

**První certifikační autorita, a.s.**



# **CERTIFIKAČNÍ PROVÁDĚCÍ SMĚRNICE VYDÁVÁNÍ KOMERČNÍCH CERTIFIKÁTŮ**

Verze 2.2

Certifikační prováděcí směrnice vydávání komerčních certifikátů 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.*

<b>Certifikační prováděcí směrnice vydávání komerčních certifikátů</b>	<b>Strana 2 (celkem 61)</b>
<b>Copyright © První certifikační autorita, a.s.</b>	

Tabulka 1 - Identifikace

<b>Název</b>	Certifikační prováděcí směrnice vydávání komerčních certifikátů
<b>Společnost</b>	První certifikační autorita, a.s.
<b>Schválil</b>	Ředitel společnosti První certifikační autorita, a.s.

Tabulka 2 – Vývoj dokumentu

1.04	18.12.2001	První verze dokumentu
2.0	01.08.2007	Vytvoření struktury dle RFC 3647, akceptace obchodního produktu
2.1	23.02.2008	Úprava dokumentu s ohledem na obchodní produkt
2.2	22.09.2015	Aktualizace a revize dokumentu

# Obsah

<b>1</b>	<b>ÚVOD .....</b>	<b>8</b>
1.1	PŘEHLED .....	8
1.2	NÁZEV A JEDNOZNAČNÉ URČENÍ DOKUMENTU .....	8
1.3	PARTICIPUJÍCÍ SUBJEKTY .....	8
1.3.1	<i>Certifikační autority (dále "CA")</i> .....	8
1.3.2	<i>Registrační autority (dále "RA")</i> .....	9
1.3.3	<i>Držitelé certifikátů, podepisující, šifrující nebo autentizující se osoby, kteří požádali o vydání certifikátu a kterým byl certifikát vydán</i> .....	9
1.3.4	<i>Spoléhající se strany</i> .....	9
1.3.5	<i>Jiné participující subjekty</i> .....	10
1.4	POUŽITÍ CERTIFIKÁTU .....	10
1.4.1	<i>Přípustné použití certifikátu</i> .....	10
1.4.2	<i>Omezení použití certifikátu</i> .....	10
1.5	SPRÁVA POLITIKY .....	10
1.5.1	<i>Organizace spravující certifikační politiku nebo certifikační prováděcí směrnici</i> .....	10
1.5.2	<i>Kontaktní osoba organizace spravující certifikační politiku nebo certifikační prováděcí směrnici</i> .....	10
1.5.3	<i>Subjekt odpovědný za rozhodování o souladu postupů poskytovatele s postupy jiných poskytovatelů certifikačních služeb</i> .....	10
1.5.4	<i>Postupy při schvalování souladu podle bodu 1.5.3</i> .....	10
1.6	PŘEHLED POUŽITÝCH POJMŮ A ZKRATEK .....	11
<b>2</b>	<b>ODPOVĚDNOSTI ZA ZVEŘEJŇOVÁNÍ A ÚLOŽIŠTĚ INFORMACÍ A DOKUMENTACE.....</b>	<b>13</b>
2.1	ÚLOŽIŠTĚ INFORMACÍ A DOKUMENTACE .....	13
2.2	ZVEŘEJŇOVÁNÍ INFORMACÍ A DOKUMENTACE.....	13
2.3	PERIODICITA ZVEŘEJŇOVÁNÍ INFORMACÍ .....	14
2.4	ŘÍZENÍ PŘÍSTUPU K JEDNOTLIVÝM TYPŮM ÚLOŽIŠŤ .....	14
<b>3</b>	<b>IDENTIFIKACE A AUTENTIZACE .....</b>	<b>15</b>
3.1	POJMENOVÁVÁNÍ.....	15
3.1.1	<i>Typy jmen</i> .....	15
3.1.2	<i>Požadavek na významovost jmen</i> .....	16
3.1.2.1	CountryName (stát) .....	16
3.1.2.2	CommonName (Obecné jméno).....	16
3.1.2.3	StateorProvinceName (kraj).....	17
3.1.2.4	LocalityName (místo).....	17
3.1.2.5	OrganizationName (organizace) .....	17
3.1.2.6	OrganizationalUnitName (organizační jednotka) .....	18
3.1.2.7	Pkcs9Email Address (elektronická poštovní adresa) .....	18
3.1.2.8	Initials (iniciály) .....	18
3.1.2.9	Title (titul) .....	18
3.1.2.10	SerialNumber (sériové číslo subjektu).....	18
3.1.2.11	GenerationQualifier (generační rozlišení) .....	18
3.1.2.12	Subject Alternative Name (alternativní jméno subjektu).....	18
3.1.3	<i>Anonymita a používání pseudonymu</i> .....	19
3.1.4	<i>Pravidla pro interpretaci různých forem jmen</i> .....	19
3.1.5	<i>Jedinečnost jmen</i> .....	19
3.1.6	<i>Obchodní značky</i> .....	19
3.2	POČÁTEČNÍ OVĚŘENÍ IDENTITY .....	19
3.2.1	<i>Ověření souladu dat, tj. postup při ověřování, zda má osoba soukromý klíč odpovídající veřejnému klíči</i> <i>19</i>	19
3.2.2	<i>Ověřování identity právnické osoby nebo organizační složky státu</i> .....	20
3.2.3	<i>Ověřování identity fyzické osoby</i> .....	20
3.2.3.1	Fyzická osoba.....	20
3.2.3.2	Fyzická osoba zaměstnanec .....	22
3.2.3.3	Právnické osoby a organizační složky státu (např. elektronická podatelna - orgán veřejné moci) .....	23
3.2.4	<i>Neověřené informace vztahující se k držiteli certifikátu nebo podepisující osobě</i> .....	23
3.2.5	<i>Ověřování specifických práv</i> .....	23
3.2.6	<i>Kritéria pro interoperabilitu</i> .....	23

<b>Certifikační prováděcí směrnice vydávání komerčních certifikátů</b>	<b>Strana 4 (celkem 61)</b>
<b>Copyright © První certifikační autorita, a.s.</b>	

3.3	IDENTIFIKACE A AUTENTIZACE PŘI ZPRACOVÁNÍ POŽADAVKŮ NA VÝMĚNU VEŘEJNÉHO KLÍČE V CERTIFIKÁTU	23
3.3.1	Identifikace a autentizace při rutinní výměně párových dat.....	23
3.3.2	Identifikace a autentizace při výměně párových dat po zneplatnění certifikátu.....	23
3.4	IDENTIFIKACE A AUTENTIZACE PŘI ZPRACOVÁNÍ POŽADAVKŮ NA ZNEPLATNĚNÍ CERTIFIKÁTU .....	24
<b>4</b>	<b>POŽADAVKY NA ŽIVOTNÍ CYKLUS CERTIFIKÁTU .....</b>	<b>25</b>
4.1	ŽÁDOST O VYDÁNÍ CERTIFIKÁTU .....	25
4.1.1	Subjekty oprávněné podat žádost o vydání certifikátu.....	25
4.1.2	Registrační proces a odpovědnosti poskytovatele a žadatele.....	25
4.2	ZPRACOVÁNÍ ŽÁDOSTI O CERTIFIKÁT .....	25
4.2.1	Identifikace a autentizace.....	25
4.2.2	Přijetí nebo odmítnutí žádosti o certifikát .....	26
4.2.3	Doba zpracování žádosti o certifikát.....	26
4.3	VYDÁNÍ CERTIFIKÁTU.....	26
4.3.1	Úkony CA v průběhu vydání certifikátu .....	26
4.3.2	Oznámení o vydání certifikátu držiteli certifikátu, podepisující osobě .....	26
4.4	PŘEVZETÍ VYDANÉHO CERTIFIKÁTU .....	26
4.4.1	Úkony spojené s převzetím certifikátu .....	26
4.4.2	Zveřejňování vydaných certifikátů poskytovatelem .....	27
4.4.3	Oznámení o vydání certifikátu jiným subjektům .....	27
4.5	POUŽITÍ PÁROVÝCH DAT A CERTIFIKÁTU .....	27
4.5.1	Použití soukromého klíče a certifikátu držitelem, podepisující, resp. šifrující osobou .....	27
4.5.2	Použití veřejného klíče a certifikátu spoléhající se stranou .....	28
4.6	OBNOVENÍ CERTIFIKÁTU .....	28
4.7	VÝMĚNA VEŘEJNÉHO KLÍČE V CERTIFIKÁTU .....	28
4.7.1	Podmínky pro výměnu veřejného klíče v certifikátu .....	28
4.7.2	Subjekty oprávněné požadovat výměnu veřejného klíče v certifikátu .....	29
4.7.3	Zpracování požadavku na výměnu veřejného klíče .....	29
4.7.4	Oznámení o vydání certifikátu s vyměněným veřejným klíčem .....	29
4.7.5	Úkony spojené s převzetím certifikátu s vyměněným veřejným klíčem .....	30
4.7.6	Zveřejnění vydaných certifikátů s vyměněným veřejným klíčem.....	30
4.7.7	Oznámení o vydání certifikátu s vyměněným veřejným klíčem jiným subjektům .....	30
4.8	ZMĚNA ÚDAJŮ V CERTIFIKÁTU .....	30
4.9	ZNEPLATNĚNÍ A POZASTAVENÍ PLATNOSTI CERTIFIKÁTU .....	30
4.9.1	Podmínky pro zneplatnění certifikátu.....	30
4.9.2	Subjekty oprávněné žádat o zneplatnění certifikátu.....	30
4.9.3	Požadavek na zneplatnění certifikátu.....	31
4.9.4	Doba odkladu požadavku na zneplatnění certifikátu.....	32
4.9.5	Maximální doba, za kterou musí poskytovatel realizovat požadavek na zneplatnění certifikátu .....	32
4.9.6	Povinnosti spoléhajících se stran při ověřování, zda nebyl certifikát zneplatněn.....	32
4.9.7	Periodicita vydávání seznamu zneplatněných certifikátů.....	32
4.9.8	Maximální zpoždění při vydávání seznamu zneplatněných certifikátů .....	32
4.9.9	Možnost ověřování statutu certifikátu on-line („dále OCSP“ ).....	32
4.9.10	Požadavky při ověřování statutu certifikátu na on-line .....	32
4.9.11	Jiné způsoby oznamování zneplatnění certifikátu.....	32
4.9.12	Případné odlišnosti postupu zneplatnění v případě kompromitace soukromého klíče .....	32
4.9.13	Podmínky pro pozastavení platnosti certifikátu.....	33
4.9.14	Subjekty oprávněné požadovat pozastavení platnosti certifikátu.....	33
4.9.15	Zpracování požadavku na pozastavení platnosti certifikátu .....	33
4.9.16	Omezení doby pozastavení platnosti certifikátu.....	33
4.10	SLUŽBY SOUVISEJÍCÍ S OVĚŘOVÁNÍM STATUTU CERTIFIKÁTU .....	33
4.10.1	Funkční charakteristiky.....	33
4.10.2	Dostupnost služeb.....	33
4.10.3	Další charakteristiky služeb statutu certifikátu .....	33
4.11	UKONČENÍ POSKYTOVÁNÍ SLUŽEB PRO DRŽITELE CERTIFIKÁTU, PODEPISUJÍCÍ OSOBU .....	33
4.12	ÚSCHOVA SOUKROMÉHO KLÍČE U DŮVĚRYHODNÉ TŘETÍ STRANY A JEJICH OBNOVA.....	34
<b>5</b>	<b>MANAGEMENT, PROVOZNÍ A FYZICKÁ BEZPEČNOST .....</b>	<b>35</b>

5.1	FYZICKÁ BEZPEČNOST .....	35
5.1.1	Umístění a konstrukce .....	35
5.1.2	Fyzický přístup.....	35
5.1.3	Elektrina a klimatizace.....	35
5.1.4	Vliv vody.....	35
5.1.5	Protipožární opatření a ochrana .....	36
5.1.6	Ukládání médií .....	36
5.1.7	Nakládání s odpady .....	36
5.1.8	Zálohy mimo budovu.....	36
5.2	PROCESNÍ BEZPEČNOST .....	36
5.2.1	Důvěryhodné role.....	36
5.2.2	Počet osob požadovaných na zajištění jednotlivých činností.....	36
5.2.3	Identifikace a autentizace pro každou roli .....	37
5.2.4	Role vyžadující rozdělení povinností .....	37
5.3	PERSONÁLNÍ BEZPEČNOST.....	37
5.3.1	Požadavky na kvalifikaci, zkušenosti a bezúhonnost.....	37
5.3.2	Posouzení spolehlivosti osob .....	37
5.3.3	Požadavky na přípravu pro výkon role, vstupní školení.....	38
5.3.4	Požadavky a periodičita školení .....	38
5.3.5	Periodičita a posloupnost rotace pracovníků mezi různými rolemi.....	38
5.3.6	Postihy za neoprávněné činnosti zaměstnanců .....	38
5.3.7	Požadavky na nezávislé zhotovitele (dodavatele).....	38
5.3.8	Dokumentace poskytovaná zaměstnancům.....	38
5.4	AUDITNÍ ZÁZNAMY (LOGY) .....	39
5.4.1	Typy zaznamenávaných událostí.....	39
5.4.2	Periodičita zpracování záznamů.....	39
5.4.3	Doba uchovávání auditních záznamů.....	39
5.4.4	Ochrana auditních záznamů .....	39
5.4.5	Postupy pro zálohování auditních záznamů.....	39
5.4.6	Systém shromažďování auditních záznamů (interní nebo externí).....	39
5.4.7	Postup při oznamování události subjektu, který ji způsobil.....	40
5.4.8	Hodnocení zranitelnosti .....	40
5.5	UCHOVÁVÁNÍ INFORMACÍ A DOKUMENTACE .....	40
5.5.1	Typy informací a dokumentace, které se uchovávají.....	40
5.5.2	Doba uchovávání uchovávaných informací a dokumentace.....	41
5.5.3	Ochrana úložiště uchovávaných informací a dokumentace.....	41
5.5.4	Postupy při zálohování uchovávaných informací a dokumentace.....	41
5.5.5	Požadavky na používání časových razítek při uchovávání informací a dokumentace.....	41
5.5.6	Systém shromažďování uchovávaných informací a dokumentace (interní, externí).....	41
5.5.7	Postupy pro získání a ověření uchovávaných informací a dokumentace .....	41
5.6	VÝMĚNA VEŘEJNÉHO KLÍČE V CERTIFIKÁTU POSKYTOVATELE.....	42
5.7	OBNOVA PO HAVÁRII NEBO KOMPROMITACI .....	42
5.7.1	Postup v případě incidentu a kompromitace.....	42
5.7.2	Poškození výpočetních prostředků, software nebo dat .....	42
5.7.3	Postup při kompromitaci soukromého klíče poskytovatele .....	42
5.7.4	Schopnosti obnovit činnost po havárii.....	43
5.8	UKONČENÍ ČINNOSTI CA NEBO RA .....	43
<b>6</b>	<b>TECHNICKÁ BEZPEČNOST .....</b>	<b>44</b>
6.1	GENEROVÁNÍ A INSTALACE PÁROVÝCH DAT .....	44
6.1.1	Generování párových dat.....	44
6.1.2	Předání soukromého klíče žadateli.....	44
6.1.3	Předání veřejného klíče poskytovateli certifikačních služeb .....	45
6.1.4	Poskytování veřejného klíče CA spoléhajícím se stranám .....	45
6.1.5	Délky párových dat.....	45
6.1.6	Generování parametrů veřejného klíče a kontrola jejich kvality.....	45
6.1.7	Omezení pro použití veřejného klíče.....	45
6.2	OCHRANA SOUKROMÉHO KLÍČE A BEZPEČNOST KRYPTOGRAFICKÝCH MODULŮ .....	46

<b>Certifikační prováděcí směrnice vydávání komerčních certifikátů</b>	<b>Strana 6 (celkem 61)</b>
<b>Copyright © První certifikační autorita, a.s.</b>	

6.3	POČÍTAČOVÁ BEZPEČNOST .....	46
6.3.1	<i>Specifické technické požadavky na počítačovou bezpečnost</i> .....	46
6.3.2	<i>Hodnocení počítačové bezpečnosti</i> .....	47
6.4	BEZPEČNOST ŽIVOTNÍHO CYKLU .....	47
6.4.1	<i>Řízení vývoje systému</i> .....	47
6.4.2	<i>Kontroly řízení bezpečnosti</i> .....	47
6.4.3	<i>Řízení bezpečnosti životního cyklu</i> .....	47
6.5	SÍŤOVÁ BEZPEČNOST .....	48
6.6	ČASOVÁ RAZÍTKA .....	48
<b>7</b>	<b>PROFILY CERTIFIKÁTU, SEZNAMU ZNEPLATNĚNÝCH CERTIFIKÁTŮ A OCSP .....</b>	<b>49</b>
7.1	PROFIL CERTIFIKÁTU .....	49
7.1.1	<i>Číslo verze</i> .....	49
7.1.2	<i>Rozšiřující položky v certifikátu</i> .....	49
7.1.3	<i>Způsoby zápisu jmen a názvů</i> .....	50
7.1.4	<i>Omezení jmen a názvů</i> .....	50
7.2	PROFIL SEZNAMU ZNEPLATNĚNÝCH CERTIFIKÁTŮ .....	51
7.2.1	<i>Číslo verze</i> .....	51
7.2.2	<i>Rozšiřující položky seznamu zneplatněných certifikátů a záznamů v seznamu zneplatněných certifikátů</i> <i>51</i>	
7.3	PROFIL OCSP .....	51
<b>8</b>	<b>HODNOCENÍ SHODY A JINÁ HODNOCENÍ .....</b>	<b>52</b>
8.1	PERIODICITA HODNOCENÍ NEBO OKOLNOSTI PRO PROVEDENÍ HODNOCENÍ .....	52
8.2	IDENTITA A KVALIFIKACE HODNOTITELE .....	52
8.3	VZTAH HODNOTITELE K HODNOCENÉMU SUBJEKTU .....	52
8.4	HODNOCENÉ OBLASTI .....	52
8.5	POSTUP V PŘÍPADĚ ZJIŠTĚNÝCH NEDOSTATKŮ .....	52
8.6	SDĚLOVÁNÍ VÝSLEDKŮ HODNOCENÍ .....	52
<b>9</b>	<b>OSTATNÍ OBCHODNÍ A PRÁVNÍ ZÁLEŽITOSTI .....</b>	<b>54</b>
9.1	POPLATKY .....	54
9.1.1	<i>Poplatky za vydání nebo obnovení certifikátu</i> .....	54
9.1.2	<i>Poplatky za přístup k certifikátu na seznamu vydaných certifikátů</i> .....	54
9.1.3	<i>Poplatky za informace o statutu certifikátu a o zneplatnění certifikátu</i> .....	54
9.1.4	<i>Poplatky za další služby</i> .....	54
9.1.5	<i>Jiná ustanovení týkající se poplatků (vč. refundací)</i> .....	54
9.2	FINANČNÍ ODPOVĚDNOST .....	54
9.2.1	<i>Krytí pojištěním</i> .....	55
9.2.2	<i>Další aktiva a záruky</i> .....	55
9.2.3	<i>Pojištění nebo krytí zárukou pro koncové uživatele</i> .....	55
9.3	CITLIVOST OBCHODNÍCH INFORMACÍ .....	55
9.3.1	<i>Výčet citlivých informací</i> .....	55
9.3.2	<i>Informace mimo rámec citlivých informací</i> .....	55
9.3.3	<i>Odpovědnost za ochranu citlivých informací</i> .....	56
9.3.4	<i>Zpřístupnění informací</i> .....	56
9.4	OCHRANA OSOBNÍCH ÚDAJŮ .....	56
9.5	PRÁVA DUŠEVNÍHO VLASTNICTVÍ .....	56
9.6	ZASTUPOVÁNÍ A ZÁRUKY .....	56
9.6.1	<i>Zastupování a záruky CA</i> .....	56
9.6.2	<i>Zastupování a záruky RA</i> .....	57
9.6.3	<i>Zastupování a záruky držitele certifikátu a podepisující osoby</i> .....	57
9.6.4	<i>Zastupování a záruky spoléhajících se stran</i> .....	57
9.6.5	<i>Zastupování a záruky ostatních zúčastněných subjektů</i> .....	57
9.7	ZŘEKNUTÍ SE ZÁRUK .....	58
9.8	OMEZENÍ ODPOVĚDNOSTI .....	58
9.9	ODPOVĚDNOST ZA ŠKODU, NÁHRADA ŠKODY .....	58
9.10	DOBA PLATNOSTI, UKONČENÍ PLATNOSTI .....	58

<b>Certifikační prováděcí směrnice vydávání komerčních certifikátů</b>	<b>Strana 7 (celkem 61)</b>
<b>Copyright © První certifikační autorita, a.s.</b>	

9.10.1	<i>Doba platnosti</i> .....	58
9.10.2	<i>Ukončení platnosti</i> .....	58
9.10.3	<i>Důsledky ukončení a přetrvání závazků</i> .....	58
9.11	KOMUNIKACE MEZI ZÚČASTNĚNÝMI SUBJEKTY .....	59
9.12	ZMĚNY .....	59
9.12.1	<i>Postup při změnách</i> .....	59
9.12.2	<i>Postup při oznamování změn</i> .....	59
9.12.3	<i>Okolnosti, při kterých musí být změněno OID</i> .....	59
9.13	ŘEŠENÍ SPORŮ .....	59
9.14	ROZHODNÉ PRÁVO.....	59
9.15	SHODA S PRÁVNÍMI PŘEDPISY .....	59
9.16	DALŠÍ USTANOVENÍ .....	60
<b>10</b>	<b>ZÁVĚREČNÁ USTANOVENÍ.....</b>	<b>61</b>

<b>Certifikační prováděcí směrnice vydávání komerčních certifikátů</b>	<b>Strana 8 (celkem 61)</b>
<b>Copyright © První certifikační autorita, a.s.</b>	

## 1 Úvod

Tento dokument, **Certifikační prováděcí směrnice vydávání komerčních certifikátů** (dále též CPS), vypracovaný společností První certifikační autorita, a. s. (dále též I.CA) se zabývá skutečnostmi, které se vztahují na I.CA, podepisující osoby, držitele, spoléhající se strany, jiné účastníky PKI a smluvní partnery a které souvisejí s vydáváním certifikátů mimo působnost ZoEP, jejich další správou, použitím, akceptací, ukončením platnosti, zneplatněním a všemi aspekty souvisejícími s nakládáním s párovými daty.

### 1.1 Přehled

Tento dokument odpovídá požadavkům stanoveným v RFC 3647, s přihlédnutím k doporučením orgánů EU a k legislativě ČR v daném oboru (jednotlivé kapitoly jsou proto v této CPS zachovány i v případě, že jsou ve vztahu k ní irelevantní).

CPS vychází zejména z následujících legislativních předpisů, norem, standardů a doporučení:

- RFC 3647 - Internet X.509 Public Key Infrastructure - Certificate Policy and Certification Practices Framework,
- RFC 3280 - Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile.

Pro oblast certifikátů, vydávaných mimo působnost ZoEP je ustanovena jednoúrovňová hierarchie certifikačních autorit. Kořenem této hierarchie je certifikační autorita společnosti První certifikační autorita, a.s, vydávající „root“ certifikát, tzv. self-signed kořenový certifikát, který veřejný klíč, odpovídající soukromému klíči, kterým I.CA podepisuje vydávané certifikáty a seznamy zneplatněných certifikátů. Vydávání a správa tohoto certifikátu je v I.CA řízena speciálními dokumenty.

Není-li uvedeno jinak, je dále v tomto dokumentu pod pojmy:

- **certifikát** míněn certifikát, vydávaný podepisující, šifrující nebo autentizující se osobě,
- **certifikát CA** míněn certifikát I.CA – obsahuje veřejný klíč, odpovídající soukromému klíči, kterým I.CA elektronicky podepisuje vydávané certifikáty a seznamy zneplatněných certifikátů.

### 1.2 Název a jednoznačné určení dokumentu

Název tohoto dokumentu: Certifikační prováděcí směrnice vydávání komerčních certifikátů verze 2.2

OID dokumentu: není přiřazeno

Tato CPS se vztahuje k následující CP:

OID	CP
1.3.6.1.4.1. 23624.1.1.1.3	Certifikační politika vydávání komerčních certifikátů

### 1.3 Participující subjekty

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

I.CA nezřizuje ani nepodporuje podřízené certifikační autority, poskytující certifikační služby, související s vydáváním certifikátů I.CA.



<b>Certifikační prováděcí směrnice vydávání komerčních certifikátů</b>	<b>Strana 9 (celkem 61)</b>
<b>Copyright © První certifikační autorita, a.s.</b>	

### 1.3.2 Registrační autority (dále "RA")

Poskytování služeb I.CA se realizuje prostřednictvím registračních autorit. RA jsou buď vlastní nebo smluvních partnerů. I.CA podporuje níže uvedené typy registračních autorit. Registrační autority jsou povinny řídit se dokumenty, které vydává I.CA, a které upravují jejich činnost (zejména relevantní certifikační politiky, směrnice pro pracovníky RA atd.).

#### Vlastní stacionární registrační autorita (VSRA):

- je základní decentralizovanou složkou výkonného aparátu I.CA,
- přijímá žádosti o služby dle této CPS, zejména přijímá žádosti o certifikáty, zprostředkovává předání certifikátů a seznamů zneplatněných certifikátů, poskytuje potřebné informace, vyřizuje reklamace atd.,
- je oprávněna z naléhavých provozních nebo technických důvodů pozastavit zcela nebo zčásti výkon své činnosti - toto opatření je povinna neprodleně hlásit řediteli I.CA, který je potvrdí, zruší nebo změní,
- je zmocněna jménem I.CA uzavírat smlouvy o poskytování certifikační služby,
- zajišťuje zpoplatňování služeb I.CA, pokud není stanoveno smlouvou jinak.

#### Vlastní mobilní registrační autorita (VMRA):

- je zvláštní decentralizovanou mobilní složkou výkonného aparátu I.CA,
- přijímá žádosti o služby dle této CPS, zejména přijímá žádosti o certifikáty, zprostředkovává předání certifikátů a seznamů zneplatněných certifikátů, poskytuje potřebné informace, vyřizuje reklamace atd.,
- je oprávněna z naléhavých provozních nebo technických důvodů pozastavit zcela nebo zčásti výkon své činnosti - toto opatření je povinna neprodleně hlásit řediteli I.CA, který je potvrdí, zruší nebo změní,
- je zmocněna jménem I.CA uzavírat smlouvy o poskytování certifikačních služeb,
- zajišťuje zpoplatňování služeb I.CA, pokud není stanoveno smlouvou jinak.

#### Smluvní registrační autorita (SRA):

- plní jménem I.CA obdobné funkce jako vlastní RA na základě písemné smlouvy mezi I.CA a provozovatelem SRA.

### 1.3.3 Držitelé certifikátů, podepisující, šifrující nebo autentizující se osoby, kteří požádali o vydání certifikátu a kterým byl certifikát vydán

Společnost První certifikační autorita, a.s. vydává certifikáty fyzickým osobám a právnickým osobám. Tyto certifikáty, vydávány v souladu s dále uvedenými pravidly, jsou následujícího typu:

- **osobní certifikáty** – certifikáty, určené jako osobní pro použití v oblasti elektronické pošty, vytváření elektronického podpisu, šifrování, autentizace,
- **certifikáty pro servery** - certifikáty pro použití v serverových aplikacích typu autentizace, šifrování.

### 1.3.4 Spoléhající se strany

Spoléhající se stranou mohou být fyzické osoby, právnické osoby a organizační složky státu.

<b>Certifikační prováděcí směrnice vydávání komerčních certifikátů</b>	<b>Strana 10 (celkem 61)</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

Certifikáty, které vydává I.CA klientům, mohou být používány v aplikacích pro následující účely:

- zajištění integrity dat,
- zajištění neodmítnutelnosti odpovědnosti,
- zajištění důvěrnosti dat,
- ustanovení sdíleného tajemství (klíče) v rámci protokolu pro bezpečnou výměnu dat,
- přímé šifrování a dešifrování dat,
- přímé podepisování dat.

### 1.4.2 Omezení použití certifikátu

Certifikáty mohou být používány způsobem uvedeným v kapitole 1.4.1 a nesmí být využívány v rozporu s vydávaným účelem a touto CPS.

## 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

Ředitel společnosti První certifikační autorita, a.s. určuje kontaktní osobu, jejíž e-mail, telefonní číslo a fax jsou uvedeny na internetové informační adrese (viz kapitola 2.2).

### 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 I.CA s postupy jiných poskytovatelů certifikačních služeb, je ředitel společnosti První certifikační autorita, a.s. Dále platí ustanovení kapitoly 3.2.6.

### 1.5.4 Postupy při schvalování souladu podle bodu 1.5.3

V případě, že je potřebné s ohledem na kapitolu 1.5.3 provést změny v této CPS a jí odpovídající CP, určuje ředitel I.CA osobu, která je oprávněna změny provádět. Proces změny je popsán v interní dokumentaci „**Změnové řízení**“.

## 1.6 Přehled použitých pojmů a zkratk

Dále uvedený přehled pojmů a zkratk je platný pro tento dokument. V případě pojmu může být na pravé straně v závorkách uveden zdroj, v němž se nachází původní pojem včetně definice. Použité zkratky mají alternativní charakter, tzn. v textu může být použit jak plný text, tak i jeho zkratka, přičemž obojí má totožnou obsahovou hodnotu.

Tabulka 3 – Pojmy a zkratky

Pojem	Vysvětlení
Autentizace	vytvoření podpisu k náhodně vygenerovaným datům, přičemž tento úkon slouží pouze k určení identity dané osoby a nemá žádné následky vzhledem k obsahu náhodně vygenerovaných dat
CA	centrální pracoviště Certifikační autority I.CA
Certifikát	datová zpráva, která je vydána poskytovatelem certifikačních služeb, spojuje veřejný klíč s podepisující, šifrující nebo autentizující se osobou a umožňuje ověřit její identitu
CP	certifikační politika (veřejný dokument)
CPS	certifikační prováděcí směrnice (neveřejný dokument)
CRL (Certificate Revocation List)	Seznam zneplatněných certifikátů
Čas	Světový čas UTC
DN	distinguished name – řetězce položky Subject, naplňované daty z žádosti o certifikát, z nichž některé jsou ověřované I.CA dle pravidel, uvedených v této CPS
Držitel certifikátu <sup>1</sup>	fyzická osoba, právnická osoba nebo organizační složka státu, která požádala o vydání certifikátu pro sebe nebo pro podepisující osobu a které byl certifikát vydán
Elektronický podpis	Údaje v elektronické podobě, které jsou připojené k datové zprávě nebo jsou s ní logicky spojené a které slouží jako metoda k jednoznačnému ověření identity podepsané osoby ve vztahu k datové zprávě
I.CA	První certifikační autorita, a.s. – poskytovatel certifikačních služeb
Následný certifikát	certifikát, který byl v souladu se smlouvou o poskytování certifikační služby, uzavřenou mezi koncovým uživatelem a I.CA vydán koncovému uživateli na základě nové žádosti o certifikát: <ul style="list-style-type: none"> <li>• účel elektronického podpisu - elektronicky podepsané platnými daty pro vytváření elektronických podpisů souvisejícími s již vydaným certifikátem, ke kterému je vydáván tento následný certifikát,</li> <li>• ostatní účely - uvedeno v rámci jednotlivých obchodních produktů</li> </ul>
OID	(Object Identifier) číselná identifikace objektu v rámci jednotné klasifikace objektů podle ISO/ITU
Párová data	soukromý a veřejný klíč
Podepisující osoba	fyzická osoba, která je držitelem prostředku pro vytváření elektronických podpisů a jedná jménem svým nebo jménem jiné fyzické či právnické osoby
Podepisování	úkon podepisující osoby, který má význam vzhledem k podepisovaným datům - podepisující osoba potvrzuje, že se s daty, která podepsala, seznámila a s jejich obsahem souhlasí
RA	registrační autorita Certifikační autority I.CA – souhrnný název pro VSRA, VMRA, SRA. Používá se v případech, kdy není podstatný majitel registrační autority ani její forma
Smluvní partner	poskytovatel certifikačních služeb, který zajišťuje na základě písemné smlouvy pro I.CA certifikační služby nebo jejich části - nejčastěji se jedná o smluvní RA

<sup>1</sup> V dalším textu bude takový subjekt nazýván také **držitelem**, pokud bude jasné, že se jedná o držitele certifikátu.

<b>Certifikační prováděcí směrnice vydávání komerčních certifikátů</b>	<b>Strana 12 (celkem 61)</b>
<b>Copyright © První certifikační autorita, a.s.</b>	

Soukromý klíč	jedinečná data pro vytváření elektronického podpisu, šifrování nebo autentizaci
Spoléhající se strana	subjekt spoléhající se při své činnosti na osobní certifikát nebo certifikát pro server
SRA	smluvní registrační autorita Certifikační autority I.CA - plní obdobné funkce jako VSRA nebo VMRA na základě písemné smlouvy mezi I.CA a provozovatelem SRA
Statut certifikátu	stav, ve kterém se certifikát nachází, tzn. ve stavech platnosti, neplatnosti, zneplatnění, zablokování
Spoléhající se strana	subjekt, spoléhající se při své činnosti na certifikát, vydaný I.CA
UPS	Uninterruptible Power Supply
UTC	<b>U</b> niversal <b>C</b> o-ordinated <b>T</b> ime, 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 (BIPM)
Veřejný klíč	jedinečná data pro ověřování elektronického podpisu, dešifrování, autentizace
VMRA	vlastní mobilní registrační autorita Certifikační autority I.CA
VSRA	vlastní stacionární registrační autorita Certifikační autority I.CA
Zablokování	stav, ve kterém se certifikát nachází od doby, kdy jej I.CA zneplatnila, do doby, kdy I.CA zveřejnila CRL, ve kterém je tento certifikát poprvé zařazen
Zneplatnění	stav certifikátu, který byl I.CA zneplatněn – tomuto certifikátu nelze již platnost obnovit
ZoEP	zákon České republiky č. 227/2000 Sb., o elektronickém podpisu a o změně některých dalších zákonů (zákon o elektronickém podpisu), jak vyplývá ze změn provedených zákonem č. 226/2002 Sb., zákonem č. 517/2002 Sb., a zákonem č. 440/2004 Sb.
Žádost o službu (Žádost)	Formální dokument žádosti o některou ze služeb poskytovaných I.CA např. žádost o vydání certifikátu, žádost o zneplatnění certifikátu atd.
Žádost o vydání certifikátu	formální, standardní dokument elektronické žádosti o vydání certifikátu dle přípustných norem a směrnic definovaných v této CPS

<b>Certifikační prováděcí směrnice vydávání komerčních certifikátů</b>	<b>Strana 13 (celkem 61)</b>
<b>Copyright © První certifikační autorita, a.s.</b>	

## 2 Odpovědnosti za zveřejňování a úložiště informací a dokumentace

### 2.1 Úložiště informací a dokumentace

I.CA zřizuje úložiště informací a dokumentace.

### 2.2 Zveřejňování informací a dokumentace

Základní adresy, na nichž lze nalézt veřejné informace o I.CA, certifikační politiky a ostatní veřejné dokumenty atd., (dále též informační adresy), 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> (dále též internetová informační adresa)
- c) sídla registračních autorit

Adresy, které slouží pro kontakt veřejnosti s I.CA (dále též kontaktní adresy), jsou:

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

I.CA zveřejňuje výše uvedené kontaktní adresy na své internetové informační adrese, pracovištích SRA a VSRA. Pracovníci I.CA a smluvních partnerů (SRA) jsou rovněž povinni tyto informace na vyžádání sdělit všem uživatelům. Totéž platí i v případě, že dojde ke změně kontaktních adres.

Informace o veřejných certifikátech (tzn. kromě certifikátů, u kterých si klient vymínil, že nebudou zveřejňovány) lze získat na adrese <http://www.ica.cz/>. Přímou se zveřejňují následující informace (ostatní informace lze získat z certifikátu):

- číslo certifikátu,
- obsah položky Obecné jméno (Common Name, kapitoly 3.1.1 a 3.1.2),
- údaj o počátku platnosti (s uvedením hodiny, minuty a sekundy),
- odkazy na místo, kde lze certifikát získat v určených formátech (DER, PEM, TXT).

I.CA garantuje zajištění nepřetržité dostupnosti a integrity seznamu vydaných veřejných certifikátů.

Informace o CRL lze získat na adrese <http://www.ica.cz/>. Přímou se zveřejňují následující informace (ostatní informace lze získat ze samotného CRL):

- datum vydání CRL,
- číslo CRL,
- odkazy na místo, kde lze CRL získat v určených formátech (DER, PEM, TXT).

Povoleným protokolem pro přístup k informacím o:

- konkrétních CP - HTTP,
- vydaných veřejných certifikátech - HTTP, HTTPS, FTP,
- seznamech zneplatněných certifikátů - HTTP, HTTPS, FTP.

<b>Certifikační prováděcí směrnice vydávání komerčních certifikátů</b>	<b>Strana 14 (celkem 61)</b>
<b>Copyright © První certifikační autorita, a.s.</b>	

Jiné protokoly nejsou povoleny. I.CA může bez udání důvodu přístup prostřednictvím některých z uvedených protokolů zrušit nebo pozastavit. Tyto změny je I.CA povinná zveřejnit prostřednictvím svých informačních adres. Podrobnější informace o možnostech a příslušných parametrech uvedených protokolů I.CA zveřejňuje tamtéž.

V případech zneužití, popř. vzniku důvodné obavy ze zneužití soukromého klíče, sloužícího pro vytváření elektronických podpisů vydávaných certifikátů nebo seznamů zneplatněných certifikátů, oznámí I.CA tuto skutečnost na své internetové informační adrese.

## 2.3 Periodicita zveřejňování informací

I.CA zveřejňuje informace s následující periodicitou:

- Certifikační politika vydávání komerčních certifikátů - před prvním vydáním certifikátu podle této CP,
- informace o zneplatnění certifikátu CA s uvedením důvodu zneplatnění (v případě zneužití nebo vzniku důvodné obavy ze zneužití soukromého klíče, určeného pro podepisování vydávaných certifikátů a seznamů zneplatněných certifikátů) – bezodkladně,
- aktualizace seznamu vydaných certifikátů – doba od vydání veřejného certifikátu do jeho zveřejnění nesmí přesáhnout 2 hodiny (viz <http://www.ica.cz/>),
- aktualizace seznamu zneplatněných certifikátů – I.CA vydává aktuální seznam zneplatněných certifikátů nejméně jednou za 24 hodin (viz <http://www.ica.cz/>),
- 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 zpřístupňuje I.CA bezplatně bez omezení.

Neveřejné informace jsou dostupné pouze pověřeným pracovníkům I.CA, smluvním partnerům nebo subjektům, definovaným platnou legislativou. Přístup k těmto informacím je řízen pravidly, uvedenými v interní dokumentaci, zejména:

- **„Operátor CA“**,
- **„Směrnice pro pracovníky RA I.CA“**,
- **„Řízení bezpečnosti informací“**,
- **„Příručka administrátora“**,
- **„Bezpečnostní incidenty“**,
- **„HSM/Private Server“**,
- **„Dokumenty agendy certifikačních služeb“**,
- **„Dílčí spisový a skartační řád pro agendy certifikačních služeb“**,
- **„Dílčí spisový a skartační plán pro agendy certifikačních služeb“**.

### 3 Identifikace a autentizace

#### 3.1 Pojmenovávání

##### 3.1.1 Typy jmen

Tabulka 4 – Základní položky žádosti o certifikát

Pořadí	Položka	Kódování	Počet	Žádost	Význam	Příklad	Doložení <sup>2</sup>
1	CountryName	PS	=1	A	kap. 3.1.2.1	CZ	primár. dokl.
2	CommonName	U8,PS	=1	A	kap. 3.1.2.2, popř. pseudonym, následovaný řetězcem „ – PSEUDONYM“	Ing. Petr Jan Holoubek PhD, popř. Kokoška – PSEUDONYM	primár. dokl.
3	StateOrProvinceName	U8,PS	1	N	kap. 3.1.2.3	Praha	primár. dokl.
4	LocalityName	U8,PS	1	N	kap. 3.1.2.4	Praha 7 Ovenecká 1047/17 17000	primár. dokl.
5	OrganizationName	U8,PS	1	N	kap. 3.1.2.5	Společnost, a.s.	VOR <sup>3</sup> , ŽL <sup>4</sup>
6	OrganizationalUnitName	U8,PS	M	N	kap. 3.1.2.6	Odbor systému a sítě	POZ <sup>5</sup>
7	Pkcs9_EmailAddress	IA5	1	N	kap. 3.1.2.7	<a href="mailto:holy@quick.cz">holy@quick.cz</a>	
8	Initials	U8,PS	1	N	kap. 3.1.2.8	PJH	primár. dokl.
9	Title	U8,PS	M	N	kap. 3.1.2.9	specialista systému a sítě	POZ
10	SerialNumber	PS	1	N1	kap. 3.1.2.10	ICA - 10020184	-
11	GenerationQualifier	U8,PS	1	N	kap. 3.1.2.11	MI.	primár. dokl.

Tabulka 4a – Rozšiřující položky žádosti o certifikát

Položka	Kódování	Počet	Žádost	Význam	Příklad	Doložení
SubjectAlternativeName						
• rfc822Name	IA5	M	N	kap. 3.1.2.12	<a href="mailto:holy@quick.cz">holy@quick.cz</a>	
• dNSName	IA5	M	N	kap. 3.1.2.12	<a href="http://www.moje.cz">www.moje.cz</a>	čestné prohlášení
• uniformResourceIdentifier	IA5	M	N	kap. 3.1.2.12	<a href="http://www.moje.cz">http:// www.moje.cz</a>	čestné prohlášení
• iPAddress	Dle RFC3280	M	N	kap. 3.1.2.12	172.17.5.3	čestné prohlášení

<sup>2</sup> Viz uvedené kapitoly ve sloupci „Význam“

<sup>3</sup> Výpis z obchodního rejstříku

<sup>4</sup> Živnostenský list

<sup>5</sup> Potvrzení o zaměstnání

<b>Certifikační prováděcí směrnice vydávání komerčních certifikátů</b>	<b>Strana 16 (celkem 61)</b>
<b>Copyright © První certifikační autorita, a.s.</b>	

Legenda:

- **Kódování** určuje množinu povolených kódování dle ASN.1 pro danou položku. Použité typy kódování jsou **PS** - PrintableString, **IA5** - IA5String, **U8** - UTF8String, **BMP** – BMPString a mohou být v rámci jednotlivých obchodních produktů omezeny.
- **Počet** udává počet výskytů dané položky DN v žádosti o certifikát, popř. v certifikátu. Použité zkratky mají následující význam:
  - **=1** - právě jedna,
  - **1** - maximálně jedna,
  - **M** - libovolný počet.
- **Žádost** udává výskyt dané položky DN v žádosti o certifikát, popř. v certifikátu. Použité zkratky mají následující význam:
  - **A** - musí být v žádosti obsaženo,
  - **N** - nemusí, ale může být v žádosti obsaženo,
  - **N1** - v prvotní žádosti o certifikát nesmí být uvedeno, je povoleno pouze v žádosti o obnovení certifikátu, pokud je obsaženo v prvotním certifikátu.

### 3.1.2 Požadavek na významovost jmen

Kontroly na RA/CA:

- přítomnost nepovolených znaků (v závislosti na typu pole) - v případě výskytu nepovolených znaků se žádost nepřijme,
- přítomnost všech povinných položek - pokud některá z povinných položek není vyplněna, žádost se nepřijme,
- odstraňují se úvodní a koncové mezery (0x20) a skupiny mezer uprostřed položky se redukuje na jedinou mezeru, toto platí i pro „whitespaces“ (ASCII, Unicode : 0x09 – 0x0D, 0x20),
- fyzická osoba nepodnikající/pseudonym: povinné položky – CommonName, CountryName,
- fyzická osoba podnikající/zaměstnanec: povinné položky – CommonName, CountryName, OrganizationName,
- v případě nepoužití diakritiky jsou řetězce „Štěpánek“ a „Stepanek“ vyhodnocovány jako shodné.

Při kontrole rozdílnosti či shodnosti DN je použitý následující způsob porovnávání řetězců:

- jestliže jsou dva stejné řetězce různě kódovány, jsou přesto považovány za shodné,
- porovnávání řetězců ve všech kódováních je závislé na velikosti písma,
- při porovnávání řetězců ve všech kódováních jsou odstraňovány mezerové znaky. (např. řetězce „Martin“ a „ Martin“ jsou shodné).

Dále se kontroluje věcná správnost jmen. Rozsah kontrol je uveden v následujících podkapitolách.

#### 3.1.2.1 CountryName (stát)

Položka Country (Stát) může obsahovat pouze kód státu, v němž má žadatel o certifikát:

- trvalé bydliště podle primárního osobního dokladu, **nebo**
- pracoviště podle VOR, ŽL, zřizovací listiny atd.

RA kontroluje správnost podle výše uvedeného dokladu (fyzická osoba nepodnikající - pokud není explicitně uveden v primárním osobním dokladu, uvede se stát, který předkládaný průkaz vydal) nebo podle VOR, ŽL, zřizovací listiny atd. V případě neshody žádost odmítne. Kód státu musí odpovídat normě ISO 3166.

#### 3.1.2.2 CommonName (Obecné jméno)

Položka CommonName (Obecné jméno) může obsahovat znaky s diakritikou a jejím obsahem je:



<b>Certifikační prováděcí směrnice vydávání komerčních certifikátů</b>	<b>Strana 17 (celkem 61)</b>
<b>Copyright © První certifikační autorita, a.s.</b>	

- celé jméno (tzn. jméno a příjmení, případně další jméno/jména a tituly), uvedené v osobním dokladu žadatele o certifikát - RA kontroluje správnost podle osobního dokladu, v případě neshody žádost odmítne, **nebo**
- uvedený pseudonym, doplněný řetězcem „ – PSEUDONYM“ - Pokud žadatel o certifikát uvedl pseudonym, může tento obsahovat jakoukoli sekvenci povolených znaků. V případě, že se jedná o ověřitelný údaj, je žadatel o certifikát povinen tuto skutečnost v rámci ověřovací procedury na RA doložit - pracovník RA provádí ověření tohoto údaje a v případě neshody danou žádost odmítne. V případě neověřitelného údaje pracovník RA pouze kontroluje, zda se nejedná o nepovolené výrazy (vulgární, propagující fašismus, rasovou a třídní nenávisť). O přípustnosti konkrétního obsahu údaje rozhoduje pracovník RA, který vyřizuje žádost o vydání certifikátu. Rovněž nesmí být dotčena práva jiných subjektů (registrované známky apod.),
- v případě certifikátu pro server zpravidla doménové jméno serveru, resp. domény. Pracovník RA pouze kontroluje, zda se nejedná o nepovolené výrazy (vulgární, propagující fašismus, rasovou a třídní nenávisť). O přípustnosti konkrétního obsahu údaje rozhoduje pracovník RA, který vyřizuje žádost o vydání certifikátu. Rovněž nesmí být dotčena práva jiných subjektů (registrované známky apod.). Pokud budou v obecném jménu uvedeny jiné skutečnosti (jméno fyzické osoby, obchodní jméno, registrovaná známka apod.), musí být takové údaje ověřeny, pokud to uvedené skutečnosti vyžadují.

### 3.1.2.3 StateorProvinceName (kraj)

Položka StateorProvinceName (Kraj) může obsahovat pouze označení nižšího územně správního celku, do něhož spadá místo:

- trvalého bydliště podle osobního dokladu žadatele o certifikát, tedy město, obec nebo jinou správní jednotku, která je v osobním dokladu uvedena, **nebo**
- sídla podle VOR, ŽL, zřizovací listiny atd., tedy město, obec nebo jinou správní jednotku, která je v dokladu uvedena.

Z obsahu musí být zřejmé, zda se jedná o kraj nebo jiný celek. RA přijímající předmětnou žádost správnost tohoto údaje v případě, že byl uveden, kontroluje, v případě neshody danou žádost odmítne. Položka může obsahovat znaky s diakritikou.

### 3.1.2.4 LocalityName (místo)

Položka LocalityName (Místo) může obsahovat místo:

- trvalého bydliště podle osobního dokladu žadatele o certifikát, tedy město, obec nebo jinou správní jednotku, která je v osobním dokladu uvedena, **nebo**
- sídla podle VOR, ŽL, zřizovací listiny atd., tedy město, obec nebo jinou správní jednotku, která je v dokladu uvedena.

RA přijímající předmětnou žádost správnost tohoto údaje v případě, že byl uveden, kontroluje, v případě neshody danou žádost odmítne. Položka může obsahovat znaky s diakritikou.

### 3.1.2.5 OrganizationName (organizace)

Položka Organization (Organizace) může obsahovat pouze obchodní název podle VOR nebo jiného zákonem určeného rejstříku/registru, živnostenského listu, zřizovací listiny atd. Žadatel o certifikát je povinen doložit oprávněnost použití obsahu dané položky nezpochybnitelným způsobem<sup>6</sup>.

RA přijímající předmětnou žádost správnost tohoto údaje v případě, že byl uveden, kontroluje, v případě neshody danou žádost odmítne. Položka může obsahovat znaky s diakritikou.

<sup>6</sup> Např. v případě obchodního jména živnostníka patřičným živnostenským listem, v případě, že podepisující osoba je majitelem firmy, společníkem nebo zaměstnancem pak výpisem z obchodního rejstříku

<b>Certifikační prováděcí směrnice vydávání komerčních certifikátů</b>	<b>Strana 18 (celkem 61)</b>
<b>Copyright © První certifikační autorita, a.s.</b>	

### **3.1.2.6 OrganizationalUnitName (organizační jednotka)**

Položka OrganizationUnitName (Organizační jednotka) může obsahovat pouze název organizační jednotky a to výhradně v tom případě, že byl použit položka Organization. Žadatel o certifikát je povinen doložit oprávněnost použití obsahu dané položky nezpochybnitelným způsobem. RA přijímající předmětnou žádost správnost tohoto údaje v případě, že byl uveden, kontroluje, v případě neshody danou žádost odmítne. Položka může obsahovat znaky s diakritikou a může se vyskytovat vícekrát.

### **3.1.2.7 Pkcs9Email Address (elektronická poštovní adresa)**

Položka E-mailAddress (Elektronická poštovní adresa) může obsahovat pouze elektronickou poštovní adresu žadatele o certifikát (dle RFC 822). Vyžaduje se hodnověrně doložené vlastnictví této elektronické poštovní adresy nebo čestné prohlášení<sup>7</sup> žadatele o certifikát certifikátu, v němž toto vlastnictví potvrzuje. V případě nesplnění této podmínky má RA právo danou žádost odmítnout. Položka nesmí obsahovat znaky s diakritikou.

### **3.1.2.8 Initials (iniciály)**

Položka Initials (Iniciály) může obsahovat pouze iniciály celého jména žadatele o certifikát. RA přijímající předmětnou žádost, pokud je položka Initials vyplněn, shodu iniciál s jménem žadatele o certifikát kontroluje, v případě neshody danou žádost odmítne. Položka může obsahovat znaky s diakritikou.

### **3.1.2.9 Title (titul)**

Obsahem položky Title (Titul) zpravidla bývá postavení žadatele o certifikát v určité (zpravidla firemní) hierarchii. Obsah této položky se kontroluje v závislosti na skutečnostech, které jsou v něm obsaženy<sup>8</sup>. Položka může obsahovat znaky s diakritikou a může se vyskytovat vícekrát.

### **3.1.2.10 SerialNumber (sériové číslo subjektu)**

Sériové číslo subjektu, které slouží k rozlišení různých subjektů v rámci klientely I.CA. Sériové číslo subjektu obecně vyplňuje CA a je naplněno řetězcem „ICA - “ a za něj je připojeno na řetězec převedené identifikační číslo žadatele o certifikát.

### **3.1.2.11 GenerationQualifier (generační rozlišení)**

Položka GenerationQualifier (Generační rozlišení) žadatele o certifikát se používá pro označení umístění v rodinném stromu. RA přijímající předmětnou položku v žádosti neověřuje, nejsou však povoleny výrazy vulgární, propagující fašismus, rasovou a třídní nenávisť. Položka může obsahovat znaky s diakritikou.

### **3.1.2.12 Subject Alternative Name (alternativní jméno subjektu)**

Pokud žadatel o certifikát použil položku Subject Alternative Name (alternativní jméno), je nutno ověřit skutečnosti v něm uváděné (pokud se jedná o skutečnosti vyžadující ověření). Jako součást alternativního jména se připouští :

<sup>7</sup> Čestné prohlášení pro účely této certifikační politiky je realizováno formou stvrzení pravdivosti údajů ve smlouvě o vydání certifikátu.

<sup>8</sup> např. pokud žadatel požaduje obsah „Praktický lékař“, je možné žádost přijmout, pokud prokáže, že je praktickým lékařem, pokud bude požadovat obsah typu „Linuxový guru“, toto nelze zkontrolovat a žádost se zamítne.

- **rfc822Name (elektronická adresa)** – v případě naplnění má tato položka přednost před „pkcs9EmailAddress“ a certifikát je přednostně spojen s touto alternativní adresou,
- **dNSName (jméno doménového serveru)** - pokud je doménové jméno registrováno, vyžaduje se hodnověrně doložený souhlas vlastníka nebo čestné prohlášení žadatele o certifikát, potvrzující vlastnictví doménového jména,
- **uniformResourceIdentifier - URI (identifikátor zdroje v Internetu)** - pokud je URI registrováno, vyžaduje se hodnověrně doložený souhlas vlastníka nebo čestné prohlášení žadatele o certifikát, v němž vlastnictví URI potvrzuje,
- **iPAddress (IP adresa)** - pokud je IP adresa registrována, vyžaduje se hodnověrně doložený souhlas vlastníka nebo čestné prohlášení žadatele o certifikát, v němž vlastnictví IP adresy potvrzuje. RA přijímající předmětnou žádost je povinna, pokud je položka vyplněna, tuto položku zkontrolovat, v případě neshody je RA povinna danou žádost odmítnout.

Jednotlivé uvedené položky se v rámci alternativního jména mohou vyskytnout jednou nebo vícekrát, případně se nemusí vyskytnout vůbec. I.CA může bez udání důvodu množinu povolených tvarů omezit, případně rozšířit.

### 3.1.3 Anonymita a používání pseudonymu

Viz kapitola 3.1.2.2

### 3.1.4 Pravidla pro interpretaci různých forem jmen

Pokud se jedná o jména nebo jiné skutečnosti, které jsou uvedeny v osobním dokladu fyzické osoby nebo v jiných dokumentech, které jsou přípustné pro prokazování identity, případně vztahu fyzické osoby k právnické osobě, přenášejí se tato jména v té podobě, v jaké jsou v dokumentu uvedena. Vlastní transkripce se zásadně pro účely vydávání certifikátů neprovádí. Dále platí ustanovení kapitoly 3.1.2.

### 3.1.5 Jedinečnost jmen

Jednoznačnost jména subjektu je zaručena použitím výše definovaného postupu pro tvorbu položky SerialNumber a jména vydavatele certifikátu.

### 3.1.6 Obchodní značky

I.CA uznává pouze ty ochranné známky, jejichž vlastnictví nebo pronájem žadatel doložil. Autentizaci ochranných známek jinými způsoby I.CA neprovádí. Ochranná známka může být součástí Obecného Jména (CN).

Veškeré důsledky plynoucí z neoprávněného užívání ochranné známky nese žadatel.

## 3.2 Počáteční ověření identity

Postup ověřování identity je detailně uveden v interní dokumentaci „Operátor RA“.

### 3.2.1 Ověření souladu dat, tj. postup při ověřování, zda má osoba soukromý klíč odpovídající veřejnému klíči

- Certifikáty vydané pro účely elektronického podpisu:

<b>Certifikační prováděcí směrnice vydávání komerčních certifikátů</b>	<b>Strana 20 (celkem 61)</b>
<b>Copyright © První certifikační autorita, a.s.</b>	

- **Osobní certifikáty** - Vlastnictví soukromého klíče, odpovídající veřejnému klíči, který bude daný certifikát obsahovat, se prokazuje předložením žádosti o vydání certifikátu, elektronicky podepsané těmito daty. Pracovník RA prostřednictvím aplikace RA toto kontroluje tím, že pomocí veřejného klíče uvedeného v žádosti o certifikát, ověří platnost elektronického podpisu na této žádosti. Pokud je ověření platnosti elektronického podpisu negativní, RA žádost nepřijme a řízení k vydání certifikátu zastaví.
  - **Certifikáty pro server** - Vlastnictví soukromého klíče, odpovídající veřejnému klíči, který bude certifikát serveru obsahovat, se prokazuje předložením žádosti o vydání certifikátu pro server, elektronicky podepsané tímto soukromým klíčem, resp. elektronicky podepsané soukromým klíčem, souvisejícími s vydaným osobním certifikátem k tomuto certifikátu serveru. Pracovník RA prostřednictvím aplikace RA toto kontroluje tím, že pomocí veřejným klíčem, uvedeným v žádosti o certifikát serveru, resp. pomocí veřejného klíče, souvisejícího s vydaným osobním certifikátem k tomuto certifikátu serveru, ověří platnost elektronického podpisu na této žádosti. Pokud je ověření platnosti elektronického podpisu negativní, RA žádost nepřijme a řízení k vydání certifikátu serveru zastaví.
- Certifikáty vydané pro ostatní účely – uvedeno v rámci jednotlivých obchodních produktů.

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

I.CA vyžaduje originál nebo notářsky ověřenou kopii výpisu z obchodního, nebo jiného zákonem určeného rejstříku/registru, živnostenského listu, zřizovací listiny a který/která musí obsahovat úplné obchodní jméno, identifikační číslo (IČO), sídlo a jména osoby/osob, oprávněné/oprávněných k zastupování (statutárních zástupců) a způsob, jakým za právnickou osobu jednájí a podepisují.

### 3.2.3 Ověřování identity fyzické osoby

I.CA vyžaduje při identifikaci žadatele o certifikát předložení jeho následujících údajů:

- celé občanské jméno,
- datum narození (nebo rodné číslo u občanů ČR nebo SR),
- číslo předloženého osobního dokladu,
- adresa trvalého bydliště (pokud je v osobním dokladu uvedena).

Pokud dojde během trvání smluvního vztahu k I.CA ke změnám ve výše uvedených údajích nebo v údajích, uvedených v certifikátu, je žadatel, popř. držitel povinen tyto změny ohlásit I.CA. Požadavky při registraci nového žadatele/držitele o certifikát jsou uvedeny v kapitolách 3.2.3.1 až 3.2.3.3.

#### 3.2.3.1 Fyzická osoba

##### **Doklady, předkládané na RA:**

- Žadatel o certifikát se osobně dostaví na RA:
  - Originál platného osobního dokladu. Osobní doklad pro občany ČR musí být občanský průkaz, popř. obdobný doklad stejné právní váhy. Osobní doklad pro cizince je platný cestovní pas, popř. obdobný doklad stejné právní váhy. Občané Slovenské republiky mohou jako osobní doklad použít občanský průkaz.
- Žadatel je na RA zastupován zmocněncem:
  - Originál osobního dokladu zmocněnce (kvalita dokladu je uvedena výše).
  - Originál, případně úředně ověřená kopie osobního dokladu žadatele o certifikát (kvalita dokladu je uvedena výše).

- Doklad, prokazující právo jednat jako zmocněnec - plné moc s úředně ověřeným podpisem zmocnitele, splňující následující požadavky:
  - Pokud je plná moc v cizím jazyce (kromě slovenštiny), musí být přeložena do češtiny úředním překladatelem. V zahraničí<sup>9</sup> provedené úřední ověření podpisů musí být tzv. „superlegalizováno“, tj. potvrzeno zastupitelským úřadem ČR v zemi původu plné moci. V případě dokladů, ověřených v zemích, uvedených na <http://www.hcch.net/>, nemusí být superlegalizace provedena<sup>10</sup>.
- Pokud je žadatel zákonným zástupcem klienta, požaduje se o tom úřední doklad:
  - Rodiče nebo osvojitelé zastupují své nezletilé děti - přestože nezletilec má omezenou svéprávnost, smlouvy s I.CA za něj musí uzavírat jeho zákonný zástupce. Dokladem je rodný list dítěte. Osvojení se dokládá buď výpisem z matriky nebo rozhodnutím soudu. Ve všech uvedených případech postačí záznam o dítěti v občanském průkazu.  
Pozn.: Zákonným zástupcem dítěte není pěstoun.
  - Poručník nebo opatrovník je osobám bez plné způsobilosti k právním úkonům, včetně dospělých, ustanoven soudem. Dokladem je soudní rozhodnutí.
    - Opatrovníkem nebo poručníkem dítěte může být ustanoven také orgán sociálně-právní ochrany dítěte (zpravidla obec nebo obcí zřízený veřejný opatrovník). V tom případě jde o právnickou osobou a vedle usnesení soudu dokládá ještě skutečnosti, vztahující se k právnickým osobám.
    - Opatrovník může být ustanoven také osobám s tělesným postižením, které nemají omezenou svéprávnost, ale potřebují při právních úkonech asistenci (např. nevidomým).

### **Doklady, kontrolované na RA:**

V případě, že se žadatel o certifikát se osobně dostaví na RA:

- zda osoba, která je uvedena v žádosti o certifikát, je totožná s osobou žadatele (dle platného osobního dokladu), a že údaje uvedené v žádosti odpovídají údajům v předloženém dokladu. Shoda je nutná u těchto údajů:
  - příjmení, jméno,
  - bydliště (město),
  - oblast (ulice, pokud je v položce uvedena),
- plnoletost žadatele,
- platnost předkládaných dokladů,
- pokud se žadatel prokazuje cestovním pasem, kontrola na shodu bydliště se neprovádí,
- příslušník cizího státu musí splňovat podmínky pro právní subjektivitu a svéprávnost alespoň podle práva ČR - pokud je nespĺňuje, je třeba ověřit, zda splňuje podmínky podle práva státu jehož je příslušníkem. V takovém případě je třeba postupovat individuálně, ve spolupráci s žadatelem a I.CA,
- v případě žádosti o certifikát serveru, čestné prohlášení o vlastnictví serveru, resp. domény

<sup>9</sup> podle slovenského zákona smí ověřování dokladů pro použití v cizině provádět pouze notář - § 2 zákona NÁRODNEJ RADY SLOVENSKEJ REPUBLIKY ze dne 22.12.1992

<sup>10</sup> v tomto případě je třeba postupovat individuálně, ve spolupráci s žadatelem o certifikát, resp. pracovníka RA s I.CA

<b>Certifikační prováděcí směrnice vydávání komerčních certifikátů</b>	<b>Strana 22 (celkem 61)</b>
<b>Copyright © První certifikační autorita, a.s.</b>	

**Doklady, u nichž byl výsledek ověření záporný (tzn. údaje nesouhlasily), jsou v evidenci dokladů vedeny jako neplatné a služba nesmí být poskytnuta.**

- Žadatel je na RA zastupován zmocněncem:
  - shodu údajů o žadateli, uvedených v žádosti o službu a na plné moci, resp. dokladu o zákonném zastupování,
  - platnost a správnost předloženého dokladu zástupce s údaji na plné moci, resp. dokladu o zákonném zastupování a oprávněnost k podání žádané služby.

### **3.2.3.2 Fyzická osoba zaměstnanec**

#### **Doklady, předkládané na RA:**

- Doklady ve stejném rozsahu, jako v kapitole 3.2.3.1, bod „Žadatel o certifikát se osobně dostaví na RA“.
- Doklad, uvedený v kapitole 3.2.2. Pokud je tento doklad v cizím jazyce, platí pro ověření pravidla, uvedená v kapitole 3.2.3.1.
- V případě zaměstnance - potvrzení o zaměstnaneckém poměru k danému zaměstnavateli, pokud není uzavřena s I.CA rámcová smlouva. Potvrzení musí být opatřeno podpisem osoby s právem jednání za příslušného zaměstnavatele. Pokud tato osoba není osobou oprávněnou k zastupování zaměstnavatele, tj. není statutárním zástupcem (není uveden na výpisu z obchodního rejstříku nebo jiného zákonem určeného rejstříku nebo registru, živnostenský list, zřizovací listina atd. jako osoba oprávněná jednat), požaduje se navíc úředně ověřený doklad (plná moc, pověření, doklad o zákonném zastupování) podepsaný statutárním zástupcem zaměstnavatele, potvrzující oprávněnost této osoby jednat za zaměstnavatele.

#### **Doklady, kontrolované na RA:**

- zda údaje, uvedené v žádosti o certifikát, se shodují s údaji v dokladech předložených žadatelem, resp. zmocněncem - při kontrole postupuje pracovník RA stejně jako u fyzické osoby nepodnikající (viz kapitola 3.2.3.1),
- potvrzení o zaměstnaneckém poměru k danému zaměstnavateli,
- zda je osoba, podepisující potvrzení o zaměstnaneckém poměru, uvedená v úředně ověřeném dokladu (plná moc pověření, doklad o zákonném zastupování), oprávněna zastupovat zaměstnavatele - pracovník RA musí zkontrolovat, zda pověřující osoba má dle výpisu z obchodního nebo jiného zákonem předepsaného rejstříku, živnostenského listu, zřizovací listiny atd. právo takovéto pověření provést, popřípadě, zda uděluje plnou moc oprávněné osobě v souladu s výpisem výše uvedených dokumentů<sup>11</sup>,
- v případě žádosti o certifikát serveru, čestné prohlášení o vlastnictví serveru, resp. domény.

**Doklady, u nichž byl výsledek ověření záporný (tzn. údaje nesouhlasily), jsou v evidenci dokladů vedeny jako neplatné a služba nesmí být poskytnuta.**

<sup>11</sup> Pokud je na výpisu z obchodního rejstříku uvedeno např. že "podpisové právo za společnost má předseda představenstva spolu s dalším členem představenstva" znamená to, že plnou moc může udělit pouze předseda představenstva spolu s dalším členem představenstva (tudíž musí být na plné moci ověřené podpisy těchto dvou osob).

<b>Certifikační prováděcí směrnice vydávání komerčních certifikátů</b>	<b>Strana 23 (celkem 61)</b>
<b>Copyright © První certifikační autorita, a.s.</b>	

### **3.2.3.3 Právnícké osoby a organizační složky státu (např. elektronická podatelna - orgán veřejné moci)**

V případě, že zástupcem organizační složky státu, resp. právnické osoby, jakožto žadatele o certifikát, je její zaměstnanec, je postupováno v souladu s kapitolou 3.2.3.2 a bodem „Žadatel o certifikát se osobně dostaví na RA“, uvedeným v kapitole 3.2.3.1.

V případě, že organizační složka státu, resp. právnická osob pověří zastupováním třetí stranu na základě smluvního vztahu, platí relevantní požadavky předchozích kapitol.

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

V případě informací, které se nedají ověřit, je postupováno v souladu s kapitolou 3.1.2.

### **3.2.5 Ověřování specifických práv**

Ověřování specifických práv je prováděno v souladu s kapitolami 3.2.2 a 3.2.3.

### **3.2.6 Kritéria pro interoperabilitu**

Případná spolupráce s jinými poskytovateli certifikačních služeb je založena na písemné smlouvě společnosti První certifikační autorita, a.s. s konkrétními poskytovateli certifikačních služeb.

## **3.3 Identifikace a autentizace při zpracování požadavků na výměnu veřejného klíče v certifikátu**

### **3.3.1 Identifikace a autentizace při rutinní výměně párových dat**

- Certifikáty, vydané pro účely elektronického podpisu:
  - Žadatel o osobní certifikát vytvoří novou žádost o vydání následného certifikátu, elektronicky podepsanou soukromým klíčem, souvisejícím s již vydaným certifikátem, ke kterému je tento následný certifikát vydáván.
  - Žadatel o certifikát serveru vytvoří novou žádost o vydání následného certifikátu serveru elektronicky podepsanou soukromým klíčem, souvisejícím s již vydaným certifikátem serveru, ke kterému je tento následný certifikát serveru vydáván, resp. elektronicky podepsané soukromým klíčem, souvisejícím s vydaným osobním certifikátem k tomuto certifikátu serveru.
- Certifikáty, vydané pro ostatní účely – uvedeno v rámci jednotlivých obchodních produktů.

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

I.CA nepodporuje výměnu párových dat již zneplatněného certifikátu. Z tohoto důvodu nelze ani přijmout žádost o následný certifikát, pokud je elektronicky podepsána soukromým klíčem, příslušným k certifikátu, který byl již zneplatněn. Jediný způsob, jak získat nový certifikát, je uveden v kapitole 4.2.2.

<b>Certifikační prováděcí směrnice vydávání komerčních certifikátů</b>	<b>Strana 24 (celkem 61)</b>
<b>Copyright © První certifikační autorita, a.s.</b>	

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

Žádost o zneplatnění certifikátu lze podat následujícími způsoby:

- Osobním předáním písemné žádosti o zneplatnění certifikátu na RA.
- Pomocí elektronické pošty ([revoke@ica.cz](mailto:revoke@ica.cz)).
- Zasláním běžné poštovní zprávy.
- Prostřednictvím elektronického formuláře, který je za tímto účelem přístupný na vyhrazené webové stránce (<http://www.ica.cz>).

Po identifikaci a autentizaci je postupováno způsobem, uvedeným v kapitole 4.9.3. Detailně je celý proces zneplatnění certifikátu uveden v interní dokumentaci:

- „**Směrnice pro pracovníky RA I.CA**“,
- „**Operátor CA**“.



<b>Certifikační prováděcí směrnice vydávání komerčních certifikátů</b>	<b>Strana 25 (celkem 61)</b>
<b>Copyright © První certifikační autorita, a.s.</b>	

## 4 Požadavky na životní cyklus certifikátu

### 4.1 Žádost o vydání certifikátu

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

Certifikáty jsou I.CA komerčně nabízenou službou a jsou vydávány každému, kdo se smluvně zaváže jednat podle odpovídající CP.

I.CA požaduje minimální věk 15 let pro osobu, která žádá o certifikát. Žadatelé o certifikát ve věku od 15 do 18 let musí žádat prostřednictvím svého zákonného zástupce.

Pokud je žadatel zastupován zmocněncem, musí mít zmocněnec oprávnění žadatele zastupovat.

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

Registrační proces, včetně odpovědností jak poskytovatele certifikační služby, tak žadatele o tuto službu, jsou uvedeny v následujících kapitolách.

### 4.2 Zpracování žádosti o certifikát

Proces zpracování žádosti o certifikát je detailně popsán v interní dokumentaci:

- „**Směrnice pro pracovníky RA I.CA**“,
- „**Operátor CA**“.

#### 4.2.1 Identifikace a autentizace

Po vygenerování žádosti o prvotní osobní certifikát (viz kapitola 3.3.1) a jejím následném uložení na záznamové médium (typ uveden na [www.ica.cz](http://www.ica.cz)), se žadatel, popř. zmocněnec s touto žádostí a potřebnými doklady (viz kapitola 3.2.3) dostává na RA.

Při registraci žadatele o prvotní certifikát pro server příslušný pracovník RA postupuje v souladu s postupem při žádosti o vydání osobního certifikátu. Žadatel má nárok současně podat žádost o osobní certifikát - bezplatně. Údaje v této žádosti je rovněž povinen doložit. V případě, že jsou v žádosti o vydání certifikátu pro server nebo v žádosti o vydání osobního certifikátu nedostatky, RA upozorní žadatele na tuto skutečnost a registraci odmítne.

Žadatel o následný certifikát vytvoří žádost postupem, uvedeným v kapitole 3.3.1.

Prokazování vlastnictví soukromého klíče, odpovídajícího veřejnému klíči je uvedeno v kapitole 3.2.1.

V procesu zpracování žádosti o certifikát provede pracovník RA kontrolu předložených originálů osobních dokladů žadatele o certifikát, popř. zmocněnce a v případě pochybností o pravosti předloženého osobního dokladu žadatele o certifikát, popř. zmocněnce odmítne a proces vydávání certifikátu ukončí. V případě, že fyzickou osobou, vyřizující žádost o vydání certifikátu je zmocněnec, provede pracovník RA dále kontrolu předloženého originálu, případně úředně ověřené kopie osobního dokladu zmocnitele a v případě pochybností o pravosti zmocnitele odmítne a proces vydávání certifikátu ukončí. Fyzická osoba, vyřizující na RA žádost o certifikát, předkládá pracovníkovi RA doklady, uvedené v odstavcích **Doklady, předkládané na RA** kapitoly 3.2.3. Pracovníkem RA jsou kontrolovány doklady, uvedené v odstavcích **Doklady, kontrolované na RA** kapitoly 3.2.3.

V procesu zpracování žádosti o následný certifikát je postupováno v souladu s kapitolou 4.7.

<b>Certifikační prováděcí směrnice vydávání komerčních certifikátů</b>	<b>Strana 26 (celkem 61)</b>
<b>Copyright © První certifikační autorita, a.s.</b>	

#### 4.2.2 Přijetí nebo odmítnutí žádosti o certifikát

V případě, že výsledek kontrol, uvedených v kapitole 4.2.1 je pozitivní, pracovník RA vytiskne dokument „Protokol o podání žádosti na vydání certifikátu I.CA“, který nechá žadateli o certifikát, popř. zmocněnci, podepsat. Pokud žadatel o certifikát, popř. zmocněnec odmítne tento protokol podepsat, je pracovník RA povinen proces vydávání certifikátu ukončit.

Postupy pro přijetí nebo odmítnutí žádosti o certifikát jsou uvedeny v konkrétní CP a v interní dokumentaci:

- **„Směrnice pro pracovníky RA I.CA“.**

#### 4.2.3 Doba zpracování žádosti o certifikát

I.CA nestanovuje pevný časový limit, ve kterém dojde ke zpracování žádosti o certifikát, neboť se jedná o časový sled následujících činností, z nichž některé záleží pouze na žadateli o certifikát. Časové údaje jsou uvedeny v následujícím seznamu:

- generování žádosti o vydání certifikátu – řádově jednotky minut ,
- vydání certifikátu:
  - prvotní certifikát (žadatel se MUSÍ osobně dostavit na RA) - doba vydání certifikátu je do 15 minut a jen ve výjimečných případech může být tato doba delší,
  - následný certifikát (žadatel se NEMUSÍ osobně dostavit na RA) – řádově jednotky minut.

### 4.3 Vydání certifikátu

#### 4.3.1 Úkony CA v průběhu vydání certifikátu

V procesu vydávání certifikátu provádějí operátoři certifikační autority nezbytné kontroly a další činnosti, popsané v interním dokumentu:

- **„Směrnice pro pracovníky RA I.CA“,**
- **„Operátor CA“.**

V případě kladného výsledku je certifikát vydán (formáty PEM, DER, TXT), v opačném případě nikoli.

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

- vydání prvotního certifikátu - klient je informován prostřednictvím pracovníka RA
- vydání následného certifikátu:
  - klient se dostaví na RA - je informován prostřednictvím pracovníka RA,
  - klient žádá o následný certifikát prostřednictvím e-mail – certifikát zaslán.

Uvedené postupy jsou detailně popsány v interní dokumentaci:

- **„Směrnice pro pracovníky RA I.CA“,**
- **„Operátor CA“.**

### 4.4 Převzetí vydaného certifikátu

#### 4.4.1 Úkony spojené s převzetím certifikátu

Pokud byly splněny podmínky pro vydání **prvotního certifikátu**, tzn.:

<b>Certifikační prováděcí směrnice vydávání komerčních certifikátů</b>	<b>Strana 27 (celkem 61)</b>
<b>Copyright © První certifikační autorita, a.s.</b>	

- splněny podmínky registrace (kapitoly 3.2, 3.3),
- zaplacení určeného poplatku (není-li smluvně stanoveno jinak) – uvedeno v aktuálním ceníku (viz kapitola 2.2),
- prokázání vlastnictví soukromého klíče, odpovídajícího veřejnému klíči, který bude vydaný certifikát obsahovat (kapitoly 3.2.1, 4.7.1),
- podepsání příslušné smlouvy – rozumí se smlouva o poskytování certifikační služby,

je povinností žadatele o certifikát tento certifikát přijmout. Jediným způsobem, jakým může žadatel postupovat v případě, že tento certifikát nemá zájem převzít, je zažádat v souladu s touto CPS o jeho zneplatnění.

Pracovník RA předá žadateli záznamové médium (typ uveden na [www.ica.cz](http://www.ica.cz)), obsahující požadovaný certifikát a odpovídající certifikát CA (v předepsaných formátech). Žadatel musí převzetí media s certifikáty potvrdit. V případě, že byla v žádosti uvedena elektronická adresa, jsou vydaný certifikát a certifikát CA (v předepsaných formátech) na tuto adresu taktéž zaslány.

V případě podání žádosti o vydání **následného certifikátu** elektronickou cestou, zašle I.CA na žadatelovu elektronickou adresu vydaný certifikát a odpovídající certifikát CA (v předepsaných formátech), v případě vyřizování žádosti na RA, získá žadatel vydaný certifikát, popř. odpovídající certifikát CA (v předepsaných formátech) od pracovníka RA.

Odpovídající CP získá žadatel na RA, popř. ji může stáhnout z informační adresy – viz kapitola 2.2.

I.CA může ve smlouvě se smluvním partnerem sjednat postup, odlišný od tohoto ustanovení CPS. Tímto postupem však nesmí být dotčena příslušná ustanovení legislativních norem, které upravují oblast poskytování certifikačních služeb nebo obchodní činnosti s tímto spojené.

Uvedené postupy jsou detailně popsány v interní dokumentaci:

- „**Směrnice pro pracovníky RA I.CA**“
- „**Operátor CA**“

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

I.CA je povinna zajistit neprodlené zveřejnění vydaných certifikátů, vyjma takových, u kterých si klient vymínil, že nebudou zveřejňovány.

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

V případech vydání prvotního certifikátu, resp. následného certifikátu při dostavení se žadatele/zmocnitele na RA, získá oznámení o vydaném certifikátu pracovník RA.

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

Veškeré subjekty, které při své činnosti používají nebo využívají certifikáty vydané I.CA, případně poskytují, používají nebo využívají služby I.CA spojené se správou certifikátů, jsou povinny dodržovat odpovídající CP a legislativní normy platné v ČR.

#### **4.5.1 Použití soukromého klíče a certifikátu držitelem, podepisujícím, resp. šifrujícím osobou**

**Držitelé certifikátů jsou povinni:**

- bez zbytečného odkladu podávat přesné, pravdivé a úplné informace I.CA ve vztahu k vydanému certifikátu,
- dodržovat veškerá ustanovení smlouvy o poskytování certifikační služby,
- seznámit s relevantními ustanoveními příslušné smlouvy o poskytování certifikační služby o vydání a používání certifikátu případné podepisující osoby a dbát na jejich dodržování ze strany těchto osob,
- dodržovat odpovídající CP a legislativní normy platné v ČR.

Držitel certifikátu, který nedodrží či nedodržel své povinnosti, nemá nárok na případnou náhradu škody.

***Podepisující, šifrující, autentizující se osoba je povinna:***

- zacházet s prostředky jakož i se soukromým klíčem s náležitou péčí tak, aby nemohlo dojít k jejich neoprávněnému použití,
- uvědomit neprodleně I.CA o tom, že hrozí nebezpečí zneužití jejího soukromého klíče,
- dodržovat veškerá relevantní ustanovení smlouvy o poskytování certifikační služby, vztahující se ke certifikátu, se kterými byla seznámena jeho případným držitelem,
- dodržovat odpovídající CP a legislativní normy platné v ČR.

Podepisující osoba, která nedodrží či nedodržela své povinnosti, nemá nárok na případnou náhradu škody.

#### **4.5.2 Použití veřejného klíče a certifikátu spoléhající se stranou**

***Spoléhající se strany jsou povinny:***

- užívat certifikáty vydané dle odpovídající CP, v souladu s ní a s legislativními normami platnými v ČR,
- provádět veškeré úkony potřebné k tomu, aby si ověřily, že proces elektronického podpisu, šifrování, autentizace je platný a odpovídající certifikát nebyl zneplatněn,
- kontrolovat elektronický podpis a důvěrnost certifikátu CA.

Uživatel, který nedodrží či nedodržel své povinnosti, nemá nárok na případnou náhradu škody. I.CA a smluvní partneři jsou povinni upozornění na povinnosti uživatelů zveřejnit prostřednictvím svých kontaktních adres.

#### **4.6 Obnovení certifikátu**

Služba obnovení již zneplatněného certifikátu není poskytována.

#### **4.7 Výměna veřejného klíče v certifikátu**

##### **4.7.1 Podmínky pro výměnu veřejného klíče v certifikátu**

- Certifikáty pro účely elektronického podpisu:
  - Jedinou akceptovatelnou formou získání následného osobního certifikátu, je certifikát, vydaný na základě nové žádosti o vydání certifikátu, elektronicky podepsané platnými daty pro vytváření elektronických podpisů, souvisejícími s již vydaným certifikátem, ke kterému

je vydáván tento následný certifikát. I.CA si vyhrazuje právo akceptování i jiných forem postupů při vydávání následných certifikátů.

- Akceptovatelnými formami získání následného certifikátu serveru jsou žádosti o vydání certifikátu serveru, elektronicky podepsané platnými daty pro vytváření elektronických podpisů, souvisejícími s již vydaným certifikátem serveru, ke kterému je vydáván tento následný certifikát serveru, resp. elektronicky podepsané platnými daty pro vytváření elektronických podpisů, souvisejícími s vydaným osobním certifikátem k tomuto certifikátu serveru.
- Certifikáty pro ostatní účely – uvedeno v rámci jednotlivých obchodních produktů.

I.CA si vyhrazuje právo akceptování i jiných forem postupů při vydávání následných certifikátů.

#### 4.7.2 Subjekty oprávněné požadovat výměnu veřejného klíče v certifikátu

Výměnu veřejného klíče jsou oprávněni požadovat držitelé certifikátu, podepisující, šifrující, autentizující se osoby, popř. jejich zmocněnci.

#### 4.7.3 Zpracování požadavku na výměnu veřejného klíče

- Certifikáty pro účely elektronického podpisu - Pracoviště CA ověřuje údaje (DN) žádosti o následný certifikát, které musí být stejné jako údaje (DN) v prvotním certifikátu, pouze veřejný klíč musí být jiný. Ostatní položky následného certifikátu podléhají aktuálním pravidlům pro certifikáty.
  - Osobní certifikáty – v případě, že je žádost zaslána na I.CA elektronickou cestou, musí být elektronicky podepsána soukromým klíčem, souvisejícím s platným osobním certifikátem, ke kterému je žádáno o následný certifikát. Pokud žádost nemá výše uvedené náležitosti, např. je sice elektronicky podepsána, ale tento elektronický podpis nelze ověřit veřejným klíčem, uvedeným v původním a následném certifikátu, I.CA následný certifikát nevydá.
  - Certifikáty serveru – v případě, že je žádost zaslána na I.CA elektronickou cestou, musí být elektronicky podepsána soukromým klíčem, souvisejícím s platným certifikátem serveru, ke kterému žádá o následný certifikát serveru, popř. elektronicky podepsána soukromým klíčem, souvisejícím s vydaným osobním certifikátem k tomuto certifikátu serveru. Pokud žádost nemá výše uvedené náležitosti, např. je sice elektronicky podepsána, ale tento elektronický podpis nelze ověřit veřejným klíčem, uvedeným ve starém a následném certifikátu serveru, I.CA následný certifikát serveru nevydá.
- Certifikáty pro ostatní účely – uvedeno v rámci jednotlivých obchodních produktů.

V případě, že se žadatel o certifikát, popř. zmocněnec dostaví s žádostí na RA, je postupováno obdobně, jako při vydávání prvotního certifikátu.

#### 4.7.4 Oznámení o vydání certifikátu s vyměněným veřejným klíčem

V případě, že se žadatel o následný certifikát, popř. zmocněnec se žádostí o vydání následného certifikátu dostaví na RA, je informován prostřednictvím pracovníka RA. V případě, že žadatel o následný certifikát zaslal žádost prostřednictvím elektronické pošty, je mu tento následný certifikát na tuto adresu elektronicky zaslán.

<b>Certifikační prováděcí směrnice vydávání komerčních certifikátů</b>	<b>Strana 30 (celkem 61)</b>
<b>Copyright © První certifikační autorita, a.s.</b>	

#### **4.7.5 Úkony spojené s převzetím certifikátu s vyměněným veřejným klíčem**

Pokud byly splněny podmínky pro vydání následného certifikátu, tzn.:

- splnění podmínek uvedených v kapitolách 3.3.1 a 4.7.1,
- zaplacení určeného poplatku (není-li smluvně stanoveno jinak) – viz aktuální ceník na <http://www.ica.cz>,

je žadatel o certifikát povinen tento certifikát přijmout. Jediným způsobem, jakým může postupovat v případě, že nemá zájem certifikát převzít, je zažádat v souladu s touto CPS o jeho zneplatnění.

V případě podání žádosti o vydání následného certifikátu elektronickou cestou, zašle I.CA na žadatelovu elektronickou adresu certifikát v předepsaných formátech, v případě vyřizování žádosti na RA, získá žadatel certifikát od pracovníka RA.

#### **4.7.6 Zveřejnění vydaných certifikátů s vyměněným veřejným klíčem**

I.CA je povinna zajistit neprodlené zveřejnění následného certifikátu.

#### **4.7.7 Oznámení o vydání certifikátu s vyměněným veřejným klíčem jiným subjektům**

V případech vydání následného certifikátu při dostavení se žadatele o certifikát, popř. zmocněnce na RA, získá oznámení o vydaném certifikátu pracovník RA.

### **4.8 Změna údajů v certifikátu**

Služba není poskytována.

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

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

Certifikát může být zneplatněn pouze na základě následujících okolností:

- držitel certifikátu nebo jím oprávněná osoba požádá o jeho zneplatnění,
- na základě klientova sdělení se věcný obsah certifikátu stane neplatným,
- na základě zjištění I.CA nebo spolupracujících subjektů se věcný obsah certifikátu stane neplatným,
- držitel certifikátu byl usvědčen ze závažného porušení smluvních povinností nebo povinností vyplývajících z CP,
- je důvodné podezření, že došlo ke kompromitaci soukromého klíče držitele nebo disponenta certifikátu,
- dojde ke kompromitaci soukromého klíče CA,
- nařídí tak soud ve svém rozsudku nebo předběžném opatření,
- držitel certifikátu zemřel.

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

O zneplatnění certifikátu může požádat:

- držitel certifikátu nebo oprávněný disponent,
- registrační autorita, jejímž prostřednictvím bylo požádáno o jeho vydání,
- I.CA,

<b>Certifikační prováděcí směrnice vydávání komerčních certifikátů</b>	<b>Strana 31 (celkem 61)</b>
<b>Copyright © První certifikační autorita, a.s.</b>	

- soud prostřednictvím oprávněné osoby,
- osoby oprávněné z pozůstalostního řízení .

Držitel certifikátu nebo oprávněný disponent musí zaslat nebo osobně předat žádost o zneplatnění certifikátu způsobem uvedeným v kapitole 3.4.

V případě, že se zneplatnění uskutečňuje na základě soudního rozhodnutí, musí pracovník RA k záznamu o zneplatnění přiložit kopii soudního rozhodnutí.

V případě, že se zneplatnění uskutečňuje na základě pozůstalostního řízení, musí pracovník RA k záznamu o zneplatnění přiložit kopii dokladů, ze kterých jednoznačně vyplývá právo žádajícího na zneplatnění.

V případě, že zneplatnění se uskutečňuje z iniciativy RA nebo I.CA, je příslušný pracovník povinen zaznamenat tuto skutečnost do protokolu včetně důvodů tohoto rozhodnutí.

Lhůta pro provedení zneplatnění je stanovena na 24 hodin.

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

Po splnění podmínek na identifikaci a autentizaci (kapitola 3.4), je postupováno následujícím způsobem:

- Osobní předání písemné žádosti o zneplatnění certifikátu na RA – operátor RA musí zkontrolovat totožnost klienta nebo vyžadovat sdělení hesla pro zneplatnění příslušného certifikátu.
- Pomocí elektronické pošty ([revoke@ica.cz](mailto:revoke@ica.cz)) - zaslání elektronické poštovní zprávy podepsané soukromým klíčem, souvisejícím s příslušným certifikátem o jehož zneplatnění se žádá. .
- Zaslání běžné poštovní zprávy společně s heslem pro zneplatnění certifikátu, zadaném při uzavírání smlouvy s I.CA. na adresu:

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

- Prostřednictvím elektronického formuláře, který je za tímto účelem přístupný na vyhrazené webové stránce (<http://www.ica.cz>).

Elektronická žádost o zneplatnění certifikátu je textová zpráva, která musí obsahovat větu "Žádám o zneplatnění mého certifikátu, sériové číslo XXXXXX".

V případě, že se zneplatnění uskutečňuje na základě soudního rozhodnutí, musí pracovník RA k záznamu o zneplatnění přiložit kopii soudního rozhodnutí.

V případě, že se zneplatnění uskutečňuje na základě pozůstalostního řízení, musí pracovník RA k záznamu o zneplatnění přiložit kopii dokladů, ze kterých jednoznačně vyplývá právo žádajícího na zneplatnění.

V případě, že zneplatnění se uskutečňuje z iniciativy RA nebo I.CA, je příslušný pracovník povinen zaznamenat tuto skutečnost do protokolu včetně důvodů tohoto rozhodnutí.

Lhůta pro provedení zneplatnění je stanovena na 24 hodin.

<b>Certifikační prováděcí směrnice vydávání komerčních certifikátů</b>	<b>Strana 32 (celkem 61)</b>
<b>Copyright © První certifikační autorita, a.s.</b>	

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

Služba není poskytována.

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

Odpovědí I.CA na platnou žádost o zneplatnění certifikátu je vytvoření a zaslání aktuálního seznamu zneplatněných certifikátů. Do doby zveřejnění CRL je dotyčný certifikát zablokován. Maximální prodloužení mezi přijetím požadavku na zneplatnění certifikátu a uvedením v seznamu zneplatněných certifikátů a zveřejněním tohoto seznamu, může činit nejvýše 25 hodin.

Po dobu zablokování je certifikát platný a případná odpovědnost za škodu vzniklou použitím takového certifikátu v době jeho zablokování je na straně klienta.

Odblokování certifikátu, který byl zablokován na základě platné žádosti o zneplatnění certifikátu I.CA nepovoluje.

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

Pro tyto účely jsou spoléhající se strany povinny používat CRL, vydaná a elektronicky podepsaná I.CA. Neověření certifikátu pomocí CRL je bráno jako hrubé porušení odpovídající CP.

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

Seznam zneplatněných certifikátů je společností První certifikační autorita, a.s. vydáván v pravidelných intervalech, uvedených v kapitole 2.3.

Činnosti operátorů CA v procesu vytváření a vydávání CRL jsou popsány v interním dokumentu:

- „Operátor CA“.

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

Maximální prodloužení mezi přijetím požadavku na zneplatnění certifikátu a uvedením v seznamu zneplatněných certifikátů a zveřejněním tohoto seznamu, může činit nejvýše 25 hodin.

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

Služba není poskytována.

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

Služba není poskytována.

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

Služba není poskytována.

#### **4.9.12 Případné odlišnosti postupu zneplatnění v případě kompromitace soukromého klíče**

Služba není poskytována.



<b>Certifikační prováděcí směrnice vydávání komerčních certifikátů</b>	<b>Strana 33 (celkem 61)</b>
<b>Copyright © První certifikační autorita, a.s.</b>	

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

Služba není poskytována.

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

Služba není poskytována.

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

Služba není poskytována.

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

Služba není poskytována.

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

#### **4.10.1 Funkční charakteristiky**

Seznamy veřejných certifikátů jsou poskytovány formou zveřejňování informací, seznamy zneplatněných certifikátů jsou poskytovány jak formou zveřejňování informací, tak uvedením distribučních míst CRL ve vydaném certifikátu.

#### **4.10.2 Dostupnost služeb**

I.CA zajišťuje nepřetržitou dostupnost služeb, uvedených v kapitole 4.10.1. Postup je uveden v interních dokumentech I.CA :

- „*Operátor CA*“,
- „*Příručka administrátora*“,
- „*Obnova komponenty provozního pracoviště*“,
- „*Přemístění provozního pracoviště*“.

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

Další služby, kromě těch, které jsou uvedené v kapitole 4.10.1, nejsou poskytovány.

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

Ukončení služeb (obchodní vztah) mezi držitelem a I.CA končí ve chvíli, kdy skončila platnost držitelova certifikátu, aniž by držitel předtím požádal o vydání následného certifikátu.

<i>Certifikační prováděcí směrnice vydávání komerčních certifikátů</i>	<i>Strana 34 (celkem 61)</i>
<i>Copyright © První certifikační autorita, a.s.</i>	

#### **4.12 Úschova soukromého klíče u důvěryhodné třetí strany a jejich obnova**

Služba není poskytována.

<b>Certifikační prováděcí směrnice vydávání komerčních certifikátů</b>	<b>Strana 35 (celkem 61)</b>
<b>Copyright © První certifikační autorita, a.s.</b>	

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

Oblasti managementu provozní a fyzické bezpečnosti jsou řešeny jak v základních dokumentech Celková bezpečnostní politika, Systémová bezpečnostní politika CA, Plán pro zvládání krizových situací a plán obnovy, tak v upřesňujících bezpečnostních normách a směrnících. Uvedené dokumenty reflektují výsledky periodicky provedené analýzy rizik.

### **5.1 Fyzická bezpečnost**

Problematika fyzické bezpečnosti je detailně uvedena v interní dokumentaci, zejména:

- *„Řízení fyzického přístupu do místností I.CA“*,
- *„Požární bezpečnost“*,
- *„Bezpečnostní incidenty“*,
- *„Příručka administrátora“*,
- *„Příprava uchovávaných informací“*,
- *„Záloha dat provozních systémů“*,
- *„Obnova komponenty provozního pracoviště“*,
- *„Přemístění provozního pracoviště“*,
- *„HSM/Private Server“*.

#### **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**

Požadavky na fyzický přístup do jednotlivých vyhrazených prostor (chráněných mechanickými a elektronickými prostředky) provozních pracovišť jsou uvedeny v interní dokumentaci společnosti. Ochrana objektů je řešena elektronickým zabezpečovacím systémem (EZS), připojením na pult centrální ochrany (PCO) a případně 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 je dostatečně dimenzovaná aktivní klimatizace, která udržuje celoroční teplotu v rozmezí 20°C ± 5°C. Přívod elektrické energie je jištěn pomocí UPS (Uninterruptible Power Supply) a diesel agregátu.

#### **5.1.4 Vliv vody**

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

<b>Certifikační prováděcí směrnice vydávání komerčních certifikátů</b>	<b>Strana 36 (celkem 61)</b>
<b>Copyright © První certifikační autorita, a.s.</b>	

### 5.1.5 Protipožární opatření a ochrana

V objektech provozních pracovišť 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.

### 5.1.8 Zálohy mimo budovu

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

## 5.2 Procesní bezpečnost

Implementovaná bezpečnostní opatření v oblasti procesní bezpečnosti jsou detailně popsána v upřesňujících interních bezpečnostních normách a směrnících a zahrnují problematiku, uvedenou v podkapitolách 5.2.1 až 5.2.4.

### 5.2.1 Důvěryhodné role

Pro činnosti, spojené s provozováním certifikačních služeb, jsou ve společnosti I.CA definovány důvěryhodné role. Základní činnosti a odpovědnosti osob v důvěryhodných rolích je definován v interní dokumentaci, zejména:

- „**Systémová bezpečnostní politika CA**“,
- „**Příručka administrátora**“.

### 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.

<b>Certifikační prováděcí směrnice vydávání komerčních certifikátů</b>	<b>Strana 37 (celkem 61)</b>
<b>Copyright © První certifikační autorita, a.s.</b>	

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 jsou přiděleny prostředky pro řádnou autentizaci k těm komponentám, které jsou pro jejich činnost nezbytné - upraveno interními směrnici:

- „**Směrnice pro pracovníky RA I.CA**“,
- „**Operátor CA**“,
- „**Příručka administrátora**“.

### 5.2.4 Role vyžadující rozdělení povinností

Role, vyžadující rozdělení povinností v procesu poskytování kvalifikovaných certifikačních služeb v oblasti certifikátů, jsou definované v interní bezpečnostní dokumentaci „**Systémová bezpečnostní politika CA**“.

## 5.3 Personální bezpečnost

Oblast personální bezpečnosti je uvedena v interní dokumentaci „**Kontrolní činnost, bezúhonnost a odbornost**“.

### 5.3.1 Požadavky na kvalifikaci, zkušenosti a bezúhonnost

Pracovníci v rolích administrátor bezpečnosti, operátor CA, auditor systému, administrátor systému, ředitel společnosti, bezpečnostní manager, manager pro zvládání krizových situací a plánu obnovy, bezpečnostní auditor jsou přijímáni na základě dále popsaných 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 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,

<b>Certifikační prováděcí směrnice vydávání komerčních certifikátů</b>	<b>Strana 38 (celkem 61)</b>
<b>Copyright © První certifikační autorita, a.s.</b>	

- veřejné zdroje informací .

Pracovníci poskytují prvotní informace osobním pohovorem při přijímání do pracovního poměru, které aktualizují při periodických pohovorech s nadřízeným 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 periodicita školení**

Pro kmenové pracovníky pořádá vedení I.CA minimálně jedenkrát ročně interní výukový seminář, zaměřený na problematiku poskytování certifikačních služeb.

### **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. Změna role je možná pouze v mimořádných případech (epidemické onemocnění, atp.) jako dočasné opatření.

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

Při zjištění neautorizované činnosti je dotyčný pracovník sankcionován podle rozsahu až do výše okamžitého propuštění a řídí se zákoníkem práce. Tento postih 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 SRA, externí zhotovitele programového aplikačního vybavení, dodavatele hardware, systémového programového vybavení, externí 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 CP i příslušné normy, směrnice, příručky a metodické pokyny, potřebné pro výkon jejich činnosti.

## 5.4 Auditní záznamy (logy)

Problematika spojená s vytvářením, zpracováním a uchováváním auditních logů je detailně řešena v interní dokumentaci:

- „*Příručka administrátora*“,
- „*Příprava uchovávaných informací*“,
- „*Záloha dat provozních systémů*“,
- „*Dokumenty agendy certifikačních služeb*“.

### 5.4.1 Typy zaznamenávaných událostí

Do elektronického auditního logu jsou zaznamenávány události, uvedené v kapitole 5.5.1. 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 jednou měsíčně, v případě bezpečnostního incidentu okamžitě.

### 5.4.3 Doba uchovávání auditních záznamů

Doba, po kterou se uchovávají auditní záznamy, je stanovena na minimálně 10 let od jejich vzniku.

### 5.4.4 Ochrana auditních záznamů

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 auditních záznamů na médium, které je umístěno mimo provozní prostory I.CA.

### 5.4.5 Postupy pro zálohování auditních záznamů

Zálohování auditních záznamů probíhá obdobným způsobem jako zálohování ostatních elektronických informací.

### 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.

<b>Certifikační prováděcí směrnice vydávání komerčních certifikátů</b>	<b>Strana 40 (celkem 61)</b>
<b>Copyright © První certifikační autorita, a.s.</b>	

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

V případě neoprávněných pokusů není subjekt informován o zapsání události do auditního záznamu.

#### 5.4.8 Hodnocení zranitelnosti

V I.CA byly provedeny následující činnosti:

- stanovení aktiv (programové vybavení, technické vybavení, data) a jejich vazeb,
- hodnocení aktiv informačního systému,
- stanovení relevantních hrozeb a zranitelností,
- hodnocení hrozeb a zranitelností,
- určení míry rizika pro každou kombinaci aktiva (skupiny aktiv), hrozby a zranitelnosti.

### 5.5 Uchovávání informací a dokumentace

Uchovávání informací a dokumentace je detailně popsány v upřesňující interní bezpečnostní dokumentaci, zahrnující problematiku, uvedenou v podkapitolách 5.5.1 až 5.5.7.

Problematika spojená s uchováváním informací a dokumentace je detailně řešena v interní dokumentaci:

- **„Řízení fyzického přístupu do místností I.CA“**,
- **„Příprava uchovávaných informací“**,
- **„Záloha dat provozních systémů“**,
- **„Příručka administrátora“**,
- **„Dokumenty agendy certifikačních služeb“**.

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

I.CA a s ní spolupracující RA zaznamenávají do auditního logu, následující události:

- záznam o registraci žadatele,
- záznam o pokusu neoprávněné registrace žadatele,
- záznam o zrušení registrace žadatele (údaje o žadateli se uchovávají),
- záznam o požadavku RA na vystavení certifikátu včetně výsledku,
- záznam o požadavku na následný certifikát včetně výsledku,
- záznam o neoprávněném požadavku na vystavení certifikátu včetně výsledku,
- záznam o neoprávněném požadavku na následný certifikát včetně výsledku,
- záznam o požadavku na zneplatnění certifikátu včetně údajů o žádající osobě a výsledku,
- záznam o neoprávněném požadavku na zneplatnění certifikátu včetně údajů o žádající osobě a výsledku,
- záznam o pokusu neoprávněného přístupu do systému,
- záznam o zveřejnění certifikátu včetně výsledku,
- záznam o zanesení zneplatněného certifikátu do CRL,
- záznam o zveřejnění CRL.

Tyto informace a dokumenty jsou konkretizovány v interních dokumentech **„Dílčí spisový a skartační řád pro agendy certifikačních služeb“**.



<b>Certifikační prováděcí směrnice vydávání komerčních certifikátů</b>	<b>Strana 41 (celkem 61)</b>
<b>Copyright © První certifikační autorita, a.s.</b>	

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

Doba uchovávaných informací a dokumentace je uvedena v interním dokumentu „**Dílčí spisový a skartační řád pro agendy certifikačních služeb**“.

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

Uchovávané informace a dokumentace obsahují i osobní data klientů a proto je vzhledem k zákonu ČR č. 101/2000 Sb. dbáno zvýšené ochrany těchto dat. Prostory, ve kterých se uchovávané informace a dokumentace nacházejí, jsou zabezpečeny formou opatření, vycházejících z požadavků objektové a fyzické bezpečnosti.

Uchovávané informace a dokumentace jsou určeny výhradně pro interní potřebu I.CA a jsou přístupné:

- pracovníkům I.CA v důvěryhodných rolích,
- 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.

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 (viz kapitola 5.5.1) 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. Samotná problematika přípravy a způsobu ukládání informací a dokumentace v elektronické i písemné podobě je upravena interními normami a směnicemi, uvedenými v záhlaví kapitoly 5.5 a dokumentem „**Dílčí spisový a skartační řád pro agendy certifikačních služeb**“.

Shromažďování archivních záznamů je evidováno.

Samotná problematika přípravy a způsobu ukládání informací a dokumentace v elektronické i písemné podobě je upravena interními normami a směnicemi, uvedenými v záhlaví kapitoly 5.5 a dokumentem „**Dílčí spisový a skartační řád pro agendy certifikačních služeb**“.

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

Pracoviště, kde jsou informace a dokumentace uchovávány, obsahuje jejich seznam včetně data uložení.

## 5.6 Výměna veřejného klíče v certifikátu poskytovatele

V případě standardních situací (uplynutí platnosti certifikátu) je výměna s dostatečným časovým předstihem (minimálně jeden rok před uplynutím doby platnosti tohoto certifikátu) prováděna formou vydání nového certifikátu poskytovatele. V případě nestandardních situací (např. dojde-li k takovému vývoji kryptoanalytických metod, že by mohla být ohrožena bezpečnost procesu vytváření 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 veřejného klíče v nadřazeném kvalifikovaném systémovém certifikátu poskytovatele veřejnosti s předstihem (je-li to možné) vhodnou formou sdělena.

## 5.7 Obnova po havárii nebo kompromitaci

### 5.7.1 Postup v případě incidentu a kompromitace

Postupy jsou uvedeny v interních dokumentech, zejména:

- „*Plán pro zvládání krizových situací a plán obnovy*“,
- „*Obnova komponenty provozního pracoviště*“,
- „*Přemístění provozního pracoviště*“,
- „*Bezpečnostní incidenty*“.

### 5.7.2 Poškození výpočetních prostředků, software nebo dat

V případě poškození výpočetních prostředků, softwaru nebo dat postupuje I.CA v souladu s interními dokumenty, zejména:

- „*Plán pro zvládání krizových situací a plán obnovy*“,
- „*Obnova komponenty provozního pracoviště*“,
- „*Přemístění provozního pracoviště*“.

### 5.7.3 Postup při kompromitaci soukromého klíče poskytovatele

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

- ukončí jejich používání,
- okamžitě a trvale zneplatní příslušný certifikát CA a jemu odpovídající soukromý klíč,
- zneplatní všechny certifikáty, které byly těmito daty podepsány,
- bezodkladně:
  - o této skutečnosti, včetně důvodu informuje na své internetové informační adrese,
  - pro zpřístupnění této informace je využit i seznam zneplatněných certifikátů, čímž je zajištěna dostupnost této informace minimálně dvěma na sobě nezávislými způsoby, umožňujícími dálkový přístup a jsou nepřetržitě dostupné,
- 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 certifikátu CA,
- v případě vzniku důvodné obavy ze zneužití soukromého klíče pro podepisování vydávaných certifikátů a seznamů zneplatněných certifikátů, nabídne I.CA výše uvedeným držitelům bezplatné

<b>Certifikační prováděcí směrnice vydávání komerčních certifikátů</b>	<b>Strana 43 (celkem 61)</b>
<b>Copyright © První certifikační autorita, a.s.</b>	

vydání nového certifikátu s tím, že případné náklady na vydání nových certifikátů sama hradí. Postup je stejný jako při vydání prvotního certifikátu.

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

V případě havárie postupuje I.CA v souladu s interními dokumenty, zejména:

- „*Plán pro zvládnutí krizových situací a plán obnovy*“,
- „*Obnova komponenty provozního pracoviště*“,
- „*Přemístění provozního pracoviště*“.

#### **5.8 Ukončení činnosti CA nebo RA**

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:

- zpřístupnění informace o ukončení své činnosti všem osobám spoléhajícím na certifikát, držitelům a jiným osobám, se kterými má smluvní nebo jiné obdobné vztahy týkající se poskytování certifikačních služeb,
- ukončí vydávání všech typů certifikátů,
- uchování údajů získaných při registraci a záznamů událostí po dobu, nejméně 10 let od ukončení platnosti vydaných certifikátů,
- prokazatelně zničí svůj soukromý klíč,
- vyvine maximální úsilí pro to, aby platné certifikáty byly převzaty jinou certifikační autoritou.

## 6 Technická bezpečnost

### 6.1 Generování a instalace párových dat

#### 6.1.1 Generování párových dat

Generování párových dat I.CA, které probíhá v zabezpečené zóně a o jehož průběhu je vyhotoven písemný protokol, je prováděno v kryptografickém modulu.

I.CA používá pro párová data, sloužící k podepisování vydávaných certifikátů a seznamů zneplatněných certifikátů délku 2048 bitů.

V průběhu procesu generování párových dat I.CA, sloužících k podepisování vydávaných certifikátů a seznamů zneplatněných certifikátů, musí být fyzicky přítomni:

- ředitel I.CA nebo jím jmenovaný člen vedení I.CA,
- bezpečnostní manager nebo bezpečnostní administrátor (konkrétně určí ředitel I.CA),
- administrátor systému, nebo jiný pověřený technicky proškolený pracovník I.CA.

Konkrétní technický postup generace párových dat I.CA, sloužících k označování, resp. podepisování vydávaných certifikátů a seznamů zneplatněných certifikátů a následné vyhotovení certifikátu CA, příslušného k těmto párovým datům, je popsán v interní dokumentaci I.CA:

- „**Rízení fyzického přístupu do místností I.CA**“ ,
- „**HSM/Private Server**“ .

O průběhu generování párových dat I.CA, sloužících k podepisování vydávaných certifikátů a seznamů zneplatněných certifikátů je vyhotoven písemný protokol obsahující:

- jmenný seznam přítomných pracovníků s uvedením: jména, příjmení, titulu,
- datum a čas zahájení a ukončení generace párových dat s přesností minimálně na minuty,
- místo, kde ke generaci párových dat došlo,
- popis zařízení, na kterém byla generace prováděna, umožňující jednoznačnou identifikaci tohoto zařízení,
- kompletní výpis certifikátu CA, obsahující data pro ověřování elektronických podpisů vydávaných certifikátů a seznamů zneplatněných certifikátů, obsažená v právě vygenerovaných párových datech,
- datum vyhotovení protokolu,
- vlastnoruční podpisy všech pracovníků, kteří generaci párových dat prováděli.

V případě generování párových dat, používaných v procesech správy systémových komponent I.CA, komunikaci s RA na vlastních zařízeních, jsou pracovníci I.CA a RA povinni využívat certifikáty, vydané I.CA.

I.CA z principiálních bezpečnostních důvodů neposkytuje službu generování párových dat klienta na svých zařízeních.

#### 6.1.2 Předání soukromého klíče žadateli

S ohledem na skutečnost, žadatel o certifikát generuje párová data zásadně na zařízení a v prostředí, která jsou v okamžiku jejich generování pod jeho výhradní kontrolou (viz kapitola 6.1.1), není tento proces uplatňován.

<b>Certifikační prováděcí směrnice vydávání komerčních certifikátů</b>	<b>Strana 45 (celkem 61)</b>
<b>Copyright © První certifikační autorita, a.s.</b>	

### 6.1.3 Předání veřejného klíče poskytovateli certifikačních služeb

Veřejný klíč je nutno I.CA doručit. I.CA podporuje následující způsoby doručení dat pro ověřování elektronického podpisu:

- osobně na datovém nosiči,
- zasláním prostřednictvím elektronické pošty.

Vydání prvotního certifikátu je možné pouze osobně. Pro následné certifikáty lze použít obou z výše uvedených způsobů předání. Veřejný klíč je součástí žádosti o vydání certifikátu.

### 6.1.4 Poskytování veřejného klíče CA spoléhajícím se stranám

Veřejný klíč CA, sloužící k ověřování vydaných certifikátů a seznamů zneplatněných certifikátů, je obsažen v certifikátu CA, jehož získání je garantováno následujícími způsoby:

- obdržení na RA (osobní návštěva),
- prostřednictvím internetových informačních adres I.CA.

Každý žadatel o certifikát obdrží certifikát 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 podepisování vydávaných certifikátů a seznamů zneplatněných certifikátů je 2048 bitů.

Mohutnost klíčů v RSA na straně klienta závisí na klientovi, pro vybraný algoritmus však nesmí být nižší než stanovená hodnota/hodnoty, uvedené v relevantních technických standardech nebo normách. I.CA doporučuje klientům:

- testovací certifikáty - velikost klíče není stanovena,
- standardní osobní certifikáty a serverové certifikáty - minimální velikost klíče je 512 bitů, doporučená velikost klíče je 1024 bitů.

Doporučený postup generování párových dat a přípravy podkladů pro vydání I.CA certifikátu je popsán na adrese <http://www.ica.cz/>.

### 6.1.6 Generování parametrů veřejného klíče a kontrola jejich kvality

Tato certifikační politika podporuje z asymetrických algoritmů pouze algoritmus RSA. Jako hashovací funkce jsou, resp. budou, podporovány MD5, SHA1 (doporučena), resp. SHA2.

Algoritmy, použité pro generování celočíselných hodnot (např. testy prvočíselnosti atd.), musí mít parametry uvedené v relevantních technických standardech nebo normách.

I.CA kontroluje možný dvojitý výskyt stejných veřejných klíčů ve vydávaných certifikátech. V případě duplicitního výskytu veřejného klíče je žadatel o certifikát požádán o vygenerování nových párových dat. Již vydaný certifikát je neprodleně zneplatněn, držitel takového certifikátu je o tomto neprodleně informován a vyzván ke generování nových párových dat.

### 6.1.7 Omezení pro použití veřejného klíče

Uvedeno v kapitole 7.1.2.

## 6.2 Ochrana soukromého klíče a bezpečnost kryptografických modulů

Soukromý klíč certifikační autority je nejdůležitější tajemství, které každá certifikační autorita má. Obdobně i I.CA věnuje ochraně soukromého klíče maximální pozornost. Podrobný popis povolených postupů při práci se soukromým klíčem I.CA je uveden v interní dokumentaci. Pro účely této CPS platí:

- Soukromý klíč je uložen ve speciálním zařízení.
- Soukromý klíč je zálohován v zašifrované formě tak, že k jeho dešifrování je potřeba dvou určených pracovníků, kteří mají k dispozici částí tajemství.
- Neexistuje možnost získat soukromý klíč jinými metodami (např. tzv. „Escrow“).
- Soukromý klíč CA je používán výhradně k podepisování I.CA vydaných certifikátů a seznamů zneplatněných certifikátů (CRL).
- Speciální zařízení, ve kterém je uložen soukromý klíč CA, je uložen v místnosti, která má objektovou bezpečnost ve stupni „Tajné“ podle vyhlášky č. 528/2005 Národního bezpečnostního úřadu.
- V místnosti jsou použity aktivní prvky významně snižující možnost kompromitace techniky odchytem elektromagnetického vyzařování.
- Místnost se nachází v objektu, který je nepřetržitě strážěn jak lidskou strážní službou, tak speciální technikou.
- Vkládání, aktivace, deaktivace, zálohování a ničení soukromého klíče CA je prováděno v souladu s interní dokumentací, vždy v přítomnosti minimálně dvou určených pracovníků I.CA.
- Ničení soukromého klíče CA je realizováno prostředky speciálního zařízení. Záloha soukromého klíče CA, uložená v zašifrované podobě na externích médiích, je rovněž zničena. Ničení spočívá ve fyzické destrukci těchto nosičů. O průběhu ničení soukromého klíče CA, sloužícího k podepisování vydávaných certifikátů a seznamů zneplatněných certifikátů, je sepsán protokol. Při ničení soukromého klíče CA, sloužícího k podepisování vydávaných certifikátů a seznamů zneplatněných certifikátů musí být fyzicky přítomni:
  - ředitel I.CA nebo jím jmenovaný člen vedení I.CA,
  - bezpečnostní manažer nebo bezpečnostní administrátor (konkrétně určí ředitel I.CA),
  - administrátor systému, nebo jiný pověřený technicky proškolený pracovník I.CA.

Konkrétní postupy jsou popsány v interní dokumentaci I.CA:

- „*Řízení fyzického přístupu do místností I.CA*“ ,
- „*HSM/Private Server*“.

## 6.3 Počítačová bezpečnost

### 6.3.1 Specifické technické požadavky na počítačovou bezpečnost

Bezpečnost použitých komponent informačních systémů pro poskytování kvalifikovaných certifikačních služeb v oblasti vydávání certifikátů je uvedeno v dokumentu CWA 14167-1 - Security Requirements for Trustworthy Systems Managing Certificates for Electronic Signatures - Part 1: System Security Requirements.

Konkrétní řešení specifických technických požadavků počítačové bezpečnosti je popsáno v interní dokumentaci, zejména:

- „*Systémová bezpečnostní politika CA*“,
- „*Plán pro zvládání krizových situací a plán obnovy*“,
- „*Obnova komponenty provozního pracoviště*“,
- „*Přemístění provozního pracoviště*“.

<b>Certifikační prováděcí směrnice vydávání komerčních certifikátů</b>	<b>Strana 47 (celkem 61)</b>
<b>Copyright © První certifikační autorita, a.s.</b>	

- „Záloha dat provozních systémů“,
- „Příprava uchovávaných informací“,
- „Příručka administrátora“,
- „Řízení fyzického přístupu do místností I.CA“,
- „HSM/Private Server“.

### 6.3.2 Hodnocení počítačové bezpečnosti

Hodnocení bezpečnosti I.CA je založeno na mezinárodních a národních standardech:

- 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 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 5280 Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile.

## 6.4 Bezpečnost životního cyklu

### 6.4.1 Řízení vývoje systému

V případě vývoje systému v oblastech provozní činnosti, systémového programového vybavení, změn v bezpečnostní dokumentační základně atd. je postupováno dle interního dokumentu „**Změnové řízení**“.

### 6.4.2 Kontroly řízení bezpečnosti

Soulad se standardy (viz kapitola 0) je ověřován pravidelnými audity a kontrolami bezpečnostní shody. Tato problematika je popsána v interním dokumentu „**Kontrolní činnost, bezúhonnost a odbornost**“.

I.CA si vyhrazuje právo provádění i jiných typů kontrol, resp. auditů.

### 6.4.3 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), 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,

<b>Certifikační prováděcí směrnice vydávání komerčních certifikátů</b>	<b>Strana 48 (celkem 61)</b>
<b>Copyright © První certifikační autorita, a.s.</b>	

- využití – na základě rozhodnutí vedení organizace provedení nápravných opatření.

## 6.5 Síťová bezpečnost

V prostředí I.CA nejsou prostředky provádějící vlastní certifikační služby přímo dostupné z veřejné sítě Internet. Informační systém je chráněn přístupovým routerem (firma Cisco) a produktem typu firewall. Veškerá komunikace mezi RA a CA je vedena šifrovaně.

Detailní řešení řízení síťové bezpečnosti je popsáno v interní dokumentaci:

- „**Systémová bezpečnostní politika CA**“,
- „**Příručka administrátora**“,
- „**Firewall – provozní pracoviště**“,
- „**Plán pro zvládání krizových situací a plán obnovy**“,
- „**Obnova komponenty provozního pracoviště**“,
- „**Přemístění provozního pracoviště**“.

## 6.6 Časová razítka

Řešení je uvedeno v kapitole 5.5.5.



## 7 Profily certifikátu, seznamu zneplatněných certifikátů a OCSP

### 7.1 Profil certifikátu

Profily certifikátů odpovídají doporučením RFC 3280. Délka klíče, podepisujícího vydávané certifikáty a seznamy zneplatněných certifikátů je 2048 bitů, minimální délka klíče vydávaného certifikátu je 512 bitů. Základní položky jsou uvedeny v Tabulce 6.

Tabulka 6 – Profil certifikátu

<b>Položka</b>	<b>Hodnota</b>
Version	verze 3
Serial Number	jedinečné číslo vydaného certifikátu
SignatureAlgorithm	algoritmus pro elektronický podpis vydávaného certifikátu
Issuer	viz Tabulka 6a
Validity <ul style="list-style-type: none"> <li>• NotBefore</li> <li>• NotAfter</li> </ul>	datum a UTC čas počátku platnosti certifikátu datum a UTC čas konce platnosti certifikátu
Subject	označení držitele certifikátu (viz kapitola 3.1)
SubjectPublicKeyInfo <ul style="list-style-type: none"> <li>• algorithm</li> <li>• SubjectPublicKey</li> </ul>	identifikátor algoritmu veřejného klíče certifikátu veřejný klíč držitele certifikátu
Signature algorithm <ul style="list-style-type: none"> <li>• algorithm</li> <li>• parameters</li> </ul>	algoritmus pro elektronický podpis vydávaného certifikátu volitelné parametry
Extensions	rozšíření certifikátu (viz Tabulka 7)
signatureValue	elektronický podpis vydaného certifikátu

Tabulka 6a – položka Issuer

<b>Položka</b>	<b>Hodnota</b>
Organization (O)	První certifikační autorita a.s.
CommonName (CN)	I.CA - Standard root certificate
Country (C)	CZ

#### 7.1.1 Číslo verze

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

#### 7.1.2 Rozšiřující položky v certifikátu

Ve vydaných certifikátech (verze 3) je použit **kritická** rozšiřující položka **Key Usage**. Položka **Basic Constraints** není použit.

Tabulka 7 – Rozšiřující položky certifikátu

<b>Položka</b>	<b>Hodnota</b>
SubjectAlternativeName <sup>12</sup> <ul style="list-style-type: none"> <li>• rfc822Name</li> </ul>	žádost – musí obsahovat @, RA – v případě pochybností žádá doložení vlastnictví adresy nebo souhlas vlastníka, za čestné prohlášení se má podpis

<sup>12</sup> V případě vydávání dvojice certifikátů (kvalifikovaný a „nekvalifikovaný“)

	smlouvy s I.CA v případě naplnění má tato položka přednost před „PKCS9_EmailAddress“ a certifikát je přednostně spojen s touto alternativní adresou.
• dNSName	Jméno DNS
• uniformResourceIdentifier	URI
• iPAddress	IP adresa
Authority Key Identifier	SHA1 hash veřejného klíče vydavatele certifikátu
Subject Key Identifier	SHA1 hash veřejného klíče vydaného certifikátu
Certificate Policies • CP	OID, uvedené v kapitole 1.2
CRL Distribution Points	[1]Distribuční místo CRL Název distribučního místa: Jméno a příjmení: URL=http://scrl dp1.ica.cz/sica04.crl [2]Distribuční místo CRL Název distribučního místa: Jméno a příjmení: URL=http://scrl dp2.ica.cz/sica04.crl  (v případě písemné smlouvy s klientem je možno doplnit klientem požadované distribuční místa CRL)
Key usage	Kritický V případě vydávání dvojice certifikátů (kvalifikovaný a „nekvalifikovaný“): <ul style="list-style-type: none"> <li>• KeyEncipherment (povinný) - nastaven,</li> <li>• DataEncipherment (povinný) - nastaven ,</li> <li>• KeyAgreement (povinný) - nastaven.</li> </ul> V ostatních případech: <ul style="list-style-type: none"> <li>• NonRepudation (povinný) - nastaven,</li> <li>• DigitalSignature (volitelný) - nastaven,</li> <li>• KeyEncipherment (volitelný) – nenastaven,</li> <li>• DataEncipherment (volitelný) - nenastaven .</li> </ul>
1.3.6.1.4.1.23624.4.3	číslo žádosti v číselném tvaru Pozn. V případě vydávání dvojice certifikátů (kvalifikovaný a „nekvalifikovaný“) na kartu Starcos v. 2.3 a vyšší, resp. Siemens

### 7.1.3 Způsoby zápisu jmen a názvů

Uvedeno v kapitole 3.1.

### 7.1.4 Omezení jmen a názvů

Pro jméno subjektu (Subject) není žádné omezení s výjimkou omezení vyplývajících z kapitoly 3.1.2. O přípustnosti konkrétního obsahu jednotlivých atributů jména subjektu (atributů položky Subject) rozhoduje s konečnou platností pracovník registrační autority, který provádí vyřizování požadavku na vydání certifikátu. V případě nesouhlasu může žadatel postupovat podle kapitoly 9.13.

## 7.2 Profil seznamu zneplatněných certifikátů

Tabulka 8 – Profil CRL

<b>Položka</b>	<b>Obsah</b>
Version	Verze v2
SignatureAlgorithm	algoritmus pro elektronický podpis vydávaného CRL ( sha1WithRSAEncryption )
Issuer	vydavatel CRL
thisUpdate	datum a UTC čas vydání CRL
nextUpdate	datum a předpokládaný UTC čas vydání následujícího CRL
revokedCertificates	seznam zneplatněných certifikátů
userCertificate	sériové číslo zneplatněného certifikátu
revocationDate	datum a čas zneplatnění certifikátu
crlEntryExtension.CRL.Reason	důvod zneplatnění certifikátu
crlExtensions	rozšíření CRL - viz 9
signatureValue	elektronický podpis vydaného CRL

### 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 9 – Rozšiřující položky CRL

<b>Položka</b>	<b>Obsah</b>
AuthorityKeyIdentifier.KeyIdentifier	hash veřejného klíče vydavatele CRL
CRLNumber	jedinečné číslo vydávaného CRL

## 7.3 Profil OCSP

Služba není poskytována.

<b>Certifikační prováděcí směrnice vydávání komerčních certifikátů</b>	<b>Strana 52 (celkem 61)</b>
<b>Copyright © První certifikační autorita, a.s.</b>	

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

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

Problematika hodnocení je upřesněna interním dokumentem „**Kontrolní činnost, bezúhonnost a odbornost**“.

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

Audit systému, poskytujícího certifikační služby je prováděn po 2 letech od předchozího auditu. Kontrola bezpečnostní shody je provedena do jednoho roku po ukončení auditu.

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

Hodnotitelem je fyzická/právnícká osoba s příslušnou certifikací, pověřená ředitelem společnosti První certifikační autorita, a.s.

### **8.3 Vztah hodnotitele k hodnocenému subjektu**

Hodnotitelem je fyzická/právnícká osoba, pověřená ředitelem společnosti První certifikační autorita, a.s.

### **8.4 Hodnocené oblasti**

Předmětem auditu a kontroly bezpečnostní shody jsou všechny systémy I.CA, poskytující certifikační služby v oblasti vydávání osobních certifikátů a certifikátů serverů.

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

V případě nedostatků, zjištěných na základě zprávy o celkové nebo částečné kontrole bezpečnostní shody (viz kapitoly 8.1, 8.4, 8.6) je bezpečnostní manager povinen do 15 dnů po obdržení zprávy určit, jaká opatření k odstranění nedostatků je I.CA povinna přijmout.

### **8.6 Sdělování výsledků hodnocení**

I.CA zajistí zpracování zprávy o kontrole bezpečnostní shody, jejímž obsahem je:

- vymezení předmětu kontroly bezpečnostní shody,
- identifikace dokumentace, která byla předmětem kontroly bezpečnostní shody ,
- popis postupu, jakým byla kontrola bezpečnostní shody prováděna,
- jméno, popřípadě jména a příjmení osoby, která kontrolu bezpečnostní shody provedla,
- prohlášení subjektu, který kontrolu bezpečnostní shody provedl, o výsledku kontroly bezpečnostní shody.

Zpráva o kontrole bezpečnostní shody je předána bezpečnostnímu managerovi do 10 dnů od ukončení kontroly, který s jejím obsahem seznámí ředitele I.CA a bezpečnostní výbor.

<b>Certifikační prováděcí směrnice vydávání komerčních certifikátů</b>	<b>Strana 53 (celkem 61)</b>
<b>Copyright © První certifikační autorita, a.s.</b>	

I.CA zajistí, že zpráva o auditu systému, poskytujícího certifikační služby, obsahuje:

- vymezení předmětu auditu, přičemž vymezením předmětu auditu se rozumí vymezení certifikačních služeb v oblasti vydávání osobních certifikátů a certifikátů serverů,
- identifikace dokumentace, která byla předmětem auditu a kterou I.CA poskytla subjektu, který audit provádí.

<b>Certifikační prováděcí směrnice vydávání komerčních certifikátů</b>	<b>Strana 54 (celkem 61)</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**

Poplatky za prvotní, popř. následný certifikát, jsou uvedeny v aktuálním ceníku služeb, který je k dispozici na internetové informační adrese I.CA. Služba obnovení certifikátu není poskytována.

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

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

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

Přístup k informacím o zneplatněných certifikátech nebo statutech certifikátů elektronickou cestou I.CA nezpoblatňuje.

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

Poplatek za předání certifikátu (prvotní, následný) prostřednictvím záznamového média (např. disketa) je uveden v aktuálním ceníku služeb, který je k dispozici na internetové informační adrese I.CA.

Zneplatnění certifikátu a stažení elektronické verze CP (v elektronické verzi ve všeobecně používaném formátu PDF) je poskytováno zdarma.

Poplatky za nadstandardní služby jsou stanovovány smluvně.

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

I.CA si vyhrazuje právo změny výše poplatku za vydání prvotního, popř. následného certifikátu. I.CA je rovněž oprávněna stanovit pro individuálně uzavřené smlouvy odlišnou výši těchto poplatků.

### **9.2 Finanční odpovědnost**

V případě, že I.CA vznikne jakákoliv škoda v přímé či nepřímé souvislosti s jednáním držitelů či uživatelů certifikátů I.CA, je I.CA oprávněna příslušnou událost vyšetřit.

Pokud bude vyšetřením zjištěno, že zjištěné skutečnosti zakládají nárok na kompenzaci ze strany držitele či uživatele certifikátu, bude tato kompenzace v souladu s příslušnými pasážemi obchodního zákoníku od příslušného subjektu vyžadována.

Vztah mezi I.CA jakožto poskytovatelem certifikačních služeb a klienty je striktně dán smlouvou. I.CA nevystupuje v žádném případě jako zmocněnec nebo jiný zástupce klientů. Totéž platí pro smluvní partnery.

<b>Certifikační prováděcí směrnice vydávání komerčních certifikátů</b>	<b>Strana 55 (celkem 61)</b>
<b>Copyright © První certifikační autorita, a.s.</b>	

### **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 provoz a 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**

Služba není poskytována.

## **9.3 Citlivost obchodních informací**

### **9.3.1 Výčet citlivých informací**

Citlivými informacemi I.CA jsou:

- veškeré soukromé klíče, příslušné k veřejným klíčům I.CA,
- ostatní kryptograficky podstatné informace sloužící k provozu I.CA,
- vybrané obchodní informace I.CA,
- veškeré informace a dokumentace s ohledem na poskytování certifikačních služeb,
- veškeré osobní údaje.

Chráněnými obchodními informacemi jednotlivých RA jsou:

- veškeré soukromé klíče, příslušné k veřejným klíčům RA,
- ostatní kryptograficky podstatné informace sloužící k provozu RA,
- veškeré informace a dokumentace s ohledem na poskytování certifikačních služeb
- veškeré osobní údaje.

Za chráněné informace se rovněž považují veškeré další informace označené některým ze subjektů jako citlivé.

S chráněnými informacemi, bez ohledu na typ nosiče, je zacházeno tak, aby byla zajištěna jejich důvěrnost a integrita.

### **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.

<b>Certifikační prováděcí směrnice vydávání komerčních certifikátů</b>	<b>Strana 56 (celkem 61)</b>
<b>Copyright © První certifikační autorita, a.s.</b>	

### 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.

### 9.3.4 Zpřístupnění informací

- Zpřístupnění informací o zneplatnění a zrušení certifikátů - informací o zneplatněných certifikátech smí obdržet libovolný uživatel.
- Zpřístupnění informací orgánům činným v trestním řízení a jiným třetím stranám - I.CA poskytne třetí straně informace označené jako citlivé pouze na základě pravomocného rozhodnutí soudu. Dále I.CA poskytne citlivé informace orgánům činným v trestním řízení pouze na základě rozhodnutí příslušného státního zástupce, a to pouze na základě písemné žádosti vybavené všemi náležitostmi.
- Zpřístupnění informací na základě občanského řízení - I.CA poskytne třetí straně informace označené jako citlivé na základě ukončeného občanského řízení (např. pozůstalým po zemřelém vlastníku certifikátu). V těchto případech se I.CA řídí příslušnými ustanoveními zákona. Konkrétní soukromé klíče, sloužící k podepisování certifikátů a CRL, neposkytne nikomu.
- Zpřístupnění na základě požadavku držitele certifikátu – v případě požadavku držitele certifikátu na zpřístupnění určených informací souvisejících s klientem a jeho certifikátem třetí straně tak I.CA učiní po kontrole vlastnického práva a na písemnou žádost.
- Ostatní okolnosti zpřístupnění informací - ostatních případech třetím stranám citlivé informace I.CA zásadně neposkytuje.

## 9.4 Ochrana osobních údajů

Ochrana osobních údajů je v I.CA řešena v souladu s požadavky zákona ČR č. 101/2000 Sb.

Osobními informacemi jsou veškeré osobní údaje klientů, uživatelů či pracovníků, podléhající ochraně ve smyslu příslušné zákonné normy (zákon ČR č. 101/2000 Sb.).

## 9.5 Práva duševního vlastnictví

Tato CPS, veškeré související dokumenty, obsah webových stránek, certifikáty CA, klíče I.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 certifikátům CA pouze k podepisování vydávaných certifikátů a seznamu zneplatněných certifikátů,
- vydávané certifikáty splňují náležitosti, uvedené v této CPS,



<b>Certifikační prováděcí směrnice vydávání komerčních certifikátů</b>	<b>Strana 57 (celkem 61)</b>
<b>Copyright © První certifikační autorita, a.s.</b>	

- zneplatní certifikáty pokud byla žádost o ukončení jejich platnosti podána způsobem definovaným v této CPS.

Veškeré záruky a z nich plynoucí plnění je možné uznat jen tehdy, pokud:

- klient neporušil povinnosti plynoucí mu ze smlouvy o poskytování certifikační služby a odpovídající CP,
- spoléhající se strana neporušila povinnosti odpovídající CP.

Klient uplatňuje záruku vždy u RA, která zpracovala jeho prvotní žádost. Pokud RA není schopna vyřídit záruční nároky ve své pravomoci, postoupí je k řízení I.CA a o této skutečnosti klienta vyrozumí. Na používání certifikátu, který I.CA nevydala, se záruky nevztahují.

I.CA poskytuje záruku na správnost použití vlastního soukromého klíče příslušného k vlastnímu certifikátu při podepisování osobních certifikátů a certifikátů pro servery. Na podepisování testovacích certifikátů se záruka neposkytuje.

I.CA poskytuje záruky na jedinečnost sériového čísla jí vydaných osobních certifikátů a certifikátů pro servery.

I.CA poskytuje záruku na použití osobních certifikátů při obchodních transakcích, jejichž hodnota nepřesahuje hodnotu uvedenou v příslušných omezeních, pokud byla dodržena odpovídající ustanovení Certifikační politiky I.CA.

Platí vždy limit záruky, který byl sjednán v písemné podobě (smlouva o poskytnutí služeb). Pokud byla výše nárokané ztráty vyšší než sjednaný limit, poskytne I.CA plnění maximálně do výše limitu. Pokud bylo zjištěno porušení povinností klienta mající souvislost s uváděnou škodou, záruční plnění se neposkytne. S touto skutečností bude klient seznámen. Tato skutečnost musí být klientovi oznámena a zaprotokolována.

Na používání certifikátu, jehož držitel není klientem I.CA se záruky nevztahují.

### **9.6.2 Zastupování a záruky RA**

RA přejímá závazek za správné vyřízení žádostí (viz kapitola 1.3.2). RA nevyřídí kladně žádost, pokud žadatel hodnověrným způsobem neprokázal svoji identitu, nedoložil údaje uvedené v žádosti o službu, odmítá potřebné údaje sdělit nebo odmítne podepsat příslušné dokumenty. Postup je popsán v této CPS. RA dále zodpovídá:

- za včasné předání žádostí o zneplatnění vydaných certifikátů k vyřízení na pracoviště CA,
- za vyřizování připomínek a stížností klientů.

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

Držitel certifikátu nebo podepisující osoba ručí za informace, jimi uvedené ve smlouvě o poskytování certifikační služby a postupují v souladu s platnou legislativou.

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

Spoléhající se strany postupují v souladu s odpovídající CP.

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

Služba není poskytována.

<b>Certifikační prováděcí směrnice vydávání komerčních certifikátů</b>	<b>Strana 58 (celkem 61)</b>
<b>Copyright © První certifikační autorita, a.s.</b>	

## 9.7 Zřeknutí se záruk

Společnost První certifikační autorita, a.s. se striktně řídí relevantní legislativou ČR a nemůže se zříci záruk, v ní určených.

## 9.8 Omezení odpovědnosti

Hranice odpovědnosti společnosti První certifikační autorita, a.s. se v oblasti poskytování certifikačních služeb řídí odpovídající CP a platnou legislativou.

## 9.9 Odpovědnost za škodu, náhrada škody

Platí vždy limit záruky, který byl sjednán v písemné podobě. Pokud výše nárokováné ztráty překračuje sjednaný limit, poskytne I.CA plnění maximálně do výše limitu. Pokud bylo zjištěno porušení povinností podepisující osoby, držitele certifikátu nebo spoléhající se osoby, mající souvislost s uváděnou škodou, záruční plnění se neposkytne. Tato skutečnost musí být klientovi oznámena a zaprotokolována.

Další možné náhrady škody vycházejí z ustanovení příslušných zákonů a o jejich výši může rozhodnout soud.

Nový certifikát bude držiteli poskytnut **zdarma** v případech:

- Důvodného podezření, že došlo ke kompromitaci soukromého klíče, popř. samotné kompromitace soukromého klíče I.CA pro podepisování vydávaných certifikátů a seznamů zneplatněných certifikátů, nabídne držitelům bezplatné vydání nového certifikátu.
- Příjem žádosti o certifikát - I.CA kontroluje při příjmu žádosti, zda již neexistuje jiný certifikát se stejným veřejným klíčem. Pokud ano, je žadatel o certifikát vyzván k vygenerování nové žádosti, a tedy i nových párových dat. Držitel již existujícího certifikátu, který vlastní veřejný klíč stejný s žadatelem o certifikát, je vyzván k vygenerování nových párových dat, jeho původní certifikát je okamžitě zneplatněn a držitel je o této skutečnosti informován. V takovém případě má držitel takto zneplatněného certifikátu nárok na vydání nového certifikátu zdarma.

## 9.10 Doba platnosti, ukončení platnosti

### 9.10.1 Doba platnosti

Tento dokument zůstává platnosti do skončení platnosti posledního certifikátu, který byl dle odpovídající CP vydán.

### 9.10.2 Ukončení platnosti

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

### 9.10.3 Důsledky ukončení a přetrvání závazků

Uvedeno v kapitole 9.10.1.

<b>Certifikační prováděcí směrnice vydávání komerčních certifikátů</b>	<b>Strana 59 (celkem 61)</b>
Copyright © První certifikační autorita, a.s.	

## 9.11 Komunikace mezi zúčastněnými subjekty

Pro individuální oznámení a komunikaci s držiteli certifikátů může I.CA využít jimi dodané e-mailové adresy, poštovní adresy, telefonická čísla nebo osobní jednání.

Podepisující osoby, držitelé certifikátů, spoléhající se strany a veřejnost mohou s I.CA komunikovat způsobem, uvedeným na adrese <http://www.ica.cz/>.

## 9.12 Změny

Postup v případě certifikačních politik je vždy popsán v konkrétní certifikační politice.

### 9.12.1 Postup při změnách

Certifikační politiky - viz kap. 9.12. V případě této CPS - postup je realizován řízeným procesem uvedeném v interním dokumentu „**Změnové řízení**“.

### 9.12.2 Postup při oznamování změn

Certifikační politiky - viz kap. 9.12. V případě této CPS - vydání nové verze je vždy oznámeno formou zveřejňování informací.

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

Certifikační politiky - viz kap. 9.12. V případě této CPS - OID není přiřazován.

## 9.13 Řešení sporů

Tato CPS a odpovídající CP, jejich výklad a aplikace se řídí platnou legislativou.

V případě, že držitel certifikátu, spoléhající se strana, žadatel o certifikát nebo smluvní partner nesouhlasí s předloženým výkladem, mohou použít následující stupně odvolání:

- odpovědný pracovník RA,
- odpovědný pracovník I.CA (nutné písemné podání),
- ředitel I.CA (nutné písemné podání a složení finanční jistiny, která je vrácena v případě kladného vyřízení stížnosti).

Uvedený postup dává nesouhlasící straně možnost prosazovat svůj názor rychlejším způsobem, než soudní cestou.

## 9.14 Rozhodné právo

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

## 9.15 Shoda s právními předpisy

Systém poskytování certifikačních služeb v oblasti vydávání certifikátů je provozován ve shodě s požadavky platné legislativy.

<i>Certifikační prováděcí směrnice vydávání komerčních certifikátů</i>	<i>Strana 60 (celkem 61)</i>
<i>Copyright © První certifikační autorita, a.s.</i>	

## **9.16 Další ustanovení**

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 prováděcí směrnice vydávání komerčních certifikátů</i>	<i>Strana 61 (celkem 61)</i>
<i>Copyright © První certifikační autorita, a.s.</i>	

## **10 Závěrečná ustanovení**

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