

První certifikační autorita, a.s.



CERTIFIKAČNÍ PROVÁDĚCÍ SMĚRNICE VYDÁVÁNÍ ROOT CERTIFIKÁTŮ SICA

Verze 2.1

Certifikační prováděcí směrnice vydávání root certifikátů SICA 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.

Certifikační prováděcí směrnice vydávání root certifikátů SICA	Strana 2 (celkem 48)
Copyright © První certifikační autorita, a.s.	

Tabulka 1 - Identifikace

Název	Certifikační prováděcí směrnice vydávání root certifikátů SICA
Společnost	První certifikační autorita, a.s.
Schválil	Ředitel společnosti První certifikační autorita, a.s.

Tabulka 2 – Vývoj dokumentu

Verze	Datum vydání	Shrnutí změn
1.00	22.02.2002	První verze dokumentu
2.0	01.02.2008	Převedení na strukturu dle RFC 3647
2.1	22.09.2015	Aktualizace a revize dokumentu

Certifikační prováděcí směrnice vydávání root certifikátů SICA	Strana 3 (celkem 48)
Copyright © První certifikační autorita, a.s.	

Obsah

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

Certifikační prováděcí směrnice vydávání root certifikátů SICA	Strana 4 (celkem 48)
Copyright © První certifikační autorita, a.s.	

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

Certifikační prováděcí směrnice vydávání root certifikátů SICA	Strana 5 (celkem 48)
Copyright © První certifikační autorita, a.s.	

4.10.13	Podmínky pro pozastavení platnosti certifikátu.....	22
4.10.14	Subjekty oprávněné požadovat pozastavení platnosti certifikátu.....	22
4.10.15	Zpracování požadavku na pozastavení platnosti certifikátu.....	22
4.10.16	Omezení doby pozastavení platnosti certifikátu.....	22
4.11	SLUŽBY SOUVISEJÍCÍ S OVĚŘOVÁNÍM STATUTU CERTIFIKÁTU.....	22
4.11.1	Funkční charakteristiky.....	22
4.11.2	Dostupnost služeb.....	22
4.11.3	Další charakteristiky služeb statutu certifikátu.....	22
4.12	UKONČENÍ POSKYTOVÁNÍ SLUŽEB PRO DRŽITELE CERTIFIKÁTU OZNAČUJÍCÍ OSOBOU.....	23
4.13	ÚSCHOVA DAT PRO VYTVÁŘENÍ ELEKTRONICKÝCH ZNAČEK U DŮVĚRYHODNÉ TŘETÍ STRANY A JEJICH OBNOVA	23
4.13.1	Politika a postupy při úschově a obnovování dat pro elektronických značek.....	23
4.13.2	Politika a postupy při zapouzdřování a obnovování šifrovacího klíče pro relaci.....	23
5	MANAGEMENT, PROVOZNÍ A FYZICKÁ BEZPEČNOST	24
5.1	FYZICKÁ BEZPEČNOST.....	24
5.1.1	Umístění a konstrukce.....	24
5.1.2	Fyzický přístup.....	24
5.1.3	Elektrína a klimatizace.....	24
5.1.4	Vliv vody.....	24
5.1.5	Protipožární opatření a ochrana.....	25
5.1.6	Ukládání médií.....	25
5.1.7	Nakládání s odpady.....	25
5.1.8	Zálohy mimo budovu provozního pracoviště.....	25
5.2	PROCESNÍ BEZPEČNOST.....	25
5.2.1	Důvěryhodné role.....	25
5.2.2	Počet osob požadovaných na zajištění jednotlivých činností.....	25
5.2.3	Identifikace a autentizace pro každou roli.....	26
5.2.4	Role vyžadující rozdělení povinností.....	26
5.3	PERSONÁLNÍ BEZPEČNOST.....	26
5.3.1	Požadavky na kvalifikaci, zkušenost a bezúhonnost.....	26
5.3.2	Posouzení spolehlivosti osob.....	26
5.3.3	Požadavky na přípravu pro výkon role, vstupní školení.....	27
5.3.4	Požadavky a periodičita školení.....	27
5.3.5	Periodičita a posloupnost rotace pracovníků mezi různými rolemi.....	27
5.3.6	Postihy za neoprávněné činnosti zaměstnanců.....	27
5.3.7	Požadavky na nezávislé zhotovitele (dodavatele).....	27
5.3.8	Dokumentace poskytovaná zaměstnancům.....	27
5.4	AUDITNÍ ZÁZNAMY (LOGY).....	28
5.4.1	Typy zaznamenávaných událostí.....	28
5.4.2	Periodičita zpracování záznamů.....	28
5.4.3	Doba uchovávání auditních záznamů.....	28
5.4.4	Ochrana auditních záznamů.....	28
5.4.5	Postupy pro zálohování auditních záznamů.....	28
5.4.6	Systém shromažďování auditních záznamů (interní nebo externí).....	29
5.4.7	Postup při oznamování události subjektu, který ji způsobil.....	29
5.4.8	Hodnocení zranitelnosti.....	29
5.5	UCHOVÁVÁNÍ INFORMACÍ A DOKUMENTACE.....	29
5.5.1	Typy informací a dokumentace, které se uchovávají.....	29
5.5.2	Doba uchovávání uchovávaných informací a dokumentace.....	30
5.5.3	Ochrana úložiště uchovávaných informací a dokumentace.....	30
5.5.4	Postupy při zálohování uchovávaných informací a dokumentace.....	30
5.5.5	Požadavky na používání časových razítek při uchovávání informací a dokumentace.....	30
5.5.6	Systém shromažďování uchovávaných informací a dokumentace (interní, externí).....	30
5.5.7	Postupy pro získání a ověření uchovávaných informací a dokumentace.....	30
5.6	VÝMĚNA DAT PRO OVĚŘOVÁNÍ ELEKTRONICKÝCH ZNAČEK V NADŘÍZENÉM KVALIFIKOVANÉM SYSTÉMOVÉM CERTIFIKÁTU POSKYTOVATELE.....	31
5.7	OBNOVA PO HAVÁRII NEBO KOMPROMITACI.....	31

Certifikační prováděcí směrnice vydávání root certifikátů SICA	Strana 6 (celkem 48)
Copyright © První certifikační autorita, a.s.	

5.7.1	Postup v případě incidentu a kompromitace.....	31
5.7.2	Poškození výpočetních prostředků, software nebo dat.....	31
5.7.3	Postup při kompromitaci dat pro vytváření elektronických značek /podpisů poskytovatele.....	31
5.7.4	Schopnosti obnovit činnost po havárii.....	32
5.8	UKONČENÍ ČINNOSTI CA.....	32
6	TECHNICKÁ BEZPEČNOST.....	33
6.1	GENEROVÁNÍ A INSTALACE PÁROVÝCH DAT.....	33
6.1.1	Generování párových dat.....	33
6.1.2	Předání dat pro vytváření elektronických značek označující osobě.....	33
6.1.3	Předání dat pro ověřování elektronických značek poskytovateli certifikačních služeb.....	34
6.1.4	Poskytování dat pro ověřování elektronických značek certifikační autoritou spoléhajícím se stranám.....	34
6.1.5	Délky párových dat.....	34
6.1.6	Generování parametrů dat pro ověřování elektronických značek a kontrola jejich kvality.....	34
6.1.7	Omezení pro použití dat pro ověřování elektronických značek.....	34
6.2	OCHRANA DAT PRO VYTVÁŘENÍ ELEKTRONICKÝCH ZNAČEK A BEZPEČNOST KRYPTOGRAFICKÝCH MODULŮ.....	34
6.2.1	Standardy a podmínky používání kryptografických modulů.....	34
6.2.2	Sdílení tajemství.....	35
6.2.3	Úschova dat pro vytváření elektronických značek.....	35
6.2.4	Zálohování dat pro vytváření elektronických značek.....	35
6.2.5	Uchovávání dat pro vytváření elektronických značek.....	35
6.2.6	Transfer dat pro vytváření elektronických značek do kryptografického modulu nebo z kryptografického modulu.....	35
6.2.7	Uložení dat pro vytváření elektronických značek v kryptografickém modulu.....	35
6.2.8	Postup při aktivaci dat pro vytváření elektronických značek.....	35
6.2.9	Postup při deaktivaci dat pro vytváření elektronických značek.....	36
6.2.10	Postup při zničení dat pro vytváření elektronických značek.....	36
6.2.11	Hodnocení kryptografického modulu.....	36
6.3	DALŠÍ ASPEKTY SPRÁVY PÁROVÝCH DAT.....	36
6.3.1	Uchovávání dat pro ověřování elektronických značek.....	36
6.3.2	Maximální doba platnosti certifikátu označující osoby a párových dat.....	36
6.4	AKTIVAČNÍ DATA.....	37
6.4.1	Generování a instalace aktivačních dat.....	37
6.4.2	Ochrana aktivačních dat.....	37
6.4.3	Ostatní aspekty aktivačních dat.....	37
6.5	POČÍTAČOVÁ BEZPEČNOST.....	37
6.5.1	Specifické technické požadavky na počítačovou bezpečnost.....	37
6.5.2	Hodnocení počítačové bezpečnosti.....	37
6.6	BEZPEČNOST ŽIVOTNÍHO CYKLU.....	38
6.6.1	Řízení vývoje systému.....	38
6.6.2	Kontroly řízení bezpečnosti.....	38
6.6.3	Řízení bezpečnosti životního cyklu.....	38
6.7	SÍŤOVÁ BEZPEČNOST.....	38
6.8	ČASOVÁ RAZÍTKA.....	38
7	PROFILY CERTIFIKÁTU, SEZNAMU ZNEPLATNĚNÝCH CERTIFIKÁTŮ A OCSP.....	39
7.1	PROFIL CERTIFIKÁTU.....	39
7.1.1	Číslo verze.....	39
7.1.2	Rozšiřující položky v certifikátu.....	39
7.1.3	Objektové identifikátory (dále OID) algoritmů.....	39
7.1.4	Způsoby zápisu jmen a názvů.....	39
7.1.5	Omezení jmen a názvů.....	39
7.1.6	OID certifikační politiky.....	39
7.1.7	Rozšiřující položka „Policy Constraints“.....	39
7.1.8	Syntaxe a sémantika rozšiřující položky kvalifikátorů politiky „Policy Qualifiers“.....	39
7.1.9	Způsob zápisu kritické rozšiřující položky „Certificate Policies“.....	40
7.2	PROFIL SEZNAMU ZNEPLATNĚNÝCH CERTIFIKÁTŮ.....	40
7.2.1	Číslo verze.....	40

Certifikační prováděcí směrnice vydávání root certifikátů SICA	Strana 7 (celkem 48)
Copyright © První certifikační autorita, a.s.	

7.2.2	<i>Rozšiřující položky seznamu zneplatněných certifikátů a záznamů v seznamu zneplatněných certifikátů</i>	40
	40	
7.3	PROFIL OCSP	40
7.3.1	Číslo verze.....	40
7.3.2	Rozšiřující položky OCSP	40
8	HODNOCENÍ SHODY A JINÁ HODNOCENÍ.....	41
8.1	PERIODICITA HODNOCENÍ NEBO OKOLNOSTI PRO PROVEDENÍ HODNOCENÍ.....	41
8.2	IDENTITA A KVALIFIKACE HODNODITELE.....	41
8.3	VZTAH HODNODITELE K HODNOCENÉ ENTITĚ	41
8.4	HODNOCENÉ OBLASTI.....	41
8.5	POSTUP V PŘÍPADĚ ZJIŠTĚNÝCH NEDOSTATKŮ	41
8.6	SDĚLOVÁNÍ VÝSLEDKŮ HODNOCENÍ.....	41
9	OSTATNÍ OBCHODNÍ A PRÁVNÍ ZÁLEŽITOSTI	42
9.1	POPLATKY	42
9.1.1	<i>Poplatky za vydání nebo obnovení certifikátu.....</i>	42
9.1.2	<i>Poplatky za přístup k certifikátu na seznamu vydaných certifikátů</i>	42
9.1.3	<i>Poplatky za informace o statutu certifikátu a o zneplatnění certifikátu.....</i>	42
9.1.4	<i>Poplatky za další služby</i>	42
9.1.5	<i>Jiná ustanovení týkající se poplatků (vč. refundací).....</i>	42
9.2	FINANČNÍ ODPOVĚDNOST	42
9.2.1	<i>Krytí pojištěním</i>	42
9.2.2	<i>Další aktiva a záruky.....</i>	42
9.2.3	<i>Pojištění nebo krytí zárukou pro koncové uživatele.....</i>	42
9.3	CITLIVOST OBCHODNÍCH INFORMACÍ.....	43
9.3.1	<i>Výčet citlivých informací.....</i>	43
9.3.2	<i>Informace mimo rámec citlivých informací</i>	43
9.3.3	<i>Odpovědnost za ochranu citlivých informací.....</i>	43
9.4	OCHRANA OSOBNÍCH ÚDAJŮ	43
9.4.1	<i>Politika ochrany osobních údajů</i>	43
9.4.2	<i>Osobní údaje.....</i>	43
9.4.3	<i>Údaje, které nejsou považovány za důvěrné</i>	44
9.4.4	<i>Odpovědnost za ochranu osobních údajů</i>	44
9.4.5	<i>Oznámení o používání důvěrných informací a souhlas s používáním citlivých informací</i>	44
9.4.6	<i>Poskytování citlivých informací pro soudní či správní účely</i>	44
9.4.7	<i>Jiné okolnosti zpřístupňování osobních údajů</i>	44
9.5	PRÁVA DUŠEVNÍHO VLASTNICTVÍ.....	44
9.6	ZASTUPOVÁNÍ A ZÁRUKY	44
9.6.1	<i>Zastupování a záruky CA</i>	44
9.6.2	<i>Zastupování a záruky RA</i>	44
9.6.3	<i>Zastupování a záruky držitele certifikátu a podepisující osoby.....</i>	45
9.6.4	<i>Zastupování a záruky spoléhajících se stran.....</i>	45
9.6.5	<i>Zastupování a záruky ostatních zúčastněných subjektů.....</i>	45
9.7	ZŘEKNUTÍ SE ZÁRUK.....	45
9.8	OMEZENÍ ODPOVĚDNOSTI.....	45
9.9	ODPOVĚDNOST ZA ŠKODU, NÁHRADA ŠKODY	45
9.10	DOBA PLATNOSTI, UKONČENÍ PLATNOSTI.....	45
9.10.1	<i>Doba platnosti</i>	45
9.10.2	<i>Ukončení platnosti.....</i>	45
9.10.3	<i>Důsledky ukončení a přetrvání závazků</i>	45
9.11	KOMUNIKACE MEZI ZÚČASTNĚNÝMI SUBJEKTY	46
9.12	ZMĚNY	46
9.12.1	<i>Postup při změnách</i>	46
9.12.2	<i>Postup při oznamování změn.....</i>	46
9.12.3	<i>Okolnosti, při kterých musí být změněno OID</i>	46
9.13	ŘEŠENÍ SPORŮ	46
9.14	ROZHODNÉ PRÁVO.....	46

Certifikační prováděcí směrnice vydávání root certifikátů SICA	Strana 8 (celkem 48)
Copyright © První certifikační autorita, a.s.	

9.15	SHODA S PRÁVNÍMI PŘEDPISY	46
9.16	DALŠÍ USTANOVENÍ	46
9.16.1	<i>Rámcová dohoda</i>	46
9.16.2	<i>Postoupení práv</i>	46
9.16.3	<i>Oddělitelnost ustanovení</i>	47
9.16.4	<i>Zřeknutí se práv</i>	47
9.16.5	<i>Vyšší moc</i>	47
9.17	DALŠÍ OPATŘENÍ	47
10	ZÁVĚREČNÁ USTANOVENÍ.....	48

Certifikační prováděcí směrnice vydávání root certifikátů SICA	Strana 9 (celkem 48)
Copyright © První certifikační autorita, a.s.	

1 Úvod

Tento dokument, **Certifikační prováděcí směrnice vydávání root certifikátů SICA** (dále též CP), vypracovaný společností První certifikační autorita, a. s. (dále též I.CA):

- se zabývá skutečnostmi, které se vztahují na I.CA a které souvisejí s vydáváním root certifikátů SICA, jejich další správou, použitím, akceptací, ukončením platnosti, zneplatněním a všemi aspekty souvisejícími s nakládáním s párovými daty,
- striktně dodržuje členění dokumentu navržené v RFC 3647, s přihlédnutím k doporučením orgánů EU. Jednotlivé kapitoly jsou proto v této CP zachovány i v případě, že jsou ve vztahu k ní irelevantní.

1.1 Přehled

Informace o dalších poskytovaných certifikačních službách je možno získat na internetové informační adrese, uvedené v kapitole 2.

1.2 Název a identifikace dokumentu

Název tohoto dokumentu: Certifikační prováděcí směrnice vydávání root certifikátů SICA, verze 2.1
 OID dokumentu: není přiřazeno

Tato CPS se vztahuje k následující CP:

OID	CP
1.3.6.1.4.1.23624.1.1.0.1	Certifikační politika vydávání root certifikátů SICA

1.3 Participující subjekty

1.3.1 Certifikační autority (dále "CA")

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

1.3.2 Registrační autority (dále "RA")

Pro potřeby této CPS irelevantní.

1.3.3 Držitelé kvalifikovaných systémových certifikátů a označující osoby, kteří požádali o vydání kvalifikovaného certifikátu a/nebo kvalifikovaného systémového certifikátu (dále certifikátu) a kterým byl certifikát vydán

Držitelem root certifikátů SICA je I.CA. Oprávněným žadatelem a následně držitelem certifikátů je I.CA jako právnická osoba.

1.3.4 Spoléhající se strany

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

Certifikační prováděcí směrnice vydávání root certifikátů SICA	Strana 10 (celkem 48)
Copyright © První certifikační autorita, a.s.	

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

Root certifikáty SICA mohou být používány v aplikacích pouze pro ověřování elektronického podpisu vydaných certifikátů a seznamu zneplatněných certifikátů.

1.4.2 Omezení použití certifikátu

Root certifikáty SICA nesmí být využívány v rozporu s vydávaným účelem.

1.5 Správa politiky

1.5.1 Organizace spravující certifikační politiku nebo certifikační prováděcí směrnici

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

1.5.2 Kontaktní osoba organizace spravující certifikační politiku nebo certifikační prováděcí směrnici

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

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. Déle platí ustanovení kapitoly 3.2.6.

1.5.4 Postupy při schvalování souladu s bodem 1.5.3

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

1.6 Přehled použitých pojmů a zkratk

Tabulka 3 – Pojmy

Pojem	Vysvětlení
CA	centrální pracoviště Certifikační autority I.CA
Certifikát	datová zpráva, která je vydána poskytovatelem certifikačních služeb, spojuje data pro ověřování elektronických podpisů s podepisující

Certifikační prováděcí směrnice vydávání root certifikátů SICA	Strana 11 (celkem 48)
Copyright © První certifikační autorita, a.s.	

Pojem	Vysvětlení
	osobou a umožňuje ověřit její identitu, nebo spojuje data pro ověřování elektronických značek s označující osobou a umožňuje ověřit její identitu
Certificate Revocation List (CRL)	seznam zneplatněných certifikátů
Čas	světový čas UTC
Distinguished Name (DN)	řetězce položky Subject, naplňované daty z žádosti o certifikát, z nichž některé jsou ověřované I.CA dle pravidel, uvedených v konkrétní CP
Držitel certifikátu	fyzická osoba, právnická osoba nebo organizační složka státu, která požádala o vydání certifikátu pro sebe nebo pro podepisující osobu a které byl certifikát vydán
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
Hash	matematicky vypočtená jedinečná hodnota, představující zhuštěnou hodnotu dlouhé zprávy, ze které byla vypočtena
I.CA	První certifikační autorita, a.s.
root certifikát SICA	kořenový certifikát I.CA
Otisk	viz hash
Párová data	jedinečná data pro vytváření elektronického podpisu spolu s odpovídajícími daty pro ověřování elektronického podpisu
Soukromý klíč	jedinečná data pro vytváření elektronického podpisu nebo elektronické značky
Spoléhající se strana	subjekt spoléhající se při své činnosti na certifikát
Veřejný klíč	jedinečná data pro ověřování elektronického podpisu

Certifikační prováděcí směrnice vydávání root certifikátů SICA	Strana 12 (celkem 48)
Copyright © První certifikační autorita, a.s.	

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 jsou:

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

Kontaktní 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 info@ica.cz

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

Root certifikáty SICA lze získat na adrese <http://www.ica.cz/>.

V případech vzniku důvodné obavy ze zneužití dat 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

S ohledem na problematiku root certifikátů SICA, zveřejňuje I.CA informace s následující periodicitou:

- Root certifikáty SICA včetně hashe – před jejich využíváním.
- Informace o zneplatnění root certifikátů SICA s uvedením důvodu zneplatnění (v případě zneužití nebo vzniku důvodné obavy ze zneužití dat pro vytváření elektronických podpisů, určených pro podepisování vydávaných certifikátů, seznamů zneplatněných certifikátů) – bezodkladně.

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:

Certifikační prováděcí směrnice vydávání root certifikátů SICA	Strana 13 (celkem 48)
Copyright © První certifikační autorita, a.s.	

- „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 – položky Subject a Issuer

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

3.1.2 Požadavek na významovost jmen

V případě výskytu nepovolených znaků se žádost nepřijme.

Dále se kontroluje přítomnost všech povinných atributů. Pokud některý z povinných atributů není vyplněn, 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).

3.1.3 Anonymita a používání pseudonymu

Tyto skutečnosti jsou pro aplikaci tohoto vydání této CPS irelevantní.

3.1.4 Pravidla pro interpretaci různých forem jmen

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

3.1.5 Jedinečnost jmen

Jedinečnost jména (Subject a Issuer) je zaručena.

3.1.6 Obchodní značky

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

3.2 Počáteční ověření identity

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

Vlastnictví dat pro vytváření elektronických podpisů, odpovídající datům pro ověřování elektronických podpisů, která bude daný root certifikát SICA obsahovat, se prokazuje předložením žádosti o vydání root certifikátu SICA, elektronicky podepsané těmito daty. Toto je kontrolováno tím, že je pomocí dat pro ověřování elektronických podpisů, uvedených v žádosti o root certifikát SICA, ověřena platnost elektronického podpisu na této žádosti.

3.2.2 Ověřování identity právnické osoby nebo organizační složky státu

Jediná fyzická osoba, která může rozhodnout o vydání root certifikátu SICA, je ředitel I.CA, který před zahájením vlastního generování párových dat:

- se identifikuje platným občanským průkazem a sekundárním osobním průkazem (viz kapitola 3.2.3),
- komisi, která provádí generaci párových dat, předloží listinné dokumenty, které dokládají jeho jmenování do funkce ředitele I.CA a originál nebo notářsky ověřenou kopii výpisu z obchodního rejstříku, na jejichž základě byla I.CA vytvořena a která musí obsahovat úplné obchodní jméno, identifikační číslo (IČO), statutární orgán a sídlo. Identifikace ostatních členů této komise se provádí v souladu s vnitřními směrnici.

3.2.3 Ověřování identity fyzické osoby

Ředitel I.CA doloží své následující údaje:

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

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

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

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

3.2.4 Neověřené informace vztahující se k držiteli certifikátu nebo označující osobě

Všechny informace musí být ověřeny.

Certifikační prováděcí směrnice vydávání root certifikátů SICA	Strana 16 (celkem 48)
Copyright © První certifikační autorita, a.s.	

3.2.5 Ověřování specifických práv

Tyto skutečnosti jsou pro aplikaci tohoto vydání této CPS irelevantní.

3.2.6 Kritéria pro interoperabilitu

Tyto skutečnosti jsou pro aplikaci tohoto vydání této CPS irelevantní.

3.3 Identifikace a autentizace při zpracování požadavků na výměnu dat pro ověřování elektronických značek v certifikátu

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

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

3.3.2 Identifikace a autentizace při výměně párových dat po zneplatnění certifikátu

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

3.4 Identifikace a autentizace při zpracování požadavků na zneplatnění certifikátu

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

Certifikační prováděcí směrnice vydávání root certifikátů SICA	Strana 17 (celkem 48)
Copyright © První certifikační autorita, a.s.	

4 Požadavky na životní cyklus certifikátu

4.1 Žádost o vydání certifikátu

4.1.1 Subjekty oprávněné podat žádost o vydání certifikátu

Viz kapitola 3.2.

4.1.2 Registrační proces a odpovědnosti poskytovatele a žadatele

Viz kapitola 3.2.

4.2 Zpracování žádosti o certifikát

4.2.1 Identifikace a autentizace

Uvedeno v kapitole 4.3.

4.2.2 Přijetí nebo odmítnutí žádosti o certifikát

Uvedeno v kapitole 4.3.

4.2.3 Doba zpracování žádosti o certifikát

Generování žádosti a vydání root certifikátu SICA – při dodržení všech potřebných podmínek řádově minuty.

4.3 Vydání certifikátu

4.3.1 Úkony CA v průběhu vydání certifikátu

V procesu vydávání root certifikát SICA jsou prováděny nezbytné kontroly a další činnosti, popsané v interní dokumentaci „*Operátor CA*“.

4.3.2 Oznámení o vydání certifikátu držiteli certifikátu nebo označující osobě

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

4.4 Převzetí vydaného certifikátu

4.4.1 Úkony spojené s převzetím certifikátu

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

4.4.2 Zveřejňování vydaných certifikátů poskytovatelem

I.CA je povinna zajistit zveřejnění root certifikátu SICA.

Certifikační prováděcí směrnice vydávání root certifikátů SICA	Strana 18 (celkem 48)
Copyright © První certifikační autorita, a.s.	

4.4.3 Oznámení o vydání certifikátu jiným subjektům

V případech vydání root certifikátu SICA získají oznámení o jeho vydání pracovníci komise.

4.5 Použití párových dat a certifikátu

4.5.1 Použití dat pro vytváření elektronických značek a certifikátu držitelem certifikátu nebo označující osobou

Viz kapitola 1.4.

4.5.2 Použití dat pro ověřování elektronických značek a certifikátu spoléhající se stranou

Spoléhající se strany jsou povinny provádět veškeré úkony potřebné k tomu, aby si ověřily, že elektronický podpis root certifikátu SICA je platný a tento certifikát nebyl zneplatněn.

4.6 Obnovení certifikátu

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

4.6.1 Podmínky pro obnovení certifikátu

Viz kapitola 4.6.

4.6.2 Subjekty oprávněné požadovat obnovení certifikátu

Viz kapitola 4.6.

4.6.3 Zpracování požadavku na obnovení certifikátu

Viz kapitola 4.6.

4.6.4 Oznámení o vydání obnoveného certifikátu držiteli certifikátu nebo označující osobě

Viz kapitola 4.6.

4.6.5 Úkony spojené s převzetím obnoveného certifikátu

Viz kapitola 4.6.

4.6.6 Zveřejnění vydaných obnovených certifikátů poskytovatelem

Viz kapitola 4.6.

Certifikační prováděcí směrnice vydávání root certifikátů SICA	Strana 19 (celkem 48)
Copyright © První certifikační autorita, a.s.	

4.6.7 Oznámení o vydání obnoveného certifikátu ostatním subjektům

Viz kapitola 4.6.

4.7 Výměna dat pro ověřování elektronických značek v certifikátu

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

4.7.1 Podmínky pro výměnu dat pro ověřování elektronických značek v certifikátu

Viz kapitola 4.7.

4.7.2 Subjekty oprávněné požadovat výměnu dat pro ověřování elektronických značek v certifikátu

Viz kapitola 4.7.

4.7.3 Zpracování požadavku na výměnu dat pro ověřování elektronických značek

Viz kapitola 4.7.

4.7.4 Oznámení o vydání certifikátu s vyměněnými daty pro ověřování elektronických značek označující osobě

Viz kapitola 4.7.

4.7.5 Úkony spojené s převzetím certifikátu s vyměněnými daty pro ověřování elektronických značek

Viz kapitola 4.7.

4.7.6 Zveřejnění vydaných certifikátů s vyměněnými daty pro ověřování elektronických značek

Viz kapitola 4.7.

4.8 Oznámení o vydání certifikátu s vyměněnými daty pro ověřování elektronických značek jiným subjektům

Viz kapitola 4.7.

4.9 Změna údajů v certifikátu

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

4.9.1 Podmínky pro změnu údajů v certifikátu

Viz kapitola 4.9.

4.9.2 Subjekty oprávněné požadovat změnu údajů v certifikátu

Viz kapitola 4.9.

4.9.3 Zpracování požadavku na změnu údajů v certifikátu

Viz kapitola 4.9.

4.9.4 Oznámení o vydání certifikátu se změněnými údaji označující osobě

Viz kapitola 4.9.

4.9.5 Úkony spojené s převzetím certifikátu se změněnými údaji

Viz kapitola 4.9.

4.9.6 Zveřejnění vydaných certifikátů se změněnými údaji

Viz kapitola 4.9.

4.9.7 Oznámení o vydání certifikátu se změněnými údaji jiným subjektům

Viz kapitola 4.9.

4.10 Zneplatnění a pozastavení platnosti certifikátu**4.10.1 Podmínky pro zneplatnění certifikátu**

Root certifikát SICA může být zneplatněn na základě následujících okolností:

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

4.10.2 Subjekty oprávněné žádat o zneplatnění certifikátu

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

Certifikační prováděcí směrnice vydávání root certifikátů SICA	Strana 21 (celkem 48)
Copyright © První certifikační autorita, a.s.	

4.10.3 Požadavek na zneplatnění certifikátu

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

4.10.4 Doba odkladu požadavku na zneplatnění certifikátu

Tyto skutečnosti jsou pro aplikaci tohoto vydání této CPS irelevantní.

4.10.5 Maximální doba, za kterou musí poskytovatel realizovat požadavek na zneplatnění certifikátu

Reakcí I.CA na přijetí platné žádosti o zneplatnění root certifikát SICA je jeho okamžité zneplatnění a zveřejnění této informace (viz kapitola 2.2). CRL obsahující sériové číslo zneplatněného certifikátu musí být vydán neprodleně po zneplatnění tohoto certifikátu. Detailní postupy jsou uvedeny v interní dokumentaci „**Operátor CA**“.

4.10.6 Povinnosti spoléhajících se stran při ověřování, zda nebyl certifikát zneplatněn

Viz kapitola 4.5.2

4.10.7 Periodicita vydávání seznamu zneplatněných certifikátů

Seznam zneplatněných certifikátů, které byly vydány I.CA, je společností První certifikační autorita, a.s. vydáván v pravidelných intervalech, minimálně jedenkrát za 24 hodin (zpravidla po 8 hodinách), v případě nutnosti bezodkladně. Činnosti operátorů CA v procesu vytváření a vydávání CRL jsou popsány v interní dokumentaci „**Operátor CA**“.

4.10.8 Maximální zpoždění při vydávání seznamu zneplatněných certifikátů

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

4.10.9 Možnost ověřování statutu certifikátu on-line („dále OCSP“)

Tyto skutečnosti jsou pro aplikaci tohoto vydání této CPS irelevantní.

4.10.10 Požadavky při ověřování statutu certifikátu na on-line

Tyto skutečnosti jsou pro aplikaci tohoto vydání této CPS irelevantní.

4.10.11 Jiné způsoby oznamování zneplatnění certifikátu

Tyto skutečnosti jsou pro aplikaci tohoto vydání této CPS irelevantní.

4.10.12 Případné odlišnosti postupu zneplatnění v případě kompromitace dat pro vytváření elektronických značek

Tyto skutečnosti jsou pro aplikaci tohoto vydání této CPS irelevantní.

4.10.13 Podmínky pro pozastavení platnosti certifikátu

Tyto skutečnosti jsou pro aplikaci tohoto vydání této CPS irelevantní.

4.10.14 Subjekty oprávněné požadovat pozastavení platnosti certifikátu

Tyto skutečnosti jsou pro aplikaci tohoto vydání této CPS irelevantní.

4.10.15 Zpracování požadavku na pozastavení platnosti certifikátu

Tyto skutečnosti jsou pro aplikaci tohoto vydání této CPS irelevantní.

4.10.16 Omezení doby pozastavení platnosti certifikátu

Tyto skutečnosti jsou pro aplikaci tohoto vydání této CPS irelevantní.

4.11 Služby související s ověřováním statutu certifikátu**4.11.1 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.

4.11.2 Dostupnost služeb

I.CA zajišťuje nepřetržitou dostupnost služeb (7 dní v týdnu, 24 hodin denně) a integrity seznamu jí vydaných certifikátů a seznamu zneplatněných certifikátů (platné CRL). Postup je uveden v interních dokumentech I.CA:

- „*Řízení fyzického přístupu do místností I.CA*“,
- „*Operátor CA*“,
- „*Požární bezpečnost*“,
- „*Obnova komponenty provozního pracoviště*“,
- „*Přemístění provozního pracoviště*“.

4.11.3 Další charakteristiky služeb statutu certifikátu

Další služby, kromě těch, které jsou uvedené v kapitole 4.11.1, nejsou poskytovány.

4.12 Ukončení poskytování služeb pro držitele certifikátu označující osobou

Viz kapitola 5.8.

4.13 Úschova dat pro vytváření elektronických značek u důvěryhodné třetí strany a jejich obnova

Tyto skutečnosti jsou pro aplikaci tohoto vydání této CPS irelevantní.

4.13.1 Politika a postupy při úschově a obnovování dat pro elektronických značek

Tyto skutečnosti jsou pro aplikaci tohoto vydání této CPS irelevantní.

4.13.2 Politika a postupy při zapouzdřování a obnovování šifrovacího klíče pro relaci

Tyto skutečnosti jsou pro aplikaci tohoto vydání této CPS irelevantní.

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 interních bezpečnostních normách a směrnících. Uvedené dokumenty reflektují výsledky provedené analýzy rizik.

5.1 Fyzická bezpečnost

Problematika fyzické bezpečnosti je detailně uvedena v interní dokumentaci:

- „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 (EVS), 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 jistěn 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 stoupanou vodou. Provozní pracoviště jsou dle potřeby vybavena čidly průniku vody pro případ zaplavení vodou z topení, nebo vodou ze střechy při prudkém dešti.

Certifikační prováděcí směrnice vydávání root certifikátů SICA	Strana 25 (celkem 48)
Copyright © První certifikační autorita, a.s.	

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 provozního pracoviště

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

5.2 Procesní bezpečnost

Problematika procesní bezpečnosti je detailně uvedena v interní dokumentaci:

- „*Systémová bezpečnostní politika CA*“,
- „*Řízení bezpečnosti informací*“,
- „*Hodnocení bezpečnosti*“,
- „*Bezpečnostní incidenty*“,
- „*Příručka administrátora*“,
- „*Operátor CA*“.

5.2.1 Důvěryhodné role

Pro činnosti, odpovídajícím rolím podle bezpečnostních požadavků standardu pro důvěryhodné systémy, jsou ve společnosti I.CA definovány důvěryhodné role. Základní činnosti a odpovědnosti osob v důvěryhodných rolích je definován v interní dokumentaci.

5.2.2 Počet osob požadovaných na zajištění jednotlivých činností

Ve společnosti První certifikační autorita, a.s. jsou pro procesy poskytování certifikačních služeb definovány činnosti, které se musí vykonávat jedinečně 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,

Certifikační prováděcí směrnice vydávání root certifikátů SICA	Strana 26 (celkem 48)
Copyright © První certifikační autorita, a.s.	

- aktivace kryptografického modulu, obsahujícího data pro vytváření elektronického podpisu I.CA vydávaných certifikátů a seznamů zneplatněných certifikátů.

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

5.2.3 Identifikace a autentizace pro každou roli

Pracovníkům jsou přiděleny prostředky pro řádnou autentizaci k těm komponentám, které jsou pro jejich činnost nezbytné - upraveno interními směrnici (viz výše).

5.2.4 Role vyžadující rozdělení povinností

V procesu poskytování certifikačních služeb v oblasti vydávání certifikátů je minimálně zaručeno, že nelze spojit role, definované bezpečnostním standardem pro důvěryhodné systémy.

5.3 Personální bezpečnost

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

5.3.1 Požadavky na kvalifikaci, zkušenost a bezúhonnost

Pracovníci v rolích podle bezpečnostních požadavků standardu pro důvěryhodné systémy a dále v rolích ředitel společnosti, bezpečnostní manager, manager pro zvládání krizových situací a plánu obnovy, bezpečnostní auditor jsou přijímáni na základě dále popsanych personálních kritérií:

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

Certifikační prováděcí směrnice vydávání root certifikátů SICA	Strana 27 (celkem 48)
Copyright © První certifikační autorita, a.s.	

- 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 bezpečnosti informací.

5.3.5 Periodicita a posloupnost rotace pracovníků mezi různými rolemi

Z důvodů možné zastupitelnosti v mimořádných případech jsou pracovníci I.CA motivováni na získávání znalostí potřebných na zastávání jiné role v I.CA. Změna role je možná pouze v mimořádných případech (epidemické onemocnění, atp.) jako dočasné opatření. Pro trvalé vykonávání jiné důvěryhodné role je potřeba jmenování ředitelem I.CA.

5.3.6 Postihy za neoprávněné činnosti zaměstnanců

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

5.3.7 Požadavky na nezávislé zhotovitele (dodavatele)

I.CA může některé činnosti zajišťovat smluvně. Tyto obchodně právní vztahy jsou ošetřeny bilaterálními obchodními smlouvami. Jedná se o např. o smluvní registrační autority, zhotovitele programového aplikačního vybavení, dodavatele hardware, systémového programového vybavení, externí 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“,
- „HSM/Private Server“,
- „Příprava uchovávaných informací“,
- „Záloha dat provozních systémů“,
- „Řízení fyzického přístupu do místností I.CA“,
- „Dokumenty agendy certifikačních služeb“.

5.4.1 Typy zaznamenávaných událostí

V důvěryhodných systémech I.CA jsou do elektronického auditního logu zaznamenávány události, požadované:

- CWA 14167-1 - Security Requirements for Trustworthy Systems Managing Certificates for Electronic Signatures - Part 1: System Security Requirements ,
- ETSI TS 102 042 - Electronic Signatures and Infrastructures: Policy requirements for certification authorities issuing public key certificates.

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 týdně, 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. 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. Shromažďování auditních záznamů je evidováno.

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.

5.5 Uchovávání informací a dokumentace

Zásady uchovávání informací a dokumentace jsou uvedeny v základních interních dokumentech:

- „*Celková bezpečnostní politika*“,
- „*Systémová bezpečnostní politika CA*“,
- „*Řízení fyzického přístupu do místností I.CA*“,
- „*Příprava uchovávaných informací*“,
- „*Záloha dat provozních systémů*“,
- „*Příručka administrátora*“,
- „*Dokumenty agendy certifikačních služeb*“,
- „*Dílčí spisový a skartační řád pro agendy certifikačních služeb*“.

5.5.1 Typy informací a dokumentace, které se uchovávají

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

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

Certifikační prováděcí směrnice vydávání root certifikátů SICA	Strana 30 (celkem 48)
Copyright © První certifikační autorita, a.s.	

5.5.2 Doba uchovávání uchovávaných informací a dokumentace

Po celou dobu své existence I.CA zajišťuje uchovávání informací a dokumentace dle kapitoly 0 po dobu nejméně 10 od jejich vzniku.

Po celou dobu existence I.CA jsou uchovávány informace, vztahující se root certifikátům SICA, s výjimkou příslušných dat pro vytváření elektronického podpisu.

5.5.3 Ochrana úložiště uchovávaných informací a dokumentace

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

5.5.4 Postupy při zálohování uchovávaných informací a dokumentace

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

- „*Rízení fyzického přístupu do místností I.CA*“,
- „*Bezpečnostní příručka administrátora*“,
- „*Operátor CA*“,
- „*HSM/PrivateServer*“,
- „*Záloha dat provozních systémů*“,
- „*Příprava uchovávaných informací*“,
- „*Dokumenty agendy certifikačních služeb*“,
- „*Dílčí spisový a skartační řád pro agendy certifikačních služeb*“.

5.5.5 Požadavky na používání časových razítek při uchovávání informací a dokumentace

V případě, že budou využívána časová razítka, musí se jednat 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 směrnicemi (viz kapitola 5.5.4). Shromažďování archivních záznamů je evidováno.

5.5.7 Postupy pro získání a ověření uchovávaných informací a dokumentace

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

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

O každém takto povoleném přístupu je pořizován písemný záznam.

Certifikační prováděcí směrnice vydávání root certifikátů SICA	Strana 31 (celkem 48)
Copyright © První certifikační autorita, a.s.	

5.6 Výměna dat pro ověřování elektronických značek v nadřazeném kvalifikovaném systémovém 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

V případě výskytu těchto událostí postupuje I.CA v souladu s interním dokumentem **Plán pro zvládání krizových situací a plán obnovy** a jím odkazované dokumentaci, zejména:

- „**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 interním dokumentem **Plán pro zvládání krizových situací a plán obnovy** a jím odkazované dokumentaci, zejména:

- „**Obnova komponenty provozního pracoviště**“,
- „**Přemístění provozního pracoviště**“,
- „**Bezpečnostní incidenty**“.

5.7.3 Postup při kompromitaci dat pro vytváření elektronických značek /podpisů poskytovatele

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

- ukončí jejich používání,
- okamžitě a trvale zneplatní vlastní certifikát SICA a jemu odpovídající data pro vytváření elektronických podpisů,
- zneplatní všechny certifikáty, které byly těmito daty označeny, resp. 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 SICA,
- oznámí příslušnému úřadu informaci o zneplatnění vlastního certifikátu SICA s uvedením důvodu zneplatnění,

- v případě vzniku důvodné obavy ze zneužití dat pro vytváření elektronických podpisů pro podepisování vydávaných certifikátů a seznamů zneplatněných certifikátů nabídne I.CA výše uvedeným držitelům bezplatné vydání nového certifikátu s tím, že případné náklady na vydání nových certifikátů sama hradí - postup je stejný jako při vydání prvotního certifikátu.

5.7.4 Schopnosti obnovit činnost po havárii

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

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

5.8 Ukončení činnosti CA

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

- zpřístupnění informací o ukončení činnosti I.CA v oblasti vydávání certifikátů na své internetové informační adrese nejméně 2 měsíce před plánovaným ukončením činnosti,
- ukončí poskytování certifikačních služeb v oblasti vydávání certifikátů,
- prokazatelně zničí svá data pro vytváření elektronických podpisů, sloužící k podepisování vydávaných certifikátů a seznamu zneplatněných certifikátů.

Problematika plánovaného ukončení činnosti I.CA, případně RA je detailně uvedena v interní dokumentaci.

6 Technická bezpečnost

6.1 Generování a instalace párových dat

Detailní popis generování a instalace párových dat je uveden v interních bezpečnostních směrnících, zahrnujících problematiku, uvedenou v podkapitolách 6.1.1 až 6.1.7.

6.1.1 Generování párových dat

Generování párových dat SICA, 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 rovnou 2048 bitů.

V průběhu procesu generování párových dat SICA, 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 a následné vyhotovení odpovídajícího certifikátu je popsán v interní dokumentaci I.CA:

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

O průběhu generování párových dat SICA, 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 root certifikátu SICA, 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.

6.1.2 Předání dat pro vytváření elektronických značek označující osobě

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

6.1.3 Předání dat pro ověřování elektronických značek poskytovateli certifikačních služeb

Tyto skutečnosti jsou pro aplikaci tohoto vydání této CPS irelevantní.

6.1.4 Poskytování dat pro ověřování elektronických značek certifikační autoritou spoléhajícím se stranám

Data pro ověřování elektronických podpisů SICA jsou obsažena v root certifikátu SICA. Možnost získání tohoto certifikátu je garantována následujícími způsoby:

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

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.

6.1.6 Generování parametrů dat pro ověřování elektronických značek a kontrola jejich kvality

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

6.1.7 Omezení pro použití dat pro ověřování elektronických značek

Uvedeno v kapitole 1.4.1.

6.2 Ochrana dat pro vytváření elektronických značek a bezpečnost kryptografických modulů

Konkrétní postupy níže uvedených podkapitol jsou popsány v interní dokumentaci I.CA:

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

6.2.1 Standardy a podmínky používání kryptografických modulů

V kryptografických modulech (viz kapitola 6.1.1):

- jsou generována párová data SICA,
- je uložen soukromý klíč SICA pro podepisování vydávaných certifikátů a seznamů zneplatněných certifikátů ,

6.2.2 Sdílení tajemství

Ochrana sdílením tajemství je realizována prostředky kryptografického modulu. Při provádění citlivých činností, které souvisejí se zásadními činnostmi I.CA (viz. kapitoly 6.1.1 a 6.2.10), je nezbytná přítomnost tří pověřených pracovníků I.CA, z nichž dva znají část kódu k provedení těchto činností.

6.2.3 Úschova dat pro vytváření elektronických značek

Tyto skutečnosti jsou pro aplikaci tohoto vydání této CPS irelevantní.

6.2.4 Zálohování dat pro vytváření elektronických značek

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

6.2.5 Uchovávání dat pro vytváření elektronických značek

Po uplynutí doby platnosti dat určených k podepisování vydávaných certifikátů a seznamů zneplatněných certifikátů jsou tato data, včetně jejich záloh zničena a jejich další zálohování se neprovádí. Uchovávání dat, určených k podepisování certifikátů a seznamů zneplatněných certifikátů představuje bezpečnostní riziko, a proto je u I.CA zakázáno.

6.2.6 Transfer dat pro vytváření elektronických značek do kryptografického modulu nebo z kryptografického modulu

Data pro vytváření elektronických podpisů příslušná k root certifikátu SICA jsou generována přímo v kryptografickém modulu.

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

6.2.7 Uložení dat pro vytváření elektronických značek v kryptografickém modulu

Data pro vytváření elektronických podpisů příslušná k root certifikátu SICA jsou v kryptografickém modulu uložena v šifrovaném tvaru.

6.2.8 Postup při aktivaci dat pro vytváření elektronických značek

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

Certifikační prováděcí směrnice vydávání root certifikátů SICA	Strana 36 (celkem 48)
Copyright © První certifikační autorita, a.s.	

6.2.9 Postup při deaktivaci dat pro vytváření elektronických značek

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

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

6.2.10 Postup při zničení dat pro vytváření elektronických značek

Data pro vytváření elektronických podpisů, sloužící k podepisování vydávaných certifikátů a seznamů zneplatněných certifikátů, jsou uložena v kryptografickém modulu. Ničení je realizováno prostředky kryptografického modulu. Zálohy těchto dat uložené v zašifrované podobě na externích médiích jsou rovněž zničeny. Ničení spočívá ve fyzické destrukci těchto nosičů.

Při ničení dat pro vytváření elektronických podpisů, sloužících 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.

O průběhu ničení dat elektronických podpisů, sloužících k podepisování vydávaných certifikátů, seznamů zneplatněných certifikátů je sepsán protokol.

6.2.11 Hodnocení kryptografického modulu

Kryptografický modul byl hodnocen dle FIPS PUB 140-2 úroveň 3.

6.3 Další aspekty správy párových dat

6.3.1 Uchovávání dat pro ověřování elektronických značek

Tato data jsou obsažena v root certifikátech SICA. Na rozdíl od jim příslušných dat pro vytváření elektronických podpisů, je důležité tato data uchovávat pro případ následné kontroly pravosti vydaných certifikátů a seznamů zneplatněných certifikátů. Se všemi root certifikáty SICA je nakládáno způsobem, uvedeným v kapitolách 5.4 a 5.5.

6.3.2 Maximální doba platnosti certifikátu označující osoby a párových dat

Platnost dat určených k ověřování vydaných certifikátů a seznamů zneplatněných certifikátů je dána platností vydaných root certifikátů SICA.

6.4 Aktivační data

6.4.1 Generování a instalace aktivačních dat

Aktivační data jsou vytvářena v průběhu procesu instalace, kdy jsou generována párová data pro označování, resp. podepisování vydávaných certifikátů a seznamů zneplatněných certifikátů. Konkrétní postupy jsou popsány v interní dokumentaci, zejména:

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

6.4.2 Ochrana aktivačních dat

Aktivační data jsou chráněna způsobem uvedeným v interní bezpečnostní dokumentaci, zejména:

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

6.4.3 Ostatní aspekty aktivačních dat

Aktivační data jsou určena výhradně pro aktivaci soukromého klíče a nesmí být použita k jiným účelům, ani přenášena nebo uchovávána v otevřené podobě.

6.5 Počítačová bezpečnost

6.5.1 Specifické technické požadavky na počítačovou bezpečnost

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

- „*Systémová bezpečnostní politika CA*“,
- „*Plán pro zvládnutí krizových situací a plán obnovy*“,
- „*Obnova komponenty provozního pracoviště*“,
- „*Přemístění provozního pracoviště*“,
- „*Záloha dat provozních systémů*“,
- „*Příprava uchovávaných dat*“,
- „*Příručka administrátora*“,
- „*Řízení fyzického přístupu do místností I.CA*“,
- „*HSM/Private Server*“.

6.5.2 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: Policy requirements for certification authorities issuing public key certificates.
- ČSN ISO/IEC 27001 Informační technologie - Bezpečnostní techniky - Systémy řízení bezpečnosti informací - Požadavky.

Certifikační prováděcí směrnice vydávání root certifikátů SICA	Strana 38 (celkem 48)
Copyright © První certifikační autorita, a.s.	

- ČSN ISO/IEC 27002 Informační technologie - Bezpečnostní techniky - Soubor postupů pro opatření bezpečnosti informací.
- ČSN EN ISO 19011 - Směrnice pro auditování systému managementu jakosti a/nebo systému environmentálního managementu.

6.6 Bezpečnost životního cyklu

6.6.1 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**“.

6.6.2 Kontroly řízení bezpečnosti

Soulad se standardy je ověřován pravidelnými audity a kontrolami bezpečnostní shody. Tato problematika je popsána v interní dokumentaci „**Kontrolní činnost, bezúhonnost a odbornost**“.

6.6.3 Řízení bezpečnosti životního cyklu

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

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

6.7 Síťová bezpečnost

V prostředí I.CA nejsou prostředky provádějící vlastní kvalifikované certifikační služby přímo dostupné z veřejné sítě Internet. Informační systém je chráněn přístupovým routerem a produktem typu firewall. Detailní řešení řízení síťové bezpečnosti je popsáno v interní dokumentaci:

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

6.8 Časová razítka

Řešení je uvedeno v kapitole 5.5.5.

7 Profily certifikátu, seznamu zneplatněných certifikátů a OCSP

Profily certifikátu a seznamu zneplatněných certifikátů, odpovídají doporučením RFC 3280, resp. RFC 5280, jsou vždy uvedeny v konkrétní CP. Délka klíče certifikační autority, označujícího vydávané certifikáty a seznamy zneplatněných certifikátů je 2048 bitů.

7.1 Profil certifikátu

Viz kapitola. 7.

7.1.1 Čísla verzí

Viz kapitola. 7.

7.1.2 Rozšiřující položky v certifikátu

Viz kapitola. 7.

7.1.3 Objektové identifikátory (dále OID) algoritmů

Viz kapitola. 7.

7.1.4 Způsoby zápisu jmen a názvů

Viz kapitola. 7.

7.1.5 Omezení jmen a názvů

Viz kapitola. 7.

7.1.6 OID certifikační politiky

Viz kapitola. 7.

7.1.7 Rozšiřující položka „Policy Constraints“

Tyto skutečnosti jsou pro aplikaci tohoto vydání CPS irelevantní.

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

Viz kapitola. 7.

7.1.9 Způsob zápisu kritické rozšiřující položky „Certificate Policies“

Viz kapitola. 7.

7.2 Profil seznamu zneplatněných certifikátů

Viz kapitola. 7.

7.2.1 Číslo verze

Viz kapitola. 7.

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

Viz kapitola. 7.

7.3 Profil OCSP

Služba není poskytována.

7.3.1 Číslo verze

Služba není poskytována.

7.3.2 Rozšiřující položky OCSP

Služba není poskytována.

Certifikační prováděcí směrnice vydávání root certifikátů SICA	Strana 41 (celkem 48)
Copyright © První certifikační autorita, a.s.	

8 Hodnocení shody a jiná hodnocení

8.1 Periodicita hodnocení nebo okolnosti pro provedení hodnocení

Externí kontroly - audit systému řízení bezpečnosti informací je prováděn každé dva roky. Interní kontroly jsou prováděny na základě rozhodnutí ředitele I.CA. 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**“.

8.2 Identita a kvalifikace hodnotitele

Identita a kvalifikace hodnotitele je upravena interním dokumentem „**Kontrolní činnost, bezúhonnost a odbornost**“.

8.3 Vztah hodnotitele k hodnocené entitě

V případě auditu systému managementu bezpečnosti informací je hodnotitelem externí, nezávislá auditující organizace.

V případě celkové kontroly bezpečnostní shody nebo částečné kontroly bezpečnostní shody je hodnotitelem fyzická/právní osoba, pověřená ředitelem společnosti První certifikační autorita, a.s.

8.4 Hodnocené oblasti

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

8.5 Postup v případě zjištěných nedostatků

V případě nedostatků, zjištěných na základě provedených kontrol, je bezpečnostní manager povinen do 15 dnů určit, jaká opatření k odstranění nedostatků je I.CA povinna přijmout.

8.6 Sdělování výsledků hodnocení

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

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

Certifikační prováděcí směrnice vydávání root certifikátů SICA	Strana 42 (celkem 48)
Copyright © První certifikační autorita, a.s.	

9 Ostatní obchodní a právní záležitosti

9.1 Poplatky

9.1.1 Poplatky za vydání nebo obnovení certifikátu

Tyto skutečnosti jsou pro aplikaci tohoto vydání CPS irelevantní.

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 elektronickou cestou I.CA nezpoblatňuje.

9.1.4 Poplatky za další služby

Předání root certifikátu SICA je poskytováno zdarma.

9.1.5 Jiná ustanovení týkající se poplatků (vč. refundací)

Tyto skutečnosti jsou pro aplikaci tohoto vydání CPS irelevantní.

9.2 Finanční odpovědnost

9.2.1 Krytí pojištěním

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

9.2.2 Další aktiva a záruky

Společnost První certifikační autorita, a.s. prohlašuje, že má k dispozici dostatečné finanční zdroje a jiné finanční zajištění na 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

Tyto skutečnosti jsou pro aplikaci tohoto vydání CPS irelevantní.

9.3 Citlivost obchodních informací

9.3.1 Výčet citlivých informací

Citlivými informacemi I.CA jsou:

- data pro vytváření elektronických podpisů příslušná k datům pro ověřování elektronických podpisů obsažených v root certifikátech SICA,
- data pro vytváření elektronických podpisů příslušná k datům pro ověřování elektronických podpisů obsažených v účelových certifikátech I.CA (např. klíče pro komunikaci s RA),
- ostatní kryptograficky podstatné informace sloužící k provozu I.CA,
- vybrané obchodní informace I.CA,
- veškeré informace a dokumentace s ohledem na poskytování certifikačních služeb.

Chráněnými obchodními informacemi jednotlivých RA jsou:

- data pro vytváření elektronických podpisů, příslušná k datům pro ověřování elektronických podpisů, obsažených v účelových certifikátech RA,
- ostatní kryptograficky podstatné informace sloužící k provozu RA,
- veškeré informace a dokumentace s ohledem na poskytování certifikačních služeb.

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.

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.

9.4 Ochrana osobních údajů

Problematika ochrany osobních údajů (kapitoly 9.4.1 až 9.4.7) je řešena interní dokumentací.

9.4.1 Politika ochrany osobních údajů

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

9.4.2 Osobní údaje

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

Certifikační prováděcí směrnice vydávání root certifikátů SICA	Strana 44 (celkem 48)
Copyright © První certifikační autorita, a.s.	

9.4.3 Údaje, které nejsou považovány za důvěrné

Informace, které nejsou považovány za důvěrné jsou takové údaje, které nepodléhají ochraně ve smyslu příslušné zákonné normy (zákon č. 101/2000 Sb. v aktuálním znění).

9.4.4 Odpovědnost za ochranu osobních údajů

Ochrana osobních údajů a dalších neveřejných informací je v I.CA řešena v souladu s požadavky zákona č. 101/2000 Sb. v aktuálním znění.

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

Ochrana osobních údajů a dalších neveřejných informací je v I.CA řešena v souladu s požadavky zákona č. 101/2000 Sb. v aktuálním znění.

9.4.6 Poskytování citlivých informací pro soudní či správní účely

Ochrana osobních údajů a dalších neveřejných informací je v I.CA řešena v souladu s požadavky zákona č. 101/2000 Sb. v aktuálním znění.

9.4.7 Jiné okolnosti zpřístupňování osobních údajů

Ochrana osobních údajů a dalších neveřejných informací je v I.CA řešena v souladu s požadavky zákona č. 101/2000 Sb. v aktuálním znění.

9.5 Práva duševního vlastnictví

Tato CPS, veškeré související dokumenty, obsah webových stránek, certifikáty/klíče SICA a procedury, zajišťující provoz systému, poskytujícího certifikační služby, 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 root certifikátům SICA pouze k podepisování vydávaných certifikátů, seznamu zneplatněných certifikátů,
- vydávané root certifikáty SICA splňují náležitosti, uvedené v této CPS a jí odpovídající CP.

9.6.2 Zastupování a záruky RA

Tyto skutečnosti jsou pro aplikaci tohoto vydání CPS irelevantní.

Certifikační prováděcí směrnice vydávání root certifikátů SICA	Strana 45 (celkem 48)
Copyright © První certifikační autorita, a.s.	

9.6.3 Zastupování a záruky držitele certifikátu a podepisující osoby

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

9.6.4 Zastupování a záruky spoléhajících se stran

Spoléhající se strany postupují v souladu s platnou legislativou.

9.6.5 Zastupování a záruky ostatních zúčastněných subjektů

Tyto skutečnosti jsou pro aplikaci tohoto vydání CPS irelevantní.

9.7 Zřeknutí se záruk

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

9.8 Omezení odpovědnosti

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

9.9 Odpovědnost za škodu, náhrada škody

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

9.10 Doba platnosti, ukončení platnosti

9.10.1 Doba platnosti

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

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.

9.11 Komunikace mezi zúčastněnými subjekty

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

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

Tyto skutečnosti jsou pro aplikaci tohoto vydání CPS irelevantní.

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 je provozován ve shodě s relevantní legislativou.

9.16 Další ustanovení

9.16.1 Rámcová dohoda

Tyto skutečnosti jsou pro aplikaci tohoto vydání CPS irelevantní.

9.16.2 Postoupení práv

Tyto skutečnosti jsou pro aplikaci tohoto vydání CPS irelevantní.

Certifikační prováděcí směrnice vydávání root certifikátů SICA	Strana 47 (celkem 48)
Copyright © První certifikační autorita, a.s.	

9.16.3 Oddělitelnost ustanovení

Tyto skutečnosti jsou pro aplikaci tohoto vydání CPS irelevantní.

9.16.4 Zřeknutí se práv

Tyto skutečnosti jsou pro aplikaci tohoto vydání CPS irelevantní.

9.16.5 Vyšší moc

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

9.17 Další opatření

Tyto skutečnosti jsou pro aplikaci tohoto vydání CPS irelevantní.

<i>Certifikační prováděcí směrnice vydávání root certifikátů SICA</i>	<i>Strana 48 (celkem 48)</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.