

První certifikační autorita, a.s.



CERTIFIKAČNÝ PORIADOK PRE VYDÁVANIE KVALIFIKOVANÝCH CERTIFIKÁTOV

Stupeň dôvernosti: verejný dokument

Tento dokument je slovenskou verziou dokumentu
„Certifikační politika vydávání kvalifikovaných certifikátů“

Verzia 2.2

Certifikační politika vydávání kvalifikovaných certifikátů je veřejným dokumentem, který je vlastnictvím společnosti První certifikační autorita, a.s. a byl vypracován jako nedílná součást komplexní bezpečnostní dokumentace. Žádná část tohoto dokumentu nesmí být kopírována bez písemného souhlasu majitele autorských práv.

Copyright © První certifikační autorita, a.s.

<i>Certifikačný poriadok pre vydávanie kvalifikovaných certifikátov</i>	<i>Strana 2 (celkom 66)</i>
<i>Copyright © První certifikační autorita, a.s.</i>	<i>Verejný dokument</i>

Tabuľka 1 – Identifikácia

Názov	Certifikačný poriadok pre vydávanie kvalifikovaných certifikátov
Pôvodný český názov	Certifikační politika vydávání kvalifikovaných certifikátů
Spoločnosť	První certifikační autorita, a.s.
Schválil	Riaditeľ spoločnosti První certifikační autorita, a.s.

Tabuľka 2 - Vývoj dokumentu

Verzia	Dátum vydania	Zhrnutie zmien
1.00	8.12.2001	Prvá verzia dokumentu
1.01	27.12.2001	Zpracovanie pripomienok
1.03	15.03.2002	Inovácia kapitoly 7
1.04	10.06.2005	Aktualizácia podľa zákona Českej republiky č. 227/2000 Sb. o elektronickom podpise a o zmene niektorých ďalších zákonů (zákon o elektronickom podpise) v znení zákona č. 226/2002 Sb., zákona č. 517/2002 Sb. a zákona č. 440/2004 Sb., aktualizácia noriem, procedúr a auditu
2.0	09.12.2005	Vytvorenie štruktúry striktne podľa RFC 3647
2.1	10.04.2006	Úprava kapitol 3, 7
2.2	14.10.2006	Úprava pojmov a kapitol 3, 7, podmienky pre akreditáciu v SR

Obsah

1	ÚVOD	9
1.1	PREHLAD	9
1.2	NÁZOV A IDENTIFIKÁCIA DOKUMENTU	10
1.3	PARTICIPUJÚCE SUBJEKTY	10
1.3.1	Certifikačné autority (ďalej „CA“)	10
1.3.2	Registračné autority	10
1.3.3	Držitelia kvalifikovaných certifikátov a podpisujúce osoby	11
1.3.4	Spoliehajúce sa strany	11
1.3.5	Iné participujúce subjekty	11
1.4	POUŽITIE CERTIFIKÁTU	11
1.4.1	Prípustné použitie certifikátu	11
1.4.2	Obmedzenie použitia certifikátu	12
1.5	SPRÁVA POLITIKY	12
1.5.1	Organizácia spravujúca certifikačný poriadok alebo CPS	12
1.5.2	Kontaktná osoba organizácie spravujúcej certifikačný poriadok alebo CPS	12
1.5.3	Subjekt zodpovedný za rozhodovanie o súlade postupov poskytovateľa s postupmi iných poskytovateľov certifikačných služieb	12
1.5.4	Postupy pri schválení súladu podľa bodu 1.5.3	12
1.6	PREHLAD POUŽITÝCH POJMOV A SKRATIEK	12
2	ZODPOVEDNOSTI ZA ZVEREJŇOVANIE A ÚLOŽISKO INFORMÁCIÍ A DOKUMENTÁCIE	16
2.1	ÚLOŽISKO INFORMÁCIÍ A DOKUMENTÁCIE	16
2.2	ZVEREJŇOVANIE INFORMÁCIÍ A DOKUMENTÁCIE	16
2.3	PERIODICITA ZVEREJŇOVANIA INFORMÁCIÍ	17
2.4	RIADENIE PRÍSTUPU K JEDNOTLIVÝM TYPOM ÚLOŽÍSK	17
3	IDENTIFIKÁCIA A AUTENTIZÁCIA	18
3.1	POMENOVÁVANIE	18
3.1.1	Typy mien	18
3.1.2	Požiadavka na významovosť mien	19
3.1.2.1	Country (Štát)	20
3.1.2.2	Common Name (Všeobecné meno)	20
3.1.2.3	StateorProvinceName (kraj)	20
3.1.2.4	Locality (mesto)	20
3.1.2.5	Organization (organizace)	20
3.1.2.6	Organizational Unit (Organizačná jednotka)	21
3.1.2.7	E-mail Address (pkcs9Email Address - elektronická poštovná adresa)	21
3.1.2.8	GivenName (Krstné meno/mená)	21
3.1.2.9	Initials (iniciály)	21
3.1.2.10	Name (Celé meno)	21
3.1.2.11	Sumame (Priezvisko)	21
3.1.2.12	Title (titul)	22
3.1.2.13	Serial number (sériové číslo)	22
3.1.2.14	Generation Qualifier (generačné rozlíšenie)	22
3.1.2.15	Pseudonym (pseudonym)	22
3.1.2.16	Subject Alternative Name (alternatívne meno subjektu)	22
3.1.3	Anonymita a používanie pseudonymu	23
3.1.4	Pravidla pre interpretáciu rôznych foriem mien	23
3.1.5	Jedinečnosť mien	23
3.1.6	Obchodné značky	23
3.2	POČIATOČNÉ OVERENIE IDENTITY	23
3.2.1	Overenie súladu dát, t.j. postup pri overovaní, či má osoba dáta pre vytváranie elektronických podpisov zodpovedajúce dátam pre overovanie elektronických podpisov	23
3.2.2	Overovanie identity právnickej osoby alebo organizačnej zložky štátu	23
3.2.3	Overovanie identity fyzickej osoby	23
3.2.4	Neoverené informácie vzťahujúce sa k držiteľovi certifikátu alebo podpisujúcej osobe	24
3.2.5	Overovanie špecifických práv	24
3.2.6	Kritériá pre interoperabilitu	24

Certifikačný poriadok pre vydávanie kvalifikovaných certifikátov	Strana 4 (celkom 66)
Copyright © První certifikační autorita, a.s.	Verejný dokument

3.3	IDENTIFIKÁCIA A AUTENTIZÁCIA PRI SPRACOVANÍ POŽIADAVIEK NA VÝMENU DÁT PRE OVEROVANIE ELEKTRONICKÝCH PODPISOV V CERTIFIKÁTE	25
3.3.1	Identifikácia a autentizácia pri rutinnej výmene dát pre vytváranie elektronických podpisov a im zodpovedajúcich dát pre overovanie elektronických podpisov (ďalej „párové dáta“)	25
3.3.2	Identifikácia a autentizácia pri výmene párových dát po zneplatnení certifikátu	25
3.4	IDENTIFIKÁCIA A AUTENTIZÁCIA PRI SPRACOVANÍ POŽIADAVIEK NA ZRUŠENIE CERTIFIKÁTU	25
4	POŽIADAVKY NA ŽIVOTNÝ CYKLUS CERTIFIKÁTU.....	26
4.1	ŽIADOŠŤ O VYDANIE CERTIFIKÁTU	26
4.1.1	Subjekty oprávnené podať žiadosť o vydanie certifikátu	26
4.1.2	Registračný proces a zodpovednosti poskytovateľa a žiadateľa	26
4.2	SPRACOVANIE ŽIADOSTI O CERTIFIKÁT	26
4.2.1	Identifikácia a autentizácia	26
4.2.2	Prijatie alebo odmietnutie žiadosti o certifikát	27
4.2.3	Doba spracovania žiadosti o certifikát	27
4.3	VYDANIE CERTIFIKÁTU	27
4.3.1	Úkony CA v priebehu vydania certifikátu	27
4.3.2	Oznámenie o vydaní certifikátu držiteľovi certifikátu alebo podpisujúcej osobe	27
4.4	PREVZATIE VYDANÉHO CERTIFIKÁTU	28
4.4.1	Úkony spojené s prevzatím certifikátu	28
4.4.2	Zverejňovanie vydaných certifikátov poskytovateľom	28
4.4.3	Oznámenie o vydaní certifikátu iným subjektom	28
4.5	POUŽITIE PÁROVÝCH DÁT A CERTIFIKÁTU	28
4.5.1	Použitie dát pre vytváranie elektronických podpisov a certifikátu držiteľom alebo podpisujúcou osobou	28
4.5.2	Použitie dát pre overovanie elektronických podpisov a certifikátu spoliehajúcou sa stranou	29
4.6	OBNOVENIE CERTIFIKÁTU	29
4.6.1	Podmienky pre obnovenie certifikátu	29
4.6.2	Subjekty oprávnené požadovať obnovenie certifikátu	29
4.6.3	Spracovanie požiadavku na obnovenie certifikátu	29
4.6.4	Oznámenie o vydaní obnoveného certifikátu držiteľovi alebo podpisujúcej osobe	29
4.6.5	Úkony spojené s prevzatím obnoveného certifikátu	29
4.6.6	Zverejňovanie vydaných obnovených kvalifikovaných certifikátov poskytovateľom	29
4.6.7	Oznámenie o vydaní obnoveného certifikátu iným subjektom	29
4.7	VÝMENA DÁT PRE OVEROVANIE ELEKTRONICKÝCH PODPISOV V CERTIFIKÁTE	30
4.7.1	Podmienky pre výmenu dát pre overovanie elektronických podpisov v certifikáte	30
4.7.2	Subjekty oprávnené požadovať výmenu dát pre overovanie elektronických podpisov v certifikáte	30
4.7.3	Spracovanie požiadavku na výmenu dát pre overovanie elektronických podpisov	30
4.7.4	Oznámenie o vydaní certifikátu s vymenenými dátami pre overovanie elektronických podpisov podpisujúcej osobe	30
4.7.5	Úkony spojené s prevzatím certifikátu s vymenenými dátami pre overovanie elektronických podpisov	30
4.7.6	Zverejňovanie vydaných certifikátov s vymenenými dátami pre overovanie elektronických podpisov	30
4.7.7	Oznámenie o vydaní certifikátu s vymenenými dátami pre overovanie elektronických podpisov iným subjektom	30
4.8	ZMENA ÚDAJOV V CERTIFIKÁTE	30
4.8.1	Podmienky pre zmenu údajov v certifikátu	30
4.8.2	Subjekty oprávnené požadovať zmenu údajov v certifikáte	30
4.8.3	Spracovanie požiadavku na zmenu údajov v certifikáte	30
4.8.4	Oznámenie o vydaní certifikátu so zmenenými údajmi podpisujúca osoba	30
4.8.5	Úkony spojené s prevzatím certifikátu so zmenenými údajmi	30
4.8.6	Zverejňovanie vydaných certifikátov so zmenenými údajmi	30
4.8.7	Oznámenie o vydaní certifikátu so zmenenými údajmi iným subjektom	30
4.9	ZRUŠENIE A POZASTAVENIE PLATNOSTI CERTIFIKÁTU	30
4.9.1	Podmienky pre zrušenie certifikátu	30
4.9.2	Subjekty oprávnené žiadať o zrušenie certifikátu	30
4.9.3	Požiadavka na zrušenie certifikátu	30
4.9.4	Doba odkladu požiadavku na zrušenie certifikátu	30
4.9.5	Maximálna doba, za ktorú musí poskytovateľ realizovať požiadavku na zrušenie certifikátu	30

Certifikačný poriadok pre vydávanie kvalifikovaných certifikátov	Strana 5 (celkom 66)
Copyright © První certifikační autorita, a.s.	Verejný dokument

4.9.6	Povinnosti spoliehajúcich sa strán pri overovaní, či nebol certifikát zrušený.....	30
4.9.7	Periodicita vydávania zoznamu zrušených certifikátov.....	30
4.9.8	Maximálne spozdzenie pri vydávaní zoznamu zrušených certifikátov.....	30
4.9.9	Možnosť overovania statutu certifikátu on-line („ďalej OCSP“).	30
4.9.10	Požiadavky pri overovaní statutu certifikátu on-line.....	30
4.9.11	Iné spôsoby oznamovania zrušenia certifikátu.....	30
4.9.12	Prípadné odlišnosti postupu zrušenia v prípade kompromitácie dát pre vytváranie elektronických podpisov	30
4.9.13	Podmienky pre pozastavenie platnosti certifikátu.....	30
4.9.14	Subjekty oprávnené požadovať pozastavenie platnosti certifikátu.....	30
4.9.15	Spracovanie požiadavky na pozastavenie platnosti certifikátu	30
4.9.16	Obmedzenie doby pozastavenia platnosti certifikátu	30
4.10	SLUŽBY SÚVISIACE S OVEROVANÍM STATUTU CERTIFIKÁTU	30
4.10.1	Funkčné charakteristiky.....	30
4.10.2	Dostupnosť služieb	30
4.10.3	Ďalšie charakteristiky služieb statutu certifikátu.....	30
4.11	UKONČENIE POSKYTOVANIA SLUŽIEB PRE DRŽITEĽOV CERTIFIKÁTU PODPISUJÚCOU OSOBOU	30
4.12	ÚSCHOVA DÁT PRE VYTÁRANIE ELEKTRONICKÝCH PODPISOV U DÔVERYHODNEJ TRETEJ STRANY A ICH OBNOVA.....	30
4.12.1	Politika a postupy pri úschove a obnovovaní dát pre vytváranie elektronických podpisov	30
4.12.2	Politika a postupy pri zapuzdrovaní a obnovovaní šifrovacieho kľúča pro relaci.....	30
5	MANAGEMENT, PREVÁDZKOVÁ A FYZICKÁ BEZPEČNOSŤ	30
5.1	FYZICKÁ BEZPEČNOSŤ	30
5.1.1	Umiestnenie a konštrukcia.....	30
5.1.2	Fyzický prístup.....	30
5.1.3	Elektrina a klimatizácia	30
5.1.4	Vplyv vody	30
5.1.5	Protipožiarne opatrenia a ochrana.....	30
5.1.6	Ukladanie médií	30
5.1.7	Nakladanie s odpadmi	30
5.1.8	Zálohy mimo budovu	30
5.2	PROCESNÁ BEZPEČNOSŤ	30
5.2.1	Dôveryhodné role.....	30
5.2.2	Počet osôb požadovaných na zaisťenie jednotlivých činností.....	30
5.2.3	Identifikácia a autentizácia pre každú rolu	30
5.2.4	Role vyžadujúce rozdelenie povinností	30
5.3	PERSONÁLNA BEZPEČNOSŤ.....	30
5.3.1	Požiadavky na kvalifikáciu, skúsenosť a bezúhonnosť	30
5.3.2	Posúdenie spoľahlivosti osôb.....	30
5.3.3	Požiadavky na prípravu pre výkon role, vstupné školenie.....	30
5.3.4	Požiadavky a periodicita školení	30
5.3.5	Periodicita a postupnosť rotácie pracovníkov medzi rôznymi rolami.....	30
5.3.6	Postihy za neoprávnené činnosti zamestnancov.....	30
5.3.7	Požiadavky na nezávislých zhotoviteľov (dodávateľov)	30
5.3.8	Dokumentácia poskytovaná zamestnancom.....	30
5.4	AUDITNÉ ZÁZNAMY (LOGY)	30
5.4.1	Typy zaznamenávaných udalostí.....	30
5.4.2	Periodicita spracovania záznamov	30
5.4.3	Doba uchovávaní auditných záznamov.....	30
5.4.4	Ochrana auditných záznamov.....	30
5.4.5	Postupy pre zálohovanie auditných záznamov.....	30
5.4.6	Systém zhromažďovania auditných záznamov (interný alebo externý)	30
5.4.7	Postup pri oznamovaní udalosti subjektu, ktorý ju spôsobil.....	30
5.4.8	Hodnotenie zraniteľnosti	30
5.5	UCHOVÁVANIE INFORMÁCIÍ A DOKUMENTÁCIE	30
5.5.1	Typy informácií a dokumentácie, ktoré sa uchovávajú	30
5.5.2	Doba uchovávaní uchovávaných informácií a dokumentácie	30

Certifikačný poriadok pre vydávanie kvalifikovaných certifikátov	Strana 6 (celkom 66)
Copyright © První certifikační autorita, a.s.	Verejný dokument

5.5.3	Ochrana úložiska uchovávaných informácií a dokumentácie	30
5.5.4	Postupy pri zálohovaní uchovávaných informácií a dokumentácie.....	30
5.5.5	Požiadavky na používanie časových pečiatok pri uchovávaní informácií a dokumentácie	30
5.5.6	Systém zhromažďovania uchovávaných informácií a dokumentácie (interný, externý).....	30
5.5.7	Postupy pre získanie a overenie uchovávaných informácií a dokumentácie	30
5.6	VÝMENA DÁT PRE OVEROVANIE ELEKTRONICKÝCH PODPISOV/ZNAČIEK V NADRIADENOM KVALIFIKOVANOM SYSTÉMOVOM CERTIFIKÁTE POSKYTOVATEĽA	30
5.7	OBNOVA PO HAVÁRII ALEBO KOMPROMITÁCIÍ	30
5.7.1	Postup v prípade incidentu a kompromitácie.....	30
5.7.2	Poškodenie výpočtových prostriedkov, software alebo dát	30
5.7.3	Postup pri kompromitácii dát pre vytváranie elektronických podpisov/značiek poskytovateľa.....	30
5.7.4	Schopnosti obnoviť činnosť po havárii.....	30
5.8	UKONČENIE ČINNOSTI CA ALEBO RA	30
6	TECHNICKÁ BEZPEČNOSŤ	30
6.1	GENEROVANIE A INŠTALÁCIA PÁROVÝCH DÁT	30
6.1.1	Generovanie párových dát.....	30
6.1.2	Odovzdanie dát pre vytváranie elektronických podpisov podpisujúcej osobe	30
6.1.3	Odovzdanie dát pre overovanie elektronických podpisov poskytovateľov certifikačných služieb.....	30
6.1.4	Poskytovanie dát pre overovanie elektronických podpisov certifikačnou autoritou spoliehajúcim sa stranám 30	
6.1.5	Dĺžky párových dát.....	30
6.1.6	Generovanie parametrov dát pre overovanie elektronických podpisov a kontrola ich kvality	30
6.1.7	Obmedzenie pre použitie dát pre overovanie elektronických podpisov	30
6.2	OCHRANA DÁT PRE VYTÁVANIE ELEKTRONICKÝCH ZNAČIEK/PODPISOV A BEZPEČNOSŤ KRYPTOGRAFICKÝCH MODULOV	30
6.2.1	Štandardy a podmienky používania kryptografických modulov	30
6.2.2	Zdieľanie tajomstva	30
6.2.3	Úschova dát pre vytváranie elektronických značiek/podpisov	30
6.2.4	Zálohovanie dát pre vytváranie elektronických značiek/podpisov.....	30
6.2.5	Uchovávanie dát pre vytváranie elektronických značiek/podpisov	30
6.2.6	Transfer dát pre vytváranie elektronických značiek/podpisov do kryptografického modulu alebo z kryptografického modulu.....	30
6.2.7	Uloženie dát pre vytváranie elektronických značiek/podpisov v kryptografickom module.....	30
6.2.8	Postup pri aktivácii dát pre vytváranie elektronických značiek/podpisov	30
6.2.9	Postup pri deaktivácii dát pre vytváranie elektronických značiek/podpisov.....	30
6.2.10	Postup pri zničení dát pre vytváranie elektronických značiek/podpisov.....	30
6.2.11	Hodnotenie kryptografických modulov	30
6.3	ĎALŠIE ASPEKTY SPRÁVY PÁROVÝCH DÁT	30
6.3.1	Uchovávanie dát pre overovanie elektronických značiek/podpisov.....	30
6.3.2	Maximálna doba platnosti certifikátu vydaného podpisujúcej alebo označujúcej osobe a párových dát 30	
6.4	AKTIVAČNÉ DÁTA	30
6.4.1	Generovanie a inštalácia aktivačných dát	30
6.4.2	Ochrana aktivačných dát.....	30
6.4.3	Ostatné aspekty aktivačných dát.....	30
6.5	POČÍTAČOVÁ BEZPEČNOSŤ	30
6.5.1	Špecifické technické požiadavky na počítačovú bezpečnosť.....	30
6.5.2	Hodnotenie počítačovej bezpečnosti.....	30
6.6	BEZPEČNOSŤ ŽIVOTNÉHO CYKLU	30
6.6.1	Riadenie vývoja systému.....	30
6.6.2	Kontroly riadenia bezpečnosti	30
6.6.3	Riadenie bezpečnosti životného cyklu.....	30
6.7	SIŤOVÁ BEZPEČNOSŤ	30
6.8	ČASOVÁ PEČIATKY	30
7	PROFILY CERTIFIKÁTOV, ZOZNAMOV ZRUŠENÝCH CERTIFIKÁTOV A OCSP	30
7.1	PROFIL CERTIFIKÁTU	30
7.1.1	Číslo verzie.....	30

Certifikačný poriadok pre vydávanie kvalifikovaných certifikátov	Strana 7 (celkom 66)
Copyright © První certifikační autorita, a.s.	Verejný dokument

7.1.2	Rozširujúce položky v certifikáte.....	30
7.1.3	Objektové identifikátory (ďalej "OID") algoritmov	30
7.1.4	Spôsoby zápisov mien a názvov.....	30
7.1.5	Obmedzenie mien a názvov.....	30
7.1.6	OID certifikačnej politiky	30
7.1.7	Rozširujúca položka „Policy Constraints“	30
7.1.8	Syntax a sémantika rozširujúca položky kvalifikátorov politiky „Policy Qualifiers“	30
7.1.9	Spôsob zápisu kritickej rozširujúcej položky „Certificate Policies“	30
7.2	PROFIL ZOZNAMU ZRUŠENÝCH CERTIFIKÁTOV	30
7.2.1	Číslo verzie.....	30
7.2.2	Rozširujúce položky zoznamu zrušených certifikátov a záznamov v zozname zrušených certifikátov.....	30
7.3	PROFIL OCSP.....	30
7.3.1	Číslo verzie.....	30
7.3.2	Rozširujúce položky OCSP	30
8	HODNOTENIE ZHODY A INÉ HODNOTENIA.....	30
8.1	PERIODICITA HODNOTENÍ ALEBO OKOLNOSTÍ PRE VÝKON HODNOTENÍ.....	30
8.2	IDENTITA A KVALIFIKÁCIA HODNOTITEĽA	30
8.3	VZŤAH HODNOTITEĽA K HODNOTENÉMU SUBJEKTU	30
8.4	HODNOTENÉ OBLASTI.....	30
8.5	POSTUP V PRÍPADE ZISTENÝCH NEDOSTATKOV.....	30
8.6	OZNAMOVANIE VÝSLEDKOV HODNOTENÍ.....	30
9	OSTATNÉ OBCHODNÉ A PRÁVNE ZÁLEŽITOSTI.....	30
9.1	POPLATKY	30
9.1.1	Poplatky za vydanie alebo obnovenie certifikátu.....	30
9.1.2	Poplatky za prístup k certifikátu na zozname vydaných certifikátov.....	30
9.1.3	Poplatky za informácie o statute certifikátu a o zrušení certifikátu.....	30
9.1.4	Poplatky za ďalšie služby.....	30
9.1.5	Iné ustanovenia týkajúce sa poplatkov (vrátane refundácií).....	30
9.2	FINANČNÁ ZODPOVEDNOSŤ.....	30
9.2.1	Krytie poistením.....	30
9.2.2	Ďalšie aktíva a záruky	30
9.2.3	Poistenie alebo krytie zárukou pre koncových používateľov.....	30
9.3	CITLIVOSŤ OBCHODNÝCH INFORMÁCIÍ	30
9.3.1	Výpočet citlivých informácií.....	30
9.3.2	Informácie mimo rámec citlivých informácií	30
9.3.3	Zodpovednosť za ochranu citlivých informácií.....	30
9.4	OCHRANA OSOBNÝCH ÚDAJOV	30
9.4.1	Politika ochrany osobných údajov.....	30
9.4.2	Osobné údaje.....	30
9.4.3	Údaje, ktoré nie sú považované za dôverné	30
9.4.4	Zodpovednosť za ochranu osobných údajov.....	30
9.4.5	Oznámenie o používaní dôverných informácií a súhlas s používaním citlivých informácií.....	30
9.4.6	Poskytovanie citlivých informácií pre súdne či správne účely.....	30
9.4.7	Iné okolnosti sprístupňovania osobných údajov.....	30
9.5	PRÁVA DUŠEVNÉHO VLASTNÍCTVA.....	30
9.6	ZASTUPOVANIE A ZÁRUKY	30
9.6.1	Zastupovanie a záruky CA.....	30
9.6.2	Zastupovanie a záruky RA.....	30
9.6.3	Zastupovanie a záruky držiteľa certifikátu a podpisujúcej osoby.....	30
9.6.4	Zastupovanie a záruky spoliehajúcich sa strán.....	30
9.6.5	Zastupovanie a záruky ostatných zúčastnených subjektov	30
9.7	ZRIEKNUTIE SA ZÁRUK	30
9.8	OBMEDZENIE ZODPOVEDNOSTI	30
9.9	ZODPOVEDNOSŤ ZA ŠKODU, NÁHRADA ŠKODY	30
9.10	DOBA PLATNOSTI, UKONČENIE PLATNOSTI	30
9.10.1	Doba platnosti	30

Certifikačný poriadok pre vydávanie kvalifikovaných certifikátov	Strana 8 (celkom 66)
Copyright © První certifikační autorita, a.s.	Verejný dokument

9.10.2	<i>Ukončenie platnosti</i>	30
9.10.3	<i>Dôsledky ukončenia a pretrvanie záväzkov</i>	30
9.11	KOMUNIKÁCIA MEDZI ZÚČASTNENÝMI SUBJEKTMI	30
9.12	ZMENY	30
9.12.1	<i>Postup pri zmenách</i>	30
9.12.2	<i>Postup pri oznamovaní zmien</i>	30
9.12.3	<i>Okolnosti, pri ktorých musí byť zmenené OID</i>	30
9.13	RIEŠENIE SPOROV	30
9.14	ROZHODNÉ PRÁVO	30
9.15	ZHODA S PRÁVNymi PREDPISMI.....	30
9.16	ĎALŠIE USTANOVENIA.....	30
9.16.1	<i>Rámcová zhoda</i>	30
9.16.2	<i>Postúpenie práv</i>	30
9.16.3	<i>Oddeliteľnosť ustanovení</i>	30
9.16.4	<i>Zrieknutie sa práv</i>	30
9.16.5	<i>Vyššia moc</i>	30
9.17	ĎALŠIE OPATRENIA	30
10	ZÁVEREČNÉ USTANOVENIA	30

Certifikačný poriadok pre vydávanie kvalifikovaných certifikátov	Strana 9 (celkom 66)
Copyright © První certifikační autorita, a.s.	Verejný dokument

1 Úvod

Tento dokument **Certifikačný poriadok pre vydávanie kvalifikovaných certifikátov** (ďalej tiež „CP“), vypracovaný spoločnosťou První certifikační autorita, a.s. (ďalej tiež „I.CA“):

- je v súlade so zákonom Českej republiky č. 227/2000 Sb. o elektronickom podpise a o zmene niektorých ďalších zákonů (zákon o elektronickom podpise) v znení zákona č. 226/2002 Sb., zákona č. 517/2002 Sb. a zákona č. 440/2004 Sb. a s ním súvisiacich predpisov a vyhlášok;
- je v súlade so zákonom Slovenskej republiky č. 215/2002 Z.z. o elektronickom podpise a o zmene a doplnení niektorých zákonov v platnom znení a s ním spojených vykonávacích vyhlášok;
- sa zaoberá skutočnosťami, ktoré sa vzťahujú na I.CA, podpisujúce osoby, držiteľov, spoliehajúce sa strany, iných účastníkov PKI a zmluvných partnerov a ktoré súvisia s vydávaním **kvalifikovaných certifikátov**, ich ďalšou správou, použitím, akceptáciou, ukončením platnosti, zrušením a všetkými ďalšími aspektmi súvisiacimi s manipuláciou s párovými dátami;
- striktno dodržiava členenie dokumentu navrhnuté v RFC 3647, s prihliadnutím k doporučeniam orgánov EÚ a k právu ČR a SR v danej oblasti. Jednotlivé kapitoly sú preto v tomto CP zachované aj v prípade, že sú vo vzťahu k nemu irelevantné.

Vzhľadom na skutočnosť, že spoločnosť První certifikační autorita, a.s., vydáva viacero druhov certifikátov podľa rôznych certifikačných poriadkov, skontrolujte si a uistite sa o tom, že tento dokument (CP) zodpovedá Vaším požiadavkám na kvalifikovaný certifikát.

1.1 Prehľad

Tento dokument môže byť okrem iného použitý nezávislými inštitúciami (napr. auditorskými spoločnosťami) ako základ pre potvrdenie toho, že kvalifikované certifikačné služby v oblasti vydávania certifikátov, poskytované spoločnosťou První certifikační autorita, a.s., je možné považovať za dôveryhodné.

Spoločnosť **První certifikační autorita, a.s.**, je :

- od 18.03.2002 prvým akreditovaným poskytovateľom certifikačných služieb v ČR pre oblasť vydávania kvalifikovaných certifikátov podľa zákona č. 227/2000 Sb. o elektronickom podpise a o zmene niektorých ďalších zákonů (zákon o elektronickom podpise) v znení zákona č. 226/2002 Sb., zákona č. 517/2002 Sb. a zákona č. 440/2004 Sb.
- od 01.02.2006 akreditovaným poskytovateľom certifikačných služieb v ČR pre oblasť vydávania kvalifikovaných systémových certifikátov podľa zákona č. 227/2000 Sb. o elektronickom podpise a o zmene niektorých ďalších zákonů (zákon o elektronickom podpise) v znení zákona č. 226/2002 Sb., zákona č. 517/2002 Sb. a zákona č. 440/2004 Sb.
- od 21.9.2006 prvou zahraničnou akreditovanou certifikačnou autoritou v SR, ktorému bola udelená akreditácia v oblasti poskytovania kvalifikovaných certifikátov a časových pečiatok podľa zákona Slovenskej republiky č. 215/2002 Z.z. o elektronickom podpise a o zmene a doplnení niektorých zákonov v platnom znení.

Vzhľadom na vyššie uvedené skutočnosti platí:

- Pre oblasť kvalifikovaných certifikátov, vydávaných v súlade s aktuálnym znením zákona Českej republiky č. 227/2000 Sb. o elektronickom podpise, je stanovená jednorovňová hierarchia certifikačných autorít. Koreňom tejto hierarchie je certifikačná autorita spoločnosti První certifikační autorita, a.s., vydávajúca nadriadený kvalifikovaný systémový certifikát I.CA, obsahujúci dáta pre overovanie elektronických značiek zodpovedajúce dátam pre vytváranie elektronických značiek, ktorými I.CA označuje:
 - kvalifikované certifikáty vydávané koncovým používateľom, kvalifikované systémové certifikáty a zoznamy zrušených certifikátov
 - nadriadený kvalifikovaný systémový certifikát serveru vydávajúceho kvalifikované časové pečiatky

Úložiskom súkromného kľúča kvalifikovaných certifikátov vydaným koncovým používateľom môže byť počítač, USB token, a tiež iná čipová karta ako STARCOS (v. 2.3 a vyššia).

Certifikačný poriadok pre vydávanie kvalifikovaných certifikátov	Strana 10 (celkom 66)
Copyright © První certifikační autorita, a.s.	Verejný dokument

- Pre oblasť kvalifikovaných certifikátov, vydávaných v súlade s platným znením zákona Slovenskej republiky č. 215/2002 Z.z. o elektronickom podpise, je stanovená dvojúrovňová hierarchia certifikačných autorít. Koreňom tejto hierarchie je certifikačná autorita Národného bezpečnostného úradu SR, ktorá vydáva certifikáty (pre účely tohto dokumentu budú nazývané „certifikáty I.CA“) pre certifikačné autority, obsahujúce verejný kľúč zodpovedajúci súkromnému kľúču, ktorým sú podpisované kvalifikované certifikáty vydávané koncovým používateľom. Úložiskom súkromného kľúča kvalifikovaných certifikátov vydávaných koncovým používateľom podľa slovenskej legislatívy môže byť iba zariadenie certifikované pre tento účel Národným bezpečnostným úradom SR (odporúča sa čipová karta STARCOS SPK 2.3). Úložiskom súkromného kľúča kvalifikovaných certifikátov vydávaných koncovým používateľom podľa českej legislatívy môže byť v tomto prípade čipová karta STARCOS (v. 2.3 a vyššia).

Vydávanie a správa nadriadeného kvalifikovaného systémového certifikátu (ZoEP ČR) alebo certifikátu I.CA (ZoEP SR) sa riadia špeciálnymi dokumentmi – certifikačným poriadkom pre nadriadený kvalifikovaný systémový certifikát (ZoEP ČR) alebo certifikát I.CA (ZoEP SR) a certifikačnou prevádzkovou smernicou pre nadriadený kvalifikovaný systémový certifikát (ZoEP ČR) alebo pravidlami pre výkon certifikačných služieb pre certifikát I.CA (ZoEP SR).

V procese poskytovania kvalifikovaných certifikačných služieb v oblasti vydávania certifikátov prevádzkuje spoločnosť První certifikační autorita, a.s., jedinú certifikačnú autoritu – vid'. kapitola 1.3.1.

Informácie o vydaných certifikátoch, nadriadených kvalifikovaných systémových certifikátoch (ZoEP ČR) alebo certifikátoch I.CA (ZoEP SR), o ďalších poskytovaných certifikačných službách, atď., je možné získať na internetovej informačnej adrese uvedenej v kapitole 2.

Ak nie je uvedené inak, pod pojmom certifikát sa v tomto dokumente ďalej rozumie kvalifikovaný certifikát.

1.2 Názov a identifikácia dokumentu

Názov tohto dokumentu: Certifikačný poriadok pre vydávanie kvalifikovaných certifikátov

Názov v českom jazyku: Certifikační politika vydávání kvalifikovaných certifikátů

OID: 1.3.6.1.4.1.23624.1.4.10.2

1.3 Participujúce subjekty

1.3.1 Certifikačné autority (ďalej „CA“)

I.CA je akreditovaným poskytovateľom certifikačných služieb. I.CA nezriaďuje ani nepodporuje podriadené certifikačné autority, poskytujúce kvalifikované certifikačné služby súvisiace s vydávaním certifikátov.

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

1.3.2 Registračné autority

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

Vlastná stacionárna registračná autorita (VSRA):

- je základnou decentralizovanou zložkou výkonného aparátu I.CA.
- prijíma žiadosti o služby podľa tohto certifikačného poriadku, najmä prijíma žiadosti o vydanie certifikátov, sprostredkováva odovzdanie certifikátov a zoznamov zrušených certifikátov, poskytuje potrebné informácie klientom, vybavuje ich reklamácie a pod.

Certifikačný poriadok pre vydávanie kvalifikovaných certifikátov	Strana 11 (celkom 66)
Copyright © První certifikační autorita, a.s.	Verejný dokument

- je oprávnená z naliehavých prevádzkových alebo technických dôvodov pozastaviť úplne alebo čiastočne výkon svojej činnosti. Toto opatrenie je povinná neodkladne hlásiť riaditeľovi I.CA, ktorý ho potvrdí, zruší alebo zmení.
- je splnomocnená v mene I.CA uzatvárať zmluvy o poskytovaní kvalifikovaných (resp. akreditovaných) certifikačných služieb
- zabezpečuje spoplatňovanie služieb I.CA, pokiaľ nie je stanovené zmluvou inak.

Vlastná mobilná registračná autorita (VMRA):

- je zvláštnymi decentralizovanou mobilnou zložkou výkonného aparátu I.CA.
- prijíma žiadosti o služby podľa tohto certifikačného poriadku, najmä prijíma žiadosti o vydanie certifikátov, sprostredkováva odovzdanie certifikátov a zoznamov zrušených certifikátov, poskytuje potrebné informácie klientom, vybavuje ich reklamácie a pod.
- je oprávnená z naliehavých prevádzkových alebo technických dôvodov pozastaviť úplne alebo čiastočne výkon svojej činnosti. Toto opatrenie je povinná neodkladne hlásiť riaditeľovi I.CA, ktorý ho potvrdí, zruší alebo zmení.
- je splnomocnená v mene I.CA uzatvárať zmluvy o poskytovaní kvalifikovaných (resp. akreditovaných) certifikačných služieb
- zabezpečuje spoplatňovanie služieb I.CA, pokiaľ nie je stanovené zmluvou inak.

Zmluvná registračná autorita (ZRA):

- Plní v mene I.CA obdobné funkcie ako VMRA alebo VSRA na základe písomnej zmluvy medzi I.CA a majiteľom ZRA.

1.3.3 Držitelia kvalifikovaných certifikátov a podpisujúce osoby

Držitelia kvalifikovaných certifikátov môžu byť fyzické osoby a v prípade českej legislatívy aj právnické osoby. Podpisujúce osoby, ktoré požiadali o vydanie certifikátu a ktorým bol certifikát vydaný, môžu byť iba fyzické osoby,

1.3.4 Spoliehajúce sa strany

Spoliehajúcou sa stranou môžu byť fyzické osoby, právnické osoby a organizačné zložky štátu. Samotná definícia spoliehajúcej sa strany je uvedená v kapitole 1.6.

1.3.5 Iné participujúce subjekty

Inými participujúcimi subjektmi sú orgány dozoru podľa aktuálneho ZoEP (ČR, SR), orgány činné v trestnom konaní a ďalšie, ktorým to prislúcha podľa zákona.

1.4 Použitie certifikátu

Certifikáty vydané podľa tohto CP je možné použiť v zhode so ZoEP (ČR, SR).

1.4.1 Prípustné použitie certifikátu

Certifikáty je možné použiť v aplikáciách pre nasledujúce účely:

- overovanie (zaručených) elektronických podpisov
- bezpečné overovanie (zaručených) elektronických podpisov
- zaistenie neodmietnuteľnosti zodpovednosti
- pokiaľ žiadateľ o certifikát pri tvorbe žiadosti nastaví zodpovedajúci kritický atribút Key usage, môže certifikát využívať aj pre nasledujúce účely:
 - NonRepudiation (povinný) – súkromný kľúč bude používaný pre vytváranie elektronického podpisu
 - DigitalSignature (nepovinný) – súkromný kľúč bude obecné používaný pre vytváranie elektronického podpisu (napr. v rámci bezpečnej elektronickej pošty)
 - KeyEncipherment (nepovinný) – verejný kľúč obsiahnutý v tomto certifikáte bude používaný pre účely šifrovania v rámci bezpečnej elektronickej pošty. V prostredí MS Outlook je tiež nutné tento bit nastaviť v prípade, že používateľ nemá iný certifikát, ktorý je možné použiť na šifrovanie

Certifikačný poriadok pre vydávanie kvalifikovaných certifikátov	Strana 12 (celkom 66)
Copyright © První certifikační autorita, a.s.	Verejný dokument

- Dáta Encipherment (nepovinný) – verejný kľúč obsiahnutý v tomto certifikáte bude používaný pre šifrovanie obecných dát, napr. dokumentov.
- v prípade, že je zaručený elektronický podpis založený na kvalifikovanom certifikáte používaný pre autentizáciu, musí byť podpisujúca osoba prevádzkovateľom príslušnej aplikácie informovaná, či má alebo nemá možnosť zoznámiť sa s údajmi, ktoré podpisuje.

1.4.2 Obmedzenie použitia certifikátu

Certifikáty nesmú byť využívané v rozpore s účelom vydania alebo so ZoEP (ČR, SR).

1.5 Správa politiky

1.5.1 Organizácia spravujúca certifikačný poriadok alebo CPS

První certifikační autorita, a.s.
Podvinný mlýn 2178 / 6
190 00 Praha 9
Česká republika

1.5.2 Kontaktná osoba organizácie spravujúcej certifikačný poriadok alebo CPS

Riaditeľ spoločnosti První certifikační autorita, a.s., určuje kontaktnú osobu, ktorej e-mail, telefónne číslo a fax sú uvedené na internetovej informačnej adrese.

1.5.3 Subjekt zodpovedný za rozhodovanie o súlade postupov poskytovateľa s postupmi iných poskytovateľov certifikačných služieb

Jedinou osobou, ktorá je zodpovedná za rozhodovanie o súlade postupov I.CA s postupmi iných poskytovateľov certifikačných služieb, je riaditeľ spoločnosti První certifikační autorita, a.s. Ďalej platí ustanovenie kapitoly 3.2.6.

1.5.4 Postupy pri schválení súladu podľa bodu 1.5.3

V prípade, že je potrebné s ohľadom na kapitolu 1.5.3 uskutočniť zmeny v zodpovedajúcej CPS a tomto CP, určuje riaditeľ I.CA osobu, ktorá je oprávnená zmeny uskutočňovať.

1.6 Prehľad použitých pojmov a skratiek

Nižšie uvedený prehľad pojmov a skratiek je platný pre tento dokument. V prípade pojmov môže byť na pravej strane v zátvorke uvedený zdroj, v ktorom sa nachádza pôvodný pojem vrátane definície. 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.

Tabuľka 3 – Pojmy a skratky

Pojem	Vysvetlenie
CA	centrálne pracovisko Certifikačnej autority I.CA
Certifikát	dátová správa, ktorá je vydaná poskytovateľom certifikačných služieb, spojuje dáta pre overovanie elektronických podpisov (ČR, SR) s podpisujúcou osobou a umožňuje overiť jej identitu, alebo spojuje dáta pre overovanie elektronických značiek (ČR) s označujúcou osobou a umožňuje overiť jej identitu
Certifikát I.CA	kvalifikovaný certifikát poskytovateľa certifikačných služieb v oblasti vydávania certifikátov, ktorý sa riadi špeciálnymi dokumentmi vydanými I.CA: § „Certifikační politika pro nadřízený kvalifikovaný systémový certifikát (ZoEP ČR) nebo certifikát I.CA (ZoEP SR)“

Certifikačný poriadok pre vydávanie kvalifikovaných certifikátov	Strana 13 (celkom 66)
Copyright © První certifikační autorita, a.s.	Verejný dokument

	§ „Certifikační prováděcí směrnici pro nadřazený kvalifikovaný systémový certifikát (ZoEP ČR) nebo certifikát I.CA (ZoEP SR)“
CP	Certifikačný poriadok (verejný dokument)
CPS	Pravidlá na výkon certifikačných činností (SR), resp. Certifikační prováděcí směrnice (ČR) (neverejný dokument)
CRL (Certificate Revocation List)	zoznam zrušených certifikátov
Čas	svetový čas (UTC)
DN	Distinguished Name – reťazce položky Subject certifikátu, naplnované údajmi zo žiadosti o kvalifikovaný certifikát, z ktorých niektoré sú overované I.CA podľa pravidiel uvedených v tomto CP
Držiteľ certifikátu ¹	§ česká legislatíva - fyzická osoba, právnická osoba alebo organizačná zložka štátu, ktorá požiadala o vydanie kvalifikovaného certifikátu alebo kvalifikovaného systémového certifikátu pre seba alebo pre podpisujúcu osobu, a ktorej bol kvalifikovaný certifikát alebo kvalifikovaný systémový certifikát vydaný § slovenská legislatíva – fyzická osoba, ktorej bol na základe slovenskej legislatívy certifikát vydaný
Elektronický podpis	Údaje v elektronickej podobe, ktoré sú pripojení k dátovej správe alebo sú s ňou logicky spojené a ktoré slúžia ako metóda k jednoznačnému overeniu identity podpísanej osoby vo vzťahu k dátovej správe
ETSI	E uropean T elecommunications S tandards I nstitute
IETF	I nternet E ngineering T ask F orce
EPS	Elektrická požiarňa signalizácia
I.CA	První certifikační autorita, a.s., akreditovaný poskytovateľ certifikačných služieb
Kvalifikovaný certifikát (QC)	certifikát, ktorý má náležitosti podľa platnej legislatívy (ZoEP ČR, SR) a bol vydaný kvalifikovaným poskytovateľom certifikačných služieb
MI ČR	Ministerstvo informatiky České republiky
Nadriadený kvalifikovaný systémový certifikát	kvalifikovaný systémový certifikát poskytovateľa certifikačných služieb v oblasti vydávania certifikátov, ktorý sa riadi špeciálnymi dokumentami vydanými I.CA : <ul style="list-style-type: none"> • „Certifikační politika pro nadřazený kvalifikovaný systémový certifikát (ZoEP ČR) nebo certifikát I.CA (ZoEP SR)“ • „Certifikační prováděcí směrnici pro nadřazený kvalifikovaný systémový certifikát (ZoEP ČR) nebo certifikát I.CA (ZoEP SR)“
Následný kvalifikovaný certifikát	kvalifikovaný certifikát, ktorý bol v súlade so zmluvou o poskytovaní kvalifikovanej certifikačnej služby, uzatvorenou medzi koncovým používateľom a I.CA vydaný koncovému používateľovi na základe novej žiadosti o kvalifikovaný certifikát elektronicke podpísanej platnými dátami pre vytváranie elektronicke podpisov súvisiacimi s už vydaným kvalifikovaným certifikátom, ku ktorému je vydávaný tento následný kvalifikovaný certifikát
NIST	N ational I nstitute of S tandards and T echnology
OID	(Object Identifier) číselná identifikácia objektu v rámci jednotnej klasifikácie objektov podľa ISO/ITU
Párové dáta	jedinečná dáta pre vytváranie elektronickeho podpisu (ČR, SR) alebo elektronicke značky (ČR) spolu so zodpovedajúcimi dátami pre overovanie elektronickeho podpisu (ČR, SR) alebo elektronicke značky (ČR)
Podpisujúca osoba	fyzická osoba, ktorá je držiteľom prostriedku pre vytváranie elektronickeho podpisov a jedná svojim menom alebo menom inej fyzickej alebo právnickej osoby

¹ V ďalšom texte budeme takýto subjekt nazývať aj držiteľom, pokiaľ bude jasné, že sa jedná o držiteľa kvalifikovaného certifikátu alebo kvalifikovaného systémového certifikátu

Certifikačný poriadok pre vydávanie kvalifikovaných certifikátov	Strana 14 (celkom 66)
Copyright © První certifikační autorita, a.s.	Verejný dokument

RA	registračná autorita Certifikačnej autority I.CA – súhrnný názov pre VSRA, VMRA, SRA. Používa sa v prípadoch, keď nie je podstatný majiteľ registračnej autority ani jej forma
Zmluvný partner	poskytovateľ certifikačných služieb, ktorý zaisťuje na základe písomnej zmluvy pre I.CA certifikačné služby alebo ich časti - najčastejšie sa jedná o zmluvné RA
Súkromný kľúč	jedinečné dáta pre vytváranie elektronického podpisu (ČR, SR) alebo elektronické značky (ČR)
SRA	zmluvná registračná autorita Certifikačnej autority I.CA - plní obdobné funkcie ako VSRA alebo VMRA na základe písomnej zmluvy medzi I.CA a prevádzkovateľom SRA
Štatút kvalifikovaného certifikátu	stav, v ktorom sa kvalifikovaný certifikát nachádza, t.j. v stave platnosti, neplatnosti, zrušenia, zablokovania
Spoliehajúca sa strana	<ul style="list-style-type: none"> • česká legislatíva - subjekt, spoliehajúci sa pri svojej činnosti na kvalifikovaný certifikát alebo kvalifikovaný systémový certifikát, vydaný I.CA • slovenská legislatíva - subjekt, spoliehajúci sa pri svojej činnosti na kvalifikovaný certifikát, vydaný I.CA
UPS	Uninterruptible Power Supply
UTC	Universal Co-ordinated Time, Štandard prijatý 1.1.1972 pre svetový koordinovaný čas. Funkciu "oficiálneho časomerača" atomového času pre celý svet vykonáva Bureau International de l'Heure (BIPM)
Veřejný kľúč	jedinečné dáta pre overovanie elektronického podpisu (ČR, SR) alebo elektronické značky (ČR)
VMRA	vlastná mobilná registračná autorita Certifikačnej autority I.CA
VoEP	<ul style="list-style-type: none"> • vyhláška České republiky č. 378/2006 Sb. o postupech kvalifikovaných poskytovateľů certifikačných služieb, o požiadavkách na nástroje elektronického podpisu a o požiadavkách na ochranu dát pro vytváření elektronických značek (vyhláška o postupoch kvalifikovaných poskytovateľov certifikačných služieb) • vyhláška Slovenskej republiky č. 540/2002 Z.z. o podmienkach na poskytovanie akreditovaných certifikačných služieb a o požiadavkách na audit, rozsah auditu a kvalifikáciu audítorov
VSRA	vlastní stacionárna registračná autorita Certifikačnej autority I.CA
Zablokovanie	stav, v ktorom sa kvalifikovaný certifikát alebo kvalifikovaný systémový certifikát nachádza od doby, keď ho I.CA zneplatnila, do doby, keď I.CA zverejnila CRL, v ktorom je tento kvalifikovaný certifikát alebo kvalifikovaný systémový certifikát po prvýkrát zaradený
Zaručený elektronický podpis	elektronický podpis, ktorý spĺňa nasledovné požiadavky : <ul style="list-style-type: none"> • je jednoznačne spojený s podpisujúcou osobou • umožňuje identifikáciu podpisujúcej osoby vo vzťahu k dátovej správe • bol vytvorený a pripojený k dátovej správe pomocou prostriedkov, ktoré podpisujúca osoba môže udržať pod svojou výhradnou kontrolou • je k dátovej správe, ku ktorej sa vzťahuje, pripojená takým spôsobom, že je možné zistiť akúkoľvek následnú zmenu dát
Zneplatnenie	stav kvalifikovaného certifikátu, ktorý bol I.CA zneplatnený – tomuto certifikátu už nie je možné obnoviť platnosť
ZoEP	<ul style="list-style-type: none"> • aktuálne znenie zákona České republiky č. 227/2000 Sb., o elektronickom podpise a o zmene niektorých ďalších zákonů (zákon o elektronickom podpise), ako vyplýva zo zmien uskutočnených zákonom č. 226/2002 Sb., zákonom č. 517/2002 Sb., a zákonom č. 440/2004 Sb. • aktuálne znenie zákona Slovenskej republiky č. 215/2002 Z.z. o elektronickom podpise a o zmene a doplnení niektorých zákonov

<i>Certifikačný poriadok pre vydávanie kvalifikovaných certifikátov</i>	<i>Strana 15 (celkom 66)</i>
<i>Copyright © První certifikační autorita, a.s.</i>	<i>Verejný dokument</i>

Žiadosť o službu (Žiadosť)	Formálny dokument žiadosti o niektorú zo služieb poskytovaných I.CA napr. žiadosť o vydanie kvalifikovaného certifikátu, žiadosť o zrušenie kvalifikovaného certifikátu, atď.
Žiadosť o vydanie kvalifikovaného certifikátu	formálny štandardný dokument elektronickej žiadosti o vydanie kvalifikovaného certifikátu podľa prípustných noriem a smerníc definovaných v tejto CP

Certifikačný poriadok pre vydávanie kvalifikovaných certifikátov	Strana 16 (celkom 66)
Copyright © První certifikační autorita, a.s.	Verejný dokument

2 Zodpovednosti za zverejňovanie a úložisko informácií a dokumentácie

2.1 Úložisko informácií a dokumentácie

S ohľadom na požiadavky ZoEP zriaďuje I.CA úložisko informácií a dokumentácie.

2.2 Zverejňovanie informácií a dokumentácie

Základné adresy, na ktorých je možné nájsť verejné informácie o I.CA, t.j. CP, Správy pre používateľa, ďalšie informácie podľa ZoEP, ostatné verejné dokumenty, atď., (ďalej tiež informačné adresy), prípadne odkazy pre zistenie ďalších informácií, sú :

- a) První certifikační autorita, a.s.
Podvinný mlýn 2178/6, 190 00 Praha 9, Česká republika
- b) internetová adresa <http://www.ica.cz> (ďalej tiež internetová informačná adresa)
- c) sídla registračných autorít

Kontaktné adresy, ktoré slúžia pre kontakt verejnosti s I.CA (ďalej tiež kontaktné adresy), sú :

- a) sídlo registračnej autority, ktorá zmluvný vzťah s I.CA sprostredkovala
- b) elektronická poštová adresa info@ica.cz

Vyššie uvedené informačné a kontaktné adresy I.CA zverejňuje na svojej internetovej informačnej adrese, pracoviskách SRA a VSRA. Pracovníci I.CA a zmluvných partnerov (SRA) sú takisto povinní tieto informácie na vyžiadanie poskytnúť všetkým používateľom. To isté platí aj v prípade, že dôjde k zmene kontaktných adries.

Informácie o verejnom certifikáte je možné získať na adrese <http://www.ica.cz/>. Priamo sa zverejňujú nasledujúce informácie (ostatné informácie je možné získať z certifikátu) :

- číslo certifikátu
- obsah atribútu Obecné meno (Common Name, kapitoly 3.1.1 a 3.1.2)
- údaj o počiatku platnosti (s uvedením hodiny, minúty a sekundy)
- odkazy na miesto, kde je možné certifikát získať v určených formátoch (DER, PEM, TXT).

I.CA garantuje zaistenie nepretržitej dostupnosti a integrity zoznamu vydaných certifikátov.

Informácie o CRL je možné získať na adrese <http://www.ica.cz/>. Priamo sa zverejňujú nasledujúce informácie (ostatné informácie je možné získať zo samotného CRL) :

- dátum vydania CRL
- číslo CRL
- odkazy na miesto, kde je možné CRL získať v určených formátoch (DER, PEM, TXT)

Povoleným protokolom pre prístup k informáciám o :

- konkrétnych CP a Správy pre používateľa - HTTP
- vydaných verejných certifikátoch - HTTP, HTTPS, FTP

Certifikačný poriadok pre vydávanie kvalifikovaných certifikátov	Strana 17 (celkom 66)
Copyright © První certifikační autorita, a.s.	Verejný dokument

- zoznamoch zrušených certifikátov - HTTP, HTTPS, FTP

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

V prípadoch odňatia akreditácie alebo zneužitia, resp. vzniku odôvodnenej obavy zo zneužitia dát pre vytváranie elektronických značiek (ZoEP ČR) alebo elektronických podpisov (ZoEP SR) vydávaných certifikátov alebo zoznamov zrušených certifikátov, oznámi I.CA túto skutočnosť na svojej internetovej informačnej adrese a prostredníctvom celoštátne distribuovaného denníka Mladá fronta Dnes (ČR).

2.3 Periodicita zverejňovania informácií

I.CA zverejňuje informácie s nasledujúcou periodicitou :

- Certifikačný poriadok - pred prvým vydaním certifikátu podľa tohto CP
- Správa pre používateľa – pri zahájení poskytovanej certifikačnej služby v oblasti vydávania certifikátov, resp. pri jej zmene
- Získanie alebo odňatie akreditácie podľa ZoEP – okamžite
- informácie o zrušení nadriadeného kvalifikovaného systémového certifikátu (ZoEP ČR) alebo certifikátu I.CA (ZoEP SR) s uvedením dôvodu zrušenia (v prípade zneužitia alebo vzniku odôvodnenej obavy zo zneužitia dát pre vytváranie elektronických značiek (ZoEP ČR) alebo elektronických podpisov (ZoEP SR), určených pre označovanie (ZoEP ČR) alebo podpisovanie (ZoEP SR) vydávaných certifikátov a zoznamov zrušených certifikátov) – bezodkladne
- Aktualizácia zoznamu vydaných certifikátov – okamžite pri každom vydaní nového certifikátu
- Vydávanie zoznamu zrušených certifikátov - táto povinnosť je realizovaná periodickým vydávaním CRL maximálne jedenkrát za 12 hodín (spravidla po 8 hodinách). Vydávanie CRL je nepretržité – 7 dní v týždni. Internetové adresy, na ktorých je možné získať CRL vzdialeným prístupom, sú uvedené na internetovej informačnej adrese I.CA a sú taktiež uvedené v každom certifikáte. I.CA zverejňuje zoznamy zrušených certifikátov najmenej dvoma na sebe nezávislými spôsobmi vzdialeného prístupu.
- Ostatné verejné informácie – nie je vopred určené, všeobecne však platí, že tieto informácie musia odrážať aktuálny stav poskytovaných kvalifikovaných certifikačných služieb.

2.4 Riadenie prístupu k jednotlivým typom úložísk

Prístup ku konkrétnym typom úložísk poverenými pracovníkmi I.CA je definovaný internou dokumentáciou.

3 Identifikácia a autentizácia

3.1 Pomenovávanie

3.1.1 Typy mien

Tabuľka 4 – nadriadený kvalifikovaný systémový certifikát (ZoEP ČR) - položky Subject a Issuer

Položka	Hodnota
Organization (O)	První certifikační autorita, a.s.
CommonName (CN)	I.CA – Qualified root certificate
Country (C)	CZ

Tabuľka 4a – certifikát I.CA (ZoEP SR) - položky Subject a Issuer

Položka	Hodnota
Organization (O)	Narodny bezpecnostny urad
CommonName (CN)	KCA NBU SR
Country (C)	SK
OrganizationUnit (OU)	Sekcia IBEP
Locality (L)	Bratislava

Tabuľka 5 – Základné položky certifikátu (Basic Certificate Fields)

Atribút	Kódovanie	Počet	Žiadosť	Význam	Príklad	Doloženie ²
CountryName	PS	=1	A	kap. 3.1.2.1	CZ	primár. dokl.
CommonName	U8,(BMP) ³	=1	A	kap. 3.1.2.2, resp. pseudonym, nasledovaný řřezazcom „ – PSEUDONYM“	Ing. Petr Jan Holoubek PhD, resp. Kokořka – PSEUDONYM	primár. dokl.
StateOrProvinceName	U8,(BMP)	1	N	kap. 3.1.2.3	Praha	primár. dokl.
LocalityName	U8,(BMP)	1	N	kap. 3.1.2.4	Praha 7 Ovinecká 1047/17 17000	primár. dokl.
OrganizationName	U8,(BMP)	1	N	kap. 3.1.2.5	Společnost, a.s.	VOR ⁴ , ŽL ⁵
OrganizationalUnitName	U8,(BMP)	M	N	kap. 3.1.2.6	Odbor systému a síte	POZ ⁶
Pkcs9_EmailAddress	IA5	1	N	kap. 3.1.2.7	holy@quick.cz	
GivenName	U8,(BMP)	1	N1	kap. 3.1.2.8	Petr Jan	primár. dokl.
Initials	U8,(BMP)	1	N	kap. 3.1.2.9	PJH	primár. dokl.
Name	U8,(BMP)	1	N1	kap. 3.1.2.10	Ing. Petr Jan	primár.

² Vid' uvedené kapitoly v stípci „Význam“

³ Pre certifikáty podľa ZoEP SR je použité iba kódovanie U8 – UTF8String

⁴ Výpis z obchodného registra

⁵ Živnostenský list

⁶ Potvrdenie o zamestnaní

					Holoubek PhD	dokl.
Surname	U8,(BMP)	1	N1	kap. 3.1.2.11	Holoubek	primár. dokl.
Title	U8,(BMP)	M	N	kap. 3.1.2.12	specialista systému a siete	POZ
SerialNumber	PS	1	N1	kap. 3.1.2.13	ICA - 10020184	-
GenerationQualifier	U8,(BMP)	1	N	kap. 3.1.2.14	MI.	primár. dokl.
Pseudonym	U8,(BMP)	1	N1	kap. 3.1.2.15	kokoska	-

Tabuľka 6 – Rozširujúce položky certifikátu (extensions)

Atribút	Kódovanie	Počet	Žiadosť	Význam	Příklad	Doložení
otherName	Dle RFC3280	M	N	kap. 3.1.2.16		
rfc822Name	IA5	M	N	kap. 3.1.2.16	holy@quick.cz	
dNSName	IA5	M	N	kap. 3.1.2.16	www.moje.cz	čestné prehlásenie
uniformResourceIdentifier	IA5	M	N	kap. 3.1.2.16	http:// www.moje.cz	čestné prehlásenie
iPAddress	Dle RFC3280	M	N	kap. 3.1.2.16	172.17.5.3	čestné prehlásenie

Legenda :

- **Kódovanie** určuje množinu povolených kódovaní podľa ASN.1 pre danú položku. Použité typy kódovaní sú : **PS** - PrintableString, **IA5** - IA5String, **U8** - UTF8String, **BMP** - BMPString.
- **Počet** udáva počet výskytov danej položky DN v žiadosti o certifikát, resp. v certifikáte. Použité skratky majú nasledujúci význam :
 - **=1** - práve jedna
 - **1** - maximálne jedna
 - **M** - ľubovoľný počet
- **Žiadosť** udáva výskyt danej položky DN v žiadosti o certifikát, resp. v certifikáte. Použité skratky majú nasledujúci význam :
 - **A** - musí byť v žiadosti obsiahnuté
 - **N** - nemusí, ale môže byť v žiadosti obsiahnuté
 - **N1** - v prvotnej žiadosti o certifikát nesmie byť uvedené, je povolené iba v žiadosti o obnovenie certifikátu, pokiaľ je obsiahnuté v prvotnom certifikáte

3.1.2 Požiadavka na významovosť mien

Kontroly :

- prítomnosť nepovolených znakov (v závislosti na typu poľa) - v prípade výskytu nepovolených znakov sa žiadosť neprijme
- prítomnosť všetkých povinných položiek - pokiaľ niektorá z povinných položiek nie je vyplnená, žiadosť sa neprijme
- odstraňujú sa úvodné a koncové medzery (0x20) a skupiny medzier uprostred položky sa redukujú na jedinú medzeru, toto platí aj pre „whitespaces“ (ASCII, Unicode : 0x09 – 0x0D, 0x20)
- fyzická osoba nepodnikateľ /pseudonym : povinné položky – CommonName, Country
- fyzická osoba podnikateľ/zamestnanec: povinné položky – CommonName, Country, Organization

Certifikačný poriadok pre vydávanie kvalifikovaných certifikátov	Strana 20 (celkom 66)
Copyright © První certifikační autorita, a.s.	Verejný dokument

Pri kontrole rozdielnosti či zhodnosti DN je použitý nasledujúci spôsob porovnávania reťazcov

:

- ak sú dva rovnaké reťazce rôzne kódované, sú napriek tomu považované za zhodné
- porovnávanie reťazcov vo všetkých kódovaniach je závislé na veľkosti písma
- pri porovnávaní reťazcov vo všetkých kódovaniach sú odstraňované medzerové znaky. (napr. reťazce „Martin“ a „ Martin“ sú zhodné)

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

3.1.2.1 Country (Štát)

Atribút Country (Štát) môže obsahovať iba kód štátu, v ktorom má žiadateľ o certifikát uvedené miesto trvalého pobytu alebo sídla - uvedené v primárnom doklade.

RA kontroluje správnosť podľa primárneho dokladu (pokiaľ nie je štát explicitne uvedený, uvedie sa štát, ktorý predkladaný doklad vydal), v prípade nezahody žiadosť odmietne. Kód štátu musí zodpovedať norme ISO 3166.

3.1.2.2 Common Name (Všeobecné meno)

Atribút CommonName (Všeobecné meno) môže obsahovať :

- celé meno (t.j. meno a priezvisko, prípadne ďalšie meno/mená a tituly), uvedené v primárnom doklade žiadateľa o certifikát - RA kontroluje správnosť podľa primárneho dokladu, v prípade nezahody žiadosť odmietne, alebo
- pseudonym, doplnený reťazcom „ – PSEUDONYM“

Atribút môže obsahovať znaky s diakritikou.

3.1.2.3 StateorProvinceName (kraj)

Atribút StateorProvinceName (Kraj) môže obsahovať iba označenie nižšieho územno-správneho celku, do ktorého spadá miesto trvalého bydliska podľa primárneho dokladu žiadateľa o certifikát, teda miesto, obec alebo inú správnu jednotku, ktorá je v osobnom doklade uvedená

Z obsahu musí byť zrejmé, či sa jedná o kraj alebo iný celok. RA prijímajúca predmetnú žiadosť správnosť tohto údaja v prípade, že bol uvedený, kontroluje; v prípade nezahody danú žiadosť odmietne. Atribút môže obsahovať znaky s diakritikou.

3.1.2.4 Locality (mesto)

Atribút Locality (Mesto) môže obsahovať mesto trvalého bydliska podľa primárneho dokladu žiadateľa o certifikát, teda mesto, obec alebo inú správnu jednotku, ktorá je v primárnom doklade uvedená.

RA prijímajúca predmetnou žiadosť správnosť tohto údaja v prípade, že bol uvedený, kontroluje; v prípade nezahody danou žiadosť odmietne. Atribút môže obsahovať znaky s diakritikou.

3.1.2.5 Organization (organizace)

Atribút Organization (Organizácia) môže obsahovať iba obchodný názov podľa VOR, ŽL, zriaďovacej listiny atď. Žiadateľ o certifikát je povinný doložiť oprávnenosť použitia obsahu daného atribútu nespochybniteľným spôsobom⁷.

RA prijímajúca predmetnú žiadosť správnosť tohto údaja v prípade, že bol uvedený, kontroluje; v prípade nezahody danú žiadosť odmietne. Atribút môže obsahovať znaky s diakritikou.

⁷ Napr. v prípade obchodného mena živnostníka príslušným živnostenským listom, v prípade, že podpisujúca osoba je majiteľom firmy, společníkom alebo zamestnancom, tak výpisom z obchodného registra

<i>Certifikačný poriadok pre vydávanie kvalifikovaných certifikátov</i>	<i>Strana 21 (celkom 66)</i>
<i>Copyright © První certifikační autorita, a.s.</i>	<i>Verejný dokument</i>

3.1.2.6 Organizational Unit (Organizačná jednotka)

Atribút Organization unit (Organizačná jednotka) môže obsahovať iba názov organizačnej jednotky a to výhradne v tom prípade, že bol použitý atribút Organization. Žiadateľ o certifikát je povinný doložiť oprávnenosť použitia obsahu daného atribútu nespochybniteľným spôsobom. RA prijímajúca predmetnú žiadosť správnosť tohto údajov v prípade, že bol uvedený, kontroluje, v prípade nezhody danú žiadosť odmietne. Atribút môže obsahovať znaky s diakritikou a môže sa vyskytovať viackrát.

3.1.2.7 E-mail Address (pkcs9Email Address - elektronická poštovná adresa)

Atribút E-mail Address (Elektronická poštovní adresa) môže obsahovať iba elektronickú poštovnú adresu žiadateľa o certifikát (podľa RFC 822). Vyžaduje sa hodnoverne doložené vlastníctvo tejto elektronickej poštovej adresy alebo čestné prehlásenie⁸ žiadateľa o certifikát, v ktorom toto vlastníctvo potvrdzuje. V prípade nesplnenia tejto podmienky má RA právo danú žiadosť odmietnuť. Atribút nesmie obsahovať znaky s diakritikou.

3.1.2.8 GivenName (Krstné meno/mená)

Atribút rodné meno (Given Name) môže obsahovať iba:

- krstné meno
- krstné meno a ďalšie krstné meno/mená
- alebo krstné a rodné meno

osoby žiadateľa o certifikát tak, ako je uvedené v jej primárnom osobnom doklade. RA, prijímajúca predmetnú žiadosť, obsah tohto atribútu pokiaľ je vyplnený kontroluje oproti predloženému primárnemu osobnému dokladu. V prípade nezhody danú žiadosť odmietne. Položka môže obsahovať znaky s diakritikou.

3.1.2.9 Initials (iniciály)

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

3.1.2.10 Name (Celé meno)

Atribút Name môže obsahovať iba celé meno žiadateľa o certifikát vrátane titulov tak, ako je uvedené v jeho primárnom osobnom doklade, resp. v ďalších dokumentoch, ak sa jedná o titul (doklad o získanom titule). Pokiaľ je atribút vyplnený, RA prijímajúca predmetnú žiadosť obsah tohto atribútu kontroluje a v prípade nezhody danú žiadosť odmietne. Pokiaľ žiadosť obsahuje titul, ktorý nie je uvedený, resp. nekorešponduje s titulom uvedeným v predloženom primárnom osobnom doklade, je žiadateľ o certifikát povinný doložiť oprávnenosť použitia uvedeného titulu nespochybniteľným spôsobom⁹. Položka môže obsahovať znaky s diakritikou.

3.1.2.11 Surname (Priezvisko)

Atribút Surname môže obsahovať iba priezvisko žiadateľa o certifikát, ktoré je v zhode s jeho primárnym osobným dokladom RA, prijímajúca predmetnú žiadosť, obsah tohto atribútu pokiaľ je vyplnený kontroluje oproti predloženému primárnemu osobnému dokladu. V prípade nezhody danú žiadosť odmietne. Položka môže obsahovať znaky s diakritikou.

⁸ Čestné prehlásenie pre účely tohto certifikačného poriadku je realizované formou potvrdenia pravdivosti údajov v zmluve o vydaní kvalifikovaného certifikátu.

⁹ napr. diplomom, v ktorom je uvedené, že žiadateľ má právo daný titul používať

Certifikačný poriadok pre vydávanie kvalifikovaných certifikátov	Strana 22 (celkom 66)
Copyright © První certifikační autorita, a.s.	Verejný dokument

3.1.2.12 Title (titul)

Obsahom atribútu Title (Titul) spravidla býva postavenie žiadateľa o certifikát v určitej (spravidla firemnej) hierarchii. Obsah tohto atribútu sa kontroluje v závislosti na skutočnostiach, ktoré sú v ňom obsiahnuté¹⁰. Atribút môže obsahovať znaky s diakritikou a môže sa vyskytovať viackrát.

3.1.2.13 Serial number (sériové číslo)

Sériové číslo subjektu, ktoré slúži k rozlíšeniu rôznych subjektov v rámci klientely I.CA. Sériové číslo obecné vyplňuje CA a je naplnené reťazcom „ICA - “ a za ním je pripojené na reťazec prevedené identifikačné číslo žiadateľa o certifikát.

3.1.2.14 Generation Qualifier (generačné rozlíšenie)

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

3.1.2.15 Pseudonym (pseudonym)

Pokiaľ žiadateľ o certifikát použil atribút Pseudonym, môže tento atribút obsahovať akúkoľvek sekvenciu povolených znakov. V prípade, že sa jedná o overiteľnú položku, vykoná pracovník RA overenie obsahu tohto atribútu a v prípade nezhody danú žiadosť odmietne. V prípade neoveriteľnej položky pracovník RA iba kontroluje, či sa nejedná o nepovolené výrazy (vulgárne, propagujúce fašizmus, rasovú a triednu nenávisť). O prípustnosti konkrétneho obsahu položky v prípade použitia pseudonymu rozhoduje pracovník RA, ktorý vybavuje žiadosť o vydanie certifikátu. Taktiež nesmú byť dotknuté práva iných subjektov (registrované známky a pod.). Atribút môže obsahovať znaky s diakritikou.

3.1.2.16 Subject Alternative Name (alternatívne meno subjektu)

Pokiaľ žiadateľ o certifikát použil atribút Subject Alternative Name (alternatívne meno), je nutné overiť skutočnosti v ňom uvádzané (pokiaľ sa jedná o skutočnosti vyžadujúce overenie). Ako súčasť alternatívneho mena sa pripúšťa:

- **otherName (ostatné) :**
 - číselný identifikátor podpisujúcej osoby, vedený v centrálnej databáze MPSV¹¹ (IK MPSV)
 - číselný identifikátor úradu, vedený v centrálnej databáze MPSV (IDS MPSV)
 - Microsoft universal principal name
- **rfc822Name (elektronická adresa)** – v prípade naplnenia má táto položka prednosť pred „pkcs9EmailAddress“ a certifikát je prednostne spojený s touto alternatívnou adresou
- **dNSName (meno doménového serveru)** - pokiaľ je doménové meno registrované, vyžaduje sa hodnoverne doložený súhlas vlastníka alebo čestné prehlásenie žiadateľa o certifikát, potvrdzujúce vlastníctvo doménového mena
- **uniformResourceIdentifier - URI (identifikátor zdroje v Internetu)** - pokiaľ je URI registrované, vyžaduje sa hodnoverne doložený súhlas vlastníka alebo čestné prehlásenie žiadateľa o certifikát, v ktorom vlastníctvo URI potvrdzuje
- **iPAddress (IP adresa)** - pokiaľ je IP adresa registrovaná, vyžaduje sa hodnoverne doložený súhlas vlastníka alebo čestné prehlásenie žiadateľa o certifikát, v ktorom vlastníctvo IP adresy potvrdzuje. RA prijímajúca predmetnú žiadosť je povinná, pokiaľ je atribút vyplnený, tuto položku skontrolovať, v prípade nezhody je RA povinná danú žiadosť odmietnuť.

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

¹⁰ napr. pokiaľ žiadateľ požaduje obsah „Praktický lekár“, je možné žiadosť prijať, pokiaľ preukáže, že je praktickým lekárom pokiaľ bude požadovať obsah typu „Linuxový guru“, toto nie je možné skontrolovať a žiadosť sa zamietne.

¹¹ Ministerstvo práce a sociálnych vecí ČR

Certifikačný poriadok pre vydávanie kvalifikovaných certifikátov	Strana 23 (celkom 66)
Copyright © První certifikační autorita, a.s.	Verejný dokument

3.1.3 Anonymita a používanie pseudonymu

Certifikát nie je možné vydať ako anonymný, je možné však vydať certifikát s atribútom Pseudonym.

3.1.4 Pravidla pre interpretáciu rôznych foriem mien

Pokiaľ sa jedná o mena alebo iné skutočnosti, ktoré sú uvedené v osobnom doklade fyzickej osoby alebo v iných dokumentoch, ktoré sú prípustné pre preukazovanie identity, 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 certifikátov nevykonávajú.

3.1.5 Jedinečnosť mien

Jednoznačnosť mena subjektu je zaručená použitím vyššie definovaného postupu pre tvorbu atribútu SerialNumber.

3.1.6 Obchodné značky

Vo vydanom certifikáte sa musia overiteľné údaje vzťahovať k fyzickej osobe. Tieto údaje overujú pracovníci RA.

3.2 Počiatkové overenie identity

3.2.1 Overenie súladu dát, t.j. postup pri overovaní, či má osoba dáta pre vytváranie elektronických podpisov zodpovedajúce dátam pre overovanie elektronických podpisov

Vlastníctvo dát pre vytváranie elektronických podpisov zodpovedajúce dátam pre overovanie elektronických podpisov, ktoré bude daný certifikát obsahovať, sa preukazuje predložením žiadosti o vydanie certifikátu elektronicke podpísanej týmito dátami. Pracovník RA prostredníctvom aplikácie RA toto kontroluje tak, že pomocou dát pre overovanie elektronických podpisov, uvedených v žiadosti o certifikát, overí platnosť elektronického podpisu na tejto žiadosti. Pokiaľ je overenie platnosti elektronického podpisu negatívne, RA žiadosť neprijme a proces vydania certifikátu zastaví.

3.2.2 Overovanie identity právnickej osoby alebo organizačnej zložky štátu

Tieto skutočnosti sú pre aplikáciu tohto vydania tohto CP irelevantné.

3.2.3 Overovanie identity fyzickej osoby

I.CA vyžaduje od žiadateľa o certifikát predloženie jeho nasledujúcich údajov :

- celé občianske meno
- dátum narodenia
- číslo predloženého primárneho osobného dokladu
- adresa trvalého bydliska

Pokiaľ dôjde počas trvania zmluvného vzťahu k I.CA k zmenám vo vyššie uvedených vyžadovaných údajoch, je žiadateľ, resp. držiteľ povinný tieto zmeny ohlásiť I.CA.

Pri registrácii nového žiadateľa/držiteľa o certifikát sa vyžaduje :

- a) V prípade, že sa žiadateľ o certifikát osobne dostaví na RA - predloženie originálu platného primárneho osobného dokladu žiadateľa o certifikát a originálu ďalšieho osobného dokladu (sekundárneho). Primárny osobný doklad pre občanov ČR musí byť občiansky preukaz, resp.

Certifikačný poriadok pre vydávanie kvalifikovaných certifikátov	Strana 24 (celkom 66)
Copyright © První certifikační autorita, a.s.	Verejný dokument

obdobný doklad rovnakej právnej váhy. Primárny osobný doklad pre cudzincov je platný cestovný pas, resp. obdobný doklad rovnakej právnej váhy. Občania Slovenskej republiky môžu ako primárny osobný doklad použiť občiansky preukaz. 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 fyzickej osoby, vybavujúcej žiadosť a ďalej najmenej jeden z nasledujúcich údajov :

- § dátum narodenia žiadateľa (alebo rodné číslo u občanov ČR alebo SR)
- § adresa trvalého bydliska žiadateľa
- § fotografia obličaja žiadateľa

Údaje požadované v sekundárnom osobnom 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 žiadosť prijatá. Príkladom akceptovateľného sekundárneho osobného dokladu sú napr. cestovný pas, vodičský preukaz, služobné preukazy štátnych úradov, preukaz poslanca, služobný preukaz polície, zbrojný preukaz, vojenská knižka, preukaz zdravotného poistenia, preukážka hromadnej dopravy, firemné preukážky, študentský preukaz atď.

V prípade, že je žiadateľ zastupovaný splnomocnencom, vyžaduje sa predloženie originálu platného primárneho osobného dokladu a originálu ďalšieho osobného dokladu (sekundárneho) splnomocnenca. Ďalej sú požadované úradne overené kópie primárneho a sekundárneho osobného dokladu žiadateľa o certifikát (splnomocniteľa). Kvalita primárnych a sekundárnych dokladov ako splnomocnenca, tak aj splnomocniteľa, je uvedená vyššie.

- b) Spôsobilosť žiadateľa o certifikát, resp. splnomocnenca a splnomocniteľa k právnym úkonom
- c) Doklady, preukazujúce právo jednať ako splnomocnenec na základe plnej moci s úradne overeným podpisom splnomocniteľa.
- d) Doklady, preukazujúce väzbu žiadateľa o certifikát na zamestnávateľa (v prípade certifikátu pre zamestnanca)

3.2.4 Neoverené informácie vzťahujúce sa k držiteľovi certifikátu alebo podpisujúcej osobe

V prípade informácií, ktoré sa nedajú overiť, sa postupuje v súlade s kapitolou 3.1.2.

3.2.5 Overovanie špecifických práv

Overovanie špecifických práv sa prevádza v súlade s kapitolou 3.2.3, odstavce c), d).

3.2.6 Kritériá pre interoperabilitu

Prípadná spolupráca s inými poskytovateľmi certifikačných služieb je založená na písomnej zmluve spoločnosti První certifikační autorita, a.s., s konkrétnymi poskytovateľmi certifikačných služieb.

Certifikačný poriadok pre vydávanie kvalifikovaných certifikátov	Strana 25 (celkom 66)
Copyright © První certifikační autorita, a.s.	Verejný dokument

3.3 Identifikácia a autentizácia pri spracovaní požiadaviek na výmenu dát pre overovanie elektronických podpisov v certifikáte

3.3.1 Identifikácia a autentizácia pri rutinnej výmene dát pre vytváranie elektronických podpisov a im zodpovedajúcich dát pre overovanie elektronických podpisov (ďalej „párové dáta“)

Žiadateľ o certifikát vytvorí novú žiadosť o vydanie následného certifikátu, elektronicky podpísanú platnými dátami pre vytváranie elektronických podpisov, súvisiacimi s už vydaným certifikátom, ku ktorému je tento následný certifikát vydávaný.

3.3.2 Identifikácia a autentizácia pri výmene párových dát po zneplatnení certifikátu

I.CA nepodporuje výmenu párových dát už zneplatneného certifikátu. Z tohto dôvodu nie je možné ani prijať žiadosť o následný certifikát, pokiaľ je elektronicky podpísaná dátami pre vytváranie elektronických podpisov príslušnými k certifikátu, ktorý bol už zneplatnený. Jediný spôsob, jak získať nový certifikát, je uvedený v kapitole 4.

3.4 Identifikácia a autentizácia pri spracovaní požiadaviek na zrušenie certifikátu

V prípade **osobného odovzdania žiadosti o zrušenie certifikátu na RA** musí žiadateľ o zrušenie certifikátu preukázať, že je podpisujúcou osobou, resp. jeho držiteľom. V prípade, že je zastupovaný splnomocnencom, platia ustanovenia kapitoly 3.2.3, ods. c). Žiadosť o zrušenie certifikátu musí byť písomná a podpísaná žiadateľom.

V prípade **odovzdania žiadosti o zrušenie certifikátu elektronickou cestou** sú prípustné nasledujúce možnosti :

- podpísaná elektronická správa - (revoke@ica.cz), elektronický podpis musí byť realizovaný dátami pre vytváranie elektronického podpisu príslušnými k predmetnému certifikátu, ktorý má byť zrušený
- nepodpísaná elektronická správa, obsahujúca heslo pre zrušenie certifikátu - (revoke@ica.cz)
- prostredníctvom formulára na internetovej informačnej adrese (<http://www.ica.cz>)

V prípade použitia **listovej zásielky o zrušenie certifikátu** musí byť táto zaslaná doporučené.

Žiadosti o zrušenie certifikátu prijíma I.CA nepretržite iba prostredníctvom odoslania žiadosti elektronickou cestou a listovou zásielkou. Osobné odovzdanie na RA je možné iba v pracovnej dobe príslušnej RA. Postupy v tejto kapitole sú detailne rozpracované v internej dokumentácii.

Po identifikácii a autentizácii sa postupuje spôsobom, uvedeným v kapitole 4.9.3.

Certifikačný poriadok pre vydávanie kvalifikovaných certifikátov	Strana 26 (celkom 66)
Copyright © První certifikační autorita, a.s.	Verejný dokument

4 Požiadavky na životní cyklus certifikátu

4.1 Žiadosť o vydanie certifikátu

4.1.1 Subjekty oprávnené podať žiadosť o vydanie certifikátu

Certifikáty sú I.CA komerčne ponúkanou službou a sú vydávané každému, kto sa zmluvne zaviazal jednať podľa tohto CP.

I.CA požaduje minimálny vek 15 rokov pre osobu, ktorá žiada o certifikát. Žiadatelia o certifikát vo veku od 15 do 18 rokov musia žiadať prostredníctvom svojho zákonného zástupcu.

V prípade fyzickej osoby môže byť žiadateľom o certifikát fyzická osoba, ktorá je spôsobilá k právnym úkonom podľa príslušnej právnej normy. Pokiaľ je žiadateľ zastupovaný splnomocnencom, musí mať splnomocnenec oprávnenie žiadateľa zastupovať.

4.1.2 Registračný proces a zodpovednosti poskytovateľa a žiadateľa

V prípade **prvotného certifikátu**, keď sa žiadateľ, resp. splnomocnenec dostaví na RA, postupuje príslušný pracovník RA v súlade s kapitolou 3.2.3.

4.2 Spracovanie žiadosti o certifikát

4.2.1 Identifikácia a autentizácia

I.CA podporuje nasledujúce typy žiadosti o certifikát :

- Fyzická osoba (podnikateľ/ nepodnikateľ) - určená pre osoby, ktoré žiadajú o certifikát pre osobné účely. Žiadateľ o certifikát, resp. splnomocnenec je povinný predložiť doklady preukazujúce jeho totožnosť a všetky overiteľné údaje uvedené v žiadosti budú na RA kontrolované.
- Fyzická osoba (zamestnanec) - jedná sa o formu certifikátu, keď sa overuje okrem totožnosti tiež väzba fyzickej osoby na jej zamestnávateľa. Žiadateľ o certifikát, resp. splnomocnenec je povinný predložiť doklady preukazujúce jeho totožnosť a všetky overiteľné údaje uvedené v žiadosti budú na RA kontrolované.
- Fyzická osoba (pseudonym) - certifikát, ktorý neobsahuje identifikáciu. Pseudonym môže obsahovať akúkoľvek sekvenciu znakov. Nie sú povolené výrazy vulgárne, propagujúce fašizmus, rasovú a triednu nenávisť. V prípade, že položka Pseudonym obsahuje overiteľný údaj, je žiadateľ povinný tuto skutočnosť v rámci overovacej procedúry na RA doložiť. Aj v tomto prípade je žiadateľ o certifikát, resp. splnomocnenec povinný predložiť doklady preukazujúce jeho totožnosť a všetky overiteľné údaje uvedené v žiadosti budú na RA kontrolované.

Žiadateľ o **prvotný certifikát** vytvorí žiadosť o vydanie certifikátu, elektronicky podpísanú dátami pre vytváranie elektronických podpisov, zodpovedajúce dátam pre overovanie elektronických podpisov. Po vygenerovaní žiadosti o prvotný certifikát a jej následnom uložení na záznamové médium (napr. disketu), sa žiadateľ, resp. splnomocnenec s touto žiadosťou a potrebnými dokladmi (viď. kapitola 3.2.3) dostaví na RA.

Žiadateľ o **následný certifikát** vytvorí žiadosť postupom, uvedeným v kapitole 3.3.1.

Certifikačný poriadok pre vydávanie kvalifikovaných certifikátov	Strana 27 (celkom 66)
Copyright © První certifikační autorita, a.s.	Verejný dokument

4.2.2 Prijatie alebo odmietnutie žiadosti o certifikát

V prípade **prvotného certifikátu** prevedie pracovník RA kontrolu predložených originálov osobných dokladov žiadateľa o certifikát, resp. splnomocnenca a v prípade pochybností o pravosti predloženého primárneho osobného dokladu žiadateľa o certifikát, resp. splnomocnenca odmietne a proces vydávania certifikátu ukončí. V prípade pochybností o pravosti predloženého sekundárneho osobného dokladu, alebo v prípade nezahy vyžadovaných údajov s primárnym osobným dokladom požiadá žiadateľa o certifikát, resp. splnomocnenca o predloženie iného sekundárneho osobného dokladu. Pokiaľ žiadateľ o certifikát, resp. splnomocnenec nepredloží sekundárny osobný doklad požadovaných vlastností, pracovník RA žiadateľa o certifikát, resp. splnomocnenca odmietne a proces vydávania certifikátu ukončí.

V prípade, že fyzickou osobou, vybavujúcou žiadosť o vydanie certifikátu je splnomocnenec, prevedie pracovník RA ďalej kontrolu predložených úradne overených kópií osobných dokladov (primárny a sekundárny) splnomocniteľa a v prípade nezahy vyžadovaných údajov sekundárneho osobného dokladu s primárnym osobným dokladom splnomocniteľa odmietne a proces vydávania certifikátu ukončí.

V prípade, že výsledok vyššie uvedených kontrol je pozitívny, pracovník RA okopíruje predložené osobné doklady (ak nie je zmluvne dohodnuté inak). Dokument „Protokol o podaní žiadosti o vydanie kvalifikovaného certifikátu I.CA“, ktorého súčasťou je veta „**Žiadateľ súhlasí s tým, aby spoločnosť První certifikační autorita, a.s., skladovala vytvorené kópie jeho osobných dokladov v súlade s platnou legislatívou.**“ nechá žiadateľa o certifikát, resp. splnomocnenca, podpísať. Pokiaľ žiadateľ o certifikát, resp. splnomocnenec odmietne tento protokol podpísať, je pracovník RA povinný proces vydávania certifikátu ukončiť a kópie osobných dokladov zničiť – skartovať (ak nie je zmluvne dohodnuté inak). Pokiaľ žiadateľ o vydanie certifikátu požiadá o publikovanie ďalších osobných údajov, musí byť táto skutočnosť explicitne uvedená v zmluve o poskytovaní kvalifikovanej certifikačnej služby.

V prípade **následného certifikátu** sa postupuje v súlade s kapitolou 4.7.

4.2.3 Doba spracovania žiadosti o certifikát

I.CA nestanovuje pevný časový limit, v ktorom dôjde ku spracovaniu žiadosti o certifikát, pretože sa jedná o časový sled nasledujúcich činností, z ktorých niektoré závisia iba na žiadateľovi o certifikát. Časové údaje sú uvedené v nasledujúcom zozname :

- generovanie žiadosti o vydanie certifikátu – rádovo jednotky minút
- vydanie certifikátu :
 - prvotný certifikát (žadateľ sa MUSÍ osobne dostaviť na RA) - doba vydania certifikátu je do 15 minút a len vo výnimočných prípadoch môže byť táto doba dlhšia
 - následný certifikát (žadateľ sa NEMUSÍ osobne dostaviť na RA) – rádovo jednotky minút

4.3 Vydanie certifikátu

4.3.1 Úkony CA v priebehu vydania certifikátu

V procese vydávania certifikátu prevádzajú operátori CA nevyhnutné kontroly a ďalšie činnosti, popísané v internej dokumentácii.

4.3.2 Oznámenie o vydaní certifikátu držiteľovi certifikátu alebo podpisujúcej osobe

V procese vydávania prvotného certifikátu je žiadateľ o certifikát, resp. splnomocnenec informovaný prostredníctvom pracovníka RA.

V procese vydávania následného certifikátu je žiadateľ o certifikát, resp. splnomocnenec, v prípade vybavovaní žiadosti na RA, informovaný prostredníctvom pracovníka RA. V prípade, že žiadateľ o certifikát žiada o následný certifikát elektronickou cestou, je mu certifikát elektronicky zaslaný.

Certifikačný poriadok pre vydávanie kvalifikovaných certifikátov	Strana 28 (celkom 66)
Copyright © První certifikační autorita, a.s.	Verejný dokument

4.4 Prevzatie vydaného certifikátu

4.4.1 Úkony spojené s prevzatím certifikátu

Pokiaľ boli splnené podmienky pre vydanie **prvotného certifikátu**, t.j. :

- splnené podmienky registrácie (kapitoly 3.2, 3.3)
- zaplatenie určeného poplatku (ak nie je zmluvne dohodnuté inak) – uvedené v aktuálnom cenníku – vid. kapitola 2.2.
- preukázané vlastníctvo dát pre vytváranie elektronických podpisov zodpovedajúcich dátam pre overovanie elektronických podpisov, ktoré bude vydaný certifikát obsahovať (kapitoly 3.2.1, 4.7.1)
- podpis príslušnej zmluvy – rozumie sa zmluva o poskytovaní kvalifikovanej certifikačnej služby

je povinnosťou žiadateľa o certifikát tento certifikát prijať. Jediným spôsobom, akým môže žiadateľ postupovať v prípade, že tento certifikát nechce, je požiadať v súlade so zodpovedajúcim CP o jeho zrušenie.

Pracovník RA odovzdá žiadateľovi záznamové médium (napr. disketa), obsahujúce požadovaný certifikát (v predpísaných formátoch) a zodpovedajúci nadriadený kvalifikovaný systémový certifikát (ZoEP ČR) alebo certifikát I.CA (ZoEP SR). V prípade, že bola v žiadosti uvedená elektronická adresa, je certifikát v predpísaných formátoch na túto adresu taktiež zaslaný.

V prípade podania žiadosti o vydanie **následného certifikátu** elektronickou cestou zašle I.CA na žiadateľovu elektronickú adresu certifikát v predpísaných formátoch, v prípade vybavovania žiadosti na RA, získa žiadateľ certifikát od pracovníka RA.

Zodpovedajúci CP získa klient na RA, resp. stiahnutím z informačnej adresy – viz kapitola 2.2.

4.4.2 Zverejňovanie vydaných certifikátov poskytovateľom

I.CA je povinná zaistiť bezodkladné zverejnenie certifikátu (verejného) vrátane tých údajov, ku ktorým dal žiadateľ, resp. držiteľ tohto certifikátu súhlas.

4.4.3 Oznámenie o vydaní certifikátu iným subjektom

V prípadoch vydania prvotného certifikátu, resp. následného certifikátu pri dostavení sa žiadateľa/splnomocniteľa na RA, získa oznámenie o vydanom certifikáte pracovník RA.

4.5 Použitie párových dát a certifikátu

4.5.1 Použitie dát pre vytváranie elektronických podpisov a certifikátu držiteľom alebo podpisujúcou osobou

Držitelia certifikátov sú povinní :

- bez zbytočného odkladu podávať presné, pravdivé a úplné informácie I.CA vo vzťahu k vydanému certifikátu
- dodržiavať všetky ustanovenia príslušnej zmluvy – rozumie sa zmluva o poskytovaní kvalifikovanej certifikačnej služby
- zoznámiť s relevantnými ustanoveniami príslušnej zmluvy o poskytovaní kvalifikovanej certifikačnej služby o vydaní a používaní certifikátu prípadné podpisujúce osoby a dbať na ich dodržiavanie zo strany týchto osôb

Podpisujúca osoba je povinná :

- používať certifikáty výhradne v súlade s zodpovedajúcim CP
- dodržiavať všetky ustanovenia zodpovedajúceho CP

Certifikačný poriadok pre vydávanie kvalifikovaných certifikátov	Strana 29 (celkom 66)
Copyright © První certifikační autorita, a.s.	Verejný dokument

- dodržiavať všetky relevantné ustanovenia príslušnej zmluvy - rozumie sa zmluva o poskytovaní kvalifikovanej certifikačnej služby, vzťahujúca sa k certifikátu, s ktorými bola zoznámená jeho prípadným držiteľom
- riadiť sa platnou legislatívou

4.5.2 Použitie dát pre overovanie elektronických podpisov a certifikátu spoliehajúcou sa stranou

Spoliehajúce sa strany sú povinné :

- používať certifikáty v súlade s zodpovedajúcim CP, legislatívou, ZoEP, VoEP
- uskutočňovať všetky úkony potrebné k tomu, aby si overili, že elektronický podpis je platný a zodpovedajúci certifikát nebol zrušený. Najmä v certifikáte kontrolovať :
 - elektronickú značku (ZoEP ČR) alebo elektronický podpis (ZoEP SR) nadriadeného kvalifikovaného systémového certifikátu (ZoEP ČR) alebo certifikátu I.CA (ZoEP SR), vytvorenú/vytvorený I.CA
 - dôveryhodnosť príslušného nadriadeného kvalifikovaného systémového certifikátu (ZoEP ČR) alebo certifikátu I.CA (ZoEP SR)

4.6 Obnovenie certifikátu

4.6.1 Podmienky pre obnovenie certifikátu

Služba nie je poskytovaná - tieto skutočnosti sú pre aplikáciu tohto vydania tohto CP irelevantné.

4.6.2 Subjekty oprávnené požadovať obnovenie certifikátu

Služba nie je poskytovaná - tieto skutočnosti sú pre aplikáciu tohto vydania tohto CP irelevantné.

4.6.3 Spracovanie požiadavku na obnovenie certifikátu

Služba nie je poskytovaná - tieto skutočnosti sú pre aplikáciu tohto vydania tohto CP irelevantné.

4.6.4 Oznámenie o vydaní obnoveného certifikátu držiteľovi alebo podpisujúcej osobe

Služba nie je poskytovaná - tieto skutočnosti sú pre aplikáciu tohto vydania tohto CP irelevantné.

4.6.5 Úkony spojené s prevzatím obnoveného certifikátu

Služba nie je poskytovaná - tieto skutočnosti sú pre aplikáciu tohto vydania tohto CP irelevantné.

4.6.6 Zverejnenie vydaných obnovených kvalifikovaných certifikátov poskytovateľom

Služba nie je poskytovaná - tieto skutočnosti sú pre aplikáciu tohto vydania tohto CP irelevantné.

4.6.7 Oznámenie o vydaní obnoveného certifikátu iným subjektom

Služba nie je poskytovaná - tieto skutočnosti sú pre aplikáciu tohto vydania tohto CP irelevantné.

Certifikačný poriadok pre vydávanie kvalifikovaných certifikátov	Strana 30 (celkom 66)
Copyright © První certifikační autorita, a.s.	Verejný dokument

4.7 Výmena dát pre overovanie elektronických podpisov v certifikáte

4.7.1 Podmienky pre výmenu dát pre overovanie elektronických podpisov v certifikáte

Jedinou akceptovateľnou formou získanie následného certifikátu, je certifikát, vydaný na základe novej žiadosti o vydanie certifikátu, elektronicky podpísanej platnými dátami pre vytváranie elektronických podpisov súvisiacimi s už vydaným certifikátom, ku ktorému je vydávaný tento následný certifikát. I.CA si vyhradzuje právo akceptovania aj iných foriem postupov pri vydávaní následných certifikátov.

4.7.2 Subjekty oprávnené požadovať výmenu dát pre overovanie elektronických podpisov v certifikáte

Výmenu dát pre overovanie elektronických podpisov sú oprávnení požadovať držitelia certifikátu alebo podpisujúce osoby.

4.7.3 Spracovanie požiadavku na výmenu dát pre overovanie elektronických podpisov

Pracovisko CA overuje údaje (DN) žiadosti o následný certifikát, ktoré musí byť rovnaké ako údaje (DN) v prvotnom certifikáte, iba dáta pre overovanie elektronických podpisov musia byť iné. Ostatné položky následného certifikátu podliehajú aktuálnym pravidlám pre certifikáty.

V prípade, že je žiadosť zaslaná na I.CA elektronickou cestou, musí byť elektronicky podpísaná dátami pre vytváranie elektronických podpisov súvisiacimi s platným certifikátom, ku ktorému žiada o následný certifikát. Pokiaľ žiadosť nemá vyššie uvedené náležitosti, napr. je síce elektronicky podpísaná, ale tento elektronický podpis nie je možné overiť dátami pre overovanie elektronických podpisov uvedených v pôvodnom a následnom certifikáte, I.CA následný certifikát nevydá.

V prípade, že sa žiadateľ o certifikát, resp. splnomocnenec dostaví so žiadosťou na RA, postupuje sa obdobne, ako pri vydávaní prvotného certifikátu.

4.7.4 Oznámenie o vydaní certifikátu s vymenenými dátami pre overovanie elektronických podpisov podpisujúcej osobe

V prípade, že sa žiadateľ o následný certifikát, resp. splnomocnenec dostaví sa žiadosťou o vydanie následného certifikátu na RA, je informovaný prostredníctvom pracovníka RA; v prípade, že žiadateľ o následný certifikát zaslal žiadosť prostredníctvom elektronickej pošty, je mu tento následný certifikát na túto adresu elektronicky zaslaný.

4.7.5 Úkony spojené s prevzatím certifikátu s vymenenými dátami pre overovanie elektronických podpisov

Pokiaľ boli splnené podmienky pre vydanie následného certifikátu, t.j. :

- splnenie podmienok uvedených v kapitolách 3.3.1 a 4.7.1
- zaplatenie určeného poplatku (ak nie je zmluvne dohodnuté inak) – vid'. aktuálny cenník na <http://www.ica.cz>

je žiadateľ o certifikát povinný tento certifikát prijať. Jediným spôsobom, akým môže postupovať v prípade, že tento certifikát nechce, je požiadať v súlade s zodpovedajúcim CP o jeho zrušenie.

V prípade podania žiadosti o vydanie následného certifikátu elektronickou cestou, zašle I.CA na žiadateľovu elektronickú adresu certifikát v predpísaných formátoch, v prípade vybavovania žiadosti na RA, získa žiadateľ certifikát od pracovníka RA.

Certifikačný poriadok pre vydávanie kvalifikovaných certifikátov	Strana 31 (celkom 66)
Copyright © První certifikační autorita, a.s.	Verejný dokument

4.7.6 Zverejnenie vydaných certifikátov s vymenenými dátami pre overovanie elektronických podpisov

I.CA je povinná zaistiť neodkladné zverejnenie následného certifikátu (verejného) vrátane tých údajov, ku ktorým dal jeho držiteľ súhlas.

4.7.7 Oznámenie o vydaní certifikátu s vymenenými dátami pre overovanie elektronických podpisov iným subjektom

V prípadoch vydania následného certifikátu pri dostavení sa žiadateľa o certifikát, resp. splnomocnenca na RA, získa oznámenie o vydanom certifikáte pracovník RA.

4.8 Zmena údajov v certifikáte

Služba nie je poskytovaná - tieto skutočnosti sú pre aplikáciu tohto vydania tohto CP irelevantné.

4.8.1 Podmienky pre zmenu údajov v certifikátu

Služba nie je poskytovaná - tieto skutočnosti sú pre aplikáciu tohto vydania tohto CP irelevantné.

4.8.2 Subjekty oprávnené požadovať zmenu údajov v certifikáte

Služba nie je poskytovaná - tieto skutočnosti sú pre aplikáciu tohto vydania tohto CP irelevantné.

4.8.3 Spracovanie požiadavku na zmenu údajov v certifikáte

Služba nie je poskytovaná - tieto skutočnosti sú pre aplikáciu tohto vydania tohto CP irelevantné.

4.8.4 Oznámení o vydaní certifikátu sa zmenenými údajmi podpisujúca osoba

Služba nie je poskytovaná - tieto skutočnosti sú pre aplikáciu tohto vydania tohto CP irelevantné.

4.8.5 Úkony spojené s prevzatím certifikátu so zmenenými údajmi

Služba nie je poskytovaná - tieto skutočnosti sú pre aplikáciu tohto vydania tohto CP irelevantné.

4.8.6 Zverejňovanie vydaných certifikátov so zmenenými údajmi

Služba nie je poskytovaná - tieto skutočnosti sú pre aplikáciu tohto vydania tohto CP irelevantné.

4.8.7 Oznámenie o vydaní certifikátu so zmenenými údajmi iným subjektom

Služba nie je poskytovaná - tieto skutočnosti sú pre aplikáciu tohto vydania tohto CP irelevantné.

4.9 Zrušenie a pozastavenie platnosti certifikátu

4.9.1 Podmienky pre zrušenie certifikátu

Certifikát môže byť zrušený na základe nasledujúcich okolností :

- o jeho zrušenie požiada :
 - podpisujúca osoba, držiteľ alebo
 - subjekt, ktorý k tomu bol explicitne určený v zmluve o poskytovaní kvalifikovanej certifikačnej služby v oblasti vydávania certifikátov (napr. pri vydávaní certifikátu pre zamestnanca) alebo
 - osoba oprávnená z pozostalostného konania

Certifikačný poriadok pre vydávanie kvalifikovaných certifikátov	Strana 32 (celkom 66)
Copyright © První certifikační autorita, a.s.	Verejný dokument

- ak nastanú skutočnosti uvedené v platnej legislatíve
- jeho držiteľ poruší závažným spôsobom ustanovenie zmluvy o poskytovaní kvalifikovanej certifikačnej služby alebo dokumentov, ktoré sú prílohou tejto zmluvy
- dôjde ku kompromitácii súkromného kľúča I.CA, používaného k označovaniu (ZoEP ČR) alebo podpisovaniu (ZoEP SR) vydávaných certifikátov a zoznamov zrušených certifikátov
- je dôvodné podozrenie, že došlo ku kompromitácii dát pre vytváranie elektronických podpisov držiteľa alebo podpisujúcej osoby

Zrušenie certifikátu vykoná I.CA na základe podnetu subjektov oprávnených zo zákona.

4.9.2 Subjekty oprávnené žiadať o zrušenie certifikátu

Žiadosť o zrušenie môžu podať subjekty, uvedené v kapitole 4.9.1.

4.9.3 Požiadavka na zrušenie certifikátu

Po splnení podmienok na identifikáciu a autentizáciu (kapitola 3.4), sa postupuje nasledujúcim spôsobom :

- V prípade **osobného podania žiadosti o zrušenie certifikátu na RA** musí žiadosť obsahovať sériové číslo certifikátu buď v dekadickom tvare alebo hexadecimálne (uvedené reťazcom „0x“), celé občianske meno fyzickej osoby, ktorej bol certifikát vydaný a heslo pre zrušenie. Pokiaľ si táto osoba heslo pre zrušenie nepamätá, musí túto skutočnosť do písomnej žiadosti explicitne uviesť, vrátane čísla primárneho osobného dokladu predloženého pri žiadosti o vydanie certifikátu. Týmto primárnym osobným dokladom sa musí pracovníkovi RA preukázať. Pracovník RA doručí vyššie uvedenú žiadosť (vzdialeným prístupom) na CA. Zodpovedný pracovník CA rozhodne, či je žiadosť oprávnená a rozhodnutie oznámi prostredníctvom pracovníka RA. V prípade, že je žiadosť oprávnená, je okamih prijatia tejto žiadosti na CA zároveň dátumom a časom zneplatnenia tohto certifikátu. V prípade, že žiadosť nie je možné akceptovať (chybné heslo pre zrušenie, nepreukázateľná identita fyzickej osoby), pokúsi sa pracovník RA v súčinnosti s touto fyzickou osobou tieto skutočnosti napraviť a pokiaľ to z ľubovoľného dôvodu nebude možné, žiadosť o zrušenie certifikátu bude zamietnutá. Pre splnomocnencov platí ustanovenie kapitoly 3.2.3, ods. c).
- V prípade **odovzdania žiadosti o zrušenie certifikátu elektronickou cestou** sú prípustné nasledujúce možnosti :

- podpísaná (ZoEP ČR, SR) alebo označená (ZoEP ČR) elektronická správa - telo správy musí byť nasledujúceho tvaru (v českom alebo slovenskom jazyku, s diakritikou alebo bez diakritiky) :

Zadam o zrusenie certifikatu cislo = xxxxxxx

alebo

Žiadam o zrušenie certifikátu číslo = xxxxxxx

kde „xxxxxx“ je sériové číslo certifikátu a musí byť buď v dekadickom tvare alebo hexadecimálne (uvedené reťazcom „0x“)

- nepodpísaná (ZoEP ČR, SR) alebo neoznačená (ZoEP ČR) elektronická správa - telo správy musí byť nasledujúceho tvaru (v českom alebo slovenskom jazyku, s diakritikou alebo bez diakritiky) :

Zadam o zrusenie certifikatu cislo = xxxxxxx

Heslo pre zrusenie = yyyyyy

Certifikačný poriadok pre vydávanie kvalifikovaných certifikátov	Strana 33 (celkom 66)
Copyright © První certifikační autorita, a.s.	Verejný dokument

alebo

Žiadam o zrušenie certifikátu číslo = xxxxxxx

Heslo pre zrušenie = yyyyyy

kde „xxxxxxx“ je sériové číslo certifikátu a „yyyyyy“ je heslo pre zrušenie. Sériové číslo musí byť buď v dekadickom tvare alebo hexadecimálne (uvedené reťazcom „0x“)

Pokiaľ žiadosť spĺňa výše uvedené požiadavky, zodpovedný pracovník CA bezodkladne certifikát zneplatní. Dátum a čas zneplatnenia je určený okamžikom prijatia platnej žiadosti o zrušenie certifikátu serverom I.CA. V prípade, že žiadosť nespĺňa uvedené požiadavky, je zamietnutá a žiadateľ je elektronickou cestou (v prípade vyplnenia elektronickej poštovej adresy) o tejto skutočnosti informovaný. O kladnom vybavení nie je žiadateľ explicitne informovaný a túto skutočnosť zistí v najbližšom vydanom zozname zrušených certifikátov.

- o prostredníctvom formulára na k tomuto účelu vyhradenej internetové informačnej adrese <http://www.ica.cz/>

Dátum a čas zneplatnenia je určený okamžikom prijatia platnej žiadosti o zrušenie certifikátu serverom I.CA. V prípade, že žiadosť nespĺňa požiadavky, je zamietnutá a žiadateľ je elektronickou cestou o tejto skutočnosti informovaný. O kladnom vybavení nie je žiadateľ explicitne informovaný a túto skutočnosť zistí v najbližšom vydanom zozname zrušených certifikátov.

- V prípade použitia **listovej zásielky** o zrušenie certifikátu musí byť táto zaslaná doporučené na adresu :

První certifikační autorita, a.s.
Podvinný mlýn 2178/6
190 00 Praha 9
Česká republika

V zásielke musí byť uvedená žiadosť v nasledujúcom tvare (v českom alebo slovenskom jazyku)

Žiadam o zrušenie certifikátu číslo = xxxxxxx

Heslo pre zrušenie = yyyyyy

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

Sériové číslo je buď v dekadickom tvare alebo hexadecimálnom (uvedené reťazcom „0x“). Pokiaľ si žiadateľ heslo pre zrušenie nepamätá, musí túto skutočnosť do písomnej žiadosti explicitne uviesť, vrátane čísla primárneho osobného dokladu predloženého pri žiadosti o vydanie certifikátu a žiadosť vlastnoručne podpísať. V prípade, že je žiadosť o zrušenie certifikátu oprávnená, je okamžik prijatia doporučenej listovej zásielky na I.CA zároveň dátumom a časom zneplatnenia tohto certifikátu. O vybavení žiadosti je žiadateľ informovaný doporučeným listom na poštovú adresu uvedenú ako adresa odosielateľa.

Žiadosti o zrušenie certifikátu prijíma I.CA nepretržite iba prostredníctvom odovzdania žiadosti elektronickou cestou a listovou zásielkou. Osobné odovzdanie na RA je možné iba v pracovnej dobe príslušnej RA.

4.9.4 Doba odkladu požiadavku na zrušenie certifikátu

Služba nie je poskytovaná - tieto skutočnosti sú pre aplikáciu tohto vydania tohto CP irelevantné.

Certifikačný poriadok pre vydávanie kvalifikovaných certifikátov	Strana 34 (celkom 66)
Copyright © První certifikační autorita, a.s.	Verejný dokument

4.9.5 Maximálna doba, za ktorú musí poskytovateľ realizovať požiadavku na zrušenie certifikátu

Reakciou I.CA na prijatie platnej žiadosti o zrušení certifikátu je jeho bezodkladné zrušenie. Do doby zverejnenia zoznamu zrušených certifikátov je dotýčny certifikát zablokovaný. Maximálne zdržanie medzi zneplatnením certifikátu a zverejnením zoznamu zrušených certifikátov, na ktorom je tento certifikát prvý krát uvedený, je najviac 12 hodín.

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

4.9.6 Povinnosti spoliehajúcich sa strán pri overovaní, či nebol certifikát zrušený

Spoliehajúce sa strany sú povinné prevádzať všetky úkony potrebné k tomu, aby si overili, že elektronické podpisy sú platné a certifikáty neboli zrušené. Pre tieto účely sú spoliehajúce sa strany povinné používať CRL, vydané a označené I.CA. Neoverenie certifikátu pomocou CRL je brané ako hrubé porušenie zodpovedajúceho CP a všetky nároky na prípadné uplatnenie záruk týmto zanikajú.

4.9.7 Periodicita vydávania zoznamu zrušených certifikátov

Zoznam zrušených certifikátov je spoločnosťou První certifikační autorita, a.s., vydávaný v pravidelných intervaloch, maximálne jedenkrát za 12 hodín (spravidla po 8 hodinách). Činnosti operátorov I.CA v procese vytvárania a vydávania CRL sú popísané v interných dokumentoch.

4.9.8 Maximálne spozdenie pri vydávaní zoznamu zrušených certifikátov

Zoznam zrušených certifikátov je spoločnosťou První certifikační autorita, a.s., vydávaný spravidla v osemhodinových intervaloch. Z tohto dôvodu nesmie maximálne spozdenie zoznamov zrušených certifikátov vydávaných I.CA presiahnuť 4 hodiny (viď. kapitola 4.9.7).

4.9.9 Možnosť overovania statutu certifikátu on-line („ďalej OCSP“)

Služba nie je poskytovaná - tieto skutočnosti sú pre aplikáciu tohto vydania tohto CP irelevantné.

4.9.10 Požiadavky pri overovaní statutu certifikátu on-line

Služba nie je poskytovaná - tieto skutočnosti sú pre aplikáciu tohto vydania tohto CP irelevantné.

4.9.11 Iné spôsoby oznamovania zrušenia certifikátu

Služba nie je poskytovaná - tieto skutočnosti sú pre aplikáciu tohto vydania tohto CP irelevantné.

4.9.12 Prípadné odlišnosti postupu zrušenia v prípade kompromitácie dát pre vytváranie elektronických podpisov

Služba nie je poskytovaná - tieto skutočnosti sú pre aplikáciu tohto vydania tohto CP irelevantné.

4.9.13 Podmienky pre pozastavenie platnosti certifikátu

Služba nie je poskytovaná - tieto skutočnosti sú pre aplikáciu tohto vydania tohto CP irelevantné.

4.9.14 Subjekty oprávnené požadovať pozastavenie platnosti certifikátu

Služba nie je poskytovaná - tieto skutočnosti sú pre aplikáciu tohto vydania tohto CP irelevantné.

4.9.15 Spracovanie požiadavky na pozastavenie platnosti certifikátu

Služba nie je poskytovaná - tieto skutočnosti sú pre aplikáciu tohto vydania tohto CP irelevantné.

Certifikačný poriadok pre vydávanie kvalifikovaných certifikátov	Strana 35 (celkom 66)
Copyright © První certifikační autorita, a.s.	Verejný dokument

4.9.16 Obmedzenie doby pozastavenia platnosti certifikátu

Služba nie je poskytovaná - tieto skutočnosti sú pre aplikáciu tohto vydania tohto CP irelevantné.

4.10 Služby súvisiace s overovaním statutu certifikátu

4.10.1 Funkčné charakteristiky

Služby súvisiace s overovaním statutu certifikátu sú poskytované formou zverejňovania informácií (viď. kapitola 2.2) :

- o verejných certifikátoch na adrese <http://www.ica.cz/>
- o zrušených certifikátoch na adresách :
 - <http://www.ica.cz/>
 - <http://qcrlp1.ica.cz/qica05.crl>
 - <http://qcrlp2.ica.cz/qica05.crl>
 - <http://qcrlp3.ica.cz/qica05.crl>

4.10.2 Dostupnosť služieb

I.CA zaisťuje nepretržitú dostupnosť služieb, uvedených v kapitole 4.10.1. Postup je uvedený v interných dokumentoch I.CA .

4.10.3 Ďalšie charakteristiky služieb statutu certifikátu

Ďalšie služby, okrem tých, ktoré sú uvedené v kapitole 4.10.1, nie sú poskytované.

4.11 Ukončenie poskytovania služieb pre držiteľov certifikátu podpisujúcou osobou

Ukončenie služieb (obchodný vzťah) medzi držiteľom a I.CA končí vo chvíli, keď skončila platnosť držiteľovho certifikátu, bez toho, aby držiteľ predtým požiadal o vydanie následného certifikátu.

4.12 Úschova dát pre vytváranie elektronických podpisov u dôveryhodnej tretej strany a ich obnova

Služba nie je poskytovaná - tieto skutočnosti sú pre aplikáciu tohto vydania tohto CP irelevantné.

4.12.1 Politika a postupy pri úschove a obnovovaní dát pre vytváranie elektronických podpisov

Služba nie je poskytovaná - tieto skutočnosti sú pre aplikáciu tohto vydania tohto CP irelevantné.

4.12.2 Politika a postupy pri zapuzdrovaní a obnovovaní šifrovacieho kľúča pro relaci

Služba nie je poskytovaná - tieto skutočnosti sú pre aplikáciu tohto vydania tohto CP irelevantné.

Certifikačný poriadok pre vydávanie kvalifikovaných certifikátov	Strana 36 (celkom 66)
Copyright © První certifikační autorita, a.s.	Verejný dokument

5 Management, prevádzková a fyzická bezpečnosť

Management bezpečnosti poskytovaných kvalifikovaných certifikačných služieb v oblasti vydávania certifikátov je zameraný predovšetkým na :

- systémy, ktoré priamo realizujú elektronické označovanie (ZoEP ČR) alebo elektronické podpisovanie (ZoEP SR) vydávaných certifikátov a zoznamu zrušených certifikátov
- všetky činnosti súvisiace s informáciami a dokumentáciou podľa platnej legislatívy (ZoEP ČR, SR)

5.1 Fyzická bezpečnosť

Implementované bezpečnostné opatrenia v oblasti fyzickej bezpečnosti, uvedené v základných interných dokumentoch :

- **Celková bezpečnostní politika**
- **Certifikační prováděcí směrnice**
- **Systémová bezpečnostní politika**
- **Plán pro zvládnání krizových situací a plán obnovy**
- **Analýza rizik**

sú detailne popísané v upresňujúcej internej bezpečnostnej dokumentácii a zahŕňajú problematiku uvedenú v podkapitolách 5.1.1 až 5.1.8.

5.1.1 Umiestnenie a konštrukcia

Zariadenia určené k výkonu hlavných kvalifikovaných certifikačných služieb, sú umiestnené v suteréne objektu, ktorý stojí osamotene. Zabezpečená oblasť má tehlové steny s najmenšou hrúbkou 300 mm. Vstupné dvere majú prienikovú odolnosť a zámkové systémy sú certifikované NBÚ ČR na kategóriu „Tajné“.

5.1.2 Fyzický prístup

Objekt je ohradený bezpečnostným plotom a je nepretržite strážený fyzickou ostrahou a špeciálnym televíznym systémom pre snímanie, prenos a zobrazovanie pohybu osôb a dopravných prostriedkov. Prístup do vlastného objektu je kontrolovaný fyzickou ostrahou.

5.1.3 Elektrina a klimatizácia

V miestnosti je dostatočne dimenzovaná aktívna klimatizácia, ktorá udržiava celoročnú teplotu v rozmedzí 20°C ± 5°C. Prívod elektrickej energie je istený pomocou UPS.

5.1.4 Vplyv vody

Objekt sa nachádza v lokalite, ktorá je postihnutelná záplavovou vodou. Všetky kritické systémy sú preto umiestnené v dostatočnej výške, aby neboli zaplavené ani storočnou vodou.

5.1.5 Protipožiarne opatrenia a ochrana

Vstupné pancierové dvere sú opatrené protipožiarou vložkou. V miestnosti sa nachádza hasiaci prístroj a zariadenie elektrickej požiarnej signalizácie.

<i>Certifikačný poriadok pre vydávanie kvalifikovaných certifikátov</i>	<i>Strana 37 (celkom 66)</i>
<i>Copyright © První certifikační autorita, a.s.</i>	<i>Verejný dokument</i>

5.1.6 Ukladanie médií

Pamäťové médiá, obsahujúce prevádzkové zálohy a záznamy v elektronickej podobe, sú ukladané v kovových skrinách, resp. trezoru riaditeľa I.CA.

Papierové médiá, ktoré je nutné podľa ZoEP archivovať, sú skladované v inej geografickej lokalite než je prevádzkové pracovisko.

5.1.7 Nakladanie s odpadmi

Všetok papierový kancelársky odpad je pred opustením pracovísk I.CA znehodnotený skartovaním.

5.1.8 Zálohy mimo budovu

Kópie prevádzkových a pracovných záloh sú uložené na mieste určenom riaditeľom I.CA a nesmú byť uložené v tom istom objekte ako originály.

5.2 Procesná bezpečnosť

Implementované bezpečnostné opatrenia v oblasti procesnej bezpečnosti, uvedené v základných interných dokumentoch :

- ***Celková bezpečnostní politika***
- ***Certifikační prováděcí směrnice***
- ***Systémová bezpečnostní politika***
- ***Plán pre zvládání krizových situací a plán obnovy***
- ***Analýza rizik***

sú detailne popísané v upresňujúcej internej bezpečnostnej dokumentácii a zahŕňajú problematiku uvedenú v podkapitolách 5.2.1 až 5.2.4.

5.2.1 Dôveryhodné role

Dôveryhodnými rolami spoločnosti I.CA sú :

- vedenie spoločnosti
- bezpečnostný manager
- manager pre zvládania krízových situácií a plán obnovy
- administrátor bezpečnosti
- administrátor systému (OS, siete, databázy)
- bezpečnostný audítor

5.2.2 Počet osôb požadovaných na zaistenie jednotlivých činností

Pre nižšie uvedené činnosti je nevyhnutná prítomnosť najmenej troch poverených pracovníkov I.CA :

- generovanie párových dát I.CA,
- ničenie dát pre vytváranie elektronickej značky (ZoEP ČR) alebo elektronickeho podpisu (ZoEP SR) I.CA vydávaných certifikátov a zoznamov zrušených certifikátov

Pre nižšie uvedené činnosti je nevyhnutná prítomnosť najmenej dvoch poverených pracovníkov I.CA :

<i>Certifikačný poriadok pre vydávanie kvalifikovaných certifikátov</i>	<i>Strana 38 (celkom 66)</i>
<i>Copyright © První certifikační autorita, a.s.</i>	<i>Verejný dokument</i>

- zálohovanie/obnova dát pre vytváranie elektronickej značky (ZoEP ČR) alebo elektronickeho podpisu (ZoEP SR) I.CA, vydávaných certifikátov a zoznamov zrušených certifikátov
- aktivácia kryptografického modulu,
- fyzická kontrola chodu kryptografického modulu pre vytváranie elektronickej značky (ZoEP ČR) alebo elektronickeho podpisu (ZoEP SR) vydávaných certifikátov a zoznamov zrušených certifikátov.

Pre realizáciu ostatných úloh nie je počet prítomných osôb určený, musí však ísť výhradne o poverených pracovníkov.

5.2.3 Identifikácia a autentizácia pre každú rolu

Pracovníkom sú pridelené prostriedky pre riadnu autentizáciu k tým komponentom, ktoré sú pre ich činnosť nevyhnutné.

5.2.4 Role vyžadujúce rozdelenie povinností

V procese poskytovania kvalifikovaných certifikačných služieb je minimálne zaručené, že nie je možné spojiť :

- rolu administrátora bezpečnosti alebo operátora CA s rolou bezpečnostného audítora
- rolu administrátora systému s rolami administrátor bezpečnosti alebo bezpečnostní audítora

5.3 Personálna bezpečnosť

Implementované bezpečnostné opatrenia v oblasti procesnej bezpečnosti, uvedené v základných interných dokumentoch :

- **Celková bezpečnostní politika**
- **Certifikační prováděcí směrnice**
- **Systémová bezpečnostní politika**
- **Plán pre zvládanie krizových situácií a plán obnovy**
- **Analýza rizik**

sú detailne popísané v upresňujúcej internej bezpečnostnej dokumentácii a zahŕňajú problematiku uvedenú v podkapitolách 5.3.1 až 5.3.8.

5.3.1 Požiadavky na kvalifikáciu, skúsenosť a bezúhonnosť

Všetci pracovníci I.CA v dôveryhodných rolách sú prijímaní na základe ďalej popísaných personálnych kritérií :

- je vyžadovaná úplná občianska bezúhonnosť - preukazované tým, že tieto osoby nemajú žiadny záznam v registri trestov (výpis z registru trestov alebo čestné prehlásenie)
- je vyžadované ukončené úplné vyššie odborné alebo úplné stredné odborné vzdelanie alebo ukončené vysokoškolské vzdelanie
- v prípade ukončeného vysokoškolského vzdelania sa požadujú 3 roky praxe
- v prípade vyššieho odborného alebo úplného stredného odborného vzdelania sa požaduje 5 rokov praxe
- v jednotlivých prípadoch je možné skrátiť dĺžku uvedenej praxe až o jednu tretinu stanovenej dĺžky na základe preskúšania, pri ktorom pracovník preukáže dostatočné znalosti k výkonu dôveryhodnej funkcie.

Certifikačný poriadok pre vydávanie kvalifikovaných certifikátov	Strana 39 (celkom 66)
Copyright © První certifikační autorita, a.s.	Verejný dokument

Menovanie alebo poverovanie pracovníkov I.CA do dôveryhodných rolí bezpečnostný manager, manager pre zvládanie krízových situácií a plán obnovy, administrátor bezpečnosti, administrátor systému a bezpečnostný audítor podlieha schváleniu riaditeľom I.CA.

5.3.2 Posúdenie spoľahlivosti osôb

Zdrojom informácií všetkých kmeňových pracovníkov I.CA sú :

- samotní títo pracovníci
- osoby, ktoré týchto pracovníkov poznajú
- verejné zdroje informácií

Pracovníci poskytujú prvotné informácie osobným pohovorom pri prijímaní do pracovného pomeru, ktoré aktualizujú pri periodických pohovoroch s nadriadeným pracovníkom v priebehu pracovného pomeru.

5.3.3 Požiadavky na prípravu pre výkon role, vstupné školenie

Pracovníci I.CA sú odborne zaškolení pre používanie určeného programového vybavenia a špeciálnych zariadení. Zaškolenie sa prevádza kombináciou metódy samo prípravy a metodickým vedením už zaškoleným pracovníkom. Bežná doba na zaškolenie je jeden mesiac.

5.3.4 Požiadavky a periodicita školení

Pre kmeňových pracovníkov uskutočňuje vedenie I.CA minimálne jedenkrát ročne interný výukový seminár zameraný na problematiku bezpečnosti informácií.

5.3.5 Periodicita a postupnosť rotácie pracovníkov medzi rôznymi rolami

Z dôvodov možnej zastupiteľnosti v mimoriadnych prípadoch sú pracovníci I.CA motivovaní na získavanie znalostí potrebných na zastavanie inej role v I.CA. Zmena role je možná iba v mimoriadnych prípadoch (epidemické ochorenie, a pod.) ako dočasné opatrenie. Pre trvalé vykonávanie inej dôveryhodnej role je potrebné menovanie riaditeľom I.CA.

5.3.6 Postihy za neoprávnené činnosti zamestnancov

Pri zistení neautorizovanej činnosti je dotýčny pracovník sankcionovaný podľa rozsahu až do výšky okamžitého prepustenia a riadi sa zákonníkom práce. Tento postih nebráni prípadnému trestnému stíhaniu, pokiaľ tomu zodpovedá závažnosť zistenej neautorizovanej činnosti.

5.3.7 Požiadavky na nezávislých zhotoviteľov (dodávateľov)

I.CA môže, alebo musí (podľa ZoEP, VoEP) niektoré činnosti zaisťovať zmluvne. Tieto obchodno - právne vzťahy sú ošetrené bilaterálnymi obchodnými zmluvami. Jedná sa o napr. o externé registračné authority, zhotoviteľov programového aplikačného vybavenia, dodávateľov hardware, systémového programového vybavenia, externých audítorov atď. Tieto subjekty sú povinné riadiť sa zodpovedajúcimi verejnými certifikačnými politikami, relevantnými časťami internej dokumentácie I.CA, ktoré im budú poskytnuté a predpísanými normatívnymi dokumentmi. V prípade porušenia týchto povinností sú vyžadované zmluvné pokuty, prípadne je s nimi okamžite ukončená zmluva.

5.3.8 Dokumentácia poskytovaná zamestnancom

Kmeňoví zamestnanci I.CA majú k dispozícii okrem CP aj príslušné normy, smernice, príručky a metodické pokyny, potrebné pre výkon ich činnosti.

Certifikačný poriadok pre vydávanie kvalifikovaných certifikátov	Strana 40 (celkom 66)
Copyright © První certifikační autorita, a.s.	Verejný dokument

5.4 Auditné záznamy (logy)

Zásady vytvárania, spracovania a uchovávania auditných logov sú uvedené v základných interných dokumentoch :

- **Certifikační prováděcí směrnice**
- **Systémová bezpečnostní politika**
- **Analýza rizik**

a detailne popísané v upresňujúcich interných bezpečnostných normách a smerniciach, zahrňujúcich problematiku, uvedenú v podkapitolách 5.4.1 až 5.4.8.

5.4.1 Typy zaznamenávaných udalostí

V dôveryhodných systémoch I.CA sú do elektronického auditneho logu zaznamenávané udalosti, požadované :

- CWA 14167-1 - Security Requirements for Trustworthy Systems Managing Certificates for Electronic Signatures - Part 1: System Security Requirements
- ETSI TS 101 456 - Electronic Signatures and Infrastructures : Policy requirements for certification authorities issuing qualified certificates
- ZoEP

Všetky auditné záznamy sú v nutnej miere vytvárané, uchovávané a spracovávané so zachovaním preukázateľnosti pôvodu, integrity, dostupnosti, dôvernosti a časovej autentičnosti.

Auditný systém je navrhnutý a prevádzkovaný spôsobom, ktorý zaručuje udržiavanie auditných dát, rezervovanie dostatočného priestoru pre auditné dáta, automatické neprepisovanie auditného súboru, prezentáciu auditných záznamov pre používateľov vhodným spôsobom a obmedzenie prístupu k auditnému súboru iba pre definovaných používateľov.

5.4.2 Periodicita spracovania záznamov

Auditné záznamy sú kontrolované a vyhodnocované jedenkrát týždenne/mesačne, v prípade bezpečnostného incidentu okamžite.

5.4.3 Doba uchovávania auditných záznamov

Doba, počas ktorej sa uchovávajú auditné záznamy, je stanovená na minimálne 10 rokov od ich vzniku.

5.4.4 Ochrana auditných záznamov

Elektronické auditné záznamy sú ukladané v dvoch kópiách, každá kópia je umiestnená v inej miestnosti prevádzkových priestorov I.CA. Jedenkrát mesačne sa prevádza uloženie auditných záznamov na médium, ktoré je umiestnené mimo prevádzkových priestorov I.CA.

5.4.5 Postupy pre zálohovanie auditných záznamov

Zálohovanie auditných záznamov prebieha obdobným spôsobom ako zálohovanie ostatných elektronických informácií.

5.4.6 Systém zhromažďovania auditných záznamov (interný alebo externý)

Systém zhromažďovania auditných záznamov je vo vzťahu k I.CA interný, vo vzťahu k zmluvným partnerom externý. Zhromažďovanie auditných záznamov je evidované.

Certifikačný poriadok pre vydávanie kvalifikovaných certifikátov	Strana 41 (celkom 66)
Copyright © První certifikační autorita, a.s.	Verejný dokument

5.4.7 Postup pri oznamovaní udalosti subjektu, ktorý ju spôsobil

V prípade neoprávnených pokusov nie je subjekt informovaný o zapísanie udalosti do auditného záznamu.

5.4.8 Hodnotenie zraniteľnosti

V I.CA boli prevedené nasledujúce činnosti :

- stanovenie aktív (programové vybavenie, technické vybavenie, dáta) a ich väzieb
- hodnotenie aktív informačného systému
- stanovenie relevantných hrozieb a zraniteľností
- hodnotenie hrozieb a zraniteľností
- určenie miery rizika pre každú kombináciu aktíva (skupiny aktív), hrozby a zraniteľnosti

5.5 Uchovávanie informácií a dokumentácie

Uchovávanie informácií a dokumentácie je v I.CA prevádzané podľa požiadaviek ZoEP (ČR, SR) a ďalších právnych noriem (aktuálne znenie zákona ČR č.499/2004 o archívnictve a spisovej službe a o zmene niektorých zákonov, zákon Slovenskej národnej rady č. 149/1975 Zb. o archívnictve v znení neskorších predpisov).

Zásady uchovávania informácií a dokumentácie sú uvedené v základných interných dokumentoch:

- **Celková bezpečnostní politika**
- **Certifikační prováděcí směrnice**
- **Systémová bezpečnostní politika**
- **Analýza rizik**

a detailne popísané v upresňujúcich interných bezpečnostných normách a smerniciach, zahŕňujúcich problematiku, uvedenú v podkapitolách 5.5.1 až 5.5.7.

5.5.1 Typy informácií a dokumentácie, ktoré sa uchovávajú

I.CA uchováva nasledujúce typy informácií a dokumentácie, ktoré súvisia s poskytovanými kvalifikovanými certifikačnými službami v oblasti vydávania certifikátov podľa ZoEP a obsahujú :

- elektronické alebo písomné informácie :
 - zmluva o poskytovaní kvalifikovanej certifikačnej služby v oblasti vydávania certifikátov, vrátane žiadosti o poskytovanie služby
 - certifikát vydaný žiadateľovi o certifikát, resp. splnomocnencovi
 - nadriadený kvalifikovaný systémový certifikát (ZoEP ČR) alebo certifikát I.CA (ZoEP SR)
 - kópie predložených osobných dokladov žiadateľa o certifikát, resp. splnomocnenca, na základe ktorých bola overená identita žiadateľa o certifikát, resp. splnomocnenca
 - potvrdenie o prevzatí certifikátu držiteľom, resp. splnomocnencom, prípadne jeho súhlas so zverejnením certifikátu v zozname vydaných certifikátov
 - prehlásenie držiteľa certifikátu o tom, že mu boli pred uzavretím zmluvy o poskytovaní kvalifikovaných služieb v oblasti vydávania certifikátov poskytnuté písomné informácie o presných podmienkach pre využívanie kvalifikovaných certifikačných služieb v oblasti vydávania certifikátov, vrátane prípadných obmedzení pre ich použitie, o podmienkach reklamácií a riešení vzniknutých sporov, a o tom, či je alebo nie je akreditovaný
 - dokumenty a záznamy súvisiace s životným cyklom vydaného certifikátu (ZoEP ČR, SR), nadriadeného kvalifikovaného systémového certifikátu (ZoEP ČR) alebo certifikátu I.CA (ZoEP SR)
 - ďalšie záznamy, požadované ZoEP SR

Certifikačný poriadok pre vydávanie kvalifikovaných certifikátov	Strana 42 (celkom 66)
Copyright © První certifikační autorita, a.s.	Verejný dokument

- auditné záznamy definované v kapitole 5.4.1 tohoto dokumentu, aplikačné programové vybavenie a všetku dokumentáciu spoločnosti, ktorá je nutná pre realizáciu informačných auditov a kontrol bezpečnostnej zhody
- identifikácia miesta, kde sú uložené informácie a dokumentácia, ktorých uchovávanie je vyžadované ZoEP
- všetky zoznamy zrušených certifikátov
- identifikačné údaje osoby, ktorá vykonala overenie totožnosti žiadateľa o certifikát, resp. splnomocnenca
- obchodný názov I.CA, alebo zmluvného partnera, ktorý túto činnosť pre I.CA zabezpečuje
- záznam o manipulácii (napr. prevzatie, odovzdanie, uloženie, kontrola, konverzia do elektronickej podoby a pod.) s informáciami
- prevádzková a bezpečnostná dokumentácia

5.5.2 Doba uchovávaní uchovávaných informácií a dokumentácie

Po celú dobu svojej existencie I.CA zaisťuje uchovávanie informácií a dokumentácie podľa kapitoly 5.5.1 po dobu najmenej 10 rokov od ich vzniku.

Po celú dobu existencie I.CA sú uchovávané informácie, vzťahujúce sa k svojim nadriadeným kvalifikovaným systémovým certifikátom (ZoEP ČR) alebo certifikátu I.CA (ZoEP SR), s výnimkou príslušných dát pre vytváranie elektronickej značky (ZoEP ČR) alebo elektronickeho podpisu (ZoEP SR).

Postupy pri uchovávaní informácií a dokumentácie sú upravené internou dokumentáciou I.CA.

5.5.3 Ochrana úložiska uchovávaných informácií a dokumentácie

Uchovávané informácie a dokumentácia obsahujú aj osobné dáta klientov a preto sa vzhľadom k zákonom ČR č. 101/2000 Sb. a SR č. 428/2002 Z.z. v aktuálnych zneniach, dbá na zvýšenú ochranu týchto dát. Priestory, v ktorých sa uchovávané informácie a dokumentácia nachádzajú, sú zabezpečené formou opatrení, vychádzajúcich z požiadaviek objektivej a fyzickej bezpečnosti.

Uchovávané informácie a dokumentácia sú určené výhradne pre internú potrebu I.CA a sú prístupné :

- pracovníkom I.CA v dôveryhodných roliach
- oprávneným kontrolným subjektom, orgánom činným v trestnom konaní a súdom, pokiaľ je to právnymi normami vyžadované.

O každom takto povolenom prístupe je vyhotovený písomný záznam.

Postupy pri ochrane úložisk uchovávaných informácií a dokumentácie sú upravené internou dokumentáciou I.CA.

5.5.4 Postupy pri zálohovaní uchovávaných informácií a dokumentácie

Postupy pri zálohovaní uchovávaných informácií a dokumentácie (viď. kapitola 5.5.1) upravené internou dokumentáciou I.CA.

5.5.5 Požiadavky na používanie časových pečiatok pri uchovávaní informácií a dokumentácie

V prípade, že budú využívané časové pečiatky, musí sa jednať o kvalifikované časové pečiatky vydané I.CA.

Certifikačný poriadok pre vydávanie kvalifikovaných certifikátov	Strana 43 (celkom 66)
Copyright © První certifikační autorita, a.s.	Verejný dokument

5.5.6 Systém zhromažďovania uchovávaných informácií a dokumentácie (interný, externý)

Informácie a dokumentácia sú ukladané na miesto, určené riaditeľom I.CA. Registračné authority sú povinné vykonať predarchiváciu v určených termínoch a vzniknuté dáta odovzdať určeným pracovníkom I.CA.

Samotná problematika prípravy a spôsobu ukladania informácií a dokumentácie v elektronickej i písomnej podobe je upravená internými normami a smernicami (vid'. kapitola 5.5.4). Zhromažďovanie archívnych záznamov je evidované.

5.5.7 Postupy pre získanie a overenie uchovávaných informácií a dokumentácie

Pracovisko, kde sú informácie a dokumentácia uchovávané, obsahuje ich zoznam vrátane dátumu uloženia.

5.6 Výmena dát pre overovanie elektronických podpisov/značiek v nadriadenom kvalifikovanom systémovom certifikáte poskytovateľa

Problematika je uvedená v kapitole 1.1.

5.7 Obnova po havárii alebo kompromitácii

5.7.1 Postup v prípade incidentu a kompromitácie

Postupy sú uvedené v internom dokumente *Plán pre zvládanie krízových situácií a plán obnovy* a ním odkazovanou dokumentáciou.

5.7.2 Poškodenie výpočtových prostriedkov, software alebo dát

V prípade poškodenia výpočtových prostriedkov, software alebo dát postupuje I.CA v súlade s interným dokumentom *Plán pre zvládanie krízových situácií a plán obnovy* a ním odkazovanou dokumentáciou.

5.7.3 Postup pri kompromitácii dát pre vytváranie elektronických podpisov/značiek poskytovateľa

V prípade kompromitácie alebo vzniku dôvodnej obavy zo zneužitia dát pre vytváranie elektronických značiek (ZoEP ČR) alebo elektronických podpisov (ZoEP SR) pre označovanie (ZoEP ČR) alebo podpisovanie (ZoEP SR) vydávaných certifikátov a zoznamov zrušených certifikátov I.CA :

- ukončí ich používanie
- okamžite a trvale zruší vlastný príslušný nadriadený kvalifikovaný systémový certifikát (ZoEP ČR) alebo certifikát I.CA (ZoEP SR) a jemu zodpovedajúce dáta pre vytváranie elektronických značiek (ZoEP ČR) alebo elektronických podpisov (ZoEP SR)
- zruší všetky certifikáty, ktoré boli týmito dátami označené (ZoEP ČR) alebo podpísané (ZoEP SR)
- bezodkladne :
 - o tejto skutočnosti, vrátane dôvodu informuje :
 - na svojej internetovej informačnej adrese
 - v jednom celoštátne distribuovanom denníku – vid'. kapitola 2.2
 - pre sprístupnenie tejto informácie je využitý aj zoznam zrušených certifikátov, čím je zaistená dostupnosť tejto informácie minimálne dvoma na sebe nezávislými spôsobmi, umožňujúcimi vzdialený prístup a sú nepretržite dostupné

Certifikačný poriadok pre vydávanie kvalifikovaných certifikátov	Strana 44 (celkom 66)
Copyright © První certifikační autorita, a.s.	Verejný dokument

- pokiaľ je to možné, informuje držiteľov platných certifikátov o zrušení týchto certifikátov, a to prostredníctvom zaslania správy elektronickou poštou na elektronickú adresu, ktorú tieto osoby uviedli v žiadosti o vydanie certifikátu; súčasťou tejto informácie je dôvod ukončenia platnosti nadriadeného kvalifikovaného systémového certifikátu (ZoEP ČR) alebo certifikátu I.CA (ZoEP SR)
- oznámi príslušnému úradu informáciu o zrušení vlastného príslušného nadriadeného kvalifikovaného systémového certifikátu (ZoEP ČR) alebo certifikátu I.CA (ZoEP SR) s uvedením dôvodu zrušenia
- v prípade vzniku odôvodnenej obavy zo zneužitia dát pre vytváranie elektronických značiek (ZoEP ČR) alebo elektronických podpisov (ZoEP SR) pre označovanie (ZoEP ČR) alebo podpisovanie (ZoEP SR) vydávaných certifikátov a zoznamov zrušených certifikátov ponúkne I.CA vyššie uvedeným držiteľom bezplatné vydanie nového certifikátu s tým, že prípadné náklady na vydanie nových certifikátov sama uhradí. Postup je rovnaký ako pri vydaní prvotného certifikátu.

5.7.4 Schopnosti obnoviť činnosť po havárii

V prípade havárie postupuje I.CA v súlade s interným dokumentom **Plán pre zvládanie krízových situácií a plán obnovy** a ním odkazovanou dokumentáciou.

5.8 Ukončenie činnosti CA alebo RA

V prípade plánovaného ukončenia činnosti I.CA ako kvalifikovaného poskytovateľa certifikačných služieb v oblasti vydávania certifikátov, t.j. z iných dôvodov, než sú mimoriadne udalosti akými sú štrajky, občianske nepokoje, vojnový stav, prírodné katastrofy celoštátneho rozsahu alebo iné výsledky pôsobenia vyššej moci, zaistí I.CA vykonanie nasledujúcich činností :

- ČR :
 - ohlási príslušnému úradu zámer ukončiť činnosť poskytovania kvalifikovaných certifikačných služieb v oblasti vydávania certifikátov najmenej 3 mesiace pred plánovaným ukončením činnosti
 - vynaloží všetko možné úsilie na to, aby evidencia, vedená podľa platnej legislatívy, bola prevzatá iným kvalifikovaným poskytovateľom certifikačných služieb v oblasti vydávania certifikátov, v prípade, že sa jej nepodarilo túto evidenciu odovzdať inému kvalifikovanému poskytovateľovi certifikačných služieb v oblasti vydávania certifikátov, ohlási najneskôr 30 dní pred plánovaným dátumom ukončenia činnosti túto skutočnosť príslušnému úradu a zaistí odovzdanie tejto evidencie príslušnému úradu - túto informáciu zahrnie do správy, odoslanej všetkým svojim klientom, ktorí sú držiteľmi platných zmlúv o poskytovaní kvalifikovaných certifikačných služieb v oblasti vydávania certifikátov, pokiaľ toto bude známe najmenej 2 mesiace pred plánovaným ukončením činnosti
 - sprístupnenie informácií o ukončení činnosti I.CA v oblasti vydávania certifikátov na svojej internetovej informačnej adrese najmenej 2 mesiace pred plánovaným ukončením činnosti
 - ukončí kvalifikované poskytovanie certifikačných služieb v oblasti vydávania certifikátov
 - preukázateľne zničí svoje dáta pre vytváranie elektronických značiek, slúžiace k označovaniu vydávaných certifikátov a zoznamu zrušených certifikátov
- SR :
 - ohlási príslušnému úradu zámer ukončiť činnosť poskytovania kvalifikovaných certifikačných služieb v oblasti vydávania certifikátov najmenej 6 mesiacov pred plánovaným ukončením činnosti
 - ohlási každému držiteľovi platného kvalifikovaného certifikátu zámer ukončiť činnosť poskytovania kvalifikovaných certifikačných služieb v oblasti vydávania certifikátov najmenej 6 mesiacov pred plánovaným ukončením činnosti
 - môže sa dohodnúť s iným kvalifikovaným poskytovateľom certifikačných služieb v oblasti vydávania certifikátov o prevzatí záznamov o vydaných a zrušených certifikátoch a prevádzkovej dokumentácie – pokiaľ žiadny kvalifikovaný poskytovateľ certifikačných služieb v oblasti vydávania certifikátov tieto záznamy neprevezme :

<i>Certifikačný poriadok pre vydávanie kvalifikovaných certifikátov</i>	<i>Strana 45 (celkom 66)</i>
<i>Copyright © První certifikační autorita, a.s.</i>	<i>Verejný dokument</i>

- zaniká platnosť všetkých ním vydaných kvalifikovaných certifikátov odo dňa zániku tohto kvalifikovaného poskytovateľa certifikačných služieb v oblasti vydávaní certifikátov
- prevezme tieto záznamy úrad

Problematika plánovaného ukončenia činnosti I.CA, prípadne RA, je detailne uvedená v internej dokumentácii.

Certifikačný poriadok pre vydávanie kvalifikovaných certifikátov	Strana 46 (celkom 66)
Copyright © První certifikační autorita, a.s.	Verejný dokument

6 Technická bezpečnosť

6.1 Generovanie a inštalácia párových dát

Detailní popis generovania a inštalácie párových dát je uvedený v internej bezpečnostnej dokumentácii, zahrňujúcej problematiku, uvedenú v podkapitolách 6.1.1 až 6.1.7.

6.1.1 Generovanie párových dát

Generovanie párových dát I.CA, ktoré prebieha v zabezpečenej zóne v súlade s dokumentom „**Systémová bezpečnostní politika**“ a o priebehu ktorého je vyhotovený písomný protokol, je prevádzané v kryptografickom module, ktorý spĺňa [požiadavky na kryptografické funkcie](#) a je uvedený v [zozname nástrojov, u ktorých bola vyslovená zhoda](#). Použitý modul svojimi vlastnosťami zodpovedá požiadavkám vyžadovaným aktuálnymi verziami ZoEP a VoEP. I.CA používa pre párové dáta, slúžiace k označovaniu (ZoEP ČR) alebo podpisovaniu (ZoEP SR) vydávaných certifikátov a zoznamov zrušených certifikátov dĺžku rovnú 2048 bitov.

V priebehu procesu generovania párových dát I.CA, slúžiacich k označovaniu (ZoEP ČR) alebo podpisovaniu (ZoEP SR) vydávaných certifikátov a zoznamov zrušených certifikátov, musia byť fyzicky prítomní :

- riaditeľ I.CA alebo ním menovaný člen vedenia I.CA
- bezpečnostný manager alebo bezpečnostný administrátor (konkrétne určí riaditeľ I.CA)
- administrátor systému, alebo iný poverený technicky preškolený pracovník I.CA.

Konkrétny technický postup generovania párových dát I.CA, slúžiacich k označovaniu (ZoEP ČR) alebo podpisovaniu (ZoEP SR) vydávaných certifikátov a zoznamov zrušených certifikátov a následné vyhotovenie nadriadeného kvalifikovaného systémového certifikátu (ZoEP ČR) alebo certifikátu I.CA (ZoEP SR), príslušného k týmto párovým dátam, je popísaný v internej dokumentácii I.CA.

O priebehu generovania párových dát I.CA, slúžiacich k označovaniu (ZoEP ČR) alebo podpisovaniu (ZoEP SR) vydávaných certifikátov a zoznamov zrušených certifikátov je vyhotovený písomný protokol obsahujúci :

- menný zoznam prítomných pracovníkov s uvedením: mena, priezviska, titulu
- dátum a čas zahájenia a ukončenia generovania párových dát s presnosťou minimálne na minúty
- miesto, kde ku generovaniu párových dát došlo
- popis zariadenia, na ktorom bolo generovanie prevádzané, umožňujúce jednoznačnú identifikáciu tohoto zariadenia
- kompletný výpis nadriadeného kvalifikovaného systémového certifikátu (ZoEP ČR) alebo certifikátu I.CA (ZoEP SR), obsahujúci dáta pre overovanie elektronických značiek (ZoEP ČR) alebo elektronických podpisov (ZoEP SR) vydávaných certifikátov a zoznamov zrušených certifikátov, obsiahnuté v práve vygenerovaných párových dátach
- dátum vyhotovenia protokolu
- vlastnoručné podpisy všetkých pracovníkov, ktorí generovanie párových dát realizovali

I.CA z principiálnych bezpečnostných dôvodov neposkytuje službu generovania párových dát klienta na svojich zariadeniach. Generovanie párových dát na klientovom počítači prebieha pomocou aplikačného vybavenia klientovho počítača a klient je povinný používať také zariadenia, resp. aplikácie, ktoré spĺňajú požiadavky ZoEP a VoEP. I.CA nešpecifikuje žiadne aplikácie ani zariadenia pre generovanie párových dát.

V prípade generovania párových dát, používaných v procesoch správy systémových komponent I.CA, komunikácii s RA na vlastných zariadeniach, sú pracovníci I.CA a RA povinní využívať certifikáty, vydané I.CA.

Certifikačný poriadok pre vydávanie kvalifikovaných certifikátov	Strana 47 (celkom 66)
Copyright © První certifikační autorita, a.s.	Verejný dokument

6.1.2 Odovzdanie dát pre vytváranie elektronických podpisov podpisujúcej osobe

Žiadateľ o certifikát generuje párové dáta zásadne na zariadení a v prostredí, ktoré sú v okamžiku ich generovania pod jeho výhradnou kontrolou (viď. kapitola 6.1.1) a preto sú tieto skutočnosti pre aplikáciu tohto vydania tohto CP irelevantné.

6.1.3 Odovzdanie dát pre overovanie elektronických podpisov poskytovateľov certifikačných služieb

Dáta pre overovanie elektronických podpisov je nutné I.CA doručiť. I.CA podporuje nasledujúce spôsoby doručenia dát pre overovanie elektronického podpisu :

- osobne na dátovom nosiči
- zaslaním prostredníctvom elektronickej pošty

Vydanie prvotného certifikátu je možné iba osobne. Pre následné certifikáty je možné použiť oboch z vyššie uvedených spôsobov odovzdania. V prípade odovzdania prostredníctvom elektronickej pošty, musí byť správa, obsahujúci dáta pre overovanie elektronických podpisov, elektronicky podpísaná dátami pre vytváranie elektronických podpisov príslušných k platnému certifikátu, ku ktorému sa požaduje vydanie následného certifikátu.

Dáta pre overovanie elektronických podpisov sú súčasťou žiadosti o vydanie certifikátu.

6.1.4 Poskytovanie dát pre overovanie elektronických podpisov certifikačnou autoritou spoliehajúcim sa stranám

Dáta pre overovanie elektronických značiek (ZoEP ČR) alebo elektronických podpisov (ZoEP SR) I.CA sú obsiahnuté v jeho nadriadenom kvalifikovanom systémovom certifikáte (ZoEP ČR) alebo certifikáte I.CA (ZoEP SR). Možnosť získania nadriadeného kvalifikovaného systémového certifikátu (ZoEP ČR) alebo certifikátu I.CA (ZoEP SR) je garantovaná nasledujúcimi spôsobmi :

- získaním na RA (osobná návšteva)
- prostredníctvom internetových informačných adries I.CA a príslušného úradu
- prostredníctvom vestníku príslušného úradu

Každý žiadateľ o certifikát získa nadriadený kvalifikovaný systémový certifikát (ZoEP ČR) alebo certifikát I.CA (ZoEP SR) pri získaní svojho prvotného certifikátu na RA.

6.1.5 Dĺžky párových dát

I.CA používa najpreverenejší klasický asymetrický šifrový algoritmus – RSA. Mohutnosť kľúčov (resp. parametrov daného algoritmu) použitých pre označovanie (ZoEP ČR) alebo podpisovanie (ZoEP SR) vydávaných certifikátov je 2048 bitov. Mohutnosť kľúčov na strane klienta závisí na klientovi, pre vybraný algoritmus však nesmie byť nižšia než stanovená hodnota/hodnoty, uvedené v relevantných technických štandardoch alebo normách.

6.1.6 Generovanie parametrov dát pre overovanie elektronických podpisov a kontrola ich kvality

Algoritmy použité pre generovanie celočíselných hodnôt nutných pre fungovanie elektronického podpisu (napr. testy prvočíselnosti atď.) musia mať parametre uvedené v relevantných technických štandardoch alebo normách.

I.CA kontroluje možný dvojitý výskyt rovnakých dát pre overenie elektronických podpisov vo vydávaných certifikátoch. V prípade duplicitného výskytu dát pre overenie elektronických podpisov je žiadateľ o certifikát požadovaný o vygenerovanie nových párových dát. Už vydaný certifikát je bezodkladne zrušený, držiteľ takéhoto certifikátu je o tomto bezodkladne informovaný a vyzvaný ku generovaniu nových párových dát.

Certifikačný poriadok pre vydávanie kvalifikovaných certifikátov	Strana 48 (celkom 66)
Copyright © První certifikační autorita, a.s.	Verejný dokument

6.1.7 Obmedzenie pre použitie dát pre overovanie elektronických podpisov

Uvedené v kapitole 7.1.2.

6.2 Ochrana dát pre vytváranie elektronických značiek/podpisov a bezpečnosť kryptografických modulov

Detailný popis je uvedený v interných bezpečnostných dokumentoch, zahrňujúcich problematiku, uvedenú v podkapitolách 6.2.1 až 6.2.10.

6.2.1 Štandardy a podmienky používania kryptografických modulov

V kryptografickom module, ktorý spĺňa [požiadavky na kryptografické funkcie](#) a je uvedený v [zozname nástrojov, u ktorých bola vyslovená zhoda](#) :

- sú generované párová dáta I.CA
- je uložený súkromný kľúč I.CA pre označovanie (ZoEP ČR) alebo podpisovanie (ZoEP SR) vydávaných certifikátov a zoznamov zrušených certifikátov

6.2.2 Zdieľanie tajomstva

Ochrana zdieľaním tajomstva je realizovaná prostriedkami kryptografického modulu. Pri výkone citlivých činností, ktoré súvisia so zásadnými činnosťami I.CA (viď. kapitoly 6.1.1 a 6.2.10), je nezbytná prítomnosť troch poverených pracovníkov I.CA, z ktorých dvaja poznajú časť kódu k uskutočneniu týchto činností.

6.2.3 Úschova dát pre vytváranie elektronických značiek/podpisov

Tieto skutočnosti sú pre aplikáciu tohto vydania tohto CP irelevantné.

6.2.4 Zálohovanie dát pre vytváranie elektronických značiek/podpisov

Kryptografický modul, použitý pre správu nadriadených kvalifikovaných systémových certifikátov (ZoEP ČR) alebo certifikátov I.CA (ZoEP SR), umožňuje zálohovanie dát pre vytváranie elektronických značiek (ZoEP ČR) alebo elektronických podpisov (ZoEP SR). Dáta v zašifrovanej podobe sú zálohované prostredníctvom čipových kariet.

6.2.5 Uchovávanie dát pre vytváranie elektronických značiek/podpisov

Po uplynutí doby platnosti dát určených k označovaniu (ZoEP ČR) alebo podpisovaniu (ZoEP SR) vydávaných certifikátov a zoznamov zrušených certifikátov sú tieto dáta, vrátane ich záloh zničené a ich ďalšie zálohovanie sa nevykonáva. Uchovávanie dát, určených k označovaniu (ZoEP ČR) alebo podpisovaniu (ZoEP SR) certifikátov a zoznamov zrušených certifikátov predstavuje bezpečnostné riziko a preto je v I.CA zakázané.

6.2.6 Transfer dát pre vytváranie elektronických značiek/podpisov do kryptografického modulu alebo z kryptografického modulu

Dáta pre vytváranie elektronických značiek (ZoEP ČR) alebo elektronických podpisov (ZoEP SR) príslušné k nadriadenému kvalifikovanému systémovému certifikátu (ZoEP ČR) alebo certifikátu I.CA (ZoEP SR) sú generované priamo v kryptografickom module.

Vkladanie dát pre vytváranie elektronických značiek (ZoEP ČR) alebo elektronických podpisov (ZoEP SR) do kryptografického modulu v prípade, že sa jedná o obnovenie týchto dát zo šifrovanej zálohy, prebieha za priamej osobnej účasti najmenej dvoch určených pracovníkov I.CA. V okamžiku vkladania dát musia byť vyhradené stanice a kryptografický modul odpojené od počítačovej siete. O vložení dát pre

Certifikačný poriadok pre vydávanie kvalifikovaných certifikátov	Strana 49 (celkom 66)
Copyright © První certifikační autorita, a.s.	Verejný dokument

vytváranie elektronických značiek (ZoEP ČR) alebo elektronických podpisov (ZoEP SR) je vytvorený písomný záznam.

6.2.7 Uloženie dát pre vytváranie elektronických značiek/podpisov v kryptografickom module

Dáta pre vytváranie elektronických značiek (ZoEP ČR) alebo elektronických podpisov (ZoEP SR) príslušné k nadriadenému kvalifikovanému systémovému certifikátu (ZoEP ČR) alebo certifikátu I.CA (ZoEP SR) sú v kryptografickom module uložené v šifrovanom tvare.

6.2.8 Postup pri aktivácii dát pre vytváranie elektronických značiek/podpisov

Aktiváciu dát pre vytváranie elektronických značiek (ZoEP ČR) alebo elektronických podpisov (ZoEP SR) I.CA v oblasti vydávania certifikátov vygenerovaných v kryptografickom module, vykonávajú určení pracovníci I.CA prostredníctvom vlastnej aktivácie kryptografického modulu a aktivačnej čipovej karty podľa presne určeného postupu, ktorý je upravený internou dokumentáciou. Po aktivácii je systém pripravený k označovaniu (ZoEP ČR) alebo podpisovaniu (ZoEP SR) vydávaných certifikátov, zoznamov zrušených certifikátov a aktivačná čipová karta sa vyberie. Po aktivácii je zariadenie prístupné iba určeným zodpovedným pracovníkom I.CA.

6.2.9 Postup pri deaktivácii dát pre vytváranie elektronických značiek/podpisov

Deaktiváciu dát pre vytváranie elektronických značiek (ZoEP ČR) alebo elektronických podpisov (ZoEP SR) I.CA v oblasti vydávania certifikátov po ich vložení do kryptografického modulu vykonávajú určení pracovníci I.CA prostredníctvom kryptografického modulu a aktivačnej čipovej karty podľa presne určeného postupu, ktorý je upravený internou dokumentáciou.

O prevedení deaktivácie dát pre vytváranie elektronických značiek (ZoEP ČR) alebo elektronických podpisov (ZoEP SR) je vytvorený písomný záznam, ktorý podpíšu určení pracovníci I.CA.

6.2.10 Postup pri zničení dát pre vytváranie elektronických značiek/podpisov

Dáta pre vytváranie elektronických značiek (ZoEP ČR) alebo elektronických podpisov (ZoEP SR), slúžiace k označovaniu (ZoEP ČR) alebo podpisovaniu (ZoEP SR) vydávaných certifikátov a zoznamov zrušených certifikátov, sú uložené v kryptografickom module. Ničenie je realizované prostriedkami kryptografického modulu. Zálohy týchto dát uložené v zašifrovanej podobe na externých médiách sú taktiež zničené. Ničenie spočíva vo fyzickej deštrukcii týchto nosičov.

Pri ničení dát pre vytváranie elektronických značiek (ZoEP ČR) alebo elektronických podpisov (ZoEP SR), slúžiacich k označovaniu (ZoEP ČR) alebo podpisovaniu (ZoEP SR) vydávaných certifikátov a zoznamov zrušených certifikátov musia byť fyzicky prítomní :

- riaditeľ I.CA alebo ním menovaný člen vedenia I.CA
- bezpečnostný manažér alebo bezpečnostný administrátor (konkrétne určí riaditeľ I.CA)
- administrátor systému, alebo iný poverený technicky preškolený pracovník I.CA

O priebehu ničenia dát elektronických značiek (ZoEP ČR) alebo elektronických podpisov (ZoEP SR), slúžiacich k označovaniu (ZoEP ČR) alebo podpisovaniu (ZoEP SR) vydávaných certifikátov a zoznamov zrušených certifikátov je spísaný protokol.

6.2.11 Hodnotenie kryptografických modulov

Nástroj elektronického podpisu (zodpovedajúci požiadavkám na kryptografické moduly podľa dokumentu „Standard pre hodnotenie bezpečnosti kryptografických modulov vydaný NIST v USA – FIPS PUB 140-1 úroveň 3“) pre označovanie vydávaných kvalifikovaných certifikátov a zoznamu kvalifikovaných certifikátov, ktoré boli zrušené, je uvedený v [zozname nástrojov, u ktorých bola vyslovená zhoda](#).

Certifikačný poriadok pre vydávanie kvalifikovaných certifikátov	Strana 50 (celkom 66)
Copyright © První certifikační autorita, a.s.	Verejný dokument

6.3 Ďalšie aspekty správy párových dát

6.3.1 Uchovávanie dát pre overovanie elektronických značiek/podpisov

Tieto dáta sú obsiahnuté v nadriadených kvalifikovaných systémových certifikátoch (ZoEP ČR) alebo certifikátoch I.CA (ZoEP SR). Na rozdiel od iných príslušných dát pre vytváranie elektronických značiek (ZoEP ČR) alebo elektronických podpisov (ZoEP SR) je dôležité tieto dáta uchovávať pre prípad následnej kontroly pravosti vydaných certifikátov a zoznamov zrušených certifikátov. So všetkými nadriadenými kvalifikovanými systémovými certifikátmi (ZoEP ČR) alebo certifikátmi I.CA (ZoEP SR) sa nakladá spôsobom, uvedeným v kapitolách 5.4 a 5.5.

6.3.2 Maximálna doba platnosti certifikátu vydaného podpisujúcej alebo označujúcej osobou a párových dát

Platnosť dát určených k overovaniu označených (ZoEP ČR) alebo podpísaných (ZoEP SR) vydávaných certifikátov a zoznamov zrušených certifikátov je daná platnosťou vydaných nadriadených kvalifikovaných systémových certifikátov (ZoEP ČR) alebo certifikátov I.CA (ZoEP SR) - platnosť párových dát, určených k označovaniu (ZoEP ČR) alebo podpisovaniu (ZoEP SR) vydávaných certifikátov a zoznamov zrušených certifikátov je stanovená na 6 rokov. Po tejto dobe je možné dáta pre overovanie elektronických značiek (ZoEP ČR) alebo elektronických podpisov (ZoEP SR) I.CA v oblasti vydávania certifikátov použiť bez záruky. Pokiaľ dôjde k neočakávanému vývoju kryptoanalytických metód, ktoré by mohli ohroziť bezpečnosť použitia párových dát, bude ich životnosť skrátená. V takom prípade sa postupuje analogicky k postupom uvedeným v kapitole 5.7.

6.4 Aktivačné dáta

6.4.1 Generovanie a inštalácia aktivačných dát

Aktivačné dáta sú vytvárané v priebehu procesu inštalácie, keď sú generované párové dáta pre označovanie (ZoEP ČR) alebo podpisovanie (ZoEP SR) vydávaných certifikátov a zoznamov zrušených certifikátov.

6.4.2 Ochrana aktivačných dát

Povinnosťou poverených pracovníkov I.CA je chrániť aktivačné dáta.

6.4.3 Ostatné aspekty aktivačných dát

Aktivačné dáta sú určené výhradne pre aktiváciu súkromného kľúča a nesmú byť použité k iným účelom, ani prenášané alebo uchovávané v otvorenej podobe.

6.5 Počítačová bezpečnosť

6.5.1 Špecifické technické požiadavky na počítačovú bezpečnosť

Úroveň bezpečnosti použitých komponent pre poskytovanie kvalifikovaných certifikačných služieb v oblasti vydávania certifikátov je definovaná ZoEP a VoEP.

Detailné riešenie špecifických technických požiadaviek počítačovej bezpečnosti je popísané v internej dokumentácii.

6.5.2 Hodnotenie počítačovej bezpečnosti

Hodnotenie bezpečnosti I.CA je založené na medzinárodných a národných štandardoch :

Certifikačný poriadok pre vydávanie kvalifikovaných certifikátov	Strana 51 (celkom 66)
Copyright © První certifikační autorita, a.s.	Verejný dokument

- CWA 14167-1 - Security Requirements for Trustworthy Systems Managing Certificates for Electronic Signatures - Part 1: System Security Requirements/Bezpečnostní požiadavky na důveryhodné systémy spravující certifikáty pre elektronický podpis – část 1: Požadavky na bezpečnost systémů.
- ETSI TS 101 456 - Electronic Signatures and Infrastructures (ESI); Policy requirements for certification authorities issuing qualified certificates
- ČSN ISO/IEC 17799 - Informační technologie – Soubor postupů pre management bezpečnosti informací.
- ČSN BS 7799-2 - Systém managementu bezpečnosti informací - Specifikace s návodem pre použití
- ČSN ISO/IEC TR 13335 - Informační technologie – Smernice pre riadenie bezpečnosti IT 1-3
- ČSN EN ISO 19011 - Smernice pre auditovanie systému managementu akosti a/alebo systému environmentálneho managementu.

6.6 Bezpečnosť životného cyklu

6.6.1 Riadenie vývoja systému

Pri vývoji systému sa postupuje v súlade s internou dokumentáciou.

6.6.2 Kontroly riadenia bezpečnosti

Súlady sa štandardami (viď. kapitola 6.5.2), ZoEP a VoEP je overovaný pravidelnými auditmi systému managementu bezpečnosti informácií, vykonávanými pracovníkmi nezávislých auditorských firiem a kontrolami bezpečnostnej zhody, vykonávanými pracovníkmi I.CA. Táto problematika je popísaná v internej dokumentácii.

6.6.3 Riadenie bezpečnosti životného cyklu

Riadenie správy bezpečnosti I.CA je vytvárané podľa britskej normy BS 7799-2. Jedná sa o procesný prístup „Plánovanie-Zavedenie-Kontrola-Využitie“ (Plan-Do-Check-Act, PDCA), ktorý sa skladá z nadväzujúcich procesov :

- vybudovanie – definovanie bezpečnostnej politiky, plánov, cieľov, procesov a postupov s ohľadom na riadenie rizík a bezpečnosť informácií tak, aby boli v súlade s celkovou bezpečnostnou politikou ;
- implementácia a prevádzka - bezpečnostnej politiky, plánov, cieľov, procesov a postupov;
- monitorovanie a prehodnocovanie – posúdenie procesu s ohľadom na bezpečnostnú politiku a odovzdanie poznatkov vedeniu spoločnosti k posúdeniu;
- využitie – na základe rozhodnutia vedenia organizácie vykonania nápravných opatrení.

6.7 Sieťová bezpečnosť

V prostredí I.CA nie sú prostriedky realizujúce vlastné kvalifikované certifikačné služby priamo dostupné z verejnej siete Internet. Informačný systém je chránený prístupovým routerom (firma Cisco) a VVOS (firma Hewlett Packard). Všetka komunikácia medzi RA a CA je vedená šifrovane. Detailné riešenie riadenia sieťovej bezpečnosti je popísané v internej dokumentácii.

6.8 Časová pečiatka

Riešenie je uvedené v kapitole 5.5.5.

7 Profily certifikátov, zoznamov zrušených certifikátov a OCSP

7.1 Profil certifikátu

Profily certifikátov zodpovedajú odporučeniam RFC 3280. Dĺžka kľúča, označujúceho (ZoEP ČR) alebo podpisujúceho (ZoEP SR) vydávané certifikáty a zoznamy zrušených certifikátov je 2048 bitov, minimálna dĺžka kľúča vydávaného certifikátu je 1024 bitov. Základné atribúty sú uvedené v Tabuľke 7.

Tabuľka 7 – Profil certifikátu

Atribút	Hodnota
Version	verzia 3
Serial Numer	jedinečné číslo vydaného certifikátu
Signature <ul style="list-style-type: none"> Algorithm Parameters 	<p>algoritmus pre elektronickú značku (ZoEP ČR) alebo elektronický podpis (ZoEP SR) vydávaného certifikátu</p> <p>voliteľné parametre</p>
Issuer DN	označenie vydavateľa certifikátu
NotBefore	dátum a UTC čas začiatku platnosti certifikátu
NotAfter	dátum a UTC čas konca platnosti certifikátu
Subject DN	označenie držiteľa certifikátu
SubjectPublicKeyInfo <ul style="list-style-type: none"> algorithm SubjectPublicKey 	<p>identifikátor algoritmu verejného kľúča certifikátu</p> <p>verejný kľúč držiteľa certifikátu</p>
Signature algorithm <ul style="list-style-type: none"> algorithm parameters 	<p>algoritmus pre elektronickú značku (ZoEP ČR) alebo elektronický podpis (ZoEP SR) vydávaného certifikátu</p> <p>voliteľné parametre</p>
signatureValue	Elektronická značka (ZoEP ČR) alebo elektronický podpis (ZoEP SR) vydaného certifikátu

7.1.1 Číslo verzie

Všetky vydávané certifikáty sú v súlade s X.509 vo verzii 3.

7.1.2 Rozširujúce položky v certifikáte

Vo vydaných certifikátoch (verzia 3) je použitý **kritický** rozširujúci atribút **Key Usage**.

Atribút **Basic Constraints** nie je použitý.

Ďalej sú použité rozširujúce atribúty:

Subject Alternative Name: položky 1. - 5. v prvom stĺpci Tabuľky 8 je možné naplniť podľa požiadaviek klienta pri dodržaní zásad uvedených v kapitole 3.1

Tabulka 8 – Rozširujúce atribúty certifikátu

Poradie	Atribút	Hodnota
1.	otherName	<ul style="list-style-type: none"> • číselný identifikátor klienta, vedený v centrálnej databáze MPSV • číselný identifikátor úradu, vedený v centrálnej databáze MPSV • Microsoft universal principal name
2.	rfc822Name	Elektronická adresa
3.	dNSName	Meno DNS
4.	uniformResourceIdentifier	URI
5.	iPAddress	IP adresa
6.	Authority Key Identifier	SHA1 hash verejného kľúča vydavateľa certifikátu
7.	Subject Key Identifier	SHA1 hash verejného kľúča vydaného certifikátu
8.	Certificate Policy <ul style="list-style-type: none"> • Policy • Explicit Text 	vid'. kapitola 7.1.6 vid'. kapitola 7.1.8
9.	CRL Distribution Points	[1]Distribučné miesto CRL Názov distribučného miesta: Meno a priezvisko: URL= http://qcrl dp1.ica.cz/qica05.crl [2]Distribuční miesto CRL Názov distribučného miesta: Meno a priezvisko: URL= http://qcrl dp2.ica.cz/qica05.crl [3]Distribuční miesto CRL Názov distribučného miesta: Meno a priezvisko: URL= http://qcrl dp3.ica.cz/qica05.crl (v prípade písomnej zmluvy s klientom je možné doplniť klientom požadované distribučné miesto CRL)
10.	Key usage	Kritický NonRepudation (povinný) A DigitalSignature N (nepovinný) KeyEncipherment N (nepovinný) DataEncipherment N (nepovinný)
11.	Qualified Certificate Statements	0.4.0.1862.1.1

7.1.3 Objektové identifikátory (ďalej "OID") algoritmov

Certifikáty, vydávané podľa tohto CP, používajú **Signature Algorithm: sha1WithRSAEncryption** (signature algorithm), ktorého OID je 1 2 840 113549 1 1 5

7.1.4 Spôsoby zápisov mien a názvov

Uvedené v kapitole 3.1.

7.1.5 Obmedzenie mien a názvov

Atribút nameConstraints nie je použitý. Pre meno subjektu (Subject) nie je žiadne obmedzenie s výnimkou obmedzení vyplývajúcich z kapitoly 3.1.2.

Certifikačný poriadok pre vydávanie kvalifikovaných certifikátov	Strana 54 (celkom 66)
Copyright © První certifikační autorita, a.s.	Verejný dokument

O prípustnosti konkrétneho obsahu jednotlivých atribútov mena subjektu (atribútov položky Subject) rozhoduje s konečnou platnosťou pracovník registračnej autority, ktorý vykonáva vybavovanie požiadavky na vydanie certifikátu. V prípade nesúhlasu môže žiadateľ postupovať podľa kapitoly 9.13.

7.1.6 OID certifikačnej politiky

Tento CP je určený pre vydávanie a správu kvalifikovaných certifikátov a je mu pridelené nasledujúce OID : 1.3.6.1.4.1. 23624.1.4.10.2

7.1.7 Rozširujúca položka „Policy Constraints“

Tieto skutočnosti sú pre aplikáciu tohoto vydania tohto CP irelevantné.

7.1.8 Syntax a sémantika rozširujúca položky kvalifikátorov politiky „Policy Qualifiers“

ZoEP ČR - úložisko súkromného kľúča : operačný systém, USB token, iná čipová karta než Starcos v. 2.3 a vyššia :

Policy: 1.3.6.1.4.1. 23624.1.4.10.2

User Notice:

Explicit Text: Tento kvalifikovaný certifikát je vydan v súlade se zakonom SR 215/2002 Z.z. v platnom znení.

ZoEP - úložisko súkromného kľúča :

- **ČR - odporúčaná čipová karta Starcos v. 2.3 a vyšší**
- **SR - zariadenie, certifikované pre tento účel Národným bezpečnostným úradom SR (odporúčaná čipová karta Starcos v. 2.3) :**

Policy: 1.3.6.1.4.1. 23624.1.4.10.2

User Notice:

Explicit Text: Tento kvalifikovaný certifikát je vydan v súlade se zakonom CR 227/2000 Sb. v platnom znení.

Policy: 1.3.158.36061701.0.0.0.1.2.2

User Notice:

Explicit Text: Tento kvalifikovaný certifikát je vydan v súlade se zakonom SR 215/2002 Z.z. v platnom znení.

7.1.9 Spôsob zápisu kritickej rozširujúcej položky „Certificate Policies“

ZoEP ČR - úložisko súkromného kľúča : operačný systém, USB token, iná čipová karta než Starcost v. 2.3 a vyššia :

Policy: 1.3.6.1.4.1. 23624.1.4.10.2

ZoEP - úložisko súkromného kľúča :

- **ČR - odporúčaná čipová karta Starcos v. 2.3 a vyšší**
- **SR - zariadenie, certifikované pre tento účel Národným bezpečnostným úradom SR (odporúčaná čipová karta Starcos v. 2.3) :**

Policy: 1.3.6.1.4.1. 23624.1.4.10.2

Policy: 1.3.158.36061701.0.0.0.1.2.2

7.2 Profil zoznamu zrušených certifikátov

7.2.1 Číslo verzie

Zoznamy zrušených certifikátov sú vydávané podľa X 509 verzia 2.

7.2.2 Rozširujúce položky zoznamu zrušených certifikátov a záznamov v zozname zrušených certifikátov

I.CA pri vydávaní CRL používa nasledujúce atribúty :

Tabuľka 9 – Profil CRL

Položka	Obsah	Príklad
Version	Verzia v2	1
Signature <ul style="list-style-type: none"> algorithm parameters 	<p>algoritmus pre elektronickú značku (ZoEP ČR) alebo elektronický podpis (ZoEP SR) vydávaného CRL</p> <p>voliteľné parametre</p>	sha1withRSAEncryption
Issuer	označení vydavateľa CRL	Tabuľka 4
thisUpdate	dátum a UTC čas vydania CRL	Nov 30 04:51:30 2005
nextUpdate	dátum a predpokladaný UTC čas vydania nasledujúceho CRL	Nov 30 16:51:30 2005
Signature algorithm <ul style="list-style-type: none"> Algorithm Parameters 	<p>algoritmus pre elektronickú značku (ZoEP ČR) alebo elektronický podpis (ZoEP SR) vydávaného CRL</p> <p>voliteľné parametre</p>	sha1withRSAEncryption
signatureValue	Elektronická značka (ČR) alebo elektronický podpis (SR) vydaného CRL	RSA (2048)
CRL Number	Číslo CRL	456

Tabuľka 10 – Rozširujúce atribúty CRL

Položka	Obsah	Príklad
revokedCertificates <ul style="list-style-type: none"> userCertificate revocationDate 	<p>jedinečné číslo vydaného certifikátu</p> <p>dátum a UTC čas zneplatnenia kvalifikovaného certifikátu</p>	<p>10100629</p> <p>Jan 30 04:51:30 2005</p>

<i>Certifikačný poriadok pre vydávanie kvalifikovaných certifikátov</i>	<i>Strana 56 (celkom 66)</i>
<i>Copyright © První certifikační autorita, a.s.</i>	<i>Verejný dokument</i>

7.3 Profil OCSP

Tieto skutočnosti sú pre aplikáciu tohto vydania tohto CP irelevantné.

7.3.1 Číslo verzie

Tieto skutočnosti sú pre aplikáciu tohto vydania tohto CP irelevantné.

7.3.2 Rozširujúce položky OCSP

Tieto skutočnosti sú pre aplikáciu tohto vydania tohto CP irelevantné.

Certifikačný poriadok pre vydávanie kvalifikovaných certifikátov	Strana 57 (celkom 66)
Copyright © První certifikační autorita, a.s.	Verejný dokument

8 Hodnotenie zhody a iné hodnotenia

V I.CA sú vykonávané hodnotenia bezpečnosti v oblastiach, uvedených v kapitole 8.4. Súčasťou týchto hodnotení je mimo iné sledovanie, či sú plne dodržiavané štandardy, uvedené v kapitole 6.5.2 s jedinou výnimkou, a to u štandardu ETSI TS 101 456, konkrétne jeho kapitoly 6.2.

8.1 Periodicita hodnotení alebo okolností pre výkon hodnotení

Celková kontrola bezpečnostnej zhody sa vykonáva po 4 rokoch od predchádzajúcej celkovej kontroly bezpečnostnej zhody. Behom týchto 4 rokov sú vykonávané ročné čiastočné kontroly bezpečnostnej zhody. Kontrola bezpečnostnej zhody sa vykonáva podľa požiadaviek technickej normy ČSN ISO/IEC TR 13335 - Informačné technológie – Smernica pre riadenie bezpečnosti IT 1-3.

Audit systému bezpečnosti informácií sa vykonáva po 2 rokoch od predchádzajúceho auditu systému bezpečnosti informácií a vykonáva sa podľa požiadaviek normy ČSN EN ISO 19011 - Smernica pre auditovanie systému managementu akosti a/alebo systému environmentálneho managementu.

8.2 Identita a kvalifikácia hodnotiteľa

Identita a kvalifikácia hodnotiteľa je upravená internou dokumentáciou I.CA..

8.3 Vzťah hodnotiteľa k hodnotenému subjektu

V prípade auditu systému managementu bezpečnosti informácií je hodnotiteľom externá, nezávislá auditujúca organizácia.

V prípade celkovej kontroly bezpečnostnej zhody alebo čiastočnej kontroly bezpečnostnej zhody je hodnotiteľom fyzická/právnická osoba, poverená riaditeľom spoločnosti První certifikační autorita, a.s.

8.4 Hodnotené oblasti

Cieľom kontroly bezpečnostnej zhody je overenie, že spoločnosť První certifikační autorita, a.s. :

- prevádzkuje dôveryhodné systémy v súlade so ZoEP a VoEP
- vykonáva zmeny v dôveryhodných systémoch v súlade s bezpečnostnou dokumentáciou, a to jej časťami upravujúcimi riadenie zmien

Predmetom kontroly bezpečnostnej zhody:

- sú všetky dôveryhodné systémy I.CA (celková kontrola bezpečnostnej zhody), alebo
- sú všetky zmeny, ktoré I.CA vykonala od predošlej kontroly bezpečnostnej zhody, a ich vplyv na dôveryhodné systémy I.CA (čiastočná kontrola bezpečnostnej zhody), alebo
- je v prípade, že v dôveryhodných systémoch I.CA nenastali od predošlej čiastočnej kontroly bezpečnostnej zhody žiadne zmeny, overenie tejto skutočnosti.

Cieľom auditu systému managementu bezpečnosti informácií je objektívne a na I.CA nezávislé overenie, že je v dôveryhodných systémoch I.CA v oblasti vydávania certifikátov zavedený a uplatňovaný systém managementu bezpečnosti informácií.

S ohľadom na uvedené, poskytne I.CA subjektu, ktorý audit systému managementu bezpečnosti informácií vykonáva :

- správu o predošlej kontrole bezpečnostnej zhody
- bezpečnostnú dokumentáciu (v aktuálnych verziách) :

Certifikačný poriadok pre vydávanie kvalifikovaných certifikátov	Strana 58 (celkom 66)
Copyright © První certifikační autorita, a.s.	Verejný dokument

- Certifikačný poriadok pre vydávanie kvalifikovaných certifikátov
- Pravidlá pre výkon certifikačných služieb (Certifikační prováděcí směrnice) pre vydávanie kvalifikovaných certifikátov alebo kvalifikovaných systémových certifikátov
- Certifikační politika pre vydávanie nadriadených kvalifikovaných systémových certifikátov (ZoEP ČR) alebo certifikátov I.CA (ZoEP SR)
- Pravidlá pre výkon certifikačných služieb (Certifikační prováděcí směrnice) pre vydávanie nadriadených kvalifikovaných certifikátov (ZoEP ČR) alebo certifikátov I.CA (ZoEP SR)
- Správa pre používateľa
- Celková bezpečnostná politika
- Systémová bezpečnostná politika
- Plán pre zvládanie krízových situácií a plán obnovy
- ďalšie dokumenty I.CA v oblasti vydávania certifikátov, na ktoré je vo vyššie uvedených dokumentoch odkazované

8.5 Postup v prípade zistených nedostatkov

V prípade nedostatkov, zistených na základe správy o celkovej alebo čiastočnej kontrole bezpečnostnej zhody (viď. kapitoly 8.1, 8.4, 8.6) je bezpečnostný manager povinný do 15 dní po obdržaní správy určiť, aké opatrenia k odstráneniu nedostatkov je I.CA povinná prijať.

Ak zistí príslušný úrad, že I.CA porušuje povinnosti stanovené ZoEP, VoEP uloží jej, aby v stanovenej lehote zjedнала nápravu a prípadne určí, aké opatrenia k odstráneniu nedostatkov je I.CA povinná prijať.

8.6 Oznamovanie výsledkov hodnotení

I.CA zaistí spracovanie správy o kontrole bezpečnostnej zhody, ktorej obsahom je :

- vymedzenie predmetu kontroly bezpečnostní zhody :
 - celková kontrola bezpečnostnej zhody - vymedzenie všetkých dôveryhodných systémov s uvedením kvalifikovaných certifikačných služieb, ktoré sú prostredníctvom týchto systémov zaisťované
 - čiastočná kontrola bezpečnostnej zhody - vymedzenie zmien, ktoré I.CA vykonala od predošlej kontroly bezpečnostní zhody a vymedzenie kvalifikovaných certifikačných služieb, ktoré sú zaisťované prostredníctvom dôveryhodných systémov, týmito zmenami ovplyvnených
- identifikácia dokumentácie, ktorá bola predmetom kontroly bezpečnostnej zhody
- popis postupu, jakým bola kontrola bezpečnostnej zhody vykonaná
- meno, poprípade mená, a priezvisko osoby, ktorá kontrolu bezpečnostnej zhody vykonala
- prehlásenie subjektu, ktorý kontrolu bezpečnostnej zhody vykonal, o výsledku kontroly bezpečnostnej zhody, ktorého súčasťou je prehlásenie o tom, že I.CA prevádzkuje dôveryhodné systémy v súlade so ZoEP, VoEP a vykonáva zmeny v dôveryhodných systémoch v súlade s bezpečnostnou dokumentáciou, a to jej časťami upravujúcimi riadenie zmien

Správa o kontrole bezpečnostní zhody :

- je odovzdaná bezpečnostnému managerovi do 10 dní od ukončenia kontroly, ktorý s jej obsahom zoznámi riaditeľa I.CA a bezpečnostný výbor
- je odovzdaná príslušnému úradu do 30 dní od ukončenia kontroly

I.CA zaistí :

- že správa o audite systému managementu bezpečnosti informácií obsahuje :
 - vymedzenie predmetu auditu systému managementu bezpečnosti informácií, pričom vymedzením predmetu auditu sa rozumie vymedzenie kvalifikovaných certifikačných služieb, ktoré sú zaisťované prostredníctvom dôveryhodných systémov,

<i>Certifikačný poriadok pre vydávanie kvalifikovaných certifikátov</i>	<i>Strana 59 (celkom 66)</i>
<i>Copyright © První certifikační autorita, a.s.</i>	<i>Verejný dokument</i>

- identifikácia dokumentácie, ktorá bola predmetom auditu systému managementu bezpečnosti informácií a ktorú I.CA poskytla subjektu, ktorý audit systému managementu bezpečnosti informácií vykonáva,
- prehlásenie subjektu, ktorý audit systému managementu bezpečnosti informácií vykonal, o výsledku auditu systému managementu bezpečnosti informácií, ktorého súčasťou je prehlásenie o tom, že je v I.CA uplatňovaný systém managementu bezpečnosti informácií podľa technickej normy ČSN BS 7799-2.
- zverejnenie prehlásenia o výsledku auditu systému managementu bezpečnosti informácií v správe pre používateľov.

Certifikačný poriadok pre vydávanie kvalifikovaných certifikátov	Strana 60 (celkom 66)
Copyright © První certifikační autorita, a.s.	Verejný dokument

9 Ostatné obchodné a právne záležitosti

9.1 Poplatky

9.1.1 Poplatky za vydanie alebo obnovenie certifikátu

Poplatky za prvotný, resp. následný certifikát, sú uvedené v aktuálnom cenníku služieb, ktorý je k dispozícii na internetovej informačnej adrese I.CA. Služba obnovenia certifikátu nie je poskytovaná.

9.1.2 Poplatky za prístup k certifikátu na zozname vydaných certifikátov

Prístup k vydaným verejným certifikátom elektronickou cestou I.CA nespoplatňuje.

9.1.3 Poplatky za informácie o statute certifikátu a o zrušení certifikátu

Prístup k informáciám o zrušených certifikátoch alebo statutoch certifikátov elektronickou cestou I.CA nespoplatňuje.

9.1.4 Poplatky za ďalšie služby

Poplatok za odovzdanie certifikátu (prvotný, následný) prostredníctvom záznamového média (napr. disketa) je uvedený v aktuálnom cenníku služieb, ktorý je k dispozícii na internetovej informačnej adrese I.CA.

Zrušenie certifikátu a stiahnutie elektronickej verzie CP (v elektronickej verzii vo všeobecne používanom formáte PDF) je poskytované zadarmo.

Poplatky za nadštandardné služby sú stanovované zmluvne.

9.1.5 Iné ustanovenia týkajúce sa poplatkov (vrátane refundácií)

I.CA si vyhradzuje právo zmeny výšky poplatku za vydanie prvotného, resp. následného certifikátu. I.CA je taktiež oprávnená stanoviť pre individuálne uzatvorené zmluvy inú výšku týchto poplatkov.

9.2 Finančná zodpovednosť

9.2.1 Krytie poistením

Spoločnosť První certifikační autorita, a.s., prehlasuje, že má uzatvorené poistenie podnikateľských rizík takým spôsobom, aby boli pokryté prípadné finančné škody.

9.2.2 Ďalšie aktíva a záruky

Spoločnosť První certifikační autorita, a.s., prehlasuje, že má k dispozícii dostatočné finančné zdroje a iné finančné zaistenie na prevádzku v súlade s požiadavkami uvedenými v ZoEP a s ohľadom na riziko vzniku zodpovednosti za škodu.

Podrobné informácie o aktívach spoločnosti První certifikační autorita, a.s., je možno získať z Výročnej správy I.CA.

9.2.3 Poistenie alebo krytie zárukou pre koncových používateľov

Služba nie je poskytovaná - tieto skutočnosti sú pre aplikáciu tohoto vydania tohto CP irelevantné.

Certifikačný poriadok pre vydávanie kvalifikovaných certifikátov	Strana 61 (celkom 66)
Copyright © První certifikační autorita, a.s.	Verejný dokument

9.3 Citlivosť obchodných informácií

9.3.1 Výpočet citlivých informácií

Citlivými informáciami I.CA sú :

- dáta pre vytváranie elektronických značiek (ZoEP ČR) alebo elektronických podpisov (ZoEP SR) prislúchajúce k dátam pre overovanie elektronických značiek (ZoEP ČR) alebo elektronických podpisov (ZoEP SR) obsiahnutých vo vlastných nadriadených kvalifikovaných systémových certifikátoch (ZoEP ČR) alebo certifikátoch I.CA (ZoEP SR)
- dáta pre vytváranie elektronických podpisov (ZoEP ČR, SR) alebo elektronických značiek (ZoEP ČR) prislúchajúce k dátam pre overovanie elektronických podpisov (ZoEP ČR, SR) alebo elektronických značiek (ZoEP ČR) obsiahnutých v účelových certifikátoch I.CA (napr. kľúče pre komunikáciu s RA)
- ostatné kryptograficky podstatné informácie slúžiace k prevádzke I.CA
- vybrané obchodné informácie I.CA
- všetky informácie a dokumentácia s ohľadom na poskytovanie kvalifikovaných certifikačných služieb podľa ZoEP

Chránenými obchodnými informáciami jednotlivých RA sú :

- dáta pre vytváranie elektronických podpisov (ZoEP ČR, SR) alebo elektronických značiek (ZoEP ČR) prislúchajúce k dátam pre overovanie elektronických podpisov (ZoEP ČR, SR) alebo elektronických značiek (ZoEP ČR) obsiahnutých vo vlastných alebo účelových certifikátoch RA
- ostatné kryptograficky podstatné informácie slúžiace k prevádzke RA
- všetky informácie a dokumentácia s ohľadom na poskytovanie kvalifikovaných certifikačných služieb podľa ZoEP

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

S chránenými informáciami, bez ohľadu na typ nosiča, sa zachádza tak, aby bola zaistená ich dôvernosť a integrita.

9.3.2 Informácie mimo rámec citlivých informácií

Za verejné sa považujú typy informácií, ktoré nepatria do žiadnej zo skupín uvedených v kapitole 9.3.1.

9.3.3 Zodpovednosť za ochranu citlivých informácií

Každý pracovník, ktorý príde do styku s informáciami uvedenými v kapitole 9.3.1, ich nesmie bez súhlasu riaditeľa I.CA poskytnúť tretej strane.

9.4 Ochrana osobných údajov

Problematika ochrany osobných údajov (kapitoly 9.4.1 až 0) je riešená internou dokumentáciou.

9.4.1 Politika ochrany osobných údajov

Ochrana osobných údajov je v I.CA riešená v súlade s požiadavkami zákonov ČR č. 101/2000 Sb. a SR č. 428/2002 Z.z. v platných zneniach.

<i>Certifikačný poriadok pre vydávanie kvalifikovaných certifikátov</i>	<i>Strana 62 (celkom 66)</i>
<i>Copyright © První certifikační autorita, a.s.</i>	<i>Verejný dokument</i>

9.4.2 Osobné údaje

Osobnými informáciami sú všetky osobní údaje klientov, používateľov či pracovníkov, podliehajúce ochrane v zmysle príslušnej zákonnej normy (zákony ČR č. 101/2000 Sb. a SR č. 428/2002 Z.z. v platných zneniach).

9.4.3 Údaje, ktoré nie sú považované za dôverné

Informácie, ktoré nie sú považované za dôverné sú také údaje, ktoré nepodliehajú ochrane v zmysle príslušnej zákonnej normy (zákony ČR č. 101/2000 Sb. a SR č. 428/2002 Z.z. v platných zneniach).

9.4.4 Zodpovednosť za ochranu osobných údajov

Ochrana osobných údajov je v I.CA riešená v súlade s požiadavkami zákonov ČR č. 101/2000 Sb. a SR č. 428/2002 Z.z. v platných zneniach.

9.4.5 Oznámenie o používaní dôverných informácií a súhlas s používaním citlivých informácií

Ochrana osobných údajov je v I.CA riešená v súlade s požiadavkami zákonov ČR č. 101/2000 Sb. a SR č. 428/2002 Z.z. v platných zneniach.

9.4.6 Poskytovanie citlivých informácií pre súdne či správne účely

Ochrana osobných údajov je v I.CA riešená v súlade s požiadavkami zákonov ČR č. 101/2000 Sb. a SR č. 428/2002 Z.z. v platných zneniach.

9.4.7 Iné okolnosti sprístupňovania osobných údajov

Ochrana osobných údajov je v I.CA riešená v súlade s požiadavkami zákonov ČR č. 101/2000 Sb. a SR č. 428/2002 Z.z. v platných zneniach.

9.5 Práva duševného vlastníctva

Tento CP, všetky súvisiace dokumenty, obsah webových stránok, nadriadené kvalifikované systémové certifikáty/klúče I.CA (ZoEP ČR) alebo certifikáty/klúče I.CA (ZoEP SR) a procedúry, zaisťujúce prevádzku systému, poskytujúceho kvalifikované certifikačné služby v oblasti certifikátov, sú chránené autorskými právami spoločnosti První certifikační autorita, a.s., a predstavujú jej významné know-how.

9.6 Zastupovanie a záruky

9.6.1 Zastupovanie a záruky CA

I.CA zaručuje, že :

- použije súkromné klúče prislúchajúce svojim nadriadeným kvalifikovaným systémovým certifikátom (ZoEP ČR) alebo certifikátom I.CA (ZoEP SR) iba k označovaniu (ZoEP ČR) alebo podpisovaniu (ZoEP SR) vydávaných certifikátov a zoznamu zrušených certifikátov
- vydávané certifikáty spĺňajú náležitosti, uvedené v ZoEP
- zruší certifikáty, pokiaľ bola žiadosť o ukončenie ich platnosti podaná spôsobom definovaným v zodpovedajúcom CP

Všetky záruky a z nich plynúce plnenia je možné uznať iba vtedy, ak :

Certifikačný poriadok pre vydávanie kvalifikovaných certifikátov	Strana 63 (celkom 66)
Copyright © První certifikační autorita, a.s.	Verejný dokument

- klient neporušil povinnosti vyplývajúce mu zo zmluvy o poskytovaní kvalifikovanej certifikačnej služby medzi ním a I.CA, z príslušného CP a kapitoly 4.5.1
- spoliehajúca sa strana neporušila povinnosti príslušného CP a kapitoly 4.5.2

Klient uplatňuje záruku vždy u RA, ktorá spracovala jeho prvotnú žiadosť. Pokiaľ RA nie je schopná vybaviť záručné nároky vo svojej právomoci, postúpi ich k vybaveniu I.CA a o tejto skutočnosti klienta upovedomí. Na používanie certifikátu, ktorý I.CA nevydala, sa záruky nevzťahujú.

9.6.2 Zastupovanie a záruky RA

RA preberá záväzok za správne vybavenie žiadostí (viď. kapitola 1.3.2). RA nevybaví kladne žiadosť, pokiaľ žiadateľ hodnoverným spôsobom nepreukázal svoju identitu, nedoložil údaje uvedené v žiadosti o službu, odmieta potrebné údaje oznámiť alebo odmietne podpísať príslušné dokumenty. Postup je popísaný v tomto CP. RA ďalej zodpovedá :

- za včasné odovzdanie žiadostí o zrušenie vydaných certifikátov k vybaveniu na pracovisko CA.
- za vybavovanie pripomienok a sťažností klientov

9.6.3 Zastupovanie a záruky držiteľa certifikátu a podpisujúcej osoby

Držiteľ certifikátu alebo podpisujúca osoba ručia za informácie, nimi uvedené v zmluve o poskytovaní kvalifikovanej certifikačnej služby a postupujú v súlade s platnou legislatívou.

9.6.4 Zastupovanie a záruky spoliehajúcich sa strán

Spoliehajúce sa strany postupujú v súlade so ZoEP.

9.6.5 Zastupovanie a záruky ostatných zúčastnených subjektov

Tieto skutočnosti sú pre aplikáciu tohto vydania tohto CP irelevantné.

9.7 Zrieknutie sa záruk

Spoločnosť První certifikační autorita, a.s., sa predovšetkým striktne riadi ZoEP a nemôže sa zriecť záruk, v ňom určených.

9.8 Obmedzenie zodpovednosti

Hranice zodpovednosti spoločnosti První certifikační autorita, a.s., sa v oblasti poskytovania kvalifikovaných certifikačných služieb riadia platnou legislatívou - ZoEP ČR, SR.

9.9 Zodpovednosť za škodu, náhrada škody

Platí vždy limit záruky, ktorý bol dojednaný v písomnej podobe. Pokiaľ výška nárokovanej straty prekračuje dojednaný limit, poskytne I.CA plnenie maximálne do výšky limitu. Pokiaľ bolo zistené porušenie povinností podpisujúcej osoby/držiteľa certifikátu/spoliehajúcej sa osoby, majúcej súvislosť s uvádzanou škodou, záručné plnenie sa neposkytne. Táto skutočnosť musí byť klientovi oznámená a zaprotokolovaná.

Ďalšie možné náhrady škody vychádzajú z ustanovení príslušných zákonov a o ich výške môže rozhodnúť súd.

Nový certifikát bude držiteľovi poskytnutý **zadarmo** v prípadoch :

- dôvodného podozrenia, že došlo ku kompromitácii dát pre vytváranie elektronických podpisov (ZoEP ČR, SR) alebo elektronických značiek (ZoEP ČR), resp. samotnej kompromitácii dát pre

Certifikačný poriadok pre vydávanie kvalifikovaných certifikátov	Strana 64 (celkom 66)
Copyright © První certifikační autorita, a.s.	Verejný dokument

vytváranie elektronických značiek (ZoEP ČR) alebo elektronických podpisov (ZoEP ČR, SR) I.CA v oblasti vydávania certifikátov, ponúkne držiteľom bezplatné vydanie nového certifikátu.

- príjem žiadosti o certifikát - I.CA kontroluje pri prijímaní žiadosti, či už neexistuje iný certifikát s rovnakým verejným kľúčom. Pokiaľ áno, je žiadateľ o certifikát vyzvaný k vygenerovaniu novej žiadosti, a teda aj nových párových dát. Držiteľ už existujúceho certifikátu, ktorý vlastní verejný kľúč zhodný s žiadateľom o certifikát, je vyzvaný k vygenerovaniu nových párových dát, jeho pôvodný certifikát je okamžite zrušený a držiteľ je o tejto skutočnosti informovaný. V takom prípade má držiteľ takto zrušeného certifikátu nárok na vydanie nového certifikátu zadarmo.

9.10 Doba platnosti, ukončenie platnosti

9.10.1 Doba platnosti

Tento dokument zostáva v platnosti do skončenia platnosti posledného certifikátu, ktorý bol podľa tohto CP vydaný.

9.10.2 Ukončenie platnosti

Jedinou osobou, ktorá je oprávnená schvaľovať ukončenie platnosti tohto CP, je riaditeľ spoločnosti První certifikační autorita, a.s.

9.10.3 Dôsledky ukončenia a pretrvanie záväzkov

Uvedené v kapitole 9.10.1.

9.11 Komunikácia medzi zúčastnenými subjektmi

Pre individuálne oznámenia a komunikáciu s držiteľmi certifikátov môže I.CA využiť nimi dodané e-mailové adresy, poštové adresy, telefonické čísla alebo osobné rokovania.

Podpisujúce osoby, označujúce osoby, drželia certifikátov, spoliehajúce sa strany a verejnosť môžu s I.CA komunikovať spôsobom, uvedeným na adrese <http://www.ica.cz/>.

9.12 Zmeny

9.12.1 Postup pri zmenách

Postup je realizovaný riadeným procesom, uvedenom v internom dokumente.

9.12.2 Postup pri oznamovaní zmien

Postup je realizovaný riadeným procesom, uvedenom v internom dokumente.

9.12.3 Okolnosti, pri ktorých musí byť zmenené OID

V prípade zmeny v tomto CP a jemu zodpovedajúcemu CPS prideli poverená osoba (vd. kapitola 1.5.4) novej verzii CP a CPS číslo a nové identifikátory (OID).

9.13 Riešenie sporov

Tento CP a zodpovedajúce CPS, ich výklad a aplikácia sa riadia legislatívou ZoEP a VoEP ČR, SR.

<i>Certifikačný poriadok pre vydávanie kvalifikovaných certifikátov</i>	<i>Strana 65 (celkom 66)</i>
<i>Copyright © První certifikační autorita, a.s.</i>	<i>Verejný dokument</i>

V prípade, že držiteľ certifikátu, spoliehajúca sa strana, žiadateľ o certifikát alebo zmluvný partner nesúhlasí s predloženým výkladom, môžu použiť nasledujúce stupne odvolania :

- zodpovedný pracovník RA
- zodpovedný pracovník I.CA (nutné písomné podanie)
- riaditeľ I.CA (nutné písomné podanie a zloženie finančnej istiny, ktorá je vrátená v prípade kladného vybavenia sťažnosti)

Uvedený postup dáva nesúhlasiacej strane možnosť presadzovať svoj názor rýchlejšim spôsobom, než súdnou cestou.

9.14 Rozhodné právo

Obchodná činnosť spoločnosti První certifikační autorita, a.s., sa riadi právnym poriadkom ČR.

9.15 Zhoda s právnymi predpismi

System poskytovania kvalifikovaných certifikačných služieb v oblasti vydávania certifikátov je prevádzkovaný v zhode s požiadavky ZoEP.

9.16 Ďalšie ustanovenia

9.16.1 Rámcová zhoda

Tieto skutočnosti sú pre aplikáciu tohto vydania CP irelevantné.

9.16.2 Postúpenie práv

Tieto skutočnosti sú pre aplikáciu tohto vydania CP irelevantné.

9.16.3 Oddeliteľnosť ustanovení

Tieto skutočnosti sú pre aplikáciu tohto vydania CP irelevantné.

9.16.4 Zrieknutie sa práv

Tieto skutočnosti sú pre aplikáciu tohto vydania CP irelevantné.

9.16.5 Vyššia moc

Zmluva o poskytovaní kvalifikovaných certifikačných služieb v oblasti vydávania certifikátov môže obsahovať ustanovenie o pôsobení vyššej moci.

9.17 Ďalšie opatrenia

Tieto skutočnosti sú pre aplikáciu tohto vydania CP irelevantné.

<i>Certifikačný poriadok pre vydávanie kvalifikovaných certifikátov</i>	<i>Strana 66 (celkom 66)</i>
<i>Copyright © První certifikační autorita, a.s.</i>	<i>Verejný dokument</i>

10 Záverečné ustanovenia

Tento CP vydaný spoločnosťou První certifikační autorita, a.s., nadobúda platnosť a účinnosť dňom 14.10.2006.