

První certifikační autorita, a.s.



Certifikačný poriadok I.CA

pre vydávanie komerčných certifikátov

Tento dokument je slovenskou verziou dokumentu
„Certifikační politika I.CA pro vydávání komerčních certifikátů“

Verzia 1.04

Obsah

1.	ÚVOD	3
1.1	VŠEOBECNÝ PREHĽAD	3
1.2	DEFINÍCIA POJMOV A SKRATIEK	3
1.3	PROSTREDIE A APLIKOVATEĽNOSŤ	6
1.4	CERTIFIKÁTY	6
1.5	KONTAKTNÉ INFORMÁCIE	7
2.	VŠEOBECNÉ USTANOVENIA	7
2.1	POVINNOSTI STRÁN	7
2.2	ZODPOVEDNOSŤ A ZÁRUKY	9
2.3	FINANČNÁ ZODPOVEDNOSŤ	10
2.4	VÝKLAD A VÝKONNÉ MECHANIZMY	10
2.5	POPLATKY	10
2.6	UVEREJŇOVANIE A UCHOVÁVANIE INFORMÁCIÍ	10
2.7	AUDIT	11
2.8	DÔVERNOSŤ	12
2.9	COPYRIGHT	13
3.	IDENTIFIKÁCIA A AUTENTIZÁCIA	13
3.1	PRVOTNÁ REGISTRÁCIA	13
3.2	POSTUP PRI VYDANÍ NÁSLEDNÉHO CERTIFIKÁTU	18
3.3	ŽIADOSŤ O ZRUŠENIE CERTIFIKÁTU	18
4.	OPERAČNÉ POŽIADAVKY	19
4.1	ŽIADOSŤ O CERTIFIKÁT	19
4.2	VYDANIE CERTIFIKÁTU	19
4.3	AKCEPTOVANIE CERTIFIKÁTU	20
4.4	ZRUŠENIE CERTIFIKÁTU	20
4.5	POŽIADAVKY NA OVEROVANIE CRL	21
4.6	PROCEDÚRY AUDITU VZHLADOM NA BEZPEČNOSŤ	21
4.7	VÝMENA PÁROVÝCH ÚDAJOV I.CA	22
4.8	ODHALENIE KOMPROMITÁCIÍ A NEHÔD	22
4.9	UKONČENIE ČINNOSTI I.CA	22
5.	FYZICKÉ, PROCEDURÁLNE A PERSONÁLNE BEZPEČNOSTNÉ MECHANIZMY	23
6.	TECHNICKÁ BEZPEČNOSŤ	23
6.1	GENEROVANIE PÁROVÝCH DÁT KLIENTA A INŠTALÁCIA	23
6.2	OCHRANA SÚKROMNÉHO KĽÚČA I.CA	24
6.3	ĎALŠIE POŽIADAVKY NA SPRÁVU PÁROVÝCH DÁT I.CA	25
6.4	BEZPEČNOSŤ POČÍTAČOVÉHO VYBAVENIA	25
6.5	KONTROLY POČÍTAČOVEJ BEZPEČNOSTI	25
6.6	BEZPEČNOSTNÉ KONTROLY PO DOBU ŽIVOTNOSTI	25
6.7	KONTROLY BEZPEČNOSTI POČÍTAČOVEJ SIETE	25
6.8	KONTROLY BEZPEČNOSTI KRYPTOGRAFICKÉHO MODULU	26
7.	CERTIFIKAČNÉ PROFILY A PROFILY CRL	26
7.1	PROFIL CERTIFIKÁTU	26
7.2	PROFIL CRL	26
8.	RIADENIE ŠPECIFIKÁCIÍ	27
8.1	PROCESY ZMIEN ŠPECIFIKÁCIÍ	27
8.2	POLITIKY ZVEREJŇOVANIA A OHLASOVANIA	27
8.3	PROCES SCHVAĽOVANIA ZÁKLADNÝCH MATERIÁLOV	27

1. ÚVOD

Tento dokument predstavuje Certifikačný poriadok (ďalej tiež CP) platný pre První certifikační autoritu, a.s. (ďalej tiež I.CA).

Tento Certifikačný poriadok sa zaoberá skutočnosťami, ktoré sa vzťahujú na I.CA, žiadateľov, klientov, používateľov a zmluvných partnerov, a ktoré súvisia s vydávaním certifikátov, s ich ďalšou správou, použitím, akceptovaním a všetkými aspektmi súvisiacimi s nakladaním s párovými údajmi.

Poznámka pre slovenskú verziu tohto dokumentu:

Certifikačné služby spoločnosti První certifikační autorita, a.s., ktorá je akreditovaným poskytovateľom certifikačných služieb v Českej republike aj v Slovenskej republike, poskytuje na Slovensku spoločnosť D. Trust Certifikačná Autorita, a.s., Plynárska 7/C, 821 09 Bratislava, IČO 35 840 005.

1.1 VŠEOBECNÝ PREHĽAD

Certifikačný poriadok zodpovedá požiadavkám stanoveným v RFC 2527, s prihliadnutím na doporučená orgánov EÚ a na právo SR v danom odbore.

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

- zákona Českej republiky č. 227/2000 Sb. o elektronickom podpise a o zmene niektorých ďalších zákonů, resp. zákona Slovenskej republiky č.215/2002 Z.z. o elektronickom podpise a o zmene a doplnení niektorých zákonov (ďalej tiež ZoEP);
- RFC 2527 – Internet X.509 Public Key Infrastructure – Certificate Policy and Certification Practices Framework (ďalej tiež RFC 2527);
- 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);

1.2 DEFINÍCIA POJMOV A SKRATIEK

Ďalej 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.

NBÚ – Národný bezpečnostný úrad;

ÚOOÚ – Úrad na ochranu osobných údajov;

I.CA – Certifikačná autorita I.CA predstavuje súhrn technických a organizačných prostriedkov, ktoré umožňujú I.CA vystupovať ako poskytovateľ certifikačných služieb;

CA – centrálné pracovisko Certifikačnej autority I.CA;

VSRA – Vlastná stacionárna registračná autorita Certifikačnej autority I.CA

- a) VSRA sú základnými decentralizovanými zložkami výkonného aparátu I.CA.
- b) VSRA je určená hlavne na to, aby plnila funkciu podateľne.
- c) VSRA prijíma žiadosti o služby podľa certifikačného poriadku I.CA a plní všetky ďalšie úlohy I.CA vyplývajúce z jej vzťahu ku klientom, hlavne prijíma žiadosti o vydanie certifikátov, sprostredkováva odovzdanie certifikátov a CRL, 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 I.CA, ktorý ho potvrdí, zruší alebo zmení.
- e) VSRA je splnomocnená uzatvárať s klientmi I.CA zmluvy o vydaní a používaní certifikátov I.CA.
- f) VSRA zabezpečuje spoplatňovanie služieb I.CA, pokiaľ nie je stanovené zmluvou inak.

VMRA – Vlastná mobilná registračná autorita Certifikačnej autority I.CA

- a) VMRA sú zvláštnymi decentralizovanými mobilnými zložkami výkonného aparátu I.CA.
- b) VMRA je určená hlavne na to, aby plnila funkciu podateľne v mieste mimo umiestnenia VSRA, spravidla na základe individuálnej zmluvy medzi klientom a I.CA.
- c) VMRA prijíma žiadosti o služby podľa certifikačného poriadku I.CA a individuálne zmluvy medzi klientom a I.CA a plní všetky ďalšie úlohy I.CA vyplývajúce zo vzťahu ku klientom. Hlavne prijíma žiadosti o certifikáty, sprostredkováva odovzdanie certifikátov a CRL, poskytuje potrebné informácie klientom, vybavuje ich reklamácie a pod.
- d) VMRA je splnomocnená uzatvárať s klientmi I.CA zmluvy o vydaní a používaní certifikátov I.CA.
- e) VMRA zabezpečuje spoplatňovanie služieb I.CA, 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 riaditeľovi I.CA, ktorý ho potvrdí, zruší alebo zmení.

ZSRA – Zmluvná stacionárna registračná autorita Certifikačnej autority I.CA. Plní obdobné funkcie ako VSRA na základe písomnej zmluvy medzi I.CA a majiteľom ZSRA;

ZMRA – Zmluvná mobilná registračná autorita Certifikačnej autority I.CA. Plní obdobné funkcie ako VMRA na základe písomnej zmluvy medzi I.CA a majiteľom ZMRA;

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

Zmluvný partner – subjekt, ktorý zabezpečuje na základe písomnej zmluvy pre I.CA certifikačné služby alebo ich časti. Najčastejšie ide o zmluvné registračné autority. Na subjekt môže byť výslovným ustanovením príslušnej zmluvy prenesená pôsobnosť na uzatváranie ďalších zmlúv s ich klientmi a zodpovednosť za vydávanie certifikátov týmto klientom podľa Certifikačného poriadku I.CA;

Certifikát – elektronický dokument vydaný certifikačnou autoritou, ktorý spája údaje na overovanie elektronických podpisov s podpisujúcim subjektom a umožňuje overiť jeho totožnosť;

Následný certifikát – certifikát, ktorý bol v súlade so zmluvou uzatvorenou medzi klientom a I.CA vydaný klientovi na základe novej žiadosti o vydanie certifikátu, podpísanej platnými údajmi na vytváranie elektronických podpisov súvisiacimi s už vydaným certifikátom, ku ktorému je vydávaný tento následný certifikát. Údaje overované I.CA musia byť rovnaké. Údaje na overovanie elektronických podpisov musia byť iné. Ostatné položky následného certifikátu podliehajú aktuálnym pravidlám pre vydávanie certifikátov;

Testovací certifikát – certifikát, ktorý slúži len na overovanie funkčnosti;

Verejný kľúč – dáta na overovanie elektronického podpisu;

Súkromný kľúč – dáta na vytváranie elektronického podpisu;

Párové dáta – dáta na vytváranie elektronického podpisu spolu s prislúchajúcimi dátami na overovanie elektronického podpisu;

CRL (Certificate Revocation List) – zoznam certifikátov I.CA, ktoré boli zrušené;

Počítačová transakcia – elektronická výmena počítačových údajov medzi dvoma subjektami s využitím výpočtovej techniky;

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

Klient – fyzická alebo právnická osoba, ktorá uzatvorila zmluvu o využívaní služieb I.CA s prevádzkovateľom jej služieb;

Držiteľ – klient, ktorý má párové údaje a ktorému I.CA na údaje na overovanie elektronického podpisu vydala certifikát;

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

Žiadosť o certifikát – formálny, štandardný dokument elektronickej žiadosti o certifikát podľa prípustných noriem a smerníc definovaných v tomto Certifikačnom poriadku I.CA;

Používateľ – subjekt používajúci pri svojej činnosti vlastné certifikáty alebo certifikáty iných subjektov vydaných I.CA;

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

Zablokovanie certifikátu – stav, v ktorom sa certifikát nachádza od doby, kedy I.CA prostredníctvom I.CA obdržala požiadavku na jeho zrušenie, do doby zaradenia tohto certifikátu do zoznamu zrušených certifikátov. Certifikát je počas doby zablokovania stále platný;

Zrušený certifikát – certifikát, u ktorého bola predčasne ukončená platnosť bez možnosti obnovenia tejto platnosti.

1.3 PROSTREDIE A APLIKOVATEĽNOSŤ

I.CA prevádzkuje koreňovú certifikačnú autoritu. I.CA nezriaďuje, ani nepodporuje podriadené certifikačné autority vydávajúce certifikáty.

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

Poskytovanie služieb I.CA sa realizuje prostredníctvom registračných autorít. RA sú buď vlastné alebo RA zmluvných partnerov.

1.4 CERTIFIKÁTY

Týmto Certifikačným poriadkom sa riadi vydávanie nasledujúcich druhov certifikátov :

- **osobné certifikáty** – certifikáty určené ako osobné pre použitie v oblasti elektronickej pošty, vytvárania podpisu a/alebo šifrovania, pre klientskú autentizáciu v rámci bezpečných protokolov. Tieto certifikáty sú vydávané v súlade s nižšie uvedenými pravidlami.
- **certifikáty pre servery** – certifikáty pre použitie v serverových aplikáciách (bezpečné protokoly – autentizácia a/alebo šifrovanie). Tieto certifikáty sú vydávané v súlade s nižšie uvedenými pravidlami.
- **testovacie certifikáty** – certifikáty určené na oboznámenie sa s technológiou a jej využitím. Testovacie certifikáty majú obmedzenú platnosť 14 dní, nie sú uvádzané v zoznamoch vydaných certifikátov, nie je možné ich revokovať a za ich použitie nenesie I.CA žiadnu zodpovednosť.

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

Certifikáty, ktoré vydáva I.CA klientom, môžu byť používané v aplikáciách pre nasledujúce účely :

- zabezpečenie integrity údajov
- zabezpečenie nepopierateľnosti zodpovednosti
- zabezpečenie dôvernosti údajov
- určenie zdieľaného tajomstva (kľúča) v rámci protokolu pre bezpečnú výmenu údajov
- priame šifrovanie a dešifrovanie údajov
- priame podpisovanie údajov.

Certifikáty I.CA sú komerčne ponúkanou službou a sú prístupné každému, kto sa zmluvne zaviazal konať podľa Certifikačného poriadku I.CA.

V prípade fyzickej osoby môže byť klientom iba osoba, ktorá je oprávnená na právne úkony podľa príslušnej legislatívnej normy. Pokiaľ žiadateľ nepožaduje služby RA priamo pre seba, ale zastupuje inú osobu, musí mať oprávnenie túto osobu zastupovať.

V prípade právnickej osoby, táto musí byť zastupovaná fyzickou osobou, ktorá má na toto zastupovanie poverenie.

1.5 KONTAKTNÉ INFORMÁCIE

Základnou adresou, na ktorej je možné nájsť informácie o I.CA, prípadne odkazy na zistenie ďalších informácií, je URL adresa:

<http://www.ica.cz>

Elektronická poštová adresa, ktorá slúži ako kontakt klienta s I.CA, je :

oper@ica.cz, info@ica.cz.

Tieto kontaktné informácie je povinná I.CA a jej zmluvní partneri zverejniť vo svojich certifikačných poriadkoch a na svojich pracoviskách. Pracovníci I.CA a zmluvných partnerov sú taktiež povinní tieto informácie na požiadanie poskytnúť všetkým používateľom.

V prípade, že dôjde ku zmene kontaktných údajov, sú I.CA a jej zmluvní partneri povinní túto skutočnosť zohľadniť v príslušných certifikačných poriadkoch.

Použitie certifikátov vydaných I.CA sa riadi týmto Certifikačným poriadkom I.CA. Tento Certifikačný poriadok I.CA sa zverejňuje na internetových stránkach I.CA a je tiež k dispozícii v tlačenej podobe na RA. Akékoľvek otázky, týkajúce sa jej interpretácie je nutné smerovať na vyššie uvedenú elektronickú poštovú adresu, ktorá slúži na kontakt klienta s I.CA.

Zmluvní partneri I.CA môžu prijať tento Certifikačný poriadok I.CA, alebo zverejniť vlastný. V prípade, že zverejnia vlastný certifikačný poriadok, musí byť v súlade s týmto Certifikačným poriadkom I.CA.

2. VŠEOBECNÉ USTANOVENIA

2.1 POVINNOSTI STRÁN

Subjektami, ktoré podliehajú tomuto CP sú certifikačná autorita I.CA. I.CA nezriaďuje ani nepodporuje podriadené certifikačné authority (viď článok 1.3).

Všetky subjekty, ktoré pri svojej činnosti používajú alebo využívajú certifikáty vydané I.CA, prípadne poskytujú, používajú alebo využívajú služby I.CA spojené so správou certifikátov, sú povinné dodržiavať legislatívne normy platné v ČR, resp. v SR.

Všetky subjekty, ktoré pri svojej činnosti používajú alebo využívajú certifikáty vydané I.CA v súlade s týmto CP, prípadne poskytujú, používajú alebo využívajú služby I.CA spojené so správou certifikátov vydaných v súlade s týmto CP, sú povinné dodržiavať tento Certifikačný poriadok I.CA.

Povinnosti I.CA

I.CA je povinná dodržiavať príslušné ustanovenia legislatívnych noriem, ktoré upravujú oblasť poskytovania certifikačných služieb alebo obchodnú činnosť s týmto spojenú. Ďalej je I.CA povinná riadiť sa vlastnými dokumentmi, ktoré vydáva. I.CA je taktiež povinná vytvárať dokumenty, ktoré upravujú činnosť zmluvných partnerov, zabezpečovať ich zverejnenie a dohliadať na ich dodržiavanie.

Povinnosti RA

Registračné authority sú povinné riadiť sa dokumentmi, ktoré vydáva I.CA, a ktoré upravujú ich činnosť (hlavne Certifikačný poriadok I.CA, Pravidlá na výkon certifikačných činností, Smernice pre pracovníkov RA, atď.).

Povinnosti držiteľov a používateľov certifikátov I.CA

Držiteľia certifikátov sú povinní :

- používať certifikáty vydané I.CA výhradne v súlade s príslušným Certifikačným poriadkom I.CA;
- dodržiavať všetky ustanovenia Certifikačného poriadku I.CA;
- dodržiavať všetky ustanovenia príslušnej zmluvy, ak bola zmluva podpísaná.

Držiteľ certifikátu, ktorý nedodržiava či nedodržel svoje povinnosti, nemá nárok na prípadnú náhradu škody.

Povinnosti používateľov certifikátov vydaných I.CA

Používatelia certifikátov sú všetky subjekty, ktorí používajú certifikáty vydané I.CA. Používatelia sú povinní používať certifikáty v súlade s certifikačným poriadkom platným pre tieto certifikáty, hlavne

- kontrolovať platnosť certifikátu
- presvedčiť sa o dôveryhodnosti certifikačnej authority, ktorá certifikát vydala.

Používateľ certifikátu, ktorý nedodržiava či nedodržel svoje povinnosti, nemá nárok na prípadnú náhradu škody. I.CA a zmluvní partneri sú povinní upozorniť na povinnosti používateľov zverejniť prostredníctvom svojich kontaktných adries.

Povinnosti skladov certifikátov vydaných I.CA

I.CA za účelom poskytovania certifikačných služieb zriaďuje sklady certifikátov. I.CA zverejňuje nasledujúce informácie o certifikátoch :

- informácie o vydaných certifikátoch vrátane odkazov, na ktorých je možné požadovaný certifikát získať. Výnimkou sú osobné alebo serverové certifikáty, u ktorých si klient vyhradil, že nebudú zverejňované.
- informácie o certifikátoch, ktoré boli zrušené, vrátane odkazov, na ktorých je možné získať aktuálne alebo archívne zoznamy zrušených certifikátov.

I.CA periodicky aktualizuje zoznam vydaných certifikátov, doba od vydania certifikátu do jeho zverejnenia nesmie presiahnuť 2 hodiny. Odkazy, na ktorých je možné požadovaný certifikát získať, zverejňuje I.CA na svojej WWW kontaktnej adrese (článok 1.5).

I.CA periodicky aktualizuje zoznam zrušených certifikátov. Za týmto účelom I.CA vydáva aktuálny zoznam zrušených certifikátov najmenej raz za 24 hodín. Odkazy, na ktorých je možné požadovaný zoznam zrušených certifikátov získať, zverejňuje I.CA na svojej WWW kontaktnej adrese (článok 1.5).

2.2 ZODPOVEDNOSŤ A ZÁRUKY

Zodpovednosť a záruky poskytované I.CA

I.CA poskytuje záruku na správnosť použitia vlastného súkromného kľúča prislúchajúceho k vlastnému certifikátu pri podpisovaní osobných certifikátov a certifikátov pre servery. Na podpisovanie testovacích certifikátov sa záruka neposkytuje.

I.CA poskytuje záruky na jedinečnosť sériového čísla ňou vydaných osobných certifikátov a certifikátov pre servery.

I.CA poskytuje záruku na použitie osobných certifikátov pri obchodných transakciách, ktorých hodnota nepresahuje hodnotu uvedenú v príslušných obmedzeniach, pokiaľ boli dodržané zodpovedajúce ustanovenia Certifikačného poriadku I.CA.

Všetky záruky a z nich plynúce plnenia je možné uznať len vtedy, pokiaľ klient neporušil povinnosti vyplývajúce mu zo zmluvy, prípadne z Certifikačného poriadku I.CA.

Vždy platí limit záruky, ktorý bol dohodnutý v písomnej podobe (zmluva o poskytnutí služieb). Pokiaľ bola výška nárokovanej straty vyššia ako dohodnutý limit, poskytuje I.CA plnenie maximálne do výšky limitu. Pokiaľ bolo zistené porušenie povinností klienta, ktoré má súvislosť s uvedenou škodou, záručné plnenie sa neposkytuje. S touto skutočnosťou bude klient oboznámený.

Klient uplatňuje záruku vždy u subjektu, ktorý ho zaregistroval.

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

Na používanie certifikátu, ktorého držiteľ nie je klientom I.CA sa záruky nevzťahujú.

Zodpovednosť RA

RA nesie zodpovednosť za správne vybavenie žiadostí o poskytovanie certifikačných služieb. RA nevybaví kladne žiadosť, pokiaľ klient hodnoverným spôsobom nepreukázal svoju totožnosť alebo odmieta poskytnúť potrebné údaje.

RA ďalej zodpovedá za včasné vybavenie oprávnených žiadostí o zrušenie certifikátov.

RA rovnako zodpovedá za vysporiadanie pripomienok a sťažností klientov.

2.3 FINANČNÁ ZODPOVEDNOSŤ

V prípade, že I.CA vznikne akákoľvek škoda v priamej či nepriamej súvislosti s konaním držiteľov alebo používateľov certifikátov I.CA, je I.CA oprávnená príslušnú udalosť vyšetriť.

Pokiaľ bude vyšetrovaním zistené, že zistené skutočnosti zakladajú nárok na kompenzáciu zo strany držiteľa alebo používateľa certifikátu, bude táto kompenzácia vyžadovaná od príslušného subjektu, v súlade s príslušnými ustanoveniami obchodného zákonníka.

Vzťah medzi I.CA ako poskytovateľa certifikačných služieb a klientmi je striktne určený zmluvou. I.CA nevystupuje v žiadnom prípade ako splnomocnenec alebo iný zástupca klientov. To isté platí pre zmluvných partnerov.

2.4 VÝKLAD A VÝKONNÉ MECHANIZMY

Právny výkon v súvislosti s týmto Certifikačným poriadkom I.CA sa riadi príslušnými legislatívnymi ustanoveniami ČR, resp. SR. Akékoľvek zmeny v tomto Certifikačnom poriadku I.CA nesmú byť v protiklade so zákonmi ČR, resp. SR.

Právo výkladu tohto Certifikačného poriadku prináleží I.CA. V prípade akýchkoľvek zmien, ktoré majú za následok neplatnosť niektorého z článkov tohto CP, ostatné články zostávajú v platnosti do vydania nového CP. Do tej doby sa taktiež bude vymáhať zodpovednosť za dodržiavanie tohto CP v platných článkoch. Výklad platnosti v prechodnom období je právom I.CA.

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 I.CA (nutné písomné podanie);
- vedenie I.CA (nutné písomné podanie a zloženie dohodnutej finančnej istiny, ktorá je vrátená v prípade kladného vybavenia sťažnosti).

Pokiaľ ani na poslednej inštancii nie je niektorá zo strán spokojná s rozhodnutím, môže sa obrátiť na nezávislý súd.

2.5 POPLATKY

Poplatky za služby spojené s vydávaním a správou certifikátov sú uvedené v Cenníku služieb I.CA. Aktuálny cenník je uverejnený na adrese www.ica.cz.

2.6 UVEREJŇOVANIE A UCHOVÁVANIE INFORMÁCIÍ

I.CA poskytuje informácie o tomto CP a o prípadných zmenách súvisiacich s poskytovaním služieb spojených s vydávaním a správou certifikátov na adrese www.ica.cz a taktiež prostredníctvom svojich registračných autorít.

I.CA uverejňuje certifikáty I.CA tak, aby boli k dispozícii všetkým používateľom. Tieto certifikáty uverejňuje na svojich stránkach najmenej 24 hodín pred nadobudnutím ich platnosti.

I.CA taktiež uverejňuje statut svojich vlastných certifikátov. Pri zmene statutu svojich certifikátov oznámi I.CA túto skutočnosť neodkladne prostredníctvom svojich WWW stránok, najneskôr však do 2 hodín.

Prístup k informáciám I.CA

Protokoly povolené pre prístup k informáciám o CP sú :

- HTTP.

Protokoly povolené pre prístup k informáciám o certifikátoch sú :

- HTTP.

Protokoly povolené pre prístup k informáciám o zrušených certifikátoch sú :

- HTTP.

Okrem vyššie uvedených protokolov môžu byť rozhodnutím riaditeľa I.CA informácie zverejňované prostredníctvom ďalších protokolov.

2.7 AUDIT

Audit sa prevádza z rozhodnutia I.CA alebo z rozhodnutia oprávneného štátneho orgánu. Dotknuté subjekty sú povinné audítorom umožniť prístup ku všetkým skutočnostiam, ktoré majú vzťah k službám poskytovania a správy certifikátov. V prípade, že ide o audit z rozhodnutia I.CA, táto menuje a odvoláva audítorov.

Audit má za úlohu vyhodnotiť zhodu činnosti subjektu s Certifikačným poriadkom I.CA a ďalšími dokumentmi, ktoré upravujú činnosť subjektu podľa zmluvy s I.CA..

Periódou vykonávania auditu a kontroly sú najmenej:

- 2 x ročne priebežný audit
- 1 x ročne hĺbkový audit
- nepravidelný audit podľa rozhodnutia I.CA.

Kvalifikácia audítora je zabezpečená splnením nasledujúcich kritérií :

- znalosti v príslušnom odbore (napr. zaradenie do zoznamu audítorov ÚOOÚ ČR pre oblasť elektronického podpisu),
- nezávislosť na audítovanom subjekte,
- vyhovenie interným kritériám audítovaného subjektu (napr. bezpečnostná previerka),
- nesmie vykonávať audit toho istého subjektu v dvoch po sebe nasledujúcich termínoch.

Zabezpečenie splnenia uvedených požiadaviek je povinnosťou I.CA.

V prípade, že ide o audit z rozhodnutia I.CA, táto špecifikuje témy zahŕňajúce audit.

2.8 DÔVERNOSŤ

Chránenými informáciami I.CA sú:

- údaje na vytváranie elektronických podpisov prislúchajúce k údajom na overovanie elektronických podpisov obsiahnutých vo vlastných certifikátoch I.CA;
- ostatné kryptograficky podstatné informácie slúžiace na prevádzku I.CA;
- všetky osobné údaje klientov či používateľov podliehajúce ochrane v zmysle príslušnej zákonnej normy (zákon č. 101/2000 Sb. o ochrane osobných údajů a o zméne některých zákonů, resp. č. 428/2002 Z.z. o ochrane osobných údajov).

Chránenými informáciami jednotlivých RA sú:

- údaje na vytváranie elektronických podpisov prislúchajúce k údajom na overovanie elektronických podpisov obsiahnutých vo vlastných certifikátoch RA;
- ostatné kryptograficky podstatné informácie slúžiace na prevádzku RA;
- všetky osobné údaje klientov či používateľov podliehajúce ochrane v zmysle príslušnej zákonnej normy (zákon č. 101/2000 Sb. resp. č. 428/2002 Z.z.)

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

Za citlivé sa nepovažujú typy informácií, ktoré nie sú v tomto článku uvedené a boli označené ako verejné.

Sprístupenie informácií o zrušení certifikátov

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

Sprístupenie informácií orgánom činným v trestnom konaní a iným tretím stranám

I.CA poskytne tretej strane informácie označené ako citlivé iba na základe rozhodnutia súdu. Ďalej I.CA poskytne citlivé informácie orgánom činným v trestnom konaní iba na základe právoplatného rozhodnutia príslušného štátneho zástupcu, a to iba na základe písomnej žiadosti vybavenej všetkými náležitosťami.

Sprístupenie informácií na základe občianskeho konania

I.CA poskytne tretej strane informácie označené ako citlivé na základe ukončeného občianskeho konania (napr. pozostalým po zomretom vlastníkovi certifikátu). V týchto prípadoch sa I.CA riadi príslušnými ustanoveniami zákona. Konkrétne hodnoty údajov na vytváranie elektronických podpisov slúžiacich na podpisovanie certifikátov a CRL neposkytne nikomu.

Sprístupenie na základe požiadavky držiteľa certifikátu

V prípade požiadavky držiteľa certifikátu na sprístupenie určených informácií súvisiacich s klientom a jeho certifikátom tretej strane, vykoná I.CA po kontrole vlastníckeho práva k certifikátu a na jeho písomnú žiadosť.

Ostatné okolnosti sprístupnenia informácií

V ostatných prípadoch tretím stranám citlivé informácie I.CA zásadne neposkytuje.

2.9 COPYRIGHT

Všetky autorské práva k tomuto Certifikačnému poriadku prináležia I.CA.

3. IDENTIFIKÁCIA A AUTENTIZÁCIA

3.1 PRVOTNÁ REGISTRÁCIA

I.CA prijíma žiadosti o vydanie certifikátu podľa nasledujúcich štandardov :

- PKCS # 10 (verzia 1.7. a nižšia)
- SPKAC

Žiadosti sú prijímané vo formáte PEM.

V súlade s požiadavkami noriem radu X.500 sú povinné položky pre jednotlivé typy žiadosti o certifikáty stanovené nasledovne:

- žiadosť o testovací certifikát
 - všeobecné meno (CN)
 - adresa elektronickej pošty (E)
 - krajina (C)
- žiadosť o certifikát pre server
 - všeobecné meno (CN)
 - krajina (C)
- žiadosť o osobný certifikát
 - všeobecné meno (CN)
 - adresa elektronickej pošty (E)
 - krajina (C)

Položka „adresa elektronickej pošty (E)“, je pre žiadosť o testovací certifikát alebo osobný certifikát povinná len v prípade, ak ide o žiadosť o certifikát, ktorý má byť používaný pre komunikáciu elektronicou poštou.

Pre všetky typy žiadosti je stanovený obsah položky krajina (C) takto:

- položka C (krajina) môže obsahovať len kód štátu, v ktorom má žiadateľ trvalý pobyt
- kód štátu musí zodpovedať norme ISO 3166.

Žiadosť o certifikát musí spĺňať nasledujúce podmienky:

- smie obsahovať iba povolené znaky (0x20 – 0x7E)
- musí obsahovať všetky povinné položky pre daný typ žiadosti o certifikát
- musí spĺňať ďalšie požiadavky kladené na položky a mená pre daný typ žiadosti o certifikát.

Podľa typu žiadosti o certifikát sú na jej položky a mená kladené nasledujúce požiadavky :

Žiadosť o certifikát pre server

- **všeobecné meno (CN)** – spravidla by malo obsahovať doménové meno servera. Pokiaľ budú vo všeobecnom mene uvedené iné skutočnosti (meno fyzickej osoby, obchodné meno, registrovaná známka a pod.), musia byť takéto údaje overené, pokiaľ to uvedené skutočnosti vyžadujú.

Žiadosť o osobný certifikát

- **všeobecné meno (CN)** – musí prislúchať niektorému z oficiálnych mien osoby alebo organizácie. Prípustné hodnoty sú:
 - pre fyzické osoby meno a priezvisko, dodatok obchodného mena (v prípade, že ho fyzická osoba preukáže)
 - pre právnické osoby obchodné meno (v prípade, že ho právnická osoba preukáže)

Uvedené hodnoty môžu byť doplnené dodatkom, ktorý si žiadateľ zvolí. Dodatok nesmie popierať vlastný názov, nesmie byť eticky nevhodný. V prípade, že dodatok tvoria skutočnosti, ktoré vyžadujú overenie, musí byť tak vykonané (registrovaná známka a pod.). Pokiaľ nie je možné niektorú zo skutočností týkajúcich sa všeobecného mena overiť, nie je možné žiadosť prijať.

- **elektronická adresa (E)** – pokiaľ je to možné, musí byť overené, že žiadateľ je vlastníkom alebo používateľom predmetnej elektronickej adresy. Pokiaľ to možné nie je, musí byť táto skutočnosť zahrnutá do zmluvy a je nutné požadovať od žiadateľa písomné potvrdenie správnosti.

Rozhodnutím riaditeľa I.CA môže byť množina používaných položiek rozšírená. Spôsob ich vyplňania a používania stanovuje I.CA.

V prípade, že došlo ku zmene údajov, ktoré boli podkladom pre vydanie certifikátu a podliehajú overeniu pracovníkom RA, je držiteľ certifikátu povinný požiadať o zrušenie certifikátu z dôvodu zmeny údajov. V prípade, že v takomto prípade klient požiada o vydanie nového certifikátu, môže mu byť poskytnutá zľava podľa obchodných podmienok I.CA.

Jednoznačnosť mien a riešenie kolízií

V prípade testovacieho certifikátu sa kontrola jednoznačnosti mien nevykonáva.

V prípade osobného certifikátu musia jednoznačnosť mena v rámci certifikátov I.CA zabezpečovať položky **CN** (všeobecné meno), **E** (elektronická adresa) – pokiaľ je uvedená, a **C** (krajina/štát). Registračná autorita je povinná prostredníctvom služieb I.CA zistiť, či žiadateľom uvedené meno nebolo v rámci vydaných certifikátov už použité.

V prípade certifikátu pre server musia jednoznačnosť mena zabezpečovať položky **CN** (všeobecné meno) a **C** (krajina/štát). Registračná autorita je povinná prostredníctvom služieb I.CA zistiť, či žiadateľom uvedené meno nebolo v rámci vydaných certifikátov už použité.

V prípade, že žiadateľom požadované meno je už obsiahnuté vo vydanom certifikáte, registračná autorita vyzve žiadateľa ku zmene, prípadne doplneniu mena. Žiadateľ je povinný túto zmenu uskutočniť. Pokiaľ tak odmietne vykonať, žiadosť sa neprijme. I.CA nie je sprostredkovateľom pri riešení eventuálnych súdnych alebo iných sporov.

Ochranné známky

I.CA uznáva iba tie ochranné známky, ktorých vlastníctvo alebo prenájom žiadateľ doložil. Autentizáciu ochranných známk inými spôsobmi I.CA nevykonáva. Ochranná známka môže byť súčasťou Všeobecného mena (CN).

Všetky dôsledky vyplývajúce z neoprávneného používania ochrannej známky nesie žiadateľ.

Preukazovanie vlastníctva súkromného kľúča

Žiadateľ je povinný preukázať vlastníctvo súkromného kľúča, pokiaľ požaduje vystavenie certifikátu, ktorého súčasťou je prislúchajúci verejný kľúč.

Žiadateľ preukazuje vlastníctvo súkromného kľúča určeného k podpisovaniu podpísaním určenej časti žiadosti pomocou predmetného súkromného kľúča.

Preukazovanie totožnosti fyzickej osoby a osôb oprávnených za ňu konať

Pri registrácii nového žiadateľa – fyzickej osoby sa vyžaduje:

- a) predloženie platného osobného dokladu žiadateľa (občiansky preukaz alebo cestovný pas)
- b) právna spôsobilosť žiadateľa (plnoletosť, svojprávnosť)
- c) doklady preukazujúce právo žiadateľa konať za inú (fyzickú alebo právnickú) osobu ako zástupcu na základe úradne overenej plnej moci.

Preukazovanie totožnosti právnickej osoby a fyzických osôb oprávnených za ňu konať

Pri registrácii klienta – právnickej osoby sa vyžaduje:

- a) predloženie úradného dokladu, ktorý preukazuje legálnu existenciu právnickej osoby (väčšinou výpis z obchodného registra alebo iného zákonom predpísaného registra – nesmie byť starší ako 3 mesiace) a určuje fyzické osoby, ktoré sú oprávnené za danú právnickú osobu konať a uzatvárať záväzky (podpisovať)
- b) preukázanie totožnosti fyzických osôb, ktoré konajú za danú právnickú osobu a spôsob, akým za právnickú osobu konajú a podpisujú
- c) pokiaľ za právnickú osobu nekoná osoba, ktorá je na to oprávnená (napr. podľa zápisu v obchodnom registri), ale iná poverená osoba, musí byť na konanie na RA vybavená platnou a úradne overenou písomnou plnou mocou. Táto osoba musí byť podľa tejto plnej moci riadne identifikovateľná.

Prehľad ďalších druhov dokladov, ktorými sa preukazujú právnické osoby :

- d) v mene obce jedná zvyčajne starosta, resp. primátor. U starostu alebo primátora sa nevyžaduje, aby mal písomné poverenie zastupiteľstva. Ak však jedná za obec iná osoba, musí takéto poverenie mať. Starosta alebo primátor sa preukazuje mimo svojich osobných dokladov taktiež osvedčením o zvolení za starostu alebo primátora, ktoré vydala príslušná volebná komisia.
- e) ďalšie právnické osoby, ktoré vznikli zo zákona, konajú v zastúpení svojimi štatutárnymi orgánmi (napr. generálny riaditeľ, riaditeľ). Pracovník RA môže požadovať od žiadateľa, aby mu preukázal, na základe ktorého zákonného ustanovenia bola daná právnická osoba zriadená a kto je jej štatutárnym orgánom, a tieto skutočnosti doložil¹.
- f) právnické osoby, ktoré sú podnikateľskými subjektami, t.j. obchodné spoločnosti (verejné obchodné spoločnosti, komanditné spoločnosti, spoločnosti s ručením obmedzeným, zahraničné právnické osoby, akciové spoločnosti), družstvá, štátne podniky, niektoré príspevkové organizácie a pod., predkladajú ako doklad o svojej legálnej existencii výpis z obchodného registra. Pracovník RA odmietne výpis z obchodného registra starší ako 3 mesiace².

Pre niektoré typy právnických osôb platí :

- fa) u verejnej obchodnej spoločnosti za ňu môže konať a podpisovať každý zo spoločníkov, pokiaľ nie je vo výpise z obchodného registra uvedené inak
- fb) u komanditnej spoločnosti sú štatutárnymi orgánmi tzv. komplementári, ktorí sú oprávnení konať v mene spoločnosti každý samostatne (ak je ich viac), pokiaľ nie je vo výpise z obchodného registra uvedené inak. Platí zásada, že pokiaľ tzv. komandista uzavrie bez splnomocnenia zmluvu v mene spoločnosti, ručí potom za záväzky z nej vyplývajúce v rovnakom rozsahu ako komplementár (t.j. celým svojim osobným majetkom)

¹ Ak koná za takúto právnickú osobu štatutárny orgán, predkladá okrem svojich osobných dokladov taktiež doklad o tom, že bol do príslušnej funkcie zvolený, menovaný, prípadne ustanovený. Iná osoba musí predložiť taktiež úradne overené písomné rozhodnutie štatutárneho orgánu o oprávnených osobách na zastupovanie.

² V obchodnom registri sú okrem iného uvedené aj tzv. štatutárne orgány danej právnickej osoby. Ak sú tieto orgány kolektívne (napr. predstavenstvo), potom sú tiež v obchodnom registri uvedené jednotlivé fyzické osoby, oprávnené za danú právnickú osobu konať a uzatvárať záväzky. Taktiež je stanovený spôsob podpisovania za danú právnickú osobu, napr. „predseda predstavenstva samostatne“, „dvaja členovia predstavenstva spoločne“ a pod. Dodržiavanie stanoveného spôsobu podpisovania je potrebné kontrolovať podľa výpisu z obchodného registra.

- fc) u spoločnosti s ručením obmedzeným je štatutárnym orgánom jej konateľ (konatelia) uvedený v obchodnom registri. Každý konateľ môže konať samostatne, pokiaľ nie je v obchodnom registri uvedený inak
- fd) u akciovej spoločnosti je štatutárnym orgánom predstavenstvo
- fe) u družstva je štatutárnym orgánom predstavenstvo
- g) okrem štatutárneho orgánu (jeho určitého člena) môžu za právnickú osobu konať aj prokuristi. Prokúrou zmocňuje podnikateľ prokuristu na všetky právnické úkony, ku ktorým dochádza pri prevádzke podniku, aj keď sa k nim inak vyžaduje plná moc. Každý prokurista musí byť zapísaný v obchodnom registri, vrátane toho, či môže konať za spoločnosť samostatne alebo spoločne (ak je prokuristov viac). V obchodnom registri je zapísané aj prípadné obmedzenie zmocnenia prokuristu (ak nie je v registri uvedené, koná prokurista v plnom rozsahu právomocí).
- h) za právnickú osobu v likvidácii je oprávnený s I.CA konať ustanovený likvidátor.

Pri kontrole oprávnenosti žiadateľa podľa výpisu z obchodného registra je pracovník RA povinný zistiť nasledujúce:

- či výpis nie je starší ako 3 mesiace (viď vyššie)
- či je výpis úradne overený, pokiaľ nejde o prvopis
- či môže fyzická osoba (osoby), ktoré podávajú žiadosť o registráciu, podľa predloženého výpisu podpisovať za danú právnickú osobu
- pokiaľ nie je žiadateľ sám oprávnený konať a podpisovať za právnickú osobu (nie je štatutárnym orgánom), potom je taktiež nutné predložiť splnomocnenie žiadateľa štatutárnym orgánom.

U inej právnickej osoby je vyžadované doloženie legálnej existencie iným dokladom. Ide hlavne o tieto doklady:

- registráciu politickej strany alebo hnutia podľa zákona o združovaní v politických stranách a v politických hnutiach,
- registráciu občianskeho združenia, ktoré vzniklo podľa zákona o združovaní občanov (v platnom znení),
- registráciu záujmového združenia právnických osôb podľa občianskeho zákonníka,
- registráciu nadácie podľa občianskeho zákonníka,
- registráciu cirkvi a náboženských spoločností.

Pri kontrole oprávnenia žiadateľa podľa takéhoto iného dokladu je pracovník prepážky RA povinný zistiť nasledujúce:

- či doklad (resp. Registračná doložka na ňom) nie je starší ako 3 mesiace
- či je doklad úradne overený, pokiaľ nejde o prvopis
- či doklad obsahuje základné nevyhnutné údaje, t.j.

- názov právnickej osoby, sídlo právnickej osoby, právna forma, IČO, štatutárny orgán, t.j. osobu alebo osoby, ktoré majú právo konať a podpisovať v mene danej právnickej osoby
- či môže fyzická osoba (osoby), ktoré podávajú žiadosť podľa predloženého výpisu, podpisovať za danú právnickú osobu
- pokiaľ je štatutárny orgán uvedený len určitou funkciou, taktiež doklad o tom, že žiadateľ – fyzická osoba bol do príslušnej funkcie zvolený, menovaný, prípadne ustanovený
- pokiaľ nie je žiadateľ sám oprávnený konať a podpisovať (nie je štatutárnym zástupcom) za právnickú osobu, potom je tiež nutné požadovať splnomocnenie žiadateľa štatutárnym orgánom.

3.2 POSTUP PRI VYDANÍ NÁSLEDNÉHO CERTIFIKÁTU

I.CA nepodporuje žiadne vystavenie ďalšieho nového certifikátu na párové dáta, ktoré prislúchali už raz vystavenému certifikátu a taktiež nepodporuje žiadne vystavenie nového certifikátu na párové dáta, ktoré prislúchali už raz zrušenému certifikátu.

Jedinou formou následného certifikátu, ktorá je akceptovaná je tá, keď na základe novej žiadosti o vydanie certifikátu podpísanej platnými dátami na vytváranie elektronických podpisov súvisiacimi s už vydaným certifikátom, ku ktorému je vydávaný tento následný certifikát. Dáta overované I.CA musia byť rovnaké. Dáta na overovanie elektronických podpisov musia byť iné. Ostatné položky následného certifikátu podliehajú aktuálnym pravidlám pre vydávanie certifikátov.

Generovanie žiadosti o následný certifikát je rovnaké ako pri žiadosti o nový certifikát. Klient má však možnosť túto žiadosť zaslať na I.CA elektronickou poštou. Táto žiadosť musí byť podpísaná dátami na vytváranie elektronických podpisov súvisiacich s platným certifikátom klienta, ku ktorému sa žiada o následný certifikát.

3.3 ŽIADOSŤ O ZRUŠENIE CERTIFIKÁTU

Žiadosť o zrušenie certifikátu je možné podať nasledujúcimi spôsobmi :

- osobným odovzdaním písomnej žiadosti o zrušenie certifikátu na RA. RA v tomto prípade musí skontrolovať totožnosť klienta alebo vyžadovať oznámenie hesla pre zrušenie príslušného certifikátu,
- prostredníctvom elektronickej pošty, zaslaním elektronickej poštovej správy podpísanej pomocou údajov na vytváranie elektronických podpisov súvisiacich s príslušným certifikátom, o ktorého zrušenie sa žiada,
- zaslaním bežnej poštovej správy spoločne s heslom pre zrušenie certifikátu, ktoré bolo zadané pri uzatváraní zmluvy s I.CA,
- prostredníctvom elektronického formulára, ktorý je pre tento účel prístupný na vyhradenej webovej stránke.

Elektronická žiadosť o zrušenie certifikátu je textová správa, ktorá musí obsahovať vetu „Žiadam o zrušenie môjho certifikátu, sériové číslo XXXXXX.“.

Odpoveďou I.CA na platnú žiadosť o zrušenie certifikátu je vytvorenie a zaslanie aktuálneho zoznamu zrušených certifikátov. Do doby zverejnenia CRL je dotýčny certifikát zablokovaný. Maximálna doba medzi prijatím požiadavky na zrušenie certifikátu a uvedením v zozname zrušených certifikátov a zverejnením tohto zoznamu, môže predstavovať najviac 25 hodín.

Počas doby zablokovania je certifikát platný a prípadná zodpovednosť za škodu vzniknutú použitím takéhoto certifikátu v dobe jeho zablokovania je na strane klienta.

Odblokovanie certifikátu, ktorý bol zablokovaný na základe platnej žiadosti o zrušenie certifikátu, I.CA nepovoľuje.

4. OPERAČNÉ POŽIADAVKY

4.1 ŽIADOSŤ O CERTIFIKÁT

Osobná registrácia žiadateľa o testovací certifikát sa nevykonáva. Žiadateľ sám zodpovedá za údaje, ktoré vloží do elektronickej žiadosti o testovací certifikát. Vložené údaje pracovníci I.CA osobne nekontrolujú, aplikácia zodpovedná za vytvorenie certifikátu kontroluje iba to, či sú splnené technické požiadavky. Takto získané údaje sú použité iba pre vytvorenie certifikátu a nie sú I.CA ďalej uchovávané.

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

Pri registrácii nového žiadateľa o certifikát pre server, príslušný pracovník RA postupuje v súlade s postupom pri žiadosti o vydanie osobného certifikátu. Žiadateľ má nárok súčasne podať žiadosť o osobný certifikát - bezplatne. Údaje v tejto žiadosti je rovnako povinný doložiť. V prípade, že sú v žiadosti o vydanie certifikátu pre server alebo v žiadosti o vydanie osobného certifikátu nedostatky, RA upozorní žiadateľa na túto skutočnosť a registráciu odmietne.

4.2 VYDANIE CERTIFIKÁTU

I.CA vydá osobný certifikát žiadateľovi, ktorý splnil podmienky registrácie (článok 4.1), zaplatil určený poplatok, pokiaľ nebol spôsob úhrady zmluvne stanovený inak, a podpísal príslušnú zmluvu. Pracovník RA odovzdá žiadateľovi médium s jeho certifikátom a prislúchajúcimi certifikátmi I.CA. Na médiu taktiež musí byť nahraný Certifikačný poriadok I.CA. Žiadateľ musí prevzatie média s certifikátmi potvrdiť písomne. Okrem toho zašle I.CA certifikáty v predpísaných formátoch a Certifikačný poriadok I.CA na elektronickú adresu uvedenú v žiadosti (pokiaľ je táto adresa známa).

I.CA vydá certifikát pre server žiadateľovi, ktorý splnil podmienky registrácie (článok 4.1), zaplatil určený poplatok, pokiaľ nebol spôsob úhrady zmluvne stanovený inak, a podpísal príslušnú zmluvu. Pracovník RA odovzdá žiadateľovi médium s jeho certifikátom a prislúchajúcimi certifikátmi I.CA. Na médiu taktiež musí byť nahraný Certifikačný poriadok I.CA. Žiadateľ musí prevzatie média s certifikátmi písomne potvrdiť. Okrem toho zašle I.CA certifikáty v predpísaných formátoch a Certifikačný poriadok I.CA na elektronickú adresu uvedenú v žiadosti.

I.CA môže zmluvne dohodnúť so svojim partnerom postup odlišujúci sa od tohto ustanovenia Certifikačného poriadku. Týmto postupom sa však nesmie dostať do rozporu s príslušnými legislatívnymi normami upravujúcimi poskytovanie certifikačných služieb alebo obchodných činností s týmto spojených.

4.3 AKCEPTOVANIE CERTIFIKÁTU

Žiadateľ je povinný prijať certifikát o ktorý požiadal, pokiaľ splnil podmienky pre vydanie certifikátu (článok 4.1). Jediný spôsob, ako môže postupovať, pokiaľ tento certifikát nechce, je požiadať o jeho zrušenie.

4.4 ZRUŠENIE CERTIFIKÁTU

Certifikát môže byť zrušený iba na základe nasledujúcich okolností :

- držiteľ certifikátu alebo ním poverená osoba požiada o jeho zrušenie,
- na základe vyjadrenia klienta sa vecný obsah certifikátu stane neplatným,
- na základe zistenia I.CA alebo spolupracujúcich subjektov sa vecný obsah certifikátu stane neplatným,
- držiteľ certifikátu bol usvedčený zo závažných porušení zmluvných povinností alebo povinností vyplývajúcich z Certifikačného poriadku,
- je dôvodné podozrenie, že došlo ku kompromitácii súkromného kľúča držiteľa alebo disponenta certifikátu,
- dôjde ku kompromitácii súkromného kľúča I.CA,
- nariadi tak súd vo svojom rozsudku alebo v predbežnom opatrení,
- držiteľ certifikátu zomrel.

O zrušenie certifikátu môže požiadať:

- držiteľ certifikátu alebo oprávnený disponent,
- registračná autorita, ktorej prostredníctvom bolo požiadané o jeho vydanie,
- I.CA,
- súd prostredníctvom oprávnenej osoby,
- osoby oprávnené z dedičného konania.

Držiteľ certifikátu, alebo oprávnený disponent, musí zaslať alebo osobne odovzdať žiadosť o zrušenie certifikátu spôsobom uvedeným v článku 3.3.

V prípade, že sa zrušenie uskutočňuje na základe súdneho rozhodnutia, musí pracovník RA k záznamu o zrušení priložiť kópiu súdneho rozhodnutia.

V prípade, že sa zrušenie uskutočňuje na základe dedičného konania, musí pracovník RA k záznamu o zrušení priložiť kópiu dokladov, z ktorých jednoznačne vyplýva právo žiadajúceho o zrušenie.

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

Lehota pre vykonanie zrušenia certifikátu je stanovená na 24 hodín.

Certifikátom vydaným podľa tohto Certifikačného poriadku nie je možné pozastaviť platnosť.

4.5 POŽIADAVKY NA OVEROVANIE CRL

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

V období medzi podaním oprávnenej žiadosti o zrušenie certifikátu a jeho zverejnením v CRL nesie všetku zodpovednosť za prípadné škody vzniknuté v súvislosti so zneužitím certifikátu klient (držiteľ certifikátu). Po zverejnení certifikátu v CRL nesie zodpovednosť používateľ, ktorý daný certifikát použil.

4.6 PROCEDÚRY AUDITU VZHLADOM NA BEZPEČNOSŤ

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

- záznam o registrácii žiadateľa,
- záznam o pokuse neoprávnenej registrácie žiadateľa,
- záznam o zrušení registrácie žiadateľa (údaje o žiadateľovi sa uschovávajú),
- záznam o požiadavke RA na vystavenie certifikátu vrátane výsledku,
- záznam o požiadavke na následný certifikát vrátane výsledku,
- záznam o neoprávnenej požiadavke na vystavenie certifikátu vrátane výsledku,
- záznam o neoprávnenej požiadavke na následný certifikát vrátane výsledku,
- záznam o požiadavke na zrušenie certifikátu vrátane údajov o žiadajúcej osobe a výsledku,
- záznam o neoprávnenej požiadavke na zrušenie certifikátu vrátane údajov o žiadajúcej osobe a výsledku,
- záznam o pokuse neoprávneného prístupu do systému,
- záznam o zverejnení certifikátu vrátane výsledku,
- záznam o zapísaní zrušeného certifikátu do CRL,
- záznam o zverejnení CRL

Auditné záznamy sú spracovávané jeden krát denne. Po preskúmaní sú záznamy uložené do archívu.

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

Auditné záznamy sú prístupné iba poverenému pracovníkovi CA. Jednotlivé auditné záznamy sú označené poradovým číslom a sú podpísané. Súkromný kľúč určený na podpis auditných záznamov nie je pracovníkom, ktorí majú oprávnenie prezerať auditné záznamy, prístupný.

Po spracovaní je celý auditný log znova podpísaný.

4.7 VÝMENA PÁROVÝCH ÚDAJOV I.CA

V prípade zmeny párových údajov I.CA určených na podpisovanie certifikátov a zoznamov zrušených certifikátov, ktorá sa prejaví vystavením nového koreňového certifikátu, I.CA zverejní tento nový certifikát na svojich WWW stránkach. Registrovaným používateľom I.CA zašle upozornenie o platnosti nového certifikátu.

4.8 ODHALENIE KOMPROMITÁCIÍ A NEHÔD

V prípade zrušenia dát na overovanie elektronických podpisov používaných na overovanie podpísaných certifikátov a zoznamu zrušených certifikátov, informuje o tejto skutočnosti I.CA na svojich oficiálnych webových stránkach. Touto situáciou sa rozumejú iné dôvody, než je kompromitácia príslušných údajov pre podpisovanie elektronických podpisov.

V prípade kompromitácie vlastného súkromného kľúča I.CA neodkladne zruší príslušný certifikát. O tejto skutočnosti informuje I.CA neodkladne na svojich WWW stránkach. Držitelia certifikátov, ktorých dôveryhodnosť bola uvedenou kompromitáciou dotknutá, I.CA vyzve neodkladne k opätovnej fyzickej registrácii a podaniu žiadosti o vystavenie nového certifikátu. Prípadné náklady na vystavenie nových certifikátov hradí I.CA.

4.9 UKONČENIE ČINNOSTI I.CA

V prípade ukončenia činnosti I.CA z iných dôvodov než z dôvodov mimoriadnych udalostí, akými sú štrajky, občianske nepokoje, vojnový stav, prírodné katastrofy alebo iné výsledky pôsobenia vyššej moci, I.CA :

- a) zabezpečí sprístupnenie informácie o ukončení svojej činnosti všetkým osobám spoliehajúcim sa na certifikát, držiteľom a iným osobám, s ktorými má zmluvné alebo iné obdobné vzťahy týkajúce sa poskytovania certifikačných služieb,
- b) ukončí vydávanie všetkých typov certifikátov,
- c) zabezpečí uchovanie údajov získaných pri registrácii a záznamov udalostí po dobu najmenej 10 rokov od ukončenia platnosti vydaných certifikátov,
- d) preukázateľne zničí svoje dáta na vytváranie elektronických podpisov,
- e) vyvinie maximálne úsilie na to, aby platné certifikáty boli prevzaté inou certifikačnou autoritou.

5. FYZICKÉ, PROCEDURÁLNE A PERSONÁLNE BEZPEČNOSTNÉ MECHANIZMY

Otázky fyzických, procedurálnych a personálnych bezpečnostných mechanizmov sú veľmi dôležitým faktorom zabezpečujúcim dôveryhodnosť certifikačných služieb I.CA. Ochrana je zameraná na hlavné systémy, ktorými sú tie, ktoré priamo vykonávajú podpisovanie certifikátov a podpisovanie CRL.

Podrobný popis a požiadavky na I.CA ako poskytovateľa certifikačných služieb v týchto oblastiach je uvedený v Pravidlách na výkon certifikačných činností I.CA (CPS).

6. TECHNICKÁ BEZPEČNOSŤ

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

6.1 GENEROVANIE PÁROVÝCH DÁT KLIENTA A INŠTALÁCIA

Párové údaje sú vzájomne zviazané dvojice údajov na vytváranie elektronického podpisu a s nimi súvisiace dáta na overovanie elektronických podpisov. Certifikát I.CA bude vydaný iba k takým párovým údajom a podpisovým algoritmom, ktoré budú spĺňať požiadavky uvedené v tomto Certifikačnom poriadku. Požiadavky na kvalitu párových údajov a použitých kryptografických algoritmov umožňujúcich vydanie kvalifikovaného certifikátu nie je obsahom tohto Certifikačného poriadku.

Párové dáta 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. I.CA neposkytuje službu generovania párových údajov klienta na svojich zariadeniach.

Tento Certifikačný poriadok podporuje z asymetrických algoritmov iba algoritmus RSA. Ako hashovacie funkcie sú podporované MD5 a SHA1.

Mohutnosť kľúčov v RSA podporovaná týmto certifikačným poriadkom je závislá na type použitých párových údajov zviazaných s certifikátom I.CA.

U klientov :

- Testovacie certifikáty: veľkosť kľúča nie je stanovená
- Osobné certifikáty a serverové certifikáty:
 - minimálna dĺžka kľúča je 512 bitov
 - odporúčaná dĺžka kľúča je 1024 bitov.

Odporúčaný postup generovania párových dát a prípravy podkladov pre vydanie certifikátu I.CA je popísaný na WWW stránkach I.CA.

Verejný kľúč klienta je súčasťou žiadosti o vystavenie certifikátu. Podľa použitého prehliadača je buď vo formáte PKCS#10 alebo Netscape SPKAC. I.CA pri prijíme žiadosti kontroluje, či už nebol vystavený iný certifikát s rovnakým verejným kľúčom. Pokiaľ áno, je klient vyzvaný k vygenerovaniu novej žiadosti, a teda aj nových párových dát. Taktiež držiteľ už vydaného certifikátu, ktorý má verejný kľúč zhodný so žiadateľom, je vyzvaný k vygenerovaniu nových párových dát. Tento certifikát je okamžite zrušený. Držiteľ certifikátu je o tejto skutočnosti neodkladne informovaný.

Koreňový certifikát I.CA obsahujúci dáta na overovanie podpisov, ktorými I.CA podpisuje certifikáty, je možné získať na oficiálnej WWW stránke I.CA (www.ica.cz). Tento certifikát taktiež dostane každý klient spolu so svojim certifikátom.

Ďalšia možnosť ako získať koreňový certifikát I.CA, je nahranie na médium (napr. disketa) v ktorejkoľvek RA I.CA.

6.2 OCHRANA SÚKROMNÉHO KL'ÚČA I.CA

Súkromný kľúč certifikačnej autority je najdôležitejšie tajomstvo, ktoré každá certifikačná autorita má. Obdobne aj I.CA venuje ochrane súkromného kľúča maximálnu pozornosť. Podrobný popis povolených postupov pri práci so súkromným kľúčom I.CA je uvedený v Pravidlách na výkon certifikačných činností I.CA (CPS).

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, level 3.
- Súkromný kľúč je zálohovaný v zašifrovanej forme tak, že k jeho dešifrovaniu sú potrební dvaja určení pracovníci, ktorí majú k dispozícii časť tajomstva, z ktorého sa dá vytvoriť kľúč pre symetrickú šifru použitú pre zašifrovanie súkromného kľúča I.CA.
- Neexistuje možnosť získať súkromný kľúč I.CA inými metódami (napr. tzv. „Key escrow“).
- Súkromný kľúč I.CA je používaný výhradne k podpisovaniu vydaných certifikátov I.CA a certifikátov vydaných I.CA a zoznamu zrušených certifikátov (CRL) I.CA .
- Kryptografický modul spolu s obsluhujúcim počítačom je uložený v miestnosti, ktorá má objektívnu bezpečnosť na stupni „TAJNÉ“ podľa vyhlášky NBÚ č. 339/1999 Sb.
- V miestnosti sú použité aktívne prvky, ktoré významne znižujú možnosť kompromitovania techniky monitorovaním elektromagnetického vyžarovania.
- Miestnosť sa nachádza v objekte, ktorý je nepretržite strážený tak ľudskou strážnou službou, ako aj špeciálnou technikou.
- Vkladanie, aktivácia, deaktivácia, zálohovanie a ničenie súkromného kľúča I.CA je vykonávané podľa platných Pravidiel na výkon certifikačných činností I.CA (CPS), vždy v prítomnosti minimálne dvoch určených pracovníkov.CA.

6.3 ĎALŠIE POŽIADAVKY NA SPRÁVU PÁROVÝCH DÁT I.CA

Verejné kľúče obsiahnuté v koreňových certifikátoch I.CA sú archivované. I.CA bude tieto kľúče archivovať, respektíve zabezpečí ich archiváciu ešte 10 rokov po prípadnom ukončení svojej činnosti. Archivácia koreňových certifikátov, ktorým prislúchajú súkromné kľúče slúžiace na podpisovanie testovacích certifikátov, sa nevykonáva.

Platnosť párových dát s dĺžkou kľúča 2048 bitov určených na podpisovanie osobných a serverových certifikátov a príslušných CRL je 6 rokov.

6.4 BEZPEČNOSŤ POČÍTAČOVÉHO VYBAVENIA

Výpočtová technika používaná v I.CA pre certifikačné služby spĺňa požiadavky na kvalitnú a bezpečnú činnosť certifikačnej autority. Sú použité výhradne značkové komponenty, ktoré spĺňajú vysoké technické kritéria. Proti poruchám elektrickej siete sú hlavné systémy zabezpečené pomocou UPS.

Bezpečnosť použitých informačných systémov je charakterizovaná podľa normy ITSEC. Pre systém pracujúci s osobnými a serverovými certifikátmi je použitý počítačový systém vyhodnocovaný podľa kritérií ITSEC E2.

6.5 KONTROLY POČÍTAČOVEJ BEZPEČNOSTI

Všeobecné požiadavky na počítačovú bezpečnosť sú určené zvolenými kritériami ITSEC. Špecifické požiadavky sú:

- systém je použitý na operácie súvisiace s poskytovaním certifikačných služieb
- je zaistená bezpečnosť údajov pre podpisovanie certifikátov a zoznamov CRL
- systém je chránený proti výpadkom elektrickej siete
- použitý hardware je zálohovaný a je zabezpečené obnovenie činnosti do 24 hodín
- prevádzka počítačového systému I.CA zabezpečujúceho certifikačné služby je pravidelne kontrolovaná určenými pracovníkmi I.CA. Podľa požiadaviek odpovedajúcim kritériám ITSEC sú zaznamenávané a vyhodnocované auditné informácie.

6.6 BEZPEČNOSTNÉ KONTROLY PO DOBU ŽIVOTNOSTI

Vykonávanie bezpečnostných kontrol je popísané v Systémovej bezpečnostnej politike I.CA.

6.7 KONTROLY BEZPEČNOSTI POČÍTAČOVEJ SIETE

Prostriedky vykonávajúce vlastné certifikačné služby nie sú priamo dostupné z verejnej siete Internet. Akákoľvek komunikácia medzi RA a centrálnou CA prebieha v šifrovanej podobe.

Ostatné aspekty kontroly bezpečnosti počítačovej siete sú popísané v Systémovej bezpečnostnej politike I.CA.

6.8 KONTROLY BEZPEČNOSTI KRYPTOGRAFICKÉHO MODULU

Použité kryptografické moduly majú stanovenú bezpečnosť podľa príslušnej úrovne zabezpečenia (level) normy FIPS 140-1. Periodické kontroly sú vykonávané za účelom zistenia, či kryptografický modul neustále spĺňa požiadavky definované vyžadovanou úrovňou zabezpečenia. O vykonaných kontrolách sa vykonávajú záznamy s hodnotením.

7. CERTIFIKAČNÉ PROFILY A PROFILY CRL

7.1 PROFIL CERTIFIKÁTU

Všetky certifikáty vydávané I.CA sú v súlade s normou X.509 verzia 3.

Certifikáty vydávané I.CA podľa tohto Certifikačného poriadku používajú štandardne používané OID. Podľa tohto Certifikačného poriadku je používané:

Signature Algorithm: sha1WithRSAEncryption

Formy mien a obmedzujúce pravidlá na mena sú podrobne rozobrané v Pravidlách na výkon certifikačných činností (CPS).

Tento Certifikačný poriadok je určený výhradne pre komerčné certifikáty.

Príslušné atribúty a OID sú:

- 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-cpsica OBJECT IDENTIFIER ::= { id-ica-cp 2 }
- id-cpsica104 OBJECT IDENTIFIER ::= { id-cpsica 1 }

Ďalej sú použité rozširujúce atribúty :

CRL Distribution Points :

URI : adresy distribučných bodov CRL

Ďalšie atribúty a vzory koreňových certifikátov I.CA sú uvedené v Pravidlách na výkon certifikačných činností (CPS)..

7.2 PROFIL CRL

Zoznamy zrušených certifikátov (CRL) sú vydávané vo verzii 2 podľa X 509.

8. RIADENIE ŠPECIFIKÁCIÍ

8.1 PROCESY ZMIEN ŠPECIFIKÁCIÍ

Tento Certifikačný poriadok bude jedenkrát ročne prehodnocovaný. Rovnako ostatné základné materiály, t.j. Pravidlá na výkon certifikačných činností a Bezpečnostná pravidlá, budú jedenkrát ročne prehodnocované. Tieto základné materiály musia byť udržiavané tak, aby boli v súlade s platnou legislatívou Českej republiky, resp. Slovenskej republiky, a zároveň v súlade so všeobecne prijímanými štandardmi a normami.

8.2 POLITIKY ZVEREJŇOVANIA A OHLASOVANIA

Zverejňovanie Certifikačného poriadku sa uskutočňuje na oficiálnej WWW stránke I.CA – <http://www.ica.cz>. Na požiadanie je možné zaslanie elektronickou poštou, prípadne za poplatok poštou na papierovom alebo inom fyzickom médiu. Tieto materiály sú taktiež k dispozícii na všetkých registračných autoritách I.CA.

8.3 PROCES SCHVAĽOVANIA ZÁKLADNÝCH MATERIÁLOV

Certifikačný poriadok a aj ďalšie základné materiály sú schvaľované riaditeľom I.CA. Pred týmto schválením nie je možné vykonávať akékoľvek zmeny v činnostiach, ktoré tento Certifikačný poriadok popisuje.

Uplatnené zmeny v základných materiáloch musia byť zverejnené pre tie subjekty, ktorých činnosť je týmito materiálmi upravená, najmenej 10 kalendárnych dní pred ich uplatnením.

Tento Certifikačný poriadok - verzia 1.04 - nadobúda platnosť dňom 1.4.2002 a účinnosť dňom 11.8.2002. Odo dňa účinnosti verzie 1.04 budú komerčné certifikáty I.CA vydávané iba podľa tohto Certifikačného poriadku.

Copyright I.CA 2002. All Rights Reserved.

Vaše otázky zodpovieme na adrese info@ica.cz.