

**První certifikační autorita, a.s.**

**CERTIFIKAČNÍ POLITIKA**

**VYDÁVÁNÍ KOŘENOVÉHO**  
**CERTIFIKÁTU I.CA – KOMERČNÍ**  
**CERTIFIKÁTY**

Verze 3.3

Dokument *Certifikační politika vydávání kořenového certifikátu I.CA – komerční certifikáty* 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.

<b>Certifikační politika vydávání kořenového certifikátu I.CA – komerční certifikáty</b>	<b>Strana 2 (celkem 47)</b>
<b>Copyright © První certifikační autorita, a.s.</b>	

Tabulka 1 - Identifikace

<b>Název</b>	Certifikační politika vydávání kořenového certifikátu I.CA – komerční certifikáty
<b>Společnost</b>	První certifikační autorita, a.s.
<b>Schválil</b>	Ředitel společnosti První certifikační autorita, a.s.

Tabulka 2 – Vývoj dokumentu

<b>Verze</b>	<b>Datum vydání</b>	<b>Shrnutí změn</b>
3.0	03.08.2009	Implementace požadavků ETSI TS 102 176-1 (rodina SHA2)
3.1.	01.04.2011	Aktualizace dokumentu
3.2	12.01.2015	Aktualizace odkazovaných norem a standardů
3.3	22.09.2015	Aktualizace a revize dokumentu

<b>Certifikační politika vydávání kořenového certifikátu I.CA – komerční certifikáty</b>	<b>Strana 3 (celkem 47)</b>
<b>Copyright © První certifikační autorita, a.s.</b>	

# Obsah

<b>1 ÚVOD .....</b>	<b>9</b>
1.1 PŘEHLED.....	9
1.2 NÁZEV A IDENTIFIKACE DOKUMENTU .....	9
1.3 PARTICIPUJÍCÍ SUBJEKTY .....	9
1.3.1 Certifikační autority (dále "CA") .....	9
1.3.2 Registrační autority (dále "RA") .....	9
1.3.3 Držitelé certifikátů a podepisující osoby, kteří požádali o vydání kořenového certifikátu (dále certifikátu) a kterým byl certifikát vydán .....	9
1.3.4 Spoléhající se strany.....	9
1.3.5 Jiné participující subjekty .....	10
1.4 POUŽITÍ CERTIFIKÁTU.....	10
1.4.1 Přípustné použití certifikátu.....	10
1.4.2 Omezení použití certifikátu .....	10
1.5 SPRÁVA POLITIKY .....	10
1.5.1 Organizace spravující certifikační politiku nebo certifikační prováděcí směrnici .....	10
1.5.2 Kontaktní osoba organizace spravující certifikační politiku nebo certifikační prováděcí směrnici	10
1.5.3 Subjekt odpovědný za rozhodování o souladu postupů poskytovatele s postupy jiných poskytovatelů certifikačních služeb.....	10
1.5.4 Postupy při schvalování souladu s bodem 1.5.3.....	10
1.6 PŘEHLED POUŽITÝCH POJMŮ A ZKRATEK.....	10
<b>2 ODPOVĚDNOSTI ZA ZVEŘEJŇOVÁNÍ A ÚLOŽIŠTĚ INFORMACÍ A DOKUMENTACE.....</b>	<b>12</b>
2.1 ÚLOŽIŠTĚ INFORMACÍ A DOKUMENTACE .....	12
2.2 ZVEŘEJŇOVÁNÍ INFORMACÍ A DOKUMENTACE .....	12
2.3 PERIODICITA ZVEŘEJŇOVÁNÍ INFORMACÍ .....	12
2.4 ŘÍZENÍ PŘÍSTUPU K JEDNOTLIVÝM TYPŮM ÚLOŽIŠŤ .....	12
<b>3 IDENTIFIKACE A AUTENTIZACE .....</b>	<b>14</b>
3.1 POJMENOVÁVÁNÍ.....	14
3.1.1 Typy jmen .....	14
3.1.2 Požadavek na významovost jmen .....	14
3.1.3 Anonymita a používání pseudonymu.....	14
3.1.4 Pravidla pro interpretaci různých forem jmen .....	14
3.1.5 Jedinečnost jmen .....	14
3.1.6 Obchodní značky .....	14
3.2 POČÁTEČNÍ OVĚŘENÍ IDENTITY.....	14
3.2.1 Ověření souladu dat, tj. postup při ověřování, zda má osoba data pro vytváření elektronických podpisů odpovídající datům pro ověřování elektronických podpisů.....	14
3.2.2 Ověřování identity právnické osoby nebo organizační složky státu.....	15
3.2.3 Ověřování identity fyzické osoby.....	15
3.2.4 Neověřené informace vztahující se k držiteli certifikátu nebo podepisující či označující osobě	15
3.2.5 Ověřování specifických práv.....	15
3.2.6 Kritéria pro interoperabilitu.....	15
3.3 IDENTIFIKACE A AUTENTIZACE PŘI ZPRACOVÁNÍ POŽADAVKŮ NA VÝMĚNU DAT PRO OVĚŘOVÁNÍ ELEKTRONICKÝCH PODPISŮ .....	16
3.3.1 Identifikace a autentizace při rutinní výměně dat pro vytváření elektronických podpisů a jim odpovídajících dat pro ověřování elektronických podpisů (dále „párová data“) .....	16
3.3.2 Identifikace a autentizace při výměně párových dat po zneplatnění certifikátu.....	16
3.4 IDENTIFIKACE A AUTENTIZACE PŘI ZPRACOVÁNÍ POŽADAVKŮ NA ZNEPLATNĚNÍ CERTIFIKÁTU .....	16
<b>4 POŽADAVKY NA ŽIVOTNÍ CYKLUS CERTIFIKÁTU .....</b>	<b>17</b>
4.1 ŽÁDOST O VYDÁNÍ CERTIFIKÁTU .....	17

<b>Certifikační politika vydávání kořenového certifikátu I.CA – komerční certifikáty</b>	<b>Strana 4 (celkem 47)</b>
<b>Copyright © První certifikační autorita, a.s.</b>	

4.1.1	Subjekty oprávněné podat žádost o vydání certifikátu.....	17
4.1.2	Registrační proces a odpovědnosti poskytovatele a žadatele .....	17
4.2	ZPRACOVÁNÍ ŽÁDOSTI O CERTIFIKÁT .....	17
4.2.1	Identifikace a autentizace .....	17
4.2.2	Přijetí nebo odmítnutí žádosti o certifikát .....	17
4.2.3	Doba zpracování žádosti o certifikát .....	17
4.3	VYDÁNÍ CERTIFIKÁTU .....	17
4.3.1	Úkony CA v průběhu vydání certifikátu.....	17
4.3.2	Oznámení o vydání certifikátu držiteli certifikátu podepisující osobě .....	17
4.4	PŘEVZETÍ VYDANÉHO CERTIFIKÁTU .....	17
4.4.1	Úkony spojené s převzetím certifikátu .....	17
4.4.2	Zveřejňování vydaných certifikátů poskytovatelem.....	18
4.4.3	Oznámení o vydání certifikátu jiným subjektům.....	18
4.5	POUŽITÍ PÁROVÝCH DAT A CERTIFIKÁTU .....	18
4.5.1	Použití dat pro vytváření elektronických podpisů a certifikátu držitelem certifikátu podepisující osobou .....	18
4.5.2	Použití dat pro ověřování elektronických podpisů a certifikátu spoléhající se stranou.....	18
4.6	OBNOVENÍ CERTIFIKÁTU .....	18
4.6.1	Podmínky pro obnovení certifikátu.....	18
4.6.2	Subjekty oprávněné požadovat obnovení certifikátu .....	18
4.6.3	Zpracování požadavku na obnovení certifikátu.....	18
4.6.4	Oznámení o vydání obnoveného certifikátu držiteli certifikátu, podepisující označující osobě .....	18
4.6.5	Úkony spojené s převzetím obnoveného certifikátu .....	18
4.6.6	Zveřejnění vydaných obnovených certifikátů poskytovatelem .....	19
4.6.7	Oznámení o vydání obnoveného certifikátu ostatním subjektům .....	19
4.7	VÝMĚNA DAT PRO OVĚŘOVÁNÍ ELEKTRONICKÝCH PODPISŮ V CERTIFIKÁTU.....	19
4.7.1	Podmínky pro výměnu dat pro ověřování elektronických podpisů v certifikátu .....	19
4.7.2	Subjekty oprávněné požadovat výměnu dat pro ověřování elektronických podpisů v certifikátu .....	19
4.7.3	Zpracování požadavku na výměnu dat pro ověřování elektronických podpisů v certifikátu....	19
4.7.4	Oznámení o vydání certifikátu s vyměněnými daty pro ověřování elektronických podpisů nebo dat pro ověřování elektronických značek podepisující nebo označující osobě .....	19
4.7.5	Úkony spojené s převzetím certifikátu s vyměněnými daty pro ověřování elektronických podpisů .....	19
4.7.6	Zveřejnění vydaných certifikátů s vyměněnými daty pro ověřování elektronických podpisů... ..	19
4.7.7	Oznámení o vydání certifikátu s vyměněnými daty pro ověřování elektronických podpisů.....	20
4.8	ZMĚNA ÚDAJŮ V CERTIFIKÁTU .....	20
4.8.1	Podmínky pro změnu údajů v certifikátu.....	20
4.8.2	Subjekty oprávněné požadovat změnu údajů v certifikátu .....	20
4.8.3	Zpracování požadavku na změnu údajů v certifikátu.....	20
4.8.4	Oznámení o vydání certifikátu se změněnými údaji podepisující osobě .....	20
4.8.5	Úkony spojené s převzetím certifikátu se změněnými údaji.....	20
4.8.6	Zveřejnění vydaných certifikátů se změněnými údaji.....	20
4.8.7	Oznámení o vydání certifikátu se změněnými údaji jiným subjektům.....	20
4.9	ZNEPLATNĚNÍ A POZASTAVENÍ PLATNOSTI CERTIFIKÁTU.....	20
4.9.1	Podmínky pro zneplatnění certifikátu .....	20
4.9.2	Subjekty oprávněné žádat o zneplatnění certifikátu.....	21
4.9.3	Požadavek na zneplatnění certifikátu .....	21
4.9.4	Doba odkladu požadavku na zneplatnění certifikátu .....	21
4.9.5	Maximální doba, za kterou musí poskytovatel realizovat požadavek na zneplatnění certifikátu .....	21
4.9.6	Povinnosti spoléhajících se stran při ověřování, zda nebyl certifikát zneplatněn .....	21
4.9.7	Periodicita vydávání seznamu zneplatněných certifikátů .....	21
4.9.8	Maximální zpoždění při vydávání seznamu zneplatněných certifikátů .....	21
4.9.9	Možnost ověřování statutu certifikátu on-line („dále OCSP“).....	21
4.9.10	Požadavky při ověřování statutu certifikátu na on-line.....	21
4.9.11	Jiné způsoby oznamování zneplatnění certifikátu.....	22

<b>Certifikační politika vydávání kořenového certifikátu I.CA – komerční certifikáty</b>	<b>Strana 5 (celkem 47)</b>
<b>Copyright © První certifikační autorita, a.s.</b>	

4.9.12	Případné odlišnosti postupu zneplatnění v případě kompromitace dat pro vytváření elektronických podpisů .....	22
4.9.13	Podmínky pro pozastavení platnosti certifikátu .....	22
4.9.14	Subjekty oprávněné požadovat pozastavení platnosti certifikátu.....	22
4.9.15	Zpracování požadavku na pozastavení platnosti certifikátu .....	22
4.9.16	Omezení doby pozastavení platnosti certifikátu.....	22
4.10	SLUŽBY SOUVISEJÍCÍ S OVĚŘOVÁNÍM STATUTU CERTIFIKÁTU .....	22
4.10.1	Funkční charakteristiky .....	22
4.10.2	Dostupnost služeb.....	22
4.10.3	Další charakteristiky služeb statutu certifikátu .....	22
4.11	UKONČENÍ POSKYTOVÁNÍ SLUŽEB PRO DRŽITELE CERTIFIKÁTU, PODEPISUJÍCÍ OSOBOU .....	23
4.12	ÚSCHOVA DAT PRO VYTVÁŘENÍ ELEKTRONICKÝCH PODPISŮ U DŮVĚRYHODNÉ TŘETÍ STRANY A JEJICH OBNOVA 23	
4.12.1	Politika a postupy při úschově a obnovování dat pro vytváření elektronických podpisů.....	23
4.12.2	Politika a postupy při zapouzdřování a obnovování šifrovacího klíče pro relaci.....	23
<b>5</b>	<b>MANAGEMENT, PROVOZNÍ A FYZICKÁ BEZPEČNOST .....</b>	<b>24</b>
5.1	FYZICKÁ BEZPEČNOST .....	24
5.1.1	Umístění a konstrukce .....	24
5.1.2	Fyzický přístup.....	24
5.1.3	Elektrina a klimatizace .....	24
5.1.4	Vliv vody.....	24
5.1.5	Protipožární opatření a ochrana.....	24
5.1.6	Ukládání médií .....	24
5.1.7	Nakládání s odpady .....	24
5.1.8	Zálohy mimo budovu provozního pracoviště .....	25
5.2	PROCESNÍ BEZPEČNOST .....	25
5.2.1	Důvěryhodné role.....	25
5.2.2	Počet osob požadovaných na zajištění jednotlivých činností.....	25
5.2.3	Identifikace a autentizace pro každou roli.....	25
5.2.4	Role vyžadující rozdělení povinností.....	25
5.3	PERSONÁLNÍ BEZPEČNOST .....	25
5.3.1	Požadavky na kvalifikaci, zkušenost a bezúhonnost .....	25
5.3.2	Posouzení spolehlivosti osob .....	26
5.3.3	Požadavky na přípravu pro výkon role, vstupní školení.....	26
5.3.4	Požadavky a periodičita školení .....	26
5.3.5	Periodičita a posloupnost rotace pracovníků mezi různými rolemi .....	26
5.3.6	Postihy za neoprávněné činnosti zaměstnanců .....	26
5.3.7	Požadavky na nezávislé zhotovitele (dodavatele) .....	26
5.3.8	Dokumentace poskytovaná zaměstnancům .....	27
5.4	AUDITNÍ ZÁZNAMY (LOGY) .....	27
5.4.1	Typy zaznamenávaných událostí.....	27
5.4.2	Periodičita zpracování záznamů .....	27
5.4.3	Doba uchovávání auditních záznamů.....	27
5.4.4	Ochrana auditních záznamů .....	27
5.4.5	Postupy pro zálohování auditních záznamů.....	27
5.4.6	Systém shromažďování auditních záznamů (interní nebo externí).....	28
5.4.7	Postup při oznamování události subjektu, který ji způsobil.....	28
5.4.8	Hodnocení zranitelnosti .....	28
5.5	UCHOVÁVÁNÍ INFORMACÍ A DOKUMENTACE .....	28
5.5.1	Typy informací a dokumentace, které se uchovávají.....	28
5.5.2	Doba uchovávání uchovávaných informací a dokumentace.....	28
5.5.3	Ochrana úložiště uchovávaných informací a dokumentace .....	28
5.5.4	Postupy při zálohování uchovávaných informací a dokumentace .....	29
5.5.5	Požadavky na používání časových razítek při uchovávání informací a dokumentace.....	29
5.5.6	Systém shromažďování uchovávaných informací a dokumentace (interní, externí) .....	29
5.5.7	Postupy pro získání a ověření uchovávaných informací a dokumentace.....	29

<b>Certifikační politika vydávání kořenového certifikátu I.CA – komerční certifikáty</b>	<b>Strana 6 (celkem 47)</b>
<b>Copyright © První certifikační autorita, a.s.</b>	

5.6	VÝMĚNA DAT PRO OVĚŘOVÁNÍ ELEKTRONICKÉHO PODPISU V NADŘÍZENÉM KOŘENOVÉM CERTIFIKÁTU POSKYTOVATELE .....	29
5.7	OBNOVA PO HAVÁRII NEBO KOMPROMITACI .....	30
5.7.1	Postup v případě incidentu a kompromitace .....	30
5.7.2	Poškození výpočetních prostředků, software nebo dat .....	30
5.7.3	Postup při kompromitaci dat pro vytváření elektronických podpisů poskytovatele .....	30
5.7.4	Schopnost obnovit činnost po havárii.....	30
5.8	UKONČENÍ ČINNOSTI CA.....	30
<b>6</b>	<b>TECHNICKÁ BEZPEČNOST .....</b>	<b>32</b>
6.1	GENEROVÁNÍ A INSTALACE PÁROVÝCH DAT .....	32
6.1.1	Generování párových dat .....	32
6.1.2	Předání dat pro vytváření elektronických podpisů podepisující osobě .....	32
6.1.3	Předání dat pro ověřování elektronických podpisů poskytovateli certifikačních služeb .....	32
6.1.4	Poskytování dat pro ověřování elektronických podpisů certifikační autoritou spoléhajícím se stranám 32	
6.1.5	Délky párových dat.....	32
6.1.6	Generování parametrů dat pro vytváření elektronických podpisů a kontrola jejich kvality.....	32
6.1.7	Omezení pro použití dat pro ověřování elektronických podpisů.....	32
6.2	OCHRANA DAT PRO VYTVÁŘENÍ ELEKTRONICKÝCH PODPISŮ A BEZPEČNOST KRYPTOGRAFICKÝCH MODULŮ 33	
6.2.1	Standardy a podmínky používání kryptografických modulů .....	33
6.2.2	Sdílení tajemství .....	33
6.2.3	Úschova pro vytváření elektronických podpisů .....	33
6.2.4	Zálohování pro vytváření elektronických podpisů .....	33
6.2.5	Uchovávání pro vytváření elektronických podpisů .....	33
6.2.6	Transfer pro vytváření elektronických podpisů do kryptografického modulu nebo z kryptografického modulu .....	33
6.2.7	Uložení pro vytváření elektronických podpisů v kryptografickém modulu .....	33
6.2.8	Postup při aktivaci dat pro vytváření elektronických podpisů .....	34
6.2.9	Postup při deaktivaci dat pro vytváření elektronických podpisů .....	34
6.2.10	Postup při zničení dat pro vytváření elektronických podpisů .....	34
6.2.11	Hodnocení kryptografického modulu .....	34
6.3	DALŠÍ ASPEKTY SPRÁVY PÁROVÝCH DAT .....	34
6.3.1	Uchovávání dat pro ověřování elektronických podpisů .....	34
6.3.2	Maximální doba platnosti certifikátu podepisující osoby a párových dat .....	34
6.4	AKTIVAČNÍ DATA .....	34
6.4.1	Generování a instalace aktivačních dat.....	35
6.4.2	Ochrana aktivačních dat .....	35
6.4.3	Ostatní aspekty aktivačních dat .....	35
6.5	POČÍTAČOVÁ BEZPEČNOST .....	35
6.5.1	Specifické technické požadavky na počítačovou bezpečnost.....	35
6.5.2	Hodnocení počítačové bezpečnosti.....	35
6.6	BEZPEČNOST ŽIVOTNÍHO CYKLU .....	36
6.6.1	Řízení vývoje systému.....	36
6.6.2	Kontroly řízení bezpečnosti .....	36
6.6.3	Řízení bezpečnosti životního cyklu.....	36
6.7	SÍŤOVÁ BEZPEČNOST.....	36
6.8	ČASOVÁ RAZÍTKA.....	36
<b>7</b>	<b>PROFILY CERTIFIKÁTU, SEZNAMU ZNEPLATNĚNÝCH CERTIFIKÁTŮ A OCSP .....</b>	<b>37</b>
7.1	PROFIL CERTIFIKÁTU.....	37
7.1.1	Čísla verzí.....	37
7.1.2	Rozšiřující položky v certifikátu.....	37
7.1.3	Objektové identifikátory (dále OID) algoritmů .....	37
7.1.4	Způsoby zápisu jmen a názvů.....	38
7.1.5	Omezení jmen a názvů.....	38

<b>Certifikační politika vydávání kořenového certifikátu I.CA – komerční certifikáty</b>	<b>Strana 7 (celkem 47)</b>
<b>Copyright © První certifikační autorita, a.s.</b>	

7.1.6	OID certifikační politiky.....	38
7.1.7	Rozšiřující položka „Policy Constraints“.....	38
7.1.8	Syntaxe a sémantika rozšiřující položky kvalifikátorů politiky „Policy Qualifiers“.....	38
7.1.9	Způsob zápisu kritické rozšiřující položky „Certificate Policies“.....	38
7.2	PROFIL SEZNAMU ZNEPLATNĚNÝCH CERTIFIKÁTŮ.....	38
7.2.1	Číslo verze.....	39
7.2.2	Rozšiřující položky seznamu zneplatněných certifikátů a záznamů v seznamu zneplatněných certifikátů.....	39
7.3	PROFIL OCSP.....	39
7.3.1	Číslo verze.....	39
7.3.2	Rozšiřující položky OCSP.....	39
<b>8</b>	<b>HODNOCENÍ SHODY A JINÁ HODNOCENÍ.....</b>	<b>40</b>
8.1	PERIODICITA HODNOCENÍ NEBO OKOLNOSTI PRO PROVEDENÍ HODNOCENÍ.....	40
8.2	IDENTITA A KVALIFIKACE HODNOTITELE.....	40
8.3	VZTAH HODNOTITELE K HODNOCENÉ ENTITĚ.....	40
8.4	HODNOCENÉ OBLASTI.....	40
8.5	POSTUP V PŘÍPADĚ ZJIŠTĚNÝCH NEDOSTATKŮ.....	40
8.6	SDĚLOVÁNÍ VÝSLEDKŮ HODNOCENÍ.....	40
<b>9</b>	<b>OSTATNÍ OBCHODNÍ A PRÁVNÍ ZÁLEŽITOSTI.....</b>	<b>41</b>
9.1	POPLATKY.....	41
9.1.1	Poplatky za vydání nebo obnovení certifikátu.....	41
9.1.2	Poplatky za přístup k certifikátu na seznamu vydaných certifikátů.....	41
9.1.3	Poplatky za informace o statutu certifikátu a o zneplatnění certifikátu.....	41
9.1.4	Poplatky za další služby.....	41
9.1.5	Jiná ustanovení týkající se poplatků (vč. refundací).....	41
9.2	FINANČNÍ ODPOVĚDNOST.....	41
9.2.1	Krytí pojištěním.....	41
9.2.2	Další aktiva a záruky.....	41
9.2.3	Pojištění nebo krytí zárukou pro koncové uživatele.....	41
9.3	CITLIVOST OBCHODNÍCH INFORMACÍ.....	42
9.3.1	Výčet citlivých informací.....	42
9.3.2	Informace mimo rámec citlivých informací.....	42
9.3.3	Odpovědnost za ochranu citlivých informací.....	42
9.4	OCHRANA OSOBNÍCH ÚDAJŮ.....	42
9.4.1	Politika ochrany osobních údajů.....	42
9.4.2	Osobní údaje.....	42
9.4.3	Údaje, které nejsou považovány za důvěrné.....	42
9.4.4	Odpovědnost za ochranu osobních údajů.....	42
9.4.5	Oznámení o používání důvěrných informací a souhlas s používáním citlivých informací.....	43
9.4.6	Poskytování citlivých informací pro soudní či správní účely.....	43
9.4.7	Jiné okolnosti zpřístupňování osobních údajů.....	43
9.5	PRÁVA DUŠEVNÍHO VLASTNICTVÍ.....	43
9.6	ZASTUPOVÁNÍ A ZÁRUKY.....	43
9.6.1	Zastupování a záruky CA.....	43
9.6.2	Zastupování a záruky RA.....	43
9.6.3	Zastupování a záruky držitele certifikátu, podepisující osoby.....	43
9.6.4	Zastupování a záruky spoléhajících se stran.....	43
9.6.5	Zastupování a záruky ostatních zúčastněných subjektů.....	44
9.7	ZŘEKnutí SE ZÁRUK.....	44
9.8	OMEZENÍ ODPOVĚDNOSTI.....	44
9.9	ODPOVĚDNOST ZA ŠKODU, NÁHRADA ŠKODY.....	44
9.10	DOBA PLATNOSTI, UKONČENÍ PLATNOSTI.....	44
9.10.1	Doba platnosti.....	44
9.10.2	Ukončení platnosti.....	44
9.10.3	Důsledky ukončení a přetrvání závazků.....	44

<b>Certifikační politika vydávání kořenového certifikátu I.CA – komerční certifikáty</b>	<b>Strana 8 (celkem 47)</b>
<b>Copyright © První certifikační autorita, a.s.</b>	

9.11	KOMUNIKACE MEZI ZÚČASTNĚNÝMI SUBJEKTY.....	44
9.12	ZMĚNY .....	44
9.12.1	<i>Postup při změnách .....</i>	44
9.12.2	<i>Postup při oznamování změn.....</i>	45
9.12.3	<i>Okolnosti, při kterých musí být změněno OID .....</i>	45
9.13	ŘEŠENÍ SPORŮ .....	45
9.14	ROZHODNÉ PRÁVO .....	45
9.15	SHODA S PRÁVNÍMI PŘEDPISY .....	45
9.16	DALŠÍ USTANOVENÍ.....	45
9.16.1	<i>Rámcová dohoda.....</i>	45
9.16.2	<i>Postoupení práv .....</i>	45
9.16.3	<i>Oddělitelnost ustanovení .....</i>	45
9.16.4	<i>Zřeknutí se práv .....</i>	45
9.16.5	<i>Vyšší moc.....</i>	45
9.17	DALŠÍ OPATŘENÍ .....	46
<b>10</b>	<b>ZÁVĚREČNÁ USTANOVENÍ.....</b>	<b>47</b>



<b>Certifikační politika vydávání kořenového certifikátu I.CA – komerční certifikáty</b>	<b>Strana 9 (celkem 47)</b>
<b>Copyright © První certifikační autorita, a.s.</b>	

## 1 Úvod

### 1.1 Přehled

Tento dokument, **Certifikační politika vydávání kořenového certifikátu I.CA – komerční certifikáty** (dále též CP), vypracovaný společností První certifikační autorita, a. s. (dále též I.CA):

- se zabývá skutečnostmi, které se vztahují na I.CA a které souvisejí s vydáváním kořenových certifikátů I.CA, jejich další správou, použitím, akceptací, ukončením platnosti, zneplatněním a všemi aspekty souvisejícími s nakládáním s párovými daty
- striktně dodržuje členění dokumentu navržené v RFC 3647, s přihlédnutím k doporučením orgánů EU a k právu ČR v dané oblasti. Jednotlivé kapitoly jsou proto v této CP zachovány i v případě, že jsou ve vztahu k ní irelevantní
- může být mimo jiné využito nezávislými institucemi (např. auditorskými společnostmi) jako základ pro potvrzení toho, že společností První certifikační autorita, a.s. poskytované certifikační služby je možné považovat za důvěryhodné.

Vydávané kořenové certifikáty I.CA jsou „self-signed“ certifikáty. Data pro ověřování elektronických podpisů, které mj. tyto certifikáty obsahují, jsou spojena s daty pro vytváření elektronických podpisů, kterými I.CA elektronicky podepisuje vydávané komerční certifikáty (dále certifikáty) a seznamy zneplatněných certifikátů.

### 1.2 Název a identifikace dokumentu

Název tohoto dokumentu : Certifikační politika vydávání kořenového certifikátu  
I.CA – komerční certifikáty  
OID : 1.3.6.1.4.1.23624.1.1.61.3.2

### 1.3 Participující subjekty

#### 1.3.1 Certifikační autority (dále “CA”)

I.CA je poskytovatelem certifikačních služeb. Podřízené certifikační autority, poskytující certifikační služby související s vydáváním certifikátů I.CA nezřizuje, ani nepodporuje.

#### 1.3.2 Registrační autority (dále “RA”)

Pro problematiku životního cyklu kořenových certifikátů jsou registrační autority využívány pouze v případě předání těchto certifikátů, resp. informací o těchto certifikátech uživatelům certifikačních služeb.

#### 1.3.3 Držitelé certifikátů a podepisující osoby, kteří požádali o vydání kořenového certifikátu (dále certifikátu) a kterým byl certifikát vydán

Držitelem kořenového certifikátu I.CA je společnost První certifikační autorita, a.s.

#### 1.3.4 Spoléhající se strany

Spoléhající se stranou mohou být fyzické osoby, právnické osoby nebo organizační složky státu, spoléhající se na vydaný certifikát dle této CP.

<b>Certifikační politika vydávání kořenového certifikátu I.CA – komerční certifikáty</b>	<b>Strana 10 (celkem 47)</b>
<b>Copyright © První certifikační autorita, a.s.</b>	

### 1.3.5 Jiné participující subjekty

Jinými participujícími subjekty jsou orgány činné v trestním řízení a další, kterým to ze zákona přísluší.

## 1.4 Použití certifikátu

### 1.4.1 Přípustné použití certifikátu

Kořenové certifikáty, vydávané dle této certifikační politiky společností První certifikační autorita, a.s., lze využívat pouze v procesech ověřování elektronického podpisu vydávaných certifikátů a seznamů zneplatněných certifikátů.

### 1.4.2 Omezení použití certifikátu

Certifikáty, vydávané dle této certifikační politiky společností První certifikační autorita, a.s. nesmí být využívány v rozporu s vydávaným účelem (definovaným touto CP).

## 1.5 Správa politiky

### 1.5.1 Organizace spravující certifikační politiku nebo certifikační prováděcí směrnici

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

### 1.5.2 Kontaktní osoba organizace spravující certifikační politiku nebo certifikační prováděcí směrnici

Touto osobou je pracovník I.CA, jmenovaný ředitelem společnosti První certifikační autorita, a.s. do role bezpečnostního manažera.

### 1.5.3 Subjekt odpovědný za rozhodování o souladu postupů poskytovatele s postupy jiných poskytovatelů certifikačních služeb

Jedinou osobou, která je odpovědná za rozhodování o souladu postupů společnosti První certifikační autorita, a.s., s postupy jiných poskytovatelů certifikačních služeb, je ředitel společnosti První certifikační autorita, a.s.

### 1.5.4 Postupy při schvalování souladu s bodem 1.5.3

V případě, že je potřebné provést změny a tedy i vytvořit novou verzi této CP, určuje ředitel společnosti První certifikační autorita, a.s., osobu, která je oprávněna tyto změny provádět. Touto osobou je pracovník I.CA, jmenovaný do role bezpečnostního manažera. Nabytí platnosti nových verzí CP předchází jejich schválení ředitelem společnosti První certifikační autorita, a.s.

## 1.6 Přehled použitých pojmů a zkratk

Tabulka 3 – Pojmy a zkratky

Pojem	Vysvětlení
CP	certifikační politika (veřejný dokument)

<b>Certifikační politika vydávání kořenového certifikátu I.CA – komerční certifikáty</b>	<b>Strana 11 (celkem 47)</b>
<b>Copyright © První certifikační autorita, a.s.</b>	

CPS	certifikační prováděcí směrnice (neveřejný dokument)
CRL	<b>Certificate Revocation List</b> (seznam zneplatněných certifikátů)
Držitel certifikátu	fyzická osoba, právnická osoba nebo organizační složka státu, která požádala o vydání certifikátu pro sebe nebo pro podepisující osobu a které byl certifikát vydán
Čas	světový čas UTC
ETSI	<b>European Telecommunications Standards Institute</b>
I.CA	První certifikační autorita, a.s. – akreditovaný poskytovatel certifikačních služeb
MRCP	Microsoft Root Certificate Program
NIST	<b>National Institute of Standards and Technology</b>
Párová data (dvojice soukromý a veřejný klíč)	jedinečná data pro vytváření elektronického podpisu spolu s odpovídajícími daty pro ověřování elektronického podpisu, resp. elektronické značky
Podepisující osoba	fyzická osoba, která je držitelem prostředku pro vytváření elektronických podpisů a jedná jménem svým nebo jménem jiné fyzické či právnické osoby
Smluvní partner	poskytovatel certifikačních služeb, který zajišťuje na základě písemné smlouvy pro I.CA certifikační služby nebo jejich části
Soukromý klíč	jedinečná data pro vytváření elektronického podpisu, resp. elektronické značky
Spoléhající se strana	subjekt, spoléhající se při své činnosti na certifikát, vydaný I.CA
UTC	<b>Universal Co-ordinated Time</b> , Standard přijatý 1.1.1972 pro světový koordinovaný čas (Coordinated Universal Time – UTC). Funkci “oficiálního časoměřiče” atomového času pro celý svět vykonává Bureau International de l'Heure (BIH)
Veřejný klíč	jedinečná data pro ověřování elektronického podpisu, resp. elektronické značky

<b>Certifikační politika vydávání kořenového certifikátu I.CA – komerční certifikáty</b>	<b>Strana 12 (celkem 47)</b>
<b>Copyright © První certifikační autorita, a.s.</b>	

## **2 Odpovědnosti za zveřejňování a úložiště informací a dokumentace**

### **2.1 Úložiště informací a dokumentace**

Společnost První certifikační autorita, a.s. zřizuje a provozuje úložiště informací a dokumentace, za která taktéž, jako poskytovatel certifikačních služeb odpovídá.

### **2.2 Zveřejňování informací a dokumentace**

Základní adresy (dále též informační adresy), na nichž lze nalézt veřejné informace o společnosti První certifikační autorita, a.s. (certifikační politiky, zprávy pro uživatele, ostatní veřejné a aktuální informace a dokumenty atd.), případně odkazy pro zjištění dalších informací, jsou:

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

Adresy, které slouží pro kontakt veřejnosti s I.CA, jsou:

- a) sídlo registrační autority, která smluvní vztah s I.CA zprostředkovala
- b) elektronická poštovní adresa [info@ica.cz](mailto:info@ica.cz)

I.CA zveřejňuje výše uvedené kontaktní adresy na své internetové adrese a pracovištích vlastních registračních autorit. Pracovníci I.CA a smluvních partnerů jsou rovněž povinni tyto informace na vyžádání sdělit veřejnosti.

V případech zneužití, popř. vzniku důvodné obavy ze zneužití dat pro vytváření elektronických podpisů vydávaných certifikátů a seznamů zneplatněných certifikátů oznámí I.CA tuto skutečnost na své internetové informační adrese a prostřednictvím nejméně jednoho celostátně distribuovaného deníku.

### **2.3 Periodicita zveřejňování informací**

S ohledem na problematiku kořenových certifikátů I.CA zveřejňuje I.CA informace s následující periodicitou:

- Kořenové certifikáty I.CA včetně hashe – před jejich využíváním,
- Informace o zneplatnění kořenových certifikátů I.CA s uvedením důvodu zneplatnění (v případě zneužití nebo vzniku důvodné obavy ze zneužití dat pro vytváření elektronických podpisů) – bezodkladně,
- ostatní veřejné informace – není předem určeno, obecně však platí, že tyto informace musí odrážet aktuální stav poskytovaných certifikačních služeb.

### **2.4 Řízení přístupu k jednotlivým typům úložišť**

Veškeré veřejné informace s právem čtení zpřístupňuje I.CA bez pro účely čtení bezplatně bez omezení.

<b><i>Certifikační politika vydávání kořenového certifikátu I.CA – komerční certifikáty</i></b>	<b><i>Strana 13 (celkem 47)</i></b>
<b><i>Copyright © První certifikační autorita, a.s.</i></b>	

Přístup ke neveřejným typům úložišť pověřenými pracovníky I.CA je definován interní dokumentací.

<b>Certifikační politika vydávání kořenového certifikátu I.CA – komerční certifikáty</b>	<b>Strana 14 (celkem 47)</b>
<b>Copyright © První certifikační autorita, a.s.</b>	

## 3 Identifikace a autentizace

### 3.1 Pojmenovávání

#### 3.1.1 Typy jmen

Tabulka 2 – Issuer, Subject

Položka	Obsah
Organization (O)	První certifikační autorita, a.s.
OrganizationUnitName(OU)	I.CA – Provider of Certification Services
CommonName (CN)	I.CA – Standard Certification Authority, MM/RRRR
Country (C)	CZ

Pozn.: MM/RRRR je měsíc a rok vydání certifikátu

#### 3.1.2 Požadavek na významovost jmen

Viz sloupec Obsah v tabulce, uvedené v kapitole 3.1.1.

#### 3.1.3 Anonymita a používání pseudonymu

Tyto skutečnosti jsou pro aplikaci tohoto vydání této CP irelevantní.

#### 3.1.4 Pravidla pro interpretaci různých forem jmen

Pokud se jedná o jména nebo jiné skutečnosti, které jsou uvedeny v předkládaných dokumentech, přenášejí se tato jména v té podobě, v jaké jsou v dokumentu uvedena. Vlastní transkripce se neprovádí.

#### 3.1.5 Jedinečnost jmen

Jedinečnost jména Subject a Issuer je zaručena.

#### 3.1.6 Obchodní značky

Ve vydaném kořenovém certifikátu I.CA se musí ověřitelné údaje vztahovat k I.CA.

### 3.2 Počáteční ověření identity

Jediná fyzická osoba, která může rozhodnout a požádat o vydání kořenového certifikátu I.CA, je ředitel společnosti První certifikační autorita, a.s.

#### 3.2.1 Ověření souladu dat, tj. postup při ověřování, zda má osoba data pro vytváření elektronických podpisů odpovídající datům pro ověřování elektronických podpisů

Vlastnictví dat pro vytváření elektronických podpisů, odpovídající datům pro ověřování elektronických podpisů, která bude daný kořenový certifikát I.CA obsahovat, se prokazuje v procesu generování párových dat. Samotný proces generování párových dat je prováděn v souladu s interními směrnici a dokumentací výrobce konkrétního HSM.

<b>Certifikační politika vydávání kořenového certifikátu I.CA – komerční certifikáty</b>	<b>Strana 15 (celkem 47)</b>
<b>Copyright © První certifikační autorita, a.s.</b>	

### **3.2.2 Ověřování identity právnické osoby nebo organizační složky státu**

Ředitel I.CA před zahájením vlastního generování párových dat předkládá listinné dokumenty, které dokládají jeho jmenování do funkce ředitele I.CA a originál nebo notářsky ověřenou kopii výpisu z obchodního rejstříku, na jejichž základě byla I.CA vytvořena a která musí obsahovat úplné obchodní jméno, identifikační číslo (IČO), statutární orgán a sídlo.

### **3.2.3 Ověřování identity fyzické osoby**

Ředitel I.CA, identifikující se platným primárním a sekundárním osobním dokladem, předloží své následující údaje:

- celé občanské jméno,
- datum narození,
- číslo předloženého primárního osobního dokladu,
- adresu trvalého bydliště.

Vyžaduje se předložení originálu platného primárního osobního dokladu a originálu dalšího osobního dokladu (sekundárního). Primární osobní doklad pro občany ČR musí být občanský průkaz, popř. obdobný doklad stejné právní váhy. Primární osobní doklad pro cizince je platný cestovní pas, popř. obdobný doklad stejné právní váhy. Sekundární osobní doklad musí být vydán orgánem veřejné moci nebo jinou organizací, jejíž existenci lze doložit. Sekundární osobní doklad musí obsahovat celé občanské jméno fyzické osoby, vyřizující žádost a dále nejméně jeden z následujících údajů:

- datum narození (nebo rodné číslo u občanů ČR),
- adresu trvalého bydliště žadatele,
- fotografii obličeje.

Údaje požadované v sekundárním osobním dokladu musí být shodné s těmito údaji v primárním osobním dokladu.

### **3.2.4 Neověřené informace vztahující se k držiteli certifikátu nebo podepisující či označující osobě**

Všechny informace musí být ověřeny.

### **3.2.5 Ověřování specifických práv**

Tyto skutečnosti jsou pro aplikaci tohoto vydání této CP irelevantní.

### **3.2.6 Kritéria pro interoperabilitu**

Tyto skutečnosti jsou pro aplikaci tohoto vydání této CP irelevantní.

<b>Certifikační politika vydávání kořenového certifikátu I.CA – komerční certifikáty</b>	<b>Strana 16 (celkem 47)</b>
<b>Copyright © První certifikační autorita, a.s.</b>	

### **3.3 Identifikace a autentizace při zpracování požadavků na výměnu dat pro ověřování elektronických podpisů**

#### **3.3.1 Identifikace a autentizace při rutinní výměně dat pro vytváření elektronických podpisů a jim odpovídajících dat pro ověřování elektronických podpisů (dále „párová data“)**

Je nutné vydat nový certifikát s novým veřejným klíčem. Platí stejné požadavky, jako v případě počátečního ověření identity.

#### **3.3.2 Identifikace a autentizace při výměně párových dat po zneplatnění certifikátu**

Je nutné vydat nový certifikát s novým veřejným klíčem. Platí stejné požadavky, jako v případě počátečního ověření identity.

### **3.4 Identifikace a autentizace při zpracování požadavků na zneplatnění certifikátu**

Žadatel o zneplatnění kořenového certifikátu I.CA musí prokázat, že je ředitelem I.CA.



<b>Certifikační politika vydávání kořenového certifikátu I.CA – komerční certifikáty</b>	<b>Strana 17 (celkem 47)</b>
<b>Copyright © První certifikační autorita, a.s.</b>	

## **4 Požadavky na životní cyklus certifikátu**

V souladu s doporučením technické specifikace ETSI TS 119 312 Electronic Signatures and Infrastructures (ESI); Cryptographic Suites je v procesu vydávání kořenového certifikátu využíván algoritmus RSA s SHA-256 (sha256RSA) a délka kryptografického klíče pro algoritmus RSA 2048 bitů.

### **4.1 Žádost o vydání certifikátu**

#### **4.1.1 Subjekty oprávněné podat žádost o vydání certifikátu**

Viz relevantní podkapitoly kapitoly 3.2.

#### **4.1.2 Registrační proces a odpovědnosti poskytovatele a žadatele**

Viz relevantní podkapitoly kapitoly 3.2.

### **4.2 Zpracování žádosti o certifikát**

#### **4.2.1 Identifikace a autentizace**

Viz relevantní podkapitoly kapitoly 3.2.

#### **4.2.2 Přijetí nebo odmítnutí žádosti o certifikát**

Viz kapitol 4.3.

#### **4.2.3 Doba zpracování žádosti o certifikát**

Při dodržení všech potřebných podmínek řádově minuty.

### **4.3 Vydání certifikátu**

#### **4.3.1 Úkony CA v průběhu vydání certifikátu**

Viz relevantní podkapitoly kapitoly 3.2.

#### **4.3.2 Oznámení o vydání certifikátu držiteli certifikátu podepisující osobě**

V procesu vydávání kořenového certifikátu I.CA je ředitel I.CA informován prostřednictvím člena komise.

### **4.4 Převzetí vydaného certifikátu**

#### **4.4.1 Úkony spojené s převzetím certifikátu**

Pokud byly splněny podmínky pro vydání kořenového certifikátu I.CA, tzn. splněny podmínky identifikace a prokázání vlastnictví dat pro vytváření elektronických podpisů odpovídajících datům pro ověřování elektronických podpisů, která bude vydaný kořenového certifikátu I.CA obsahovat, je povinností ředitele I.CA tento certifikát přijmout.

<b>Certifikační politika vydávání kořenového certifikátu I.CA – komerční certifikáty</b>	<b>Strana 18 (celkem 47)</b>
<b>Copyright © První certifikační autorita, a.s.</b>	

#### **4.4.2 Zveřejňování vydaných certifikátů poskytovatelem**

I.CA je povinna zajistit zveřejnění kořenového certifikátu I.CA.

#### **4.4.3 Oznámení o vydání certifikátu jiným subjektům**

V případech vydání kořenového certifikátu I.CA získají oznámení o jeho vydání pracovníci komise. Dále platí ustanovení kapitoly 4.4.2.

### **4.5 Použití párových dat a certifikátu**

#### **4.5.1 Použití dat pro vytváření elektronických podpisů a certifikátu držitelem certifikátu podepisující osobou**

Viz kapitola 1.4.

#### **4.5.2 Použití dat pro ověřování elektronických podpisů a certifikátu spoléhající se stranou**

Spoléhající se strany jsou zejména povinny:

- získat z bezpečného zdroje kořenový certifikát I.CA a ověřit kontrolní součet tohoto certifikátu,
- provádět veškeré úkony potřebné k tomu, aby si ověřily, že tento certifikát nebyl zneplatněn.

### **4.6 Obnovení certifikátu**

Tato služba není podporována. Je nutné vydat nový certifikát s novým veřejným klíčem. Platí stejné požadavky jako v případě počátečního ověření identity.

#### **4.6.1 Podmínky pro obnovení certifikátu**

Viz kapitola 4.6.

#### **4.6.2 Subjekty oprávněné požadovat obnovení certifikátu**

Viz kapitola 4.6.

#### **4.6.3 Zpracování požadavku na obnovení certifikátu**

Viz kapitola 4.6.

#### **4.6.4 Oznámení o vydání obnoveného certifikátu držiteli certifikátu, podepisující označující osobě**

Viz kapitola 4.6.

#### **4.6.5 Úkony spojené s převzetím obnoveného certifikátu**

Viz kapitola 4.6.

<b>Certifikační politika vydávání kořenového certifikátu I.CA – komerční certifikáty</b>	<b>Strana 19 (celkem 47)</b>
<b>Copyright © První certifikační autorita, a.s.</b>	

#### **4.6.6 Zveřejnění vydaných obnovených certifikátů poskytovatelem**

Viz kapitola 4.6.

#### **4.6.7 Oznámení o vydání obnoveného certifikátu ostatním subjektům**

Viz kapitola 4.6.

### **4.7 Výměna dat pro ověřování elektronických podpisů v certifikátu**

Tato služba není podporována. Je nutné vydat nový certifikát s novým veřejným klíčem. Platí stejné požadavky jako v případě počátečního ověření identity.

#### **4.7.1 Podmínky pro výměnu dat pro ověřování elektronických podpisů v certifikátu**

Viz kapitola 4.7.

#### **4.7.2 Subjekty oprávněné požadovat výměnu dat pro ověřování elektronických podpisů v certifikátu**

Viz kapitola 4.7.

#### **4.7.3 Zpracování požadavku na výměnu dat pro ověřování elektronických podpisů v certifikátu**

Viz kapitola 4.7.

#### **4.7.4 Oznámení o vydání certifikátu s vyměněnými daty pro ověřování elektronických podpisů nebo dat pro ověřování elektronických značek podepisující nebo označující osobě**

Viz kapitola 4.7.

#### **4.7.5 Úkony spojené s převzetím certifikátu s vyměněnými daty pro ověřování elektronických podpisů**

Viz kapitola 4.7.

#### **4.7.6 Zveřejnění vydaných certifikátů s vyměněnými daty pro ověřování elektronických podpisů**

Viz kapitola 4.7.

<b>Certifikační politika vydávání kořenového certifikátu I.CA – komerční certifikáty</b>	<b>Strana 20 (celkem 47)</b>
<b>Copyright © První certifikační autorita, a.s.</b>	

#### **4.7.7 Oznámení o vydání certifikátu s vyměněnými daty pro ověřování elektronických podpisů**

Viz kapitola 4.7.

### **4.8 Změna údajů v certifikátu**

Tato služba není podporována. Je nutné vydat nový certifikát s novým veřejným klíčem. Platí stejné požadavky jako v případě počátečního ověření identity.

#### **4.8.1 Podmínky pro změnu údajů v certifikátu**

Viz kapitola 4.8.

#### **4.8.2 Subjekty oprávněné požadovat změnu údajů v certifikátu**

Viz kapitola 4.8.

#### **4.8.3 Zpracování požadavku na změnu údajů v certifikátu**

Viz kapitola 4.8.

#### **4.8.4 Oznámení o vydání certifikátu se změněnými údaji podepisující osobě**

Viz kapitola 4.8.

#### **4.8.5 Úkony spojené s převzetím certifikátu se změněnými údaji**

Viz kapitola 4.8.

#### **4.8.6 Zveřejnění vydaných certifikátů se změněnými údaji**

Viz kapitola 4.8.

#### **4.8.7 Oznámení o vydání certifikátu se změněnými údaji jiným subjektům**

Viz kapitola 4.8.

### **4.9 Zneplatnění a pozastavení platnosti certifikátu**

#### **4.9.1 Podmínky pro zneplatnění certifikátu**

Kořenový certifikát I.CA může být zneplatněn na základě následujících okolností:

- dojde ke kompromitaci, resp. existuje důvodné podezření, že došlo ke kompromitaci, soukromého klíče, odpovídajícího veřejnému klíči tohoto certifikátu,
- na žádost ředitele I.CA.

<b>Certifikační politika vydávání kořenového certifikátu I.CA – komerční certifikáty</b>	<b>Strana 21 (celkem 47)</b>
<b>Copyright © První certifikační autorita, a.s.</b>	

#### **4.9.2 Subjekty oprávněné žádat o zneplatnění certifikátu**

Žádost o zneplatnění mohou podat subjekty oprávněné dle platné legislativy nebo ředitel I.CA.

#### **4.9.3 Požadavek na zneplatnění certifikátu**

Po splnění podmínek na identifikaci a autentizaci je postupováno následujícím způsobem. Žádost musí obsahovat sériové číslo kořenového certifikátu buď v dekadickém tvaru nebo hexadecimální (uvozeno řetězcem „0x“), celé občanské jméno ředitele I.CA, kterému byl kořenový certifikát vydán a heslo pro zneplatnění. Pokud žádost splňuje výše uvedené požadavky, odpovědný pracovník CA neprodleně kořenový certifikát zneplatní. Datum a čas zneplatnění je určen okamžikem přijetí platné žádosti o zneplatnění kořenového certifikátu serverem I.CA.

#### **4.9.4 Doba odkladu požadavku na zneplatnění certifikátu**

Tyto skutečnosti jsou pro aplikaci tohoto vydání této CP irelevantní.

#### **4.9.5 Maximální doba, za kterou musí poskytovatel realizovat požadavek na zneplatnění certifikátu**

Reakcí I.CA na přijetí platné žádosti o zneplatnění kořenového certifikátu I.CA je jeho neprodlené zneplatnění a zveřejnění této informace. CRL obsahující sériové číslo zneplatněného certifikátu musí být vydán neprodleně po zneplatnění tohoto certifikátu.

#### **4.9.6 Povinnosti spoléhajících se stran při ověřování, zda nebyl certifikát zneplatněn**

Viz kapitola 4.5.2.

#### **4.9.7 Periodicita vydávání seznamu zneplatněných certifikátů**

Seznam zneplatněných certifikátů je společností První certifikační autorita, a.s. vydáván v pravidelných intervalech, minimálně jedenkrát za 24 hodin, v případě nutnosti bezodkladně. Činnosti operátorů CA v procesu vytváření a vydávání CRL jsou popsány v interních dokumentech.

#### **4.9.8 Maximální zpoždění při vydávání seznamu zneplatněných certifikátů**

Seznam zneplatněných certifikátů je zveřejňován neprodleně po jeho vydání. Maximální zpoždění vydání seznamů zneplatněných certifikátů nesmí přesáhnout 24 hodiny.

#### **4.9.9 Možnost ověřování statutu certifikátu on-line („dále OCSP“)**

Tyto skutečnosti jsou pro aplikaci tohoto vydání této CP irelevantní.

#### **4.9.10 Požadavky při ověřování statutu certifikátu na on-line**

Tyto skutečnosti jsou pro aplikaci tohoto vydání této CP irelevantní.

<b>Certifikační politika vydávání kořenového certifikátu I.CA – komerční certifikáty</b>	<b>Strana 22 (celkem 47)</b>
<b>Copyright © První certifikační autorita, a.s.</b>	

#### **4.9.11 Jiné způsoby oznamování zneplatnění certifikátu**

Tyto skutečnosti jsou pro aplikaci tohoto vydání této CP irelevantní.

#### **4.9.12 Případné odlišnosti postupu zneplatnění v případě kompromitace dat pro vytváření elektronických podpisů**

Tyto skutečnosti jsou pro aplikaci tohoto vydání této CP irelevantní.

#### **4.9.13 Podmínky pro pozastavení platnosti certifikátu**

Tyto skutečnosti jsou pro aplikaci tohoto vydání této CP irelevantní.

#### **4.9.14 Subjekty oprávněné požadovat pozastavení platnosti certifikátu**

Tyto skutečnosti jsou pro aplikaci tohoto vydání této CP irelevantní.

#### **4.9.15 Zpracování požadavku na pozastavení platnosti certifikátu**

Tyto skutečnosti jsou pro aplikaci tohoto vydání této CP irelevantní.

#### **4.9.16 Omezení doby pozastavení platnosti certifikátu**

Tyto skutečnosti jsou pro aplikaci tohoto vydání této CP irelevantní.

### **4.10 Služby související s ověřováním statutu certifikátu**

#### **4.10.1 Funkční charakteristiky**

Služby související s ověřováním statutu kořenového certifikátu I.CA jsou poskytovány I.CA prostřednictvím internetových informačních adres I.CA.

#### **4.10.2 Dostupnost služeb**

Služba poskytování veřejných certifikátů formou zveřejňování informací je dostupná 7 dní v týdnu 24 hodin denně.

I.CA garantuje zajištění nepřetržité dostupnosti (7dní v týdnu 24 hodin denně) a integrity seznamu zneplatněných certifikátů (platné CRL).

#### **4.10.3 Další charakteristiky služeb statutu certifikátu**

Další charakteristiky služeb statutu certifikátu nejsou poskytovány. I.CA může poskytování charakteristik služeb statutu certifikátu rozšířit.

#### **4.11 Ukončení poskytování služeb pro držitele certifikátu, podepisující osobou**

Viz kapitola 5.8.

#### **4.12 Úschova dat pro vytváření elektronických podpisů u důvěryhodné třetí strany a jejich obnova**

Tyto skutečnosti jsou pro aplikaci tohoto vydání této CP irelevantní.

##### **4.12.1 Politika a postupy při úschově a obnovování dat pro vytváření elektronických podpisů**

Tyto skutečnosti jsou pro aplikaci tohoto vydání této CP irelevantní.

##### **4.12.2 Politika a postupy při zapouzdřování a obnovování šifrovacího klíče pro relaci**

Tyto skutečnosti jsou pro aplikaci tohoto vydání této CP irelevantní.

<b>Certifikační politika vydávání kořenového certifikátu I.CA – komerční certifikáty</b>	<b>Strana 24 (celkem 47)</b>
<b>Copyright © První certifikační autorita, a.s.</b>	

## **5 Management, provozní a fyzická bezpečnost**

### **5.1 Fyzická bezpečnost**

#### **5.1.1 Umístění a konstrukce**

Objekty provozního pracoviště jsou umístěny v geograficky odlišných lokalitách, které jsou dále jiné, než ředitelství společnosti, obchodní a vývojová pracoviště, pracoviště registračních autorit a obchodních míst.

Zařízení určená k výkonu hlavních certifikačních služeb jsou umístěna ve vyhrazených prostorách provozních pracovišť. Tyto prostory jsou zabezpečené obdobně, jako zabezpečené oblasti kategorie „Důvěrné“ podle zákona o ochraně utajovaných informací.

#### **5.1.2 Fyzický přístup**

Fyzický přístup do jednotlivých vyhrazených prostor (chráněných mechanickými a elektronickými prostředky) provozního pracoviště je uveden v interní dokumentaci společnosti. Ochrana objektu je řešena elektronickým zabezpečovacím systémem (EZS), připojením na pult centrální ochrany (PCO) a speciálním systémem pro snímání, přenos a zobrazování pohybu osob a dopravních prostředků.

#### **5.1.3 Elektřina a klimatizace**

V prostorách, určených k výkonu hlavních certifikačních služeb v oblasti vydávání certifikátů, je dostatečně dimenzovaná aktivní klimatizace, která udržuje celoroční teplotu v rozmezí 20°C ± 5°C. Přívod elektrické energie je jistěn pomocí UPS (Uninterruptible Power Supply), resp. diesel agregátu.

#### **5.1.4 Vliv vody**

Všechny kritické systémy provozních pracovišť jsou umístěny takovým způsobem, aby nemohly být zaplaveny ani stoletou vodou. Provozní pracoviště jsou podle potřeby vybavena čidly průniku vody pro případ zaplavení vodou z topení, nebo vodou ze střechy při prudkém dešti.

#### **5.1.5 Protipožární opatření a ochrana**

V objektech provozních pracovišť a pracovišť pro uchovávání informací je instalována elektronická požární signalizace (EPS). Vstupní dveře vyhrazených prostor, ve kterých jsou umístěna zařízení, určená k výkonu hlavních certifikačních služeb, jsou opatřeny protipožární vložkou. V samotných prostorách se nachází hasicí přístroj.

#### **5.1.6 Ukládání médií**

Paměťová média, obsahující provozní zálohy a záznamy v elektronické podobě, jsou ukládána v kovových skříních, popř. trezorech. Kopie jsou ukládány v jiné geografické lokalitě, než kde je umístěno provozní pracoviště.

Papírová média, která je nutno, mj. podle platné legislativy týkající se elektronického podpisu, archivovat, jsou skladována v jiné geografické lokalitě, než je umístěno provozní pracoviště.

#### **5.1.7 Nakládání s odpady**

Veškerý papírový kancelářský odpad je před opuštěním provozních pracovišť I.CA znehodnocen skartováním.



<b>Certifikační politika vydávání kořenového certifikátu I.CA – komerční certifikáty</b>	<b>Strana 25 (celkem 47)</b>
<b>Copyright © První certifikační autorita, a.s.</b>	

### **5.1.8 Zálohy mimo budovu provozního pracoviště**

Kopie provozních a pracovních záloh jsou uloženy na místě určeném ředitelem I.CA a popsáném v interní dokumentaci.

## **5.2 Procesní bezpečnost**

### **5.2.1 Důvěryhodné role**

Pro vybrané činnosti jsou ve společnosti I.CA definovány důvěryhodné role, která jsou spolu s odpovídajícími činnostmi a odpovědnostmi definovány v interní dokumentaci.

### **5.2.2 Počet osob požadovaných na zajištění jednotlivých činností**

Ve společnosti První certifikační autorita, a.s. jsou pro procesy poskytování certifikačních služeb definovány činnosti, které se musí vykonávat jedině za účasti více než jediné osoby. Jedná se zejména o:

- generování párových dat pro vytváření/ověřování elektronického podpisu I.CA vydávaných certifikátů a seznamů zneplatněných certifikátů,
- ničení dat pro vytváření elektronického podpisu I.CA vydávaných certifikátů a seznamů zneplatněných certifikátů,
- zálohování/obnovu dat pro vytváření elektronického podpisu I.CA vydávaných certifikátů a seznamů zneplatněných certifikátů,
- aktivace kryptografického modulu, obsahujícího data pro vytváření elektronického podpisu I.CA vydávaných certifikátů a seznamů zneplatněných certifikátů.

Pro provádění ostatních úloh není počet přítomných osob určen, musí však jít výhradně o pověřené pracovníky.

### **5.2.3 Identifikace a autentizace pro každou roli**

Pracovníkům každé role jsou přiděleny prostředky pro řádnou identifikaci (jméno, certifikát) a autentizaci (heslo, soukromý klíč) k těm komponentám, které jsou pro jejich činnost nezbytné.

### **5.2.4 Role vyžadující rozdělení povinností**

Role, vyžadující rozdělení povinností v procesu poskytování certifikačních služeb v oblasti certifikátů, jsou definovány v interní bezpečnostní dokumentaci.

## **5.3 Personální bezpečnost**

### **5.3.1 Požadavky na kvalifikaci, zkušenost a bezúhonnost**

Pracovníci v důvěryhodných rolích jsou vybíráni a přijímáni na základě dále popsanych personálních kritérií:

- naprostá občanská bezúhonnost - prokazováno tím, že tyto osoby nemají žádný záznam v rejstříku trestů (výpis z registru trestů nebo čestné prohlášení),
- vysokoškolské vzdělání v rámci akreditovaného bakalářského nebo magisterského studijního programu a nejméně 3 roky praxe v oblasti informačních a komunikačních technologií, nebo

<b>Certifikační politika vydávání kořenového certifikátu I.CA – komerční certifikáty</b>	<b>Strana 26 (celkem 47)</b>
<b>Copyright © První certifikační autorita, a.s.</b>	

středoškolské vzdělání a nejméně 5 let praxe v oblasti informačních a komunikačních technologií, přičemž z toho nejméně 1 rok v oblasti poskytování certifikačních služeb,

- znalost v oblasti infrastruktury veřejných klíčů a informační bezpečnosti,
- v jednotlivých případech lze zkrátit délku uvedené praxe až o jednu třetinu stanovené délky na základě přezkoušení, při němž pracovník prokáže dostatečné znalosti k výkonu důvěryhodné funkce.

Ostatní pracovníci jsou přijímáni na základě následujících kritérií:

- vysokoškolské vzdělání v rámci akreditovaného bakalářského, resp. magisterského studijního programu, nebo středoškolské vzdělání,
- základní orientace v oblasti infrastruktury veřejných klíčů a informační bezpečnosti.

### **5.3.2 Posouzení spolehlivosti osob**

Zdrojem informací všech kmenových pracovníků I.CA jsou:

- sami tyto pracovníci,
- osoby, které tyto pracovníky znají,
- veřejné zdroje informací .

Pracovníci poskytují prvotní informace osobním pohovorem při přijímání do pracovního poměru, které aktualizují při periodických pohovorech s nadřazeným pracovníkem v průběhu pracovního poměru.

### **5.3.3 Požadavky na přípravu pro výkon role, vstupní školení**

Pracovníci I.CA jsou odborně zaškoleni pro používání určeného programového vybavení a speciálních zařízení. Zaškolení se provádí kombinací metody samopřípravy a metodickým vedením již zaškoleným pracovníkem. Běžná doba na zaškolení je jeden měsíc.

### **5.3.4 Požadavky a periodicitu školení**

Pro kmenové pracovníky pořádá vedení I.CA minimálně jedenkrát ročně interní výukový seminář, zaměřený na problematiku bezpečnosti informací.

### **5.3.5 Periodicita a posloupnost rotace pracovníků mezi různými rolemi**

Z důvodů možné zastupitelnosti v mimořádných případech jsou pracovníci I.CA motivováni na získávání znalostí potřebných na zastávání jiné role v I.CA.

### **5.3.6 Postihy za neoprávněné činnosti zaměstnanců**

Při zjištění neautorizované činnosti je s dotyčným pracovníkem postupováno způsobem, uvedeným v interních dokumentech společnosti a řídí se zákoníkem práce (tento proces nebrání případnému trestnímu stíhání, pokud tomu odpovídá závažnost zjištěné neautorizované činnosti).

### **5.3.7 Požadavky na nezávislé zhotovitele (dodavatele)**

I.CA může, nebo musí některé činnosti zajišťovat smluvně. Tyto obchodně právní vztahy jsou ošetřeny bilaterálními obchodními smlouvami. Jedná se o např. o smluvní registrační autority, zhotovitele programového aplikačního vybavení, dodavatele hardware, systémového programového vybavení, externí

<b>Certifikační politika vydávání kořenového certifikátu I.CA – komerční certifikáty</b>	<b>Strana 27 (celkem 47)</b>
<b>Copyright © První certifikační autorita, a.s.</b>	

auditory atd. Tyto subjekty jsou povinny se řídit odpovídajícími veřejnými certifikačními politikami, relevantními částmi interní dokumentace I.CA, které jim budou poskytnuty a předepsanými normativními dokumenty. V případě porušení těchto povinností jsou vyžadovány smluvní pokuty, případně je s nimi okamžitě ukončena smlouva.

### **5.3.8 Dokumentace poskytovaná zaměstnancům**

Kmenoví zaměstnanci I.CA mají k dispozici kromě certifikační politiky, certifikační prováděcí směrnice, bezpečnostní a provozní dokumentace veškeré další příslušné normy, směrnice, příručky a metodické pokyny, potřebné pro výkon jejich činnosti.

## **5.4 Auditní záznamy (logy)**

### **5.4.1 Typy zaznamenávaných událostí**

Všechny auditní záznamy jsou v nutné míře pořizovány, uchovávány a zpracovávány se zachováním prokazatelnosti původu, integrity, dostupnosti, důvěrnosti a časové autentičnosti.

Auditní systém je navržen a provozován způsobem, který zaručuje udržování auditní dat, rezervování dostatečného prostoru pro auditní data, automatické nepřepisování auditního souboru, prezentaci auditních záznamů pro uživatele vhodným způsobem a omezení přístupu k auditnímu souboru pouze pro definované uživatele.

### **5.4.2 Periodicita zpracování záznamů**

Auditní záznamy jsou kontrolovány a vyhodnocovány v intervalech, definovaných v interní bezpečnostní dokumentaci, v případě bezpečnostního incidentu okamžitě.

### **5.4.3 Doba uchovávání auditních záznamů**

Nestanoví-li relevantní legislativní norma jinak, jsou auditní záznamy uchovávány po dobu nejméně 10 let od jejich vzniku.

### **5.4.4 Ochrana auditních záznamů**

Auditní záznamy v elektronické a papírové podobě jsou uloženy způsobem, zajišťujícím jejich ochranu před jejich změnami, krádeží a zničením (ať již úmyslnému, tak neúmyslnému).

Elektronické auditní záznamy jsou ukládány ve dvou kopiích, každá kopie je umístěna v jiné místnosti provozních prostor I.CA. Minimálně jedenkrát měsíčně se provádí uložení těchto auditních záznamů na médium, které je umístěno mimo provozní prostory I.CA.

Auditní záznamy v papírové formě jsou umístěny mimo provozních prostory I.CA.

Ochrana výše uvedených typů auditních záznamů je definována v interní bezpečnostní dokumentaci.

### **5.4.5 Postupy pro zálohování auditních záznamů**

Zálohování elektronických auditních záznamů probíhá obdobným způsobem jako zálohování ostatních elektronických informací. Zálohování auditních záznamů v papírové formě prováděno není.

<b>Certifikační politika vydávání kořenového certifikátu I.CA – komerční certifikáty</b>	<b>Strana 28 (celkem 47)</b>
<b>Copyright © První certifikační autorita, a.s.</b>	

#### **5.4.6 Systém shromažďování auditních záznamů (interní nebo externí)**

Systém shromažďování auditních záznamů je ve vztahu k I.CA interní, ve vztahu k smluvním partnerům externí.

#### **5.4.7 Postup při oznamování události subjektu, který ji způsobil**

Subjekt není o zapsání události do auditního záznamu informován.

#### **5.4.8 Hodnocení zranitelnosti**

Hodnocení zranitelnosti je ve společnosti První certifikační autorita, a.s. prováděno v periodických intervalech, v případě incidentu, majícího vliv na bezpečnost poskytovaných služeb okamžitě.

### **5.5 Uchovávání informací a dokumentace**

#### **5.5.1 Typy informací a dokumentace, které se uchovávají**

I.CA uchovává následující typy informací a dokumentace, které souvisejí s problematikou kořenového certifikátu I.CA:

- elektronické nebo písemné informace dle platné legislativy:
  - samotný kořenový certifikát I.CA,
  - kopie předložených osobních dokladů žadatele o kořenový certifikát I.CA, na jejichž základě byla ověřena jeho identita,
  - dokumenty a záznamy související s životním cyklem vydaného kořenového certifikátu I.CA,
- auditní záznamy definované v kapitole 5.4.1 tohoto dokumentu, aplikační programové vybavení a veškerou dokumentaci společnosti, která je nutná pro provádění informačních auditů a kontrol bezpečnostní shody,
- identifikace místa, kde jsou uloženy informace a dokumentace, jejichž uchování je vyžadováno,
- veškeré seznamy zneplatněných certifikátů,
- identifikační údaje osoby, která provedla ověření totožnosti žadatele o kořenový certifikát I.CA,
- záznam o manipulaci (tj. např. převzetí, předání, uložení, kontrola, konverze do elektronické podoby atp.) s informacemi,
- provozní a bezpečnostní dokumentaci.

#### **5.5.2 Doba uchovávání uchovávaných informací a dokumentace**

I.CA zajišťuje uchovávání informací a dokumentace dle kapitoly 5.5.1 po dobu nejméně 10 let od jejich vzniku (nestanoví-li relevantní legislativní norma jinak).

Po celou dobu existence I.CA jsou uchovávány informace, vztahující se ke kořenovému certifikátu I.CA, s výjimkou příslušných dat pro vytváření elektronického podpisu.

Postupy při uchovávání informací a dokumentace jsou upraveny interní dokumentací I.CA.

#### **5.5.3 Ochrana úložiště uchovávaných informací a dokumentace**

Prostory, ve kterých se uchovávají informace a dokumentace nacházejí, jsou zabezpečeny formou opatření, vycházejících z požadavků objektové a fyzické bezpečnosti.

<b>Certifikační politika vydávání kořenového certifikátu I.CA – komerční certifikáty</b>	<b>Strana 29 (celkem 47)</b>
<b>Copyright © První certifikační autorita, a.s.</b>	

Postupy při ochraně úložiště uchovávaných informací a dokumentace jsou upraveny interní dokumentací I.CA.

#### **5.5.4 Postupy při zálohování uchovávaných informací a dokumentace**

Postupy při zálohování uchovávaných informací a dokumentace jsou upraveny interní dokumentací I.CA.

#### **5.5.5 Požadavky na používání časových razítek při uchovávání informací a dokumentace**

V případě, že jsou využívána časová razítka, jedná se o kvalifikovaná časová razítka, vydána I.CA.

#### **5.5.6 Systém shromažďování uchovávaných informací a dokumentace (interní, externí)**

Informace a dokumentace jsou ukládány na místo, určené ředitelem I.CA. Registrační autority jsou povinny provést předarchivaci v určených termínech a vzniklá data předat pověřeným pracovníkům I.CA.

Samotná problematika přípravy a způsobu ukládání informací a dokumentace v elektronické i písemné podobě je upravena interními normami a směrnicemi. Shromažďování uchovávaných informací je evidováno.

#### **5.5.7 Postupy pro získání a ověření uchovávaných informací a dokumentace**

Uchovávané informace a dokumentace jsou umístěny k tomu určených lokalitách a jsou přístupné:

- pracovníkům I.CA, pokud je to k jejich činnosti vyžadováno,
- oprávněným kontrolním subjektům, orgánům činných v trestním řízení a soudům, pokud je to právními normami vyžadováno.

O každém takto povoleném přístupu je pořizován písemný záznam.

### **5.6 Výměna dat pro ověřování elektronického podpisu v nadřazeném kořenovém certifikátu poskytovatele**

Výměna dat pro ověřování elektronických podpisů v kořenovém certifikátu I.CA je v případě standardních situací (vypršení platnosti certifikátu) s dostatečným časovým předstihem před vypršením doby platnosti tohoto certifikátu prováděna formou vydání nového kořenového certifikátu I.CA. V případě nestandardních situací (např. dojde-li k takovému vývoji kryptoanalytických metod, které by mohly ohrozit bezpečnost procesu tvorby elektronických značek, tzn. změny kryptografických algoritmů, délky klíčů atd.) je tato činnost prováděna v adekvátním časovém období.

Jak v případě standardních situací, tak nestandardních situací je výměna dat pro ověřování elektronických podpisů v kořenovém certifikátu I.CA držitelům certifikátů a veřejnosti s předstihem (je-li to možné) vhodnou formou sdělena.

<b>Certifikační politika vydávání kořenového certifikátu I.CA – komerční certifikáty</b>	<b>Strana 30 (celkem 47)</b>
<b>Copyright © První certifikační autorita, a.s.</b>	

## **5.7 Obnova po havárii nebo kompromitaci**

### **5.7.1 Postup v případě incidentu a kompromitace**

V případě výskytu uvedených událostí postupuje I.CA v souladu s interním dokumentem Plán pro zvládnání krizových situací a plán obnovy a jím odkazované dokumentaci.

### **5.7.2 Poškození výpočetních prostředků, software nebo dat**

V případě poškození výpočetních prostředků, softwaru nebo dat postupuje I.CA v souladu s interním dokumentem Plán pro zvládnání krizových situací a plán obnovy a jím odkazované dokumentaci.

### **5.7.3 Postup při kompromitaci dat pro vytváření elektronických podpisů poskytovatele**

V případě kompromitace nebo vzniku důvodné obavy ze zneužití dat pro vytváření elektronických podpisů podepisování vydávaných certifikátů a seznamů zneplatněných certifikátů I.CA:

- ukončí jejich používání,
- okamžitě a trvale zneplatní příslušný kořenový certifikát I.CA a jemu odpovídající data pro vytváření elektronických podpisů,
- zneplatní všechny platné certifikáty, které byly výše uvedenými daty označeny, resp. podepsány,
- bezodkladně o této skutečnosti, včetně důvodu informuje na své internetové informační adrese, pro zpřístupnění této informace je využít i seznam zneplatněných certifikátů,
- pokud je to možné, informuje držitele platných certifikátů o zneplatnění těchto certifikátů, a to prostřednictvím zaslání zprávy elektronickou poštou na elektronickou adresu, kterou tyto osoby uvedly v žádosti o vydání certifikátu, součástí této informace je důvod ukončení platnosti příslušného kořenového certifikátu I.CA,
- v případě vzniku důvodné obavy ze zneužití dat pro vytváření elektronických podpisů pro podepisování vydávaných certifikátů a seznamů zneplatněných certifikátů, nabídne I.CA výše uvedeným držitelům bezplatné vydání nového certifikátu s tím, že případné náklady na vydání nových certifikátů sama hradí. Postup je stejný jako při vydání prvotního certifikátu.

Obdobné postupy budou uplatněny i v případě, že dojde k takovému vývoji kryptoanalytických metod (např. změny kryptografických algoritmů, délky klíčů atd.), které by mohly bezprostředně ohrozit bezpečnost procesu vydávání certifikačních služeb.

### **5.7.4 Schopnosti obnovit činnost po havárii**

V případě havárie postupuje I.CA v souladu s interním dokumentem Plán pro zvládnání krizových situací a plán obnovy a jím odkazované dokumentaci.

## **5.8 Ukončení činnosti CA**

V případě plánovaného ukončení činnosti I.CA jako poskytovatele certifikačních služeb v oblasti vydávání certifikátů, tzn. z jiných důvodů, než-li jsou mimořádné události jakými jsou stávky, občanské nepokoje, válečný stav, přírodní katastrofy celostátního rozsahu nebo jiné výsledky působení vyšší moci, zajistí I.CA provedení následujících činností:

- ohlásí záměr ukončit činnost poskytování certifikačních služeb v oblasti vydávání certifikátů na své internetové informační adrese nejméně 3 měsíce před plánovaným ukončením činnosti,
- ukončí poskytování certifikačních služeb v oblasti vydávání certifikátů,

<b><i>Certifikační politika vydávání kořenového certifikátu I.CA – komerční certifikáty</i></b>	<b><i>Strana 31 (celkem 47)</i></b>
<b><i>Copyright © První certifikační autorita, a.s.</i></b>	

- prokazatelné zničí svá data pro vytváření elektronických podpisů, sloužící k podepisování vydávaných certifikátů a seznamu zneplatněných certifikátů.

<b>Certifikační politika vydávání kořenového certifikátu I.CA – komerční certifikáty</b>	<b>Strana 32 (celkem 47)</b>
<b>Copyright © První certifikační autorita, a.s.</b>	

## **6 Technická bezpečnost**

### **6.1 Generování a instalace párových dat**

#### **6.1.1 Generování párových dat**

Generování párových dat I.CA, souvisejících s kořenovým certifikátem I.CA, které probíhá v zabezpečené zóně o jehož průběhu je vyhotoven písemný protokol, je prováděno v kryptografickém modulu. Veškeré požadavky na proces generování párových dat I.CA, sloužících k podepisování vydávaných certifikátů a seznamů zneplatněných certifikátů jsou definovány v interní bezpečnostní dokumentaci.

#### **6.1.2 Předání dat pro vytváření elektronických podpisů podepisující osobě**

Generování párových dat, souvisejících s kořenovým certifikátem I.CA, je prováděno na zařízení a v prostředí, která jsou v okamžiku jejich generování pod výhradní kontrolou I.CA, a proto jsou tyto skutečnosti pro aplikaci tohoto vydání této CP irelevantní.

#### **6.1.3 Předání dat pro ověřování elektronických podpisů poskytovateli certifikačních služeb**

Tyto skutečnosti jsou pro aplikaci tohoto vydání této CP irelevantní.

#### **6.1.4 Poskytování dat pro ověřování elektronických podpisů certifikační autoritou spoléhajícím se stranám**

Data pro ověřování elektronických podpisů jsou obsažena v kořenovém certifikátu I.CA a možnost jeho získání je garantována následujícími způsoby:

- obdržení na RA (osobní návštěva),
- prostřednictvím internetových informačních adres I.CA,
- každý koncový žadatel obdrží kořenový certifikát I.CA při získání svého prvotního certifikátu na RA.

#### **6.1.5 Délky párových dat**

I.CA používá nejprověřenější klasický asymetrický šifrový algoritmus – RSA. Mohutnost klíčů (resp. parametrů daného algoritmu) použitých pro označování, resp. podepisování vydávaných certifikátů, seznamů zneplatněných certifikátů a časových razítek je 2048 bitů.

#### **6.1.6 Generování parametrů dat pro vytváření elektronických podpisů a kontrola jejich kvality**

Algoritmy, použité pro generování celočíselných hodnot nutných pro fungování elektronického podpisu (např. testy prvočíselnosti atd.) musí mít parametry uvedené v mezinárodně uznávaných technických standardech nebo normách.

#### **6.1.7 Omezení pro použití dat pro ověřování elektronických podpisů**

Uvedeno v kapitole 1.4.1.



<b>Certifikační politika vydávání kořenového certifikátu I.CA – komerční certifikáty</b>	<b>Strana 33 (celkem 47)</b>
<b>Copyright © První certifikační autorita, a.s.</b>	

## **6.2 Ochrana dat pro vytváření elektronických podpisů a bezpečnost kryptografických modulů**

### **6.2.1 Standardy a podmínky používání kryptografických modulů**

Generování párových dat I.CA, souvisejících s kořenovým certifikátem I.CA, uložení soukromého klíče I.CA, sloužícího pro vytváření elektronických podpisů vydávaných certifikátů a seznamů zneplatněných certifikátů probíhá v kryptografickém modulu, který splňuje požadavky standardu FIPS PUB 140-2, úroveň 3.

### **6.2.2 Sdílení tajemství**

Ochrana sdílením tajemství je realizována prostředky kryptografického modulu. Při provádění citlivých činností, které souvisejí se zásadními činnostmi I.CA, je nezbytná přítomnost tří pověřených pracovníků I.CA, z nichž dva znají část kódu k provedení těchto činností.

### **6.2.3 Úschova pro vytváření elektronických podpisů**

Tyto skutečnosti jsou pro aplikaci tohoto vydání této CP irelevantní.

### **6.2.4 Zálohování pro vytváření elektronických podpisů**

Kryptografické moduly, použité pro správu elektronických podpisů, umožňují zálohování dat pro vytváření elektronických podpisů. Data v zašifrované podobě jsou zálohována prostřednictvím čipových karet.

### **6.2.5 Uchovávání pro vytváření elektronických podpisů**

Po uplynutí doby platnosti soukromého klíče dat určených k podepisování vydávaných certifikátů a seznamů zneplatněných certifikátů je tento (včetně záloh) zničen a jeho další zálohování se neprovádí. Uchovávání těchto soukromých klíčů představuje bezpečnostní riziko, a proto je u I.CA zakázáno.

### **6.2.6 Transfer pro vytváření elektronických podpisů do kryptografického modulu nebo z kryptografického modulu**

Soukromý klíč, sloužící pro vytváření elektronických podpisů vydávaných certifikátů a seznamů zneplatněných certifikátů, je generován přímo v kryptografickém modulu.

Vkládání soukromého klíče do kryptografického modulu v případě, že se jedná o jeho obnovení ze šifrované zálohy, probíhá za přímé osobní účasti nejméně dvou určených pracovníků I.CA. V okamžiku jeho vkládání musí být vyhrazená stanice a kryptografický modul odpojeny od počítačové sítě. O vložení soukromého klíče je pořízen písemný záznam.

### **6.2.7 Uložení pro vytváření elektronických podpisů v kryptografickém modulu**

Soukromý klíč, sloužící k vytváření elektronických podpisů je uložen bezpečným způsobem v kryptografickém modulu, splňujícím požadavky FIPS 140-2 úroveň 3.

<b>Certifikační politika vydávání kořenového certifikátu I.CA – komerční certifikáty</b>	<b>Strana 34 (celkem 47)</b>
<b>Copyright © První certifikační autorita, a.s.</b>	

### **6.2.8 Postup při aktivaci dat pro vytváření elektronických podpisů**

Aktivaci dat pro vytváření elektronických podpisů vydávaných kořenových certifikátů a seznamů zneplatněných certifikátů vygenerovaných v kryptografického modulu, provádí určení pracovníci I.CA prostřednictvím vlastní aktivace kryptografického modulu a aktivační čipové karty podle přesně určeného postupu, který je upraven interní dokumentací. Po aktivaci je systém připraven k podepisování vydávaných certifikátů a seznamů zneplatněných certifikátů a aktivační čipová karta se vyjme. Po aktivaci je zařízení přístupné pouze určeným odpovědným pracovníkům I.CA.

### **6.2.9 Postup při deaktivaci dat pro vytváření elektronických podpisů**

Deaktivaci dat pro vytváření elektronických podpisů I.CA vydávaných certifikátů a seznamů zneplatněných certifikátů po jejich vložení do kryptografického modulu provádí určení pracovníci I.CA prostřednictvím kryptografického modulu a aktivační čipové karty podle přesně určeného postupu, který je upraven interní dokumentací.

O provedení deaktivace dat pro vytváření elektronických podpisů I.CA vydávaných certifikátů a seznamů zneplatněných certifikátů je pořízen písemný záznam, který podepíše určení pracovníci I.CA.

### **6.2.10 Postup při zničení dat pro vytváření elektronických podpisů**

Data pro vytváření elektronických podpisů, sloužící k podepisování vydávaných certifikátů a seznamů zneplatněných certifikátů, jsou uložena v kryptografickém modulu. Ničení těchto dat je realizováno prostředky kryptografického modulu. Zálohy těchto dat uložené v zašifrované podobě na externích médiích jsou rovněž zničeny. Ničení spočívá ve fyzické destrukci těchto nosičů. Veškeré požadavky na proces ničení párových dat I.CA, sloužících k podepisování vydávaných certifikátů a seznamů zneplatněných certifikátů jsou definovány v interní bezpečnostní dokumentaci.

### **6.2.11 Hodnocení kryptografického modulu**

Nástroj elektronického podpisu pro elektronické podepisování vydávaných certifikátů a seznamů zneplatněných certifikátů, byl certifikován na shodu s požadavky standardu FIPS PUB 140-2 úroveň 3.

## **6.3 Další aspekty správy párových dat**

### **6.3.1 Uchovávání dat pro ověřování elektronických podpisů**

Problematika uchovávání dat pro ověřování elektronických podpisů je řešena v souladu s touto CP.

### **6.3.2 Maximální doba platnosti certifikátu podepisující osoby a párových dat**

Maximální doba platnosti každého vydaného certifikátu je uvedena v těle tohoto certifikátu.

## **6.4 Aktivační data**

<b>Certifikační politika vydávání kořenového certifikátu I.CA – komerční certifikáty</b>	<b>Strana 35 (celkem 47)</b>
<b>Copyright © První certifikační autorita, a.s.</b>	

#### **6.4.1 Generování a instalace aktivačních dat**

Aktivační data jsou vytvářena v průběhu procesu instalace, kdy jsou generována párová data pro podepisování vydávaných certifikátů a seznamů zneplatněných certifikátů.

#### **6.4.2 Ochrana aktivačních dat**

Všechna výše uvedená aktivační data jsou pracovníky I.CA chráněna způsobem, uvedeným v interní bezpečnostní dokumentaci.

#### **6.4.3 Ostatní aspekty aktivačních dat**

Výše uvedená aktivační data jsou určena výhradně pro procesy poskytování certifikačních služeb a nesmí být použita k jiným účelům, ani přenášena nebo uchovávána v otevřené podobě.

### **6.5 Počítačová bezpečnost**

#### **6.5.1 Specifické technické požadavky na počítačovou bezpečnost**

Úroveň bezpečnosti použitých komponent pro poskytování certifikačních služeb v oblasti vydávání certifikátů je definována mezinárodními technickými standardy.

Detailní řešení specifických technických požadavků počítačové bezpečnosti je popsáno v interní dokumentaci.

#### **6.5.2 Hodnocení počítačové bezpečnosti**

Hodnocení bezpečnosti je založeno na mezinárodních a národních standardech, zejména:

- CWA 14167-1 - Security Requirements for Trustworthy Systems Managing Certificates for Electronic Signatures - Part 1: System Security Requirements/Bezpečnostní požadavky na důvěryhodné systémy spravující certifikáty pro elektronický podpis – část 1: Požadavky na bezpečnost systémů,
- ETSI TS 102 042 – Electronic Signatures and Infrastructures (ESI); Policy requirements for certification authorities issuing public key certificates,
- ČSN ETSI EN 319 411-3 Elektronické podpisy a infrastruktury (ESI) - Požadavky politiky a bezpečnosti na poskytovatele důvěryhodných služeb vydávající certifikáty - Část 3: Požadavky politiky na certifikační autority vydávající certifikáty veřejného klíče,
- ČSN ISO/IEC 27001 Informační technologie - Bezpečnostní techniky - Systémy řízení bezpečnosti informací – Požadavky,
- ČSN ISO/IEC 27002 Informační technologie - Bezpečnostní techniky - Soubor postupů pro opatření bezpečnosti informací,
- ČSN ISO/IEC 27003 Informační technologie - Bezpečnostní techniky - Směrnice pro implementaci systému řízení bezpečnosti informací,
- ČSN ISO/IEC 27005 Informační technologie - Bezpečnostní techniky – Řízení rizik bezpečnosti informací,
- ČSN ISO/IEC 15408 Informační technologie – Kritéria pro hodnocení bezpečnosti IT,
- RFC 3647 - Internet X.509 Public Key Infrastructure - Certificate Policy and Certification Practices Framework (dále též RFC 3647),
- RFC 2630 – Cryptographic Message Syntax,

<b>Certifikační politika vydávání kořenového certifikátu I.CA – komerční certifikáty</b>	<b>Strana 36 (celkem 47)</b>
<b>Copyright © První certifikační autorita, a.s.</b>	

- ETSI TS 119 312 Electronic Signatures and Infrastructures (ESI); Cryptographic Suites<sup>1</sup>,
- RFC 5280 - Internet X.509 Public Key Infrastructure, Certificate and Certificate Revocation List (CRL) Profile.

## **6.6 Bezpečnost životního cyklu**

### **6.6.1 Řízení vývoje systému**

Při vývoji systému je postupováno v souladu s interní dokumentací.

### **6.6.2 Kontroly řízení bezpečnosti**

Soulad se standardy je ověřován pravidelnými audity systému managementu bezpečnosti informací, prováděnými pracovníky nezávislých auditorských firem a interními kontrolami, prováděnými pracovníky I.CA. Tato problematika je popsána v interní dokumentaci. I.CA si vyhrazuje právo provádění i jiných typů kontrol, resp. auditů.

### **6.6.3 Řízení bezpečnosti životního cyklu**

Řízení bezpečnosti životního cyklu je v I.CA je vytvářeno procesním přístupem typu „Plánování-Zavedení-Kontrola-Využití“ (Plan-Do-Check-Act, PDCA), který se skládá z navazujících procesů:

- vybudování – definování bezpečnostní politiky, plánů, cílů, procesů a postupů s ohledem na řízení rizik a bezpečnost informací tak, aby byly v souladu s celkovou bezpečnostní politikou,
- implementace a provoz - bezpečnostní politiky, plánů, cílů, procesů a postupů,
- monitorování a přehodnocování – posouzení procesu s ohledem na bezpečnostní politiku a předání poznatků vedení společnosti k posouzení,
- využití – na základě rozhodnutí vedení organizace provedení nápravných opatření.

## **6.7 Síťová bezpečnost**

V prostředí I.CA nejsou prostředky provádějící vlastní certifikační služby přímo dostupné z veřejné sítě Internet. Informační systém je mimo jiné chráněn komerčním produktem typu firewall. Veškerá komunikace mezi RA a provozním pracovištěm certifikační autority je vedena šifrovaně. Detailní řešení řízení síťové bezpečnosti je popsáno v interní dokumentaci.

## **6.8 Časová razítka**

Uvedeno v kapitole 5.5.5.

<sup>1</sup> Nahrazující ALGO paper (viz <http://www.mvcr.cz/clanek/e-podpis-povinne-zverejnovane-informace-kryptograficke-algoritmy-a-jejich-parametry-podle-vyhlasaky-c-378-2006-sb.aspx>)

<b>Certifikační politika vydávání kořenového certifikátu I.CA – komerční certifikáty</b>	<b>Strana 37 (celkem 47)</b>
<b>Copyright © První certifikační autorita, a.s.</b>	

## 7 Profily certifikátu, seznamu zneplatněných certifikátů a OCSP

### 7.1 Profil certifikátu

Tabulka 3 – Základní pole

Zápis v ASN.1	Stručný popis
Certificate ::= SEQUENCE {	
tbsCertificate TBSCertificate,	viz Tabulka 4
signatureAlgorithm AlgorithmIdentifier,	identifikátor algoritmu, použitého I.CA pro elektronický podpis kořenového certifikátu I.CA
signature BIT STRING}	elektronický podpis kořenového certifikátu I.CA

Tabulka 4 – Základní položky

Položka	Obsah
Version	verze v3
Serial Number	jedinečné číslo vydaného certifikátu
SignatureAlgorithm	identifikátor kryptografického algoritmu, použitého pro elektronický podpis kořenového certifikátu I.CA ( sha256WithRSAEncryption)
Issuer	vydavatel certifikátu (viz kapitola 3.1.1)
Validity	
• NotBefore	počátek platnosti kořenového certifikátu I.CA
• NotAfter	konec platnosti kořenového certifikátu I.CA
Subject	viz Issuer
SubjectPublicKeyInfo	
• Algorithm	rsaEncryption
• SubjectPublicKey	veřejný klíč kořenového certifikátu I.CA (2048 bit)
Extensions	rozšíření kořenového certifikátu I.CA (viz Tabulka 5)

#### 7.1.1 Čísla verzí

Všechny vydávané certifikáty jsou v souladu s X.509 ve verzi 3.

#### 7.1.2 Rozšiřující položky v certifikátu

Tabulka 5 – Rozšiřující atributy

Položka	Obsah	Kritická
Subject Key Identifier	hash veřejného klíče kořenového certifikátu I.CA	NE
Certificate Policy		NE
• Policy	viz kapitola 7.1.6	
• Explicit Text	viz kapitola 7.1.8	
Basic Constraints	cA:true	ANO
Key Usage (critical)	Certificate Sign, CRL Sign	ANO

#### 7.1.3 Objektové identifikátory (dále OID) algoritmů

V procesu poskytování certifikačních služeb je využívány algoritmy, odkazované příslušnými technickými standardy.

<b>Certifikační politika vydávání kořenového certifikátu I.CA – komerční certifikáty</b>	<b>Strana 38 (celkem 47)</b>
<b>Copyright © První certifikační autorita, a.s.</b>	

#### 7.1.4 Způsoby zápisu jmen a názvů

Uvedeno v kapitole 3.1.1.

#### 7.1.5 Omezení jmen a názvů

Atribut nameConstraints není použit. Pro jméno subjektu (Subject) není žádné omezení s výjimkou omezení vyplývajících z kapitoly 3.1.2.

#### 7.1.6 OID certifikační politiky

OID tohoto dokumentu je uvedené v kapitole 1.2. V kořenovém certifikátu I.CA, vydávaného v souladu s touto CP, je uvedeno speciální označení politiky anyPolicy, jehož OID je 2.5.29.32.0.

#### 7.1.7 Rozšiřující položka „Policy Constraints“

Tyto skutečnosti jsou pro aplikaci tohoto vydání CP irelevantní.

#### 7.1.8 Syntaxe a sémantika rozšiřující položky kvalifikátorů politiky „Policy Qualifiers“

Tyto skutečnosti jsou pro aplikaci tohoto vydání této CP irelevantní.

#### 7.1.9 Způsob zápisu kritické rozšiřující položky „Certificate Policies“

Položka je nekritická.

## 7.2 Profil seznamu zneplatněných certifikátů

Tabulka 6 – Základní pole CRL

Zápis v ASN.1	Stručný popis
Certificate ::= SEQUENCE {	
tbsCertlist TBSCertlist	viz Tabulka 7
signatureAlgorithm AlgorithmIdentifier,	identifikátor a parametry algoritmu, použitého pro elektronický podpis vydávaného kořenového certifikátu I.CA (sha256WithRSAEncryption)
signature BIT STRING}	elektronická podpis vydávaného kořenovém certifikátu I.CA

Tabulka 7 – Základní položky CRL

Položka	Obsah
Version	verze v2
SignatureAlgorithm	algoritmus, použitý I.CA pro elektronický podpis vydávaného CRL (sha256WithRSAEncryption)
Issuer	vydavatel CRL (viz kapitola 3.1.1)
thisUpdate	datum a čas vydání CRL (UTC)
nextUpdate	datum a předpokládaný čas vydání následujícího CRL (UTC)
revokedCertificates	seznam zneplatněných certifikátů

<b>Certifikační politika vydávání kořenového certifikátu I.CA – komerční certifikáty</b>	<b>Strana 39 (celkem 47)</b>
<b>Copyright © První certifikační autorita, a.s.</b>	

<ul style="list-style-type: none"> <li>• userCertificate</li> <li>• revocationDate</li> <li>• crlEntryExtensions.CRLReason</li> </ul>	<p>jedinečné sériové číslo zneplatněného certifikátu</p> <p>datum a čas zneplatnění certifikátu</p> <p>důvod zneplatnění certifikátu</p>
crlExtensions	Rozšíření CRL (viz Tabulka 8)

### 7.2.1 Číslo verze

Seznamy zneplatněných certifikátů jsou vydávány dle X 509 verze 2.

### 7.2.2 Rozšiřující položky seznamu zneplatněných certifikátů a záznamů v seznamu zneplatněných certifikátů

Tabulka 8 – Rozšiřující atributy CRL

<b>Položka</b>	<b>Obsah</b>	<b>Kritická</b>
AuthorityKeyIdentifier.KeyIdentifier	hash veřejného klíče vydavatele certifikátu	NE
CRL Number	Číslo CRL	NE

## 7.3 Profil OCSP

Tyto skutečnosti jsou pro aplikaci vydání této CP irelevantní.

### 7.3.1 Číslo verze

Tyto skutečnosti jsou pro aplikaci vydání této CP irelevantní.

### 7.3.2 Rozšiřující položky OCSP

Tyto skutečnosti jsou pro aplikaci vydání této CP irelevantní.

<b>Certifikační politika vydávání kořenového certifikátu I.CA – komerční certifikáty</b>	<b>Strana 40 (celkem 47)</b>
<b>Copyright © První certifikační autorita, a.s.</b>	

## **8 Hodnocení shody a jiná hodnocení**

### **8.1 Periodicita hodnocení nebo okolnosti pro provedení hodnocení**

Externí kontroly - audit systému řízení bezpečnosti informací je prováděn každé dva roky, audit dle požadavků MRCP jednou ročně. Interní kontroly jsou prováděny na základě rozhodnutí ředitele I.CA.

Společnost První certifikační autorita, a.s. si vyhrazuje právo provádění i jiných forem kontrol.

### **8.2 Identita a kvalifikace hodnotitele**

V případě externích auditů je vždy vyžadována certifikace pro uvedenou činnost.

### **8.3 Vztah hodnotitele k hodnocené entitě**

V případě externích kontrol se jedná o pracovníky nezávislých auditorských firem, v případě interních kontrol se jedná o pracovníky I.CA.

### **8.4 Hodnocené oblasti**

Hodnocené oblasti jsou dány standardy, dle kterých je hodnocení prováděno.

### **8.5 Postup v případě zjištěných nedostatků**

Se zjištěními všech typů prováděných hodnocení je seznámen bezpečnostní manager, který je povinen zajistit odstranění případných nedostatků.

### **8.6 Sdělování výsledků hodnocení**

Sdělování výsledků hodnocení je prováděno formou písemné závěrečné zprávy, která je hodnotícím subjektem předána řediteli, resp. bezpečnostnímu managerovi společnosti.

V nejbližším možném termínu svolá bezpečnostní manager schůzi bezpečnostního výboru, na které budou mimo vedení společnosti přítomni vedoucí jednotlivých oddělení a které s výsledky hodnocení seznámí.



<b>Certifikační politika vydávání kořenového certifikátu I.CA – komerční certifikáty</b>	<b>Strana 41 (celkem 47)</b>
<b>Copyright © První certifikační autorita, a.s.</b>	

## **9 Ostatní obchodní a právní záležitosti**

### **9.1 Poplatky**

#### **9.1.1 Poplatky za vydání nebo obnovení certifikátu**

Tyto skutečnosti jsou pro aplikaci tohoto vydání CP irelevantní.

#### **9.1.2 Poplatky za přístup k certifikátu na seznamu vydaných certifikátů**

Přístup k vydaným veřejným certifikátům elektronickou cestou I.CA nezaplatňuje.

#### **9.1.3 Poplatky za informace o statutu certifikátu a o zneplatnění certifikátu**

Přístup k informacím o zneplatněných certifikátech elektronickou cestou I.CA nezaplatňuje.

#### **9.1.4 Poplatky za další služby**

Předání kořenového certifikátu I.CA je poskytováno zdarma.

#### **9.1.5 Jiná ustanovení týkající se poplatků (vč. refundací)**

Tyto skutečnosti jsou pro aplikaci tohoto vydání CP irelevantní.

### **9.2 Finanční odpovědnost**

#### **9.2.1 Krytí pojištěním**

Společnost První certifikační autorita, a.s. prohlašuje, že má uzavřené pojištění podnikatelských rizik takovým způsobem, aby byly pokryty případné finanční škody.

#### **9.2.2 Další aktiva a záruky**

Společnost První certifikační autorita, a.s. prohlašuje, že má k dispozici dostatečné finanční zdroje a jiné finanční zajištění na poskytování certifikačních služeb s ohledem na riziko vzniku odpovědnosti za škodu.

Podrobné informace o aktivech společnosti První certifikační autorita, a.s. je možno získat z Výroční zprávy I.CA.

#### **9.2.3 Pojištění nebo krytí zárukou pro koncové uživatele**

Tyto skutečnosti jsou pro aplikaci tohoto vydání CP irelevantní.

<b>Certifikační politika vydávání kořenového certifikátu I.CA – komerční certifikáty</b>	<b>Strana 42 (celkem 47)</b>
<b>Copyright © První certifikační autorita, a.s.</b>	

## **9.3 Citlivost obchodních informací**

### **9.3.1 Výčet citlivých informací**

Citlivými a důvěrnými informacemi I.CA jsou veškeré informace, které nejsou zveřejňovány způsobem, uvedeným v kapitole 2.2, zejména:

- data pro vytváření elektronických podpisů, příslušná k datům pro ověřování elektronických podpisů, obsažených v kořenových certifikátech I.CA,
- data pro vytváření elektronických podpisů příslušná k datům pro ověřování elektronických podpisů obsažených v účelových certifikátech I.CA (např. klíče pro komunikaci s RA),
- ostatní kryptograficky podstatné informace sloužící k provozu I.CA a RA,
- vybrané obchodní informace I.CA,
- veškeré interní informace a dokumentace,
- veškeré osobní údaje.

### **9.3.2 Informace mimo rámec citlivých informací**

Za veřejné se považují typy informací, které nepatří do žádné z uvedených skupin v kapitole 9.3.1.

### **9.3.3 Odpovědnost za ochranu citlivých informací**

Každý pracovník, který přijde do styku s informacemi uvedenými v kapitole 9.3.1, je nesmí bez souhlasu ředitele I.CA poskytnout třetí straně.

Zaměstnanci I.CA, případně jiné fyzické osoby, které přicházejí do styku s osobními údaji, jsou povinni zachovávat mlčenlivost o těchto údajích a datech a o bezpečnostních opatřeních, jejichž zveřejnění by ohrozilo zabezpečení těchto údajů a dat. Povinnost mlčenlivosti trvá i po skončení pracovního nebo jiného obdobného poměru nebo po provedení příslušných prací.

## **9.4 Ochrana osobních údajů**

### **9.4.1 Politika ochrany osobních údajů**

Ochrana osobních údajů a dalších neveřejných informací je v I.CA řešena v souladu s požadavky příslušných zákonných norem.

### **9.4.2 Osobní údaje**

Osobními informacemi jsou veškeré osobní údaje klientů, uživatelů či pracovníků, podléhající ochraně ve smyslu příslušné zákonné normy.

### **9.4.3 Údaje, které nejsou považovány za důvěrné**

Informace, které nejsou považovány za důvěrné jsou takové údaje, které nepodléhají ochraně ve smyslu příslušné zákonné normy.

### **9.4.4 Odpovědnost za ochranu osobních údajů**

Za ochranu osobních údajů a dalších neveřejných informací je odpovědná I.CA.

<b>Certifikační politika vydávání kořenového certifikátu I.CA – komerční certifikáty</b>	<b>Strana 43 (celkem 47)</b>
<b>Copyright © První certifikační autorita, a.s.</b>	

#### **9.4.5 Oznámení o používání důvěrných informací a souhlas s používáním citlivých informací**

Problematiky oznámování o používání důvěrných informací a souhlasu s používáním citlivých informací je v I.CA řešena v souladu s požadavky příslušných zákonných norem.

#### **9.4.6 Poskytování citlivých informací pro soudní či správní účely**

Poskytování citlivých informací pro soudní, resp. správní účely je v I.CA řešena v souladu s požadavky příslušných zákonných norem.

#### **9.4.7 Jiné okolnosti zpřístupňování osobních údajů**

V případě zpřístupňování osobních údajů postupuje I.CA řešeno striktně dle požadavků příslušných zákonných norem.

Osoby, uvedené v kapitole 9.3.3, může zbavit mlčenlivosti ten, v jehož zájmu tuto povinnost mají, nebo soud.

### **9.5 Práva duševního vlastnictví**

Tato CP, veškeré související dokumenty, obsah webových stránek, certifikáty CA, klíče CA a procedury, zajišťující provoz systému, poskytujícího certifikační služby v oblasti certifikátů, jsou chráněny autorskými právy společnosti První certifikační autorita, a.s. a představují její významné know-how.

### **9.6 Zastupování a záruky**

#### **9.6.1 Zastupování a záruky CA**

I.CA zaručuje, že:

- použije soukromé klíče, příslušné kořenovým certifikátům I.CA pouze k podepisování vydávaných certifikátů a seznamu zneplatněných certifikátů,
- vydávané certifikáty a seznamy zneplatněných certifikátů splňují náležitosti, uvedené v této CP požadované mezinárodními standardy.

#### **9.6.2 Zastupování a záruky RA**

Tyto skutečnosti jsou pro aplikaci tohoto vydání CP irelevantní.

#### **9.6.3 Zastupování a záruky držitele certifikátu, podepisující osoby**

Držitel certifikátu postupuje v souladu s touto CP a ručí za informace, uvedené ve vydaném certifikátu.

#### **9.6.4 Zastupování a záruky spoléhajících se stran**

Spoléhající se strany postupují v souladu s platnou legislativou.

<b>Certifikační politika vydávání kořenového certifikátu I.CA – komerční certifikáty</b>	<b>Strana 44 (celkem 47)</b>
<b>Copyright © První certifikační autorita, a.s.</b>	

#### **9.6.5 Zastupování a záruky ostatních zúčastněných subjektů**

Služba není poskytována.

#### **9.7 Zřeknutí se záruk**

Společnost První certifikační autorita, a.s. se nemůže zříci záruk, požadovaných relevantní legislativou.

#### **9.8 Omezení odpovědnosti**

Společnost První certifikační autorita, a.s., neodpovídá za škody způsobené spoléhajícím se stranám v případech, kdy nesplnily povinnosti, požadované certifikační politikou, dle které byl certifikát vydán.

#### **9.9 Odpovědnost za škodu, náhrada škody**

Není relevantní pro tento dokument, je řešeno v politikách pro vydávání certifikátů koncovým klientům.

#### **9.10 Doba platnosti, ukončení platnosti**

##### **9.10.1 Doba platnosti**

Tato CP platí minimálně po dobu platnosti posledního podle ní vydaného certifikátu.

##### **9.10.2 Ukončení platnosti**

Jedinou osobou, která je oprávněna schvalovat ukončení platnosti této CP, je ředitel společnosti První certifikační autorita, a.s.

##### **9.10.3 Důsledky ukončení a přetrvání závazků**

Uvedeno v kapitole 9.10.1.

#### **9.11 Komunikace mezi zúčastněnými subjekty**

Všechny zúčastněné subjekty jsou organizačními částmi I.CA a komunikace mezi nimi se řídí interními pravidly I.CA.

#### **9.12 Změny**

##### **9.12.1 Postup při změnách**

Postup je realizován řízeným procesem, uvedeném v interním dokumentu.

<b>Certifikační politika vydávání kořenového certifikátu I.CA – komerční certifikáty</b>	<b>Strana 45 (celkem 47)</b>
<b>Copyright © První certifikační autorita, a.s.</b>	

### **9.12.2 Postup při oznamování změn**

Vydání nové verze certifikační politiky je vždy oznámeno formou zveřejňování informací.

### **9.12.3 Okolnosti, při kterých musí být změněno OID**

V případě změn, majících vliv na obsah vydávaného certifikátu, je vždy změněn i její OID.

## **9.13 Řešení sporů**

Tyto skutečnosti jsou pro aplikaci tohoto vydání CP irelevantní.

## **9.14 Rozhodné právo**

Obchodní činnost společnosti První certifikační autorita, a.s. se řídí právním řádem České republiky.

## **9.15 Shoda s právními předpisy**

Systém poskytování certifikačních služeb je provozován ve shodě s platné legislativy.

## **9.16 Další ustanovení**

### **9.16.1 Rámcová dohoda**

Tyto skutečnosti jsou pro aplikaci tohoto vydání CP irelevantní.

### **9.16.2 Postoupení práv**

Tyto skutečnosti jsou pro aplikaci tohoto vydání CP irelevantní.

### **9.16.3 Oddělitelnost ustanovení**

Tyto skutečnosti jsou pro aplikaci tohoto vydání CP irelevantní.

### **9.16.4 Zřeknutí se práv**

Tyto skutečnosti jsou pro aplikaci tohoto vydání CP irelevantní.

### **9.16.5 Vyšší moc**

Společnost První certifikační autorita, a.s., neodpovídá za porušení svých povinností vyplývajících ze zásahu vyšší moci, např. přírodních nebo lidskou činností způsobených katastrof velkého rozsahu, stávek či občanských nepokojů vždy spojených s vyhlášením nouzového stavu, nebo vyhlášení stavu ohrožení státu nebo válečného stavu.

<i>Certifikační politika vydávání kořenového certifikátu I.CA – komerční certifikáty</i>	<i>Strana 46 (celkem 47)</i>
<i>Copyright © První certifikační autorita, a.s.</i>	

### **9.17 Další opatření**

Tyto skutečnosti jsou pro aplikaci tohoto vydání CP irelevantní.

<i>Certifikační politika vydávání kořenového certifikátu I.CA – komerční certifikáty</i>	<i>Strana 47 (celkem 47)</i>
<i>Copyright © První certifikační autorita, a.s.</i>	

## **10 Závěrečná ustanovení**

Tato CP vydaná společností První certifikační autorita, a.s., nabývá platnosti a účinnosti dnem 22.09.2015.