxxx

Heslo pre zrušenie = yyyyyy

kde „xxxxxxx“ je sériové číslo kvalifikovaného certifikátu „yyyyyy“ je heslo pre zrušenie.

Sériové číslo QC je buď v dekadickom tvare alebo hexadecimálnom (v tomto prípade musí začínať reťazcom „0x“);

- prostredníctvom formulára zverejneného na internetovej stránke vyhradenej pre na tento účel.

Správa musí byť zaslaná na adresu elektronickej pošty DTCA. Pokiaľ žiadosť spĺňa vyššie uvedené požiadavky, bude príslušný QC bezodkladne zrušený. Dátum a čas zneplatnenia je určený okamihom prijatia platnej žiadosti o zrušenie serverom ICA. V prípade, že žiadosť nespĺňa uvedené požiadavky, je zamietnutá a žiadateľ je elektronickou cestou o tejto skutočnosti informovaný. O kladnom vybavení nie je explicitne informovaný, túto skutočnosť zistí v najbližšom zozname zrušených kvalifikovaných certifikátov.

3.3.3 Podanie žiadosti listovou zásielkou

Listová zásielka musí byť zaslaná doporučeným listom na adresu sídla DTCA.

V zásielke musí byť uvedená žiadosť v nasledujúcom tvare:

Žiadam o zrušenie certifikátu číslo = xxxxxx

Heslo pre zrušenie = yyyyyy

Sériové číslo QC je buď v dekadickom alebo hexadecimálnom tvare (v tomto prípade musí začínať reťazcom „0x“). Pokiaľ si žiadateľ heslo pre zrušenie certifikátu nepamätá, musí to explicitne uviesť do písomnej žiadosti o zrušenie QC. V takom prípade musí v žiadosti uviesť číslo primárneho osobného dokladu predloženého pri žiadosti o vydanie QC a žiadosť vlastnoručne podpísať.

V prípade, že žiadosť o zrušenie certifikátu je oprávnená, bude byť príslušný QC bezodkladne zrušený. Dátum a čas zneplatnenia je určený okamihom prijatia doporučenej zásielky. O vybavení žiadosti o zrušenie QC je žiadateľ informovaný doporučeným listom na poštovú adresu uvedenú ako adresa odosielateľa na doporučenom liste žiadateľa.

3.3.4 Okolnosti zrušenia certifikátu

Žiadosti o zrušenie kvalifikovaných certifikátov prijíma DTCA nepretržite len prostredníctvom podania žiadosti elektronickou cestou a listovou zásielkou. Osobné podanie na RA je možné len v pracovnej dobe príslušnej RA.

Reakciou DTCA na prijatie platnej žiadosti o zrušenie kvalifikovaného certifikátu je bezodkladné zneplatnenie, tohto kvalifikovaného certifikátu. Do doby zverejnenia QCRL je dotýčny kvalifikovaný certifikát zablokovaný. Maximálna doba medzi prijatím žiadosti o zrušenie kvalifikovaného certifikátu a zverejnením zoznamu zrušených kvalifikovaných certifikátov, na ktorom je tento kvalifikovaný certifikát po prvý krát uvedený, je najviac 12 hodín.

Počas doby zablokovania kvalifikovaného certifikátu zodpovedá za prípadné škody, vzniknuté takýmto kvalifikovaným certifikátom, jeho držiteľ.

Odblokovanie kvalifikovaného certifikátu, ktorý bol zablokovaný na základe platnej žiadosti o zrušenie kvalifikovaného certifikátu, DTCA nepovoľuje.

4 OPERAČNÉ POŽIADAVKY

4.1 Vzor žiadosti o poskytnutie služby

Žiadosť o poskytnutie služby DTCA

Meno a priezvisko:

Trvalé bydlisko:

Číslo občianskeho preukazu:

žiadam týmto o

.....
.....
.....
.....
.....
.....
.....
.....

K žiadosti prikladám:

.....
.....

V dňa o

.....

podpis žiadateľa

.....

podpis a pečiatka zástupcu DTCA

4.2 Žiadosť o kvalifikovaný certifikát

Pri registrácii nového žiadateľa o kvalifikovaný certifikát, príslušný pracovník RA na základe predložených dokladov kontroluje náležitosti podľa článku 3.1.

Vzor žiadosti o vydanie kvalifikovaného certifikátu:

| Žiadosť o vydanie kvalifikovaného certifikátu DTCA | |
|--|-------------|
| Registračné číslo žiadosti : | |
| Číslo registračnej autority : | |
| Dátum a čas podania žiadosti : | |
| Údaje o žiadateľovi uvedené v predložennom doklade totožnosti : | |
| Titul : | |
| Priezvisko : | |
| Meno : | |
| Typ a číslo dokladu : | |
| Rodné číslo : | |
| Adresa pobytu : | |
| Ostatné doklady : | |
| Položky žiadosti, za ktorých úplnosť a správnosť sa žiadateľ zaručuje : | |
| : | |
| : | |
| : | |
| : | |
| Požiadavky na služby DTCA : | |
| Zasielanie aktuálneho CRL : | |
| Zverejnenie certifikátu : | |
| Heslo pre zrušenie certifikátu : | |
| <p>Žiadateľ prehlasuje, že súkromný kľúč zodpovedajúci verejnému kľúču predloženému v tejto žiadosti o kvalifikovaný certifikát bol vygenerovaný na zariadení, ktoré spĺňa požiadavky na vyhotovovanie zaručených elektronických podpisov podľa zákona č. 215/2002 Z.z a bolo pre tento účel certifikované Národným bezpečnostným úradom SR.</p> <p>Žiadateľ súhlasí v zmysle zákona č. 428/2002 Z.z. o ochrane osobných údajov so spracovaním vyššie uvedených osobných údajov spoločnosťou D. Trust Certifikačná Autorita, a.s., pre účely vydania a správy kvalifikovaného certifikátu podľa podmienok zákona č. 215/2002 Z.z. o elektronickom podpise. Žiadateľ bol oboznámený s tým, že pre účely vydania a správy kvalifikovaného certifikátu DTCA dochádza k cezhraničnému toku osobných údajov s Českou republikou.</p> <p>Žiadateľ súhlasí s tým, aby D. Trust Certifikačná Autorita, a.s., uchovávala ako neoddeliteľnú súčasť tejto žiadosti kópiu predložených osobných dokladov v zmysle požiadaviek zákona č.215/2002 Z.z.</p> <p>Informačný systém Registračná autorita DTCA, Certifikačná autorita DTCA je v zmysle zákona č. 428/2002 Z.z. registrovaný Úradom na ochranu osobných údajov a bolo mu pridelené registračné číslo 190829.</p> | |
| Meno a priezvisko operátora RA : | |
| Žiadateľ skontroloval vyššie uvedené údaje a potvrdzuje ich správnosť. | |
| V dňa | |
| _____ | _____ |
| žiadateľ | operátor RA |

4.3 Vydanie kvalifikovaného certifikátu

I.CA prostredníctvom DTCA vydáva kvalifikovaný certifikát žiadateľovi, ktorý splnil podmienky registrácie (článok 4.2), zaplatil určený poplatok, preukázal vlastníctvo súkromného kľúča zodpovedajúceho verejnému kľúču, ktorý je obsiahnutý v QC a podpísal príslušnú zmluvu.

Vlastníctvo súkromného kľúča zodpovedajúceho verejnému kľúču, ktorý je obsiahnutý v QC, sa preukazuje predložením žiadosti, ktorá obsahuje tento verejný kľúč a je podpísaná uvedeným súkromným kľúčom. Pracovník RA vykoná kontrolu tejto skutočnosti tak, že pomocou verejného kľúča uvedeného v žiadosti o QC overí elektronický podpis na tejto žiadosti. Ak nie je možné overiť podpis žiadosti, I.CA prostredníctvom DTCA kvalifikovaný certifikát nevydá.

Po vydaní QC, pracovník RA vyhotoví kópie dokladov, na základe ktorých je kvalifikovaný certifikát vystavovaný (viď. kap. 3.1.5). Pritom musí dbať na príslušné ustanovenia zákona o ochrane osobných údajov.

Pracovník RA odovzdá žiadateľovi médium, ktoré obsahuje jeho kvalifikovaný certifikát, zodpovedajúce kvalifikované certifikáty DTCA a Certifikačný poriadok. Žiadateľ musí prevzatie média potvrdiť. Okrem toho zašle DTCA na vyžiadanie kvalifikované certifikáty v predpísaných formátoch a Certifikačný poriadok DTCA na adresu elektronickej pošty uvedenú v žiadosti (pokiaľ je táto adresa známa).

4.4 Akceptovanie kvalifikovaného certifikátu

Žiadateľ je povinný akceptovať kvalifikovaný certifikát, o ktorý požiadal, ak splnil podmienky pre vydanie kvalifikovaného certifikátu (článok 4.2). Jediný spôsob ako môže postupovať, pokiaľ tento kvalifikovaný certifikát akceptovať odmieta, je požiadať v súlade s týmto CP o jeho zrušenie.

4.5 Zrušenie kvalifikovaného certifikátu

Kvalifikovaný certifikát môže byť zrušený len na základe nasledujúcich okolností:

- oprávnená osoba požiada o zrušenie kvalifikovaného certifikátu;
- nastanú skutočnosti, na základe ktorých je certifikačná autorita v zmysle ZoEP povinná zrušiť kvalifikovaný certifikát
- ak zrušenie nariadi v zmysle zákona o elektronickej podpise kompetentný úrad,
- držiteľ kvalifikovaného certifikátu poruší závažným spôsobom ustanovenie zmluvy o vydaní kvalifikovaného certifikátu alebo dokumentov, ktoré sú prílohou tejto zmluvy;
- dôjde ku kompromitácii súkromného kľúča I.CA;
- je dôvodné podozrenie, že došlo ku kompromitácii súkromného kľúča držiteľa.

Zrušenie kvalifikovaného certifikátu vykoná DTCA na základe podnetu:

- subjektov oprávnených zo zákona;
- registračnej autority, prostredníctvom ktorej bolo požiadané o jeho vydanie;

- DTCA;
- I.CA;
- osoby oprávnenej z pozostalostného konania;
- subjektu, ktorý bol k tomu explicitne určený v zmluve o poskytnutí služby (napr. pri vydaní kvalifikovaného certifikátu pre zamestnanca organizácie).

Oprávnený subjekt musí zaslať alebo osobne podať žiadosť o zrušenie kvalifikovaného certifikátu spôsobom uvedeným v článku 3.3.

V prípade, že sa zrušenie uskutočňuje na základe súdneho rozhodnutia, musí pracovník DTCA k záznamu o zrušení priložiť doklad o súdnom rozhodnutí.

V prípade, že sa zrušenie uskutočňuje na základe pozostalostného konania, musí pracovník DTCA k záznamu o zrušení priložiť doklady, z ktorých jednoznačne vyplýva právo žiadateľa na zrušenie certifikátu.

V prípade, že sa zrušenie uskutočňuje z iniciatívy RA alebo DTCA, je príslušný pracovník povinný zaznamenať túto skutočnosť do protokolu, vrátane dôvodu tohto rozhodnutia.

Doba medzi prijatím žiadosti o zrušenie QC a zverejnením zoznamu zrušených kvalifikovaných certifikátov po prvýkrát obsahujúceho zrušený QC, musí byť kratšia ako 12 hodín. Počas doby zablokovania kvalifikovaného certifikátu zodpovedá za prípadné škody vzniknuté použitím takéhoto kvalifikovaného certifikátu vždy jeho držiteľ.

Kvalifikovaným certifikátom vydávaným podľa tohto Certifikačného poriadku DTCA nie je možné dočasne pozastaviť platnosť.

4.6 Požiadavky na overovanie zoznamu zrušených kvalifikovaných certifikátov

Užívatelia kvalifikovaných certifikátov sú povinní overovať, či kvalifikované certifikáty, ktoré používa s nimi komunikujúca strana, nie sú zrušené. Pre tieto účely sú povinní používať QCRL vydané a podpísané I.CA. Neoverenie kvalifikovaného certifikátu pomocou QCRL je kvalifikované ako hrubé porušenie Certifikačného poriadku a zanikajú týmto akékoľvek nároky na prípadné uznanie záruk.

V období medzi prijatím žiadosti o zrušenie kvalifikovaného certifikátu a zverejnením QCRL, v ktorom je po prvýkrát uvedený tento QC, nesie všetku zodpovednosť za prípadné škody vzniknuté v súvislosti so zneužitím tohto QC držiteľ tohto QC. Po zverejnení QCRL, v ktorom je po prvýkrát uvedený tento zrušený QC, nesie zodpovednosť užívateľ, ktorý daný QC použil.

4.7 Procedúry auditu vzhľadom k bezpečnosti

I.CA a s ňou spolupracujúce RA DTCA zaznamenávajú do auditného logu nasledujúce udalosti:

- záznam o registrácii žiadateľa;

- záznam o pokus neoprávnenej registrácie žiadateľa (s maximom dosiahnuteľných informácií o neoprávnenom žiadateľovi);
- záznam o zrušení registrácie žiadateľa (údaje o žiadateľovi sa uchovávajú);
- záznam o požiadavke RA na vydanie kvalifikovaného certifikátu vrátane výsledku;
- záznam o požiadavke na vydanie následného kvalifikovaného certifikátu vrátane výsledku;
- záznam o neoprávnenej požiadavke na vydanie kvalifikovaného certifikátu vrátane výsledku;
- záznam o neoprávnenej požiadavke na vydanie následného kvalifikovaného certifikátu vrátane výsledku;
- záznam o požiadavke na zrušenie kvalifikovaného certifikátu vrátane údajov o žiadajúcej osobe a o výsledku;
- záznam o neoprávnenej požiadavke na zrušenie kvalifikovaného certifikátu vrátane údajov o žiadajúcej osobe a o výsledku;
- záznam o ukončení platnosti QC;
- záznam o zrušení QC;
- záznam o pokuse neoprávneného prístupu do systému;
- záznam o zverejnení kvalifikovaného certifikátu vrátane výsledku;
- záznam o zaradení kvalifikovaného certifikátu do QCRL;
- záznam o zverejnení QCRL;

Všetky auditné záznamy obsahujú dátum (rok, mesiac, deň) a čas (hodina, minúta, sekunda). Pod pojmom čas sa rozumie svetový čas.

Doba, počas ktorej sa uchovávajú auditné záznamy, je stanovená na 10 rokov.

4.8 Výmena párových údajov CA

V prípade zmeny párových údajov I.CA, určených k podpisovaniu kvalifikovaných certifikátov a zoznamov zrušených kvalifikovaných certifikátov, požiadá DTCA Národný bezpečnostný úrad SR o vydanie nového kvalifikovaného certifikátu akreditovanej certifikačnej autority DTCA a zverejní tento nový certifikát v súlade s týmto CP.

4.9 Odhalenie kompromitácií a nehôd

V prípade zrušenia verejného kľúča, používaného k overovaniu podpísaných kvalifikovaných certifikátov a zoznamov zrušených kvalifikovaných certifikátov, DTCA informuje o tejto skutočnosti na oficiálnych internetových stránkach. Touto situáciou sa rozumejú iné dôvody, než kompromitácia príslušných súkromných kľúčov.

V prípade kompromitácie súkromného kľúča I.CA používaného k podpisovaniu kvalifikovaných certifikátov, DTCA okamžite požiadá Národný bezpečnostný úrad SR o zrušenie príslušného kvalifikovaného certifikátu akreditovanej certifikačnej autority. O tejto

skutočnosti DTCA bezodkladne informuje na svojich internetových stránkach. Túto informáciu uvedie aj NBÚv zozname zrušených kvalifikovaných certifikátov, čím je zaistená dostupnosť tejto informácie minimálne dvoma na sebe nezávislými spôsobmi, ktoré umožňujú diaľkový prístup a sú nepretržite dostupné. Ďalej I.CA zruší QC, ktoré boli týmto súkromným kľúčom podpísané. Držiteľov týchto QC DTCA informuje o tejto skutočnosti, vrátane uvedenia dôvodu zrušenia kvalifikovaného certifikátu DTCA, doporučenou listovou zásielkou a aj elektronickou poštou (pokiaľ je to možné). DTCA ponúkne týmto klientom vystavenie nového QC štandardným postupom popísaným v tomto CP. Prípadné náklady na vystavenie nových kvalifikovaných certifikátov hradí DTCA. Počas doby zablokovania týchto QC nesie všetku zodpovednosť za prípadné škody vzniknuté v súvislosti so zneužitím týchto kvalifikovaných certifikátov poskytovateľ akreditovaných certifikačných služieb – DTCA.

4.10 Ukončenie činnosti DTCA

V prípade ukončenia činnosti DTCA ako akreditovanej certifikačnej autority z iných dôvodov, než ako sú mimoriadne udalosti, (štrajky, občianske nepokoje, vojnový stav, prírodné katastrofy celoštátneho rozsahu alebo iné výsledky pôsobenia vyššej moci) DTCA zaistí vykonanie nasledujúcich činností:

- a) ohlásí NBÚ SR zámer ukončiť činnosť ako akreditovaná certifikačná autorita najmenej 6 mesiacov pred plánovaným ukončením činnosti,
- b) ukončí vydávanie kvalifikovaných certifikátov,
- c) sprístupní informáciu o ukončení činnosti akreditovanej certifikačnej autority na svojej internetovej informačnej adrese najmenej 6 mesiacov pred plánovaným ukončením činnosti,
- d) oznámi ukončenie činnosti akreditovanej certifikačnej autority všetkým svojim klientom, ktorí sú držiteľia platných kvalifikovaných certifikátov, najmenej 6 mesiacov pred plánovaným ukončením činnosti,
- e) vyvinie maximálne úsilie pre to, aby platné kvalifikované certifikáty vydané I.CA prostredníctvom DTCA boli prevzaté inou akreditovanou certifikačnou autoritou,
- f) bezodkladne upozorní NBÚ SR na prípad, keď sa jej nepodarí dohodnúť prevzatie zoznamov vydaných a zrušených certifikátov a prevádzkovej dokumentácie s inou akreditovanou certifikačnou autoritou. V takom prípade zaistí odovzdanie evidencie vydaných a zrušených kvalifikovaných certifikátov NBÚ SR a túto informáciu oznámi všetkým svojim klientom, ktorí sú držiteľmi platných kvalifikovaných certifikátov,
- g) štatutárny zástupca DTCA zabezpečí vykonanie kontroly dodržania zákona o ochrane osobných údajov.

5 FYZICKÉ, PROCEDURÁLNE A PERSONÁLNE BEZPEČNOSTNÉ MECHANIZMY

Fyzické, procedurálne a personálne bezpečnostné mechanizmy sú veľmi dôležitým faktorom zaisťujúcim dôveryhodnosť akreditovaných certifikačných služieb DTCA. Ochrana

je zameraná na hlavné prevádzkové systémy I.CA, ktorými sú tie, ktoré priamo vykonávajú podpisovanie kvalifikovaných certifikátov a podpisovanie QCRL.

Podrobný popis a požiadavky na DTCA a na I.CA v týchto oblastiach sú uvedené v interných dokumentoch DTCA a I.CA.

Bezpečnostné mechanizmy sú nastavené podľa platných právnych predpisov upravujúcich činnosť akreditovanej certifikačnej authority.

6 TECHNICKÁ BEZPEČNOSŤ

V tejto kapitole sú uvedené požiadavky, ktoré musia spĺňať párové údaje, ktoré si vytvára žiadateľ a ku ktorým má byť vydaný kvalifikovaný certifikát. Ďalej sú špecifikované požiadavky na párové údaje I.CA, ktoré sú používané k podpisovaniu a overovaniu kvalifikovaných certifikátov a QCRL.

6.1 Generovanie párových údajov CA

Kvalifikované certifikáty vydáva pre DTCA na základe zmluvy certifikačná autorita I.CA, pričom sa využívajú párové údaje, ktoré sú vo vlastníctve I.CA a ktoré I.CA používa výhradne pre vydávanie kvalifikovaných certifikátov. Generovanie párových údajov I.CA sa vykonáva prostredníctvom špeciálneho kryptografického modulu. Použitý modul svojimi vlastnosťami zodpovedá požiadavkám vyžadovaným podľa ZoEP. Charakteristiky určujúce kvalitu zodpovedajú požiadavkám uvedeným v nasledujúcej tabuľke:

| Podpisová schéma | Asymetrický algoritmus | Minimálne parametre asymetrického algoritmu | Algoritmus pre generovanie kľúčov | Metóda na doplnenie (padding) | Hašovacia funkcia |
|------------------|------------------------|---|-----------------------------------|-------------------------------|-------------------|
| 002 | RSA | MinModLen=1020 | Rsagen1 | emsa-pss | SHA1 |

I.CA používa pre párové údaje, slúžiace k podpisovaniu kvalifikovaných certifikátov a zoznamov zrušených kvalifikovaných certifikátov, vyššie uvedenú podpisovú schému s dĺžkou modulu (*ModLen*) 2048 bitov.

6.2 Generovanie párových údajov klienta a inštalácia

Párové údaje, tj. vzájomne previazaná dvojica súkromného a verejného kľúča, sú základom kryptografických postupov realizujúcich elektronické podpisy. Kvalifikovaný certifikát bude vydaný len párovým údajom a podpisovým algoritmom, uvedeným v nasledujúcej tabuľke:

| Podpisová schéma | Asymetrický algoritmus | Minimálne parametre asymetrického algoritmu | Metóda na doplnenie (padding) | Hašovacia funkcia |
|------------------|------------------------|---|-------------------------------|-------------------|
| 001 | RSA | MinModLen=1020 | emsa-pkcs #1-v1.5 | SHA1 |
| 002 | RSA | MinModLen=1020 | emsa-pss | SHA1 |
| 003 | RSA | MinModLen=1020 | emsa-pkcs #1-v1.5 | RIPEMD160 |
| 004 | RSA | MinModLen=1020 | emsa-pss | RIPEMD160 |
| 005 | DSA | pMinLen=1024 qMinLen=160 | - | SHA1 |
| 006 | ECDSA-F _q | qMinLen=160 r0Min=10000 MinClass=200 | - | SHA1 |
| 007 | ECDSA-F2 ^m | qMinLen=160 r0Min=10000 MinClass=200 | - | SHA1 |

Párové údaje sa zásadne generujú na zariadení, ktoré je v okamihu generovania pod výhradnou kontrolou klienta. Týmto zariadením môže byť počítač, špeciálna čipová karta alebo napríklad USB token.

DTCA neposkytuje službu generovania párových údajov klienta na svojich zariadeniach.

Doporučený postup generovania párových údajov a prípravy podkladov pre vydanie kvalifikovaného certifikátu je popísaný na internetových stránkach DTCA.

Verejný kľúč klienta je súčasťou žiadosti o vydanie kvalifikovaného certifikátu. Podľa použitého prehliadača je buď vo formáte PKCS #10 alebo Netscape SPKAC.

DTCA kontroluje pri prijatí žiadosti, či už nebol vydaný iný kvalifikovaný certifikát s rovnakým verejným kľúčom. Ak áno, je klient vyzvaný k vygenerovaniu novej žiadosti, a teda i nových párových údajov. Taktiež držiteľ už vydaného kvalifikovaného certifikátu, ktorý má verejný kľúč rovnaký so žiadateľom, je vyzvaný k vygenerovaniu nových párových údajov. Tento kvalifikovaný certifikát je okamžite zrušený a držiteľ tohto kvalifikovaného certifikátu je o tejto skutočnosti bezodkladne informovaný. V takomto prípade má držiteľ takto zrušeného kvalifikovaného certifikátu nárok na vydanie nového kvalifikovaného certifikátu zdarma. V prípade použitia kvalitných metód generovania náhodných čísel uvedených v Prílohe vyhlášky č. 537/2002 Z.z. je pravdepodobnosť výskytu takejto situácie veľmi malá.

Kvalifikovaný certifikát akreditovanej certifikačnej authority DTCA je možné získať na oficiálnych internetových stránkach DTCA. Tento kvalifikovaný certifikát DTCA tiež dostane každý klient spolu so svojim kvalifikovaným certifikátom. Ďalšia možnosť ako získať tento kvalifikovaný certifikát, je nahratie na médium (napr. disketu) na ktorejkoľvek RA DTCA. Tento kvalifikovaný certifikát môže byť šírený aj ďalšími dôveryhodnými spôsobmi.

6.3 Ochrana súkromného kľúča CA

Súkromný kľúč certifikačnej autority je najdôležitejšie tajomstvo, ktoré každá certifikačná autorita má. Rovnako aj I.CA venuje ochrane súkromného kľúča CA, ktorý sa používa na vydávanie kvalifikovaných certifikátov, maximálnu pozornosť. Podrobný popis povolených postupov pri práci so súkromným kľúčom I.CA používaným pre vydávanie kvalifikovaných certifikátov, je uvedený v interných dokumentoch I.CA. Pre účely tohto certifikačného poriadku platí:

- súkromný kľúč je uložený v špeciálnom zariadení (kryptografický modul), ktorý je certifikovaný podľa medzinárodne prijímaného amerického štandardu FIPS 140 – 1 na úrovni (level) 3;
- súkromný kľúč je zálohovaný v zašifrovanej forme, tak, že k jeho dešifrovaniu sú potrební dvaja určení pracovníci I.CA, ktorí majú k dispozícii časť tajomstva, z ktorého sa dá vytvoriť kľúč do symetrickej šifry použitej pre zašifrovanie súkromného kľúča I.CA;
- nie je známa možnosť získať súkromný kľúč inými metódami (napr. tzv. „Escrow“);
- súkromný kľúč I.CA je používaný výhradne k podpisovaniu vydaných kvalifikovaných certifikátov všetkých typov a zoznamov zrušených kvalifikovaných certifikátov (QCRL);
- kryptografický modul spolu s obsluhujúcim počítačom je uložený v priestoroch, ktoré sú zabezpečené ako objekty kategórie „D“ podľa českej vyhlášky č. 339/1999 Sb., o objektivej bezpečnosti;
- tieto zabezpečené priestory sa nachádzajú v objekte, ktorý okrem fyzickej ostrahy a technických prostriedkov vyžadovaných k vonkajšej ochrane objektu kategórie „D“ je navyše chránený i špeciálnym televíznym systémom pre snímanie, prenos a zobrazovanie pohybu osôb a dopravných prostriedkov;
- vkladanie, aktivácia, deaktivácia, zálohovanie a ničenie súkromného kľúča I.CA je vykonávané podľa platnej CPS (Certifikační prováděcí směrnice) I.CA, vždy v prítomnosti minimálne dvoch určených pracovníkov I.CA.

6.4 Ďalšie požiadavky na správu párových údajov CA

Verejné kľúče obsiahnuté v kvalifikovaných certifikátoch sú archivované v I.CA. I.CA bude tieto kľúče archivovať, resp. zaistí ich archiváciu, ešte 10 rokov po prípadnom ukončení svojej činnosti. Platnosť párových údajov s mohutnosťou kľúča 2048 bitov určených k podpisovaniu kvalifikovaných certifikátov a príslušných QCRL je 6 rokov. I.CA si vyhradzuje právo túto dobu zmeniť.

6.5 Bezpečnosť počítačového vybavenia

Výpočtová technika používaná v I.CA a DTCA pre akreditované certifikačné služby spĺňa požiadavky na kvalitnú bezpečnú činnosť akreditovanej certifikačnej autority podľa požiadaviek uvedených v ZoEP. Sú použité výhradne značkové komponenty spĺňajúce vysoké technické kritériá. Proti poruchám elektrickej siete sú hlavné systémy zabezpečené pomocou záložných zdrojov elektrickej energie.

Bezpečnosť použitých informačných systémov pre certifikačné služby je určená ZoEP a príslušnými vykonávacími vyhláškami.

6.6 Kontroly počítačovej bezpečnosti

Všeobecné požiadavky na počítačovú bezpečnosť sú určené ZoEP a príslušnými vykonávacími vyhláškami. Špecifické požiadavky sú:

- systém je použitý výhradne k operáciám súvisiacim s poskytovaním certifikačných služieb;
- je zaistená bezpečnosť údajov pre podpisovanie kvalifikovaných certifikátov a QCRL;
- systém je chránený proti výpadkom elektrickej siete;
- použitý hardware je zálohovaný a je zaistené obnovenie činnosti do 24 hodín;
- zálohovaním hardware je zaistené vydanie podpísaného QCRL do 12 hodín od zrušenia každého kvalifikovaného certifikátu;
- prevádzka počítačového systému I.CA zaisťujúceho akreditované certifikačné služby je pravidelne kontrolovaná určenými pracovníkmi I.CA;
- Podľa požiadaviek zodpovedajúcich požiadavkám ZoEP a príslušných vykonávacích vyhlášok sú zaznamenávané a vyhodnocované auditné informácie.

6.7 Bezpečnostné kontroly v dobe životnosti

Vykonávanie bezpečnostných kontrol je popísané v interných dokumentoch DTCA a I.CA.

6.8 Kontroly bezpečnosti počítačovej siete

Prostriedky vykonávajúce vlastné certifikačné služby nie sú priamo dostupné z verejnej siete Internet. Všetka komunikácia medzi RA DTCA a centrálnym pracoviskom certifikačnej autority je vedená šifrovane.

Ostatné aspekty kontroly bezpečnosti počítačovej siete s ohľadom na požiadavky ZoEP a príslušných vykonávacích vyhlášok sú popísané v interných dokumentoch DTCA a I.CA.

6.9 Kontroly bezpečnosti kryptografického modulu

Použitý kryptografický modul má stanovenú bezpečnosť podľa normy FIPS 140 na úrovni (*level*) 3. Periodické kontroly sú vykonávané za účelom zistenia, či kryptografický modul neustále spĺňa požiadavky definované vyžadovanou úrovňou zabezpečenia.

7 CERTIFIKAČNÉ PROFILY A PROFILY QCRL

7.1 Profil kvalifikovaného certifikátu

Profily certifikátov sú podľa ISO/IEC 9594-8. Navyiac tieto profily zodpovedajú doporučeniu RFC 3739, prípadne ETSI 101862.

Všetky kvalifikované certifikáty sú X.509 verzia 3 podľa ISO/IEC 9594-8.

Kvalifikované systémové certifikáty poskytovateľa v zmysle českého zákona č. 227/2000 Sb.

V kvalifikovaných systémových certifikátoch poskytovateľa (I.CA) sú použité nasledujúce **kritické** rozširujúce atribúty pre certifikáty verzie 3:

| | | |
|---------------------------|----------|----------------------------|
| Basic Constraints: | critical | CA:TRUE |
| Key Usage: | critical | Certificate Sign, CRL Sign |

Automaticky sú vkladané nasledujúce rozširujúce atribúty:

| | |
|---------------------------------|--|
| Subject Key Identifier | (identifikácia kľúča certifikačnej autority) |
| alebo | |
| Authority Key Identifier | (identifikácia kľúča certifikačnej autority) |

Používaným algoritmom je:

| | |
|-----------------------------|-----------------------|
| Signature Algorithm: | sha1WithRSAEncryption |
|-----------------------------|-----------------------|

Osobné kvalifikované certifikáty

V kvalifikovaných certifikátoch je použitý nasledujúci kritický rozširujúci atribút pre certifikáty verzie 3:

| | | |
|-------------------|----------|------------------------------|
| Key Usage: | critical | nonRepudiation (povinný) |
| | | digitalSignature (voliteľný) |
| | | keyEncipherment (voliteľný) |
| | | dataEncipherment (voliteľný) |

Atribút **Basic Constraints** nie je pre tieto certifikáty použitý.

Ďalej sú použité rozširujúce atribúty:

Subject Alternative Name: (je možné naplniť podľa požiadaviek klienta pri dodržaní zásad v kap. 3.1)

CRL Distribution Points:

URI: adresy distribučných bodov CRL

Automaticky sú vkladané nasledujúce rozširujúce atribúty:

Authority Key Identifier (identifikácia kľúča certifikačnej autority)

Subject Key Identifier (identifikácia kľúča klienta)

Kvalifikovaný certifikát DTCA obsahuje rozširujúci atribút „ICA Statements“, v ktorom je uvedené, že tento certifikát bol vydaný ako kvalifikovaný certifikát v zmysle zákona NR SR č. 215/2002 Z.z.

Používané algoritmy musia zodpovedať kap. 6.2.

Formy a obmedzenia mien

Atribút nameConstraints nie je použitý. Na identifikačné údaje subjektu (*Subject*) nie je žiadne obmedzenie s výnimkou obmedzení vyplývajúcich z kapitoly 3.1.

Ďalšiu výnimku tvorí použitie pseudonymu v rámci položky *Pseudonym*, kde nie sú povolené výrazy vulgárne, propagujúce fašizmus, rasovú a triednu nenávisť. O prípustnosti konkrétneho obsahu položky *Pseudonym* rozhoduje pracovník registračnej autority, ktorý vykonáva vybavovanie klientovej žiadosti na vydanie kvalifikovaného certifikátu. V prípade nesúhlasu môže žiadateľ postupovať podľa odstavca 2.4.

Formy mien a ďalšie obmedzujúce pravidlá na mená sú popísané v kapitole 3.1.

Identifikátory certifikačného poriadku

- id-ianaPrivate OBJECT IDENTIFIER ::= { 1 3 6 1 4 1 },
- id-pvt OBJECT IDENTIFIER ::= { id-ianaPrivate 6625 },
- id-ICA OBJECT IDENTIFIER ::= { id-pvt 1 },
- id-ica-cp OBJECT IDENTIFIER ::= { id-ICA 1 },
- id-ica-cp-qica OBJECT IDENTIFIER ::= { id-ica-cp 4 },
- id-cpqrca OBJECT IDENTIFIER ::= { id-ica-cp-qica 5 },
- id-cppqica OBJECT IDENTIFIER ::= { id-ica-cp-qica 6 },

Obsah rozšírenia CertificatePolicy je nasledujúci:

CertificatePolicy=

id-cppqica (Qualified Personal ICA CP OID)

- explicitText: Tento kvalifikovaný certifikát je vydaný v súlade so zákonom 227/2000Sb.

Syntax a sémantika pre kvalifikátory CP sa riadia RFC 3739.

Sémantika pre rozhodujúce rozšírenie vzťahujúce sa k certifikačnému poriadku nie je kritická.

7.2 Profil QCRL

Čísla verzií

Zoznam kvalifikovaných certifikátov, ktoré boli zrušené (QCRL) sú vydávané podľa RFC 3280, X509 vo verzii 2.

QCRL a rozšírenia položiek QCRL

I.CA pri vydávaní QCRL používa nasledujúce položky:

Signature Algorithm: sha1WithRSAEncryption

- Issuer -** má rovnaký obsah ako príslušný kvalifikovaný certifikát poskytovateľa, ktorého údaje pre vytváranie podpisu boli pri podpísaní v QCRL použité
- This Update -** čas vydania zoznamu zrušených kvalifikovaných certifikátov,
- Next Update -** predpokladaný čas vydania nasledujúceho zoznamu zrušených kvalifikovaných certifikátov.

Použité rozšírenia pre verziu 2 sú:

Authority Key Identifier: identifikácia kľúča certifikačnej autority

CRL Number: poradové číslo QCRL

Použité položky a rozšírenia pre položky zrušených certifikátov sú:

Revoked Certificates: vkladá sa sériové číslo zrušeného certifikátu

Revocation Date: vkladá sa čas zrušenia

8 RIADENIE ŠPECIFIKÁCIÍ

8.1 Procesy zmien špecifikácií

Tento Certifikačný poriadok bude jeden krát ročne, alebo podľa nutnosti, prehodnocovaný tak, aby bol v súlade s platným právom Slovenskej republiky a zároveň v súlade s dokumentom „Certifikačná politika pro vydávání osobních kvalifikovaných certifikátů“ I.CA, ako aj so všeobecne prijímanými štandardmi a normami.

8.2 Politiky zverejňovania a ohlasovania

Zverejňovanie Certifikačného poriadku DTCA sa uskutočňuje na oficiálnej WWW stránke DTCA – <http://www.dtca.sk>. Na požiadanie je možné zaslanie elektronickou poštou, prípadne za poplatok poštou na papierovom alebo inom fyzickom médiu a na všetkých registračných autoritách DTCA.

8.3 Proces schvaľovania základných materiálov

Certifikačný poriadok je schvaľovaný vedením DTCA. Pred týmto schválením nie je možné vykonávať akékoľvek zmeny v činnostiach, ktoré tento Certifikačný poriadok popisuje.

Uplatnené zmeny v Certifikačnom poriadku musia byť zverejnené pre tie subjekty, ktorých činnosť je týmto dokumentom upravená.

8.4 Platnosť a účinnosť

Certifikačný poriadok pre vydávanie kvalifikovaných certifikátov, verzia 1.03, nadobúda platnosť a účinnosť dňom 01.07.2005.