První certifikační autorita, a.s.

Certifikační politika

vydávání certifikátů OCSP respondérů

(algoritmus RSA)

Verze 1.10

OBSAH

1 Úvod 12
1.1 Přehled 12
1.2 Název a jednoznačné určení dokumentu 13
1.3 Participující subjekty 13
1.3.1 Certifikační autority (dále „CA") 13
1.3.2 Registrační autority (dále „RA") 13
1.3.3 Držitelé kvalifikovaných certifikátů a podepisující nebo označující osoby, kteří požádali o vydání kvalifikovaného certifikátu nebo kvalifikovaného systémového certifikátu (dále certifikátu), a kterým byl certifikát vydán 13
1.3.4 Spoléhající se strany 13
1.3.5 Jiné participující subjekty 14
1.4 Použití certifikátu 14
1.4.1 Přípustné použití certifikátu 14
1.4.2 Omezení použití certifikátu 14
1.5 Správa politiky 14
1.5.1 Organizace spravující certifikační politiku nebo certifikační prováděcí směrnici 14
1.5.2 Kontaktní osoba organizace spravující certifikační politiku nebo certifikační prováděcí směrnici 14
1.5.3 Subjekt odpovědný za rozhodování o souladu postupů poskytovatele s postupy jiných poskytovatelů certifikačních služeb 14
1.5.4 Postupy při schvalování souladu podle bodu 1.5.3 14
1.6 Přehled použitých pojmů a zkratek 15
1.6.1 Použité pojmy a zkratky 15
2 Odpovědnost za zveřejňování a úložiště informací a dokumentace 18
2.1 Úložiště informací a dokumentace 18
2.2 Zveřejňování informací a dokumentace 18
2.3 Periodicita zveřejňování informací 19
2.4 Řízení přístupu k jednotlivým typům úložišť 19
3 Identifikace a autentizace 20
3.1 Pojmenování 20
3.1.1 Typy jmen 20
3.1.2 Požadavek na významovost jmen 20
3.1.3 Anonymita a používání pseudonymu 20
3.1.4 Pravidla pro interpretaci různých forem jmen 20

3.1.5 Jedinečnost jmen....20
3.1.6 Obchodní značky....20
3.2 Počáteční ověření identity....20
3.2.1 Ověřování souladu dat, tj. postup při ověřování, zda má osoba data pro vytváření elektronických podpisů odpovídající datům pro ověřování elektronických podpisů nebo data pro vytváření elektronických značek odpovídající datům pro ověřování elektronických značek....20
3.2.2 Ověřování identity právnické osoby nebo organizační složky státu....21
3.2.3 Ověřování identity fyzické osoby....21
3.2.4 Neověřené informace vztahující se k držiteli certifikátu nebo podepisující či označující osobě....21
3.2.5 Ověřování specifických práv....21
3.2.6 Kritéria pro interoperabilitu....21
3.3 Identifikace a autentizace při zpracování požadavků na výměnu dat pro ověřování elektronických podpisů nebo dat pro ověřování elektronických značek v certifikátu....22
3.3.1 Identifikace a autentizace při rutinní výměně dat pro vytváření elektronických podpisů nebo dat pro vytváření elektronických značek a jim odpovídajících dat pro ověřování elektronických podpisů nebo dat pro ověřování elektronických značek (dále „párová data“)....22
3.3.2 Identifikace a autentizace při výměně párových dat po zneplatnění certifikátu....22
3.4 Identifikace a autentizace při zpracování požadavků na zneplatnění certifikátu....22
4 Požadavky na životní cyklus certifikátu....23
4.1 Žádost o vydání certifikátu....23
4.1.1 Subjekty oprávněné podat žádost o vydání certifikátu....23
4.1.2 Registrační proces a odpovědnosti poskytovatele a žadatele....23
4.2 Zpracování žádosti o certifikát....23
4.2.1 Identifikace a autentizace....23
4.2.2 Přijetí nebo zamítnutí žádosti o certifikát....23
4.2.3 Doba zpracování žádosti o certifikát....24
4.3 Vydání certifikátů....24
4.3.1 Úkony CA v průběhu vydávání certifikátu....24
4.3.2 Oznámení o vydání certifikátu držiteli certifikátu, podepisující nebo označující osobě....24
4.4 Převzetí vydaného certifikátu....24
4.4.1 Úkony spojené s převzetím certifikátu....24
4.4.2 Zveřejňování vydaných certifikátů poskytovatelem....24

4.4.3 Oznámení o vydání certifikátu jiným subjektům 24
4.5 Použití párových dat a certifikátu 25
4.5.1 Použití dat pro vytváření elektronických podpisů nebo dat pro vytváření elektronických značek a certifikátu držitelem certifikátu, podepisující nebo označující osobou 25
4.5.2 Použití dat pro ověřování elektronických podpisů nebo dat pro ověřování elektronických značek a certifikátu spoléhající se stranou 25
4.6 Obnovení certifikátu 25
4.6.1 Podmínky pro obnovení certifikátu 25
4.6.2 Subjekty oprávněné požadovat obnovení certifikátu 25
4.6.3 Zpracování požadavku na obnovení certifikátu 25
4.6.4 Oznámení o vydání obnoveného certifikátu držiteli certifikátu, podepisující nebo označující osobě 25
4.6.5 Úkony spojené s převzetím obnoveného certifikátu 25
4.6.6 Zveřejňování vydaných obnovených certifikátů poskytovatelem 26
4.6.7 Oznámení o vydání obnoveného certifikátu jiným subjektům 26
4.7 Výměna dat pro ověřování elektronických podpisů nebo dat pro ověřování elektronických značek v certifikátu 26
4.7.1 Podmínky pro výměnu dat pro ověřování elektronických podpisů nebo dat pro ověřování elektronických značek v certifikátu 26
4.7.2 Subjekty oprávněné požadovat výměnu dat pro ověřování elektronických podpisů nebo dat pro ověřování elektronických značek v certifikátu 26
4.7.3 Zpracování požadavku na výměnu dat pro ověřování elektronických podpisů nebo dat pro ověřování elektronických značek 26
4.7.4 Oznámení o vydání certifikátu s vyměněnými daty pro ověřování elektronických podpisů nebo daty pro ověřování elektronických značek podepisující nebo označující osobě 26
4.7.5 Úkony spojené s převzetím certifikátu s vyměněnými daty pro ověřování elektronických podpisů nebo daty pro ověřování elektronických značek 26
4.7.6 Zveřejnění vydaných certifikátů s vyměněnými daty pro ověřování elektronických podpisů nebo daty pro ověřování elektronických značek 26
4.7.7 Oznámení o vydání certifikátu s vyměněnými daty pro ověřování elektronických podpisů nebo daty pro ověřování elektronických značek jiným subjektům 27
4.8 Změna údajů v certifikátu 27
4.8.1 Podmínky pro změnu údajů v certifikátu 27
4.8.2 Subjekty oprávněné požadovat změnu údajů v certifikátu 27

4.8.3 Zpracování požadavku na změnu údajů v certifikátu 27
4.8.4 Oznámení o vydání certifikátu se změněnými údaji podepisující nebo označující osobě 27
4.8.5 Úkony spojené s převzetím certifikátu se změněnými údaji 27
4.8.6 Zveřejňování vydaných certifikátů se změněnými údaji 27
4.8.7 Oznámení o vydání certifikátu se změněnými údaji jiným subjektům 27
4.9 Zneplatnění a pozastavení platnosti certifikátu 27
4.9.1 Podmínky pro zneplatnění certifikátu 28
4.9.2 Subjekty oprávněné žádat o zneplatnění certifikátu 28
4.9.3 Požadavek na zneplatnění certifikátu 28
4.9.4 Doba odkladu požadavku na zneplatnění certifikátu 28
4.9.5 Maximální doba, za kterou musí poskytovatel realizovat požadavek na zneplatnění certifikátu 28
4.9.6 Povinnosti spoléhajících se stran při ověřování, zda nebyl certifikát zneplatněn 28
4.9.7 Periodicita vydávání seznamu zneplatněných certifikátů 28
4.9.8 Maximální zpoždění při vydávání seznamu zneplatněných certifikátů 29
4.9.9 Možnost ověřování statutu certifikátu on-line (dále „OCSP“) 29
4.9.10 Požadavky při ověřování statutu certifikátu on-line 29
4.9.11 Jiné způsoby oznamování zneplatnění certifikátu 29
4.9.12 Případné odlišnosti postupu zneplatnění v případě kompromitace dat pro vytváření elektronických podpisů nebo dat pro vytváření elektronických značek 29
4.9.13 Podmínky pro pozastavení platnosti certifikátu 29
4.9.14 Subjekty oprávněné požadovat pozastavení platnosti certifikátu 29
4.9.15 Zpracování požadavku na pozastavení platnosti certifikátu 29
4.9.16 Omezení doby pozastavení platnosti certifikátu 29
4.10 Služby související s ověřováním statutu certifikátu 29
4.10.1 Funkční charakteristiky 30
4.10.2 Dostupnost služeb 30
4.10.3 Další charakteristiky služeb statutu certifikátu 30
4.11 Ukončení poskytování služeb pro držitele certifikátu, podepisující nebo označující osobu 30
4.12 Úschova dat pro vytváření elektronických podpisů nebo pro vytváření elektronických značek u důvěryhodné třetí strany a jejich obnova 30
4.12.1 Politika a postupy při úschově a obnovování dat pro vytváření elektronických podpisů nebo dat pro vytváření elektronických značek 30

4.12.2 Politika a postupy při zapouzdřování a obnovování šifrovacího klíče pro relaci 30
5 Management, provozní a fyzická bezpečnost 31
5.1 Fyzická bezpečnost 31
5.1.1 Umístění a konstrukce 31
5.1.2 Fyzický přístup 31
5.1.3 Elektřina a klimatizace 31
5.1.4 Vlivy vody 31
5.1.5 Protipožární opatření a ochrana 32
5.1.6 Ukládání médií 32
5.1.7 Nakládání s odpady 32
5.1.8 Zálohy mimo budovu 32
5.2 Procesní bezpečnost 32
5.2.1 Důvěryhodné role 32
5.2.2 Počet osob požadovaných na zajištění jednotlivých činností 32
5.2.3 Identifikace a autentizace pro každou roli 33
5.2.4 Role vyžadující rozdělení povinností 33
5.3 Personální bezpečnost 33
5.3.1 Požadavky na kvalifikaci, zkušenosti a bezúhonnost 33
5.3.2 Posouzení spolehlivosti osob 33
5.3.3 Požadavky na přípravu pro výkon role, vstupní školení 34
5.3.4 Požadavky a periodicita školení 34
5.3.5 Periodicita a posloupnost rotace pracovníků mezi různými rolemi 34
5.3.6 Postihy za neoprávněné činnosti zaměstnanců 34
5.3.7 Požadavky na nezávislé zhotovitele (dodavatele) 34
5.3.8 Dokumentace poskytovaná zaměstnancům 34
5.4 Auditní záznamy (logy) 34
5.4.1 Typy zaznamenávaných událostí 34
5.4.2 Periodicita zpracování záznamů 35
5.4.3 Doba uchování auditních záznamů 35
5.4.4 Ochrana auditních záznamů 35
5.4.5 Postupy pro zálohování auditních záznamů 35
5.4.6 Systém shromažďování auditních záznamů (interní nebo externí) 35
5.4.7 Postup při oznamování události subjektu, který ji způsobil 35
5.4.8 Hodnocení zranitelnosti 36
5.5 Uchovávání informací a dokumentace 36
5.5.1 Typy informací a dokumentace, které se uchovávají 36

5.5.2 Doba uchování uchovávaných informací a dokumentace 36
5.5.3 Ochrana úložiště uchovávaných informací a dokumentace 36
5.5.4 Postupy při zálohování uchovávaných informací a dokumentace 36
5.5.5 Požadavky na používání časových razítek při uchovávání informací a dokumentace 37
5.5.6 Systém shromažďování uchovávaných informací a dokumentace (interní nebo externí) 37
5.5.7 Postupy pro získání a ověření uchovávaných informací a dokumentace 37
5.6 Výměna dat pro ověřování elektronických značek v nadřízeném kvalifikovaném systémovém certifikátu poskytovatele 37
5.7 Obnova po havárii nebo kompromitaci 37
5.7.1 Postup v případě incidentu a kompromitace 37
5.7.2 Poškození výpočetních prostředků, softwaru nebo dat 38
5.7.3 Postup při kompromitaci dat pro vytváření elektronických značek poskytovatele 38
5.7.4 Schopnost obnovit činnost po havárii 38
5.8 Ukončení činnosti CA nebo RA 38
6 Technická bezpečnost 39
6.1 Generování a instalace párových dat 39
6.1.1 Generování párových dat 39
6.1.2 Předání dat pro vytváření elektronických podpisů nebo dat pro vytváření elektronických značek podepisující nebo označující osobě 39
6.1.3 Předání dat pro ověřování elektronických podpisů nebo dat pro ověřování elektronických značek poskytovateli certifikačních služeb 39
6.1.4 Poskytování dat pro ověřování elektronických podpisů nebo dat pro ověřování elektronických značek certifikační autoritou spoléhajícím se stranám 39
6.1.5 Délky párových dat 39
6.1.6 Generování parametrů dat pro ověřování elektronických podpisů nebo dat pro ověřování elektronických značek a kontrola jejich kvality 39
6.1.7 Omezení pro použití dat pro ověřování elektronických podpisů nebo dat pro ověřování elektronických značek 40
6.2 Ochrana dat pro vytváření elektronických podpisů nebo dat pro vytváření elektronických značek a bezpečnost kryptografických modulů 40
6.2.1 Standardy a podmínky používání kryptografických modulů 40
6.2.2 Sdílení tajemství 40

6.2.3 Úschova dat pro vytváření elektronických podpisů nebo dat pro vytváření elektronických značek 40
6.2.4 Zálohování dat pro vytváření elektronických podpisů nebo dat pro vytváření elektronických značek 40
6.2.5 Uchovávání dat pro vytváření elektronických podpisů nebo dat pro vytváření elektronických značek 40
6.2.6 Transfer dat pro vytváření elektronických značek do kryptografického modulu nebo z kryptografického modulu 40
6.2.7 Uložení dat pro vytváření elektronických značek v kryptografickém modulu 41
6.2.8 Postup při aktivaci dat pro vytváření elektronických podpisů nebo dat pro vytváření elektronických značek 41
6.2.9 Postup při deaktivaci dat pro vytváření elektronických podpisů nebo dat pro vytváření elektronických značek 41
6.2.10 Postup při zničení dat pro vytváření elektronických podpisů nebo dat pro vytváření elektronických značek 41
6.2.11 Hodnocení kryptografických modulů 42
6.3 Další aspekty správy párových dat 42
6.3.1 Uchovávání dat pro ověřování elektronických podpisů nebo dat pro ověřování elektronických značek 42
6.3.2 Maximální doba platnosti certifikátu vydaného podepisující nebo označující osobě a párových dat 42
6.4 Aktivační data 42
6.4.1 Generování a instalace aktivačních dat 42
6.4.2 Ochrana aktivačních dat 42
6.4.3 Ostatní aspekty aktivačních dat 42
6.5 Počítačová bezpečnost 42
6.5.1 Specifické technické požadavky na počítačovou bezpečnost 42
6.5.2 Hodnocení počítačové bezpečnosti 43
6.6 Bezpečnost životního cyklu 44
6.6.1 Řízení vývoje systému 44
6.6.2 Kontroly řízení bezpečnosti 44
6.6.3 Řízení bezpečnosti životního cyklu 44
6.7 Síťová bezpečnost 44
6.8 Časová razítka 44
7 Profily certifikátu, seznamu zneplatněných certifikátů a OCSP 45
7.1 Profil certifikátu 45
7.1.1 Číslo verze 45
7.1.2 Rozšiřující položky v certifikátu 46

7.1.3 Objektové identifikátory (dále „OID") algoritmů 47
7.1.4 Způsoby zápisu jmen a názvů 47
7.1.5 Omezení jmen a názvů 47
7.1.6 OID certifikační politiky 47
7.1.7 Rozšiřující položka „Policy Constrainsts" 47
7.1.8 Syntaxe a sémantika rozšiřující položky kvalifikátorů politiky „Policy Qualifiers" 47
7.1.9 Způsob zápisu kritické rozšiřující položky „Certificate Policies" 47
7.2 Profil seznamu zneplatněných certifikátů 48
7.2.1 Číslo verze 48
7.2.2 Rozšíření CRL a záznamů CRL 48
7.3 Profil OCSP 49
7.3.1 Číslo verze 49
7.3.2 Rozšiřující položky OCSP 49
8 Hodnocení shody a jiná hodnocení 50
8.1 Periodicita hodnocení nebo okolnosti pro provedení hodnocení 50
8.2 Identita a kvalifikace hodnotitele 50
8.3 Vztah hodnotitele k hodnocenému subjektu 50
8.4 Hodnocené oblasti 50
8.5 Postup v případě zjištění nedostatků 50
8.6 Sdělování výsledků hodnocení 50
9 Ostatní obchodní a právní záležitosti 51
9.1 Poplatky 51
9.1.1 Poplatky za vydání nebo obnovení certifikátu 51
9.1.2 Poplatky za přístup k certifikátu na seznamu vydaných certifikátů 51
9.1.3 Poplatky za informace o statutu certifikátu nebo o zneplatnění certifikátu 51
9.1.4 Poplatky za další služby 51
9.1.5 Jiná ustanovení týkající se poplatků (vč. refundací) 51
9.2 Finanční odpovědnost 51
9.2.1 Krytí pojištěním 51
9.2.2 Další aktiva a záruky 51
9.2.3 Pojištění nebo krytí zárukou pro koncové uživatele 52
9.3 Citlivost obchodních informací 52
9.3.1 Výčet citlivých informací 52
9.3.2 Informace mimo rámec citlivých informací 52
9.3.3 Odpovědnost za ochranu citlivých informací 52

9.4 Ochrana osobních údajů 52
9.4.1 Politika ochrany osobních údajů 52
9.4.2 Osobní údaje 52
9.4.3 Údaje, které nejsou považovány za citlivé 52
9.4.4 Odpovědnost za ochranu osobních údajů 53
9.4.5 Oznámení o používání důvěrných informací a souhlas s používáním citlivých informací 53
9.4.6 Poskytnutí citlivých informací pro soudní či správní účely 53
9.4.7 Jiné okolnosti zpřístupňování osobních údajů 53
9.5 Práva duševního vlastnictví 53
9.6 Zastupování a záruky 53
9.6.1 Zastupování a záruky CA 53
9.6.2 Zastupování a záruky RA 53
9.6.3 Zastupování a záruky držitele certifikátu, podepisující nebo označující osoby 54
9.6.4 Zastupování a záruky spoléhajících se stran 54
9.6.5 Zastupování a záruky ostatních zúčastněných subjektů 54
9.7 Zřeknutí se záruk 54
9.8 Omezení odpovědnosti 54
9.9 Odpovědnost za škodu, náhrada škody 54
9.10 Doba platnosti, ukončení platnosti 54
9.10.1 Doba platnosti 54
9.10.2 Ukončení platnosti 54
9.10.3 Důsledky ukončení a přetrvání závazků 54
9.11 Komunikace mezi zúčastněnými subjekty 55
9.12 Změny 55
9.12.1 Postup při změnách 55
9.12.2 Postup při oznamování změn 55
9.12.3 Okolnosti, při kterých musí být změněn OID 55
9.13 Řešení sporů 55
9.14 Rozhodné právo 55
9.15 Shoda s právními předpisy 55
9.16 Další ustanovení 56
9.16.1 Rámcová dohoda 56
9.16.2 Postoupení práv 56
9.16.3 Oddělitelnost ustanovení 56
9.16.4 Zřeknutí se práv 56

9.16.5 Vyšší moc....56
9.17 Další opatření....56
10 Závěrečná ustanovení....57

tab. 1 - Vývoj dokumentu

Verze	Datum vydání	Schválil	Poznámka
1.0	15.07.2015	Ředitel společnosti První certifikační autorita, a.s.	První vydání.
1.10	02.11.2015	Ředitel společnosti První certifikační autorita, a.s.	Úprava profilu certifikátu.

1 ÚVOD

Tento dokument byl vypracován na základě požadavků platných standardů vztahujících se k problematice využívání kryptografických algoritmů v procesu poskytování certifikačních služeb. Kořenová kvalifikovaná certifikační autorita (algoritmus RSA) společnosti První certifikační autorita, a.s., dále též I.CA, vydává v hierarchické dvoustupňové struktuře certifikačních autorit, v souladu s požadavky technických standardů certifikáty s algoritmem RSA pro vydávající certifikační autority - všechny provozuje I.CA. Vydávající certifikační autorita může, v závislosti na požadavcích platné legislativy a technických standardů, nebo na dalších požadavcích, které jsou na ni kladeny, provozovat svůj OCSP respondér a vydávat pro něj certifikáty. Jejich vydávání se řídí touto certifikační politikou.

Pozn.: Pokud jsou v dalším textu uváděny odkazy na standardy nebo zákony, jedná se vždy buď o uvedený standard nebo zákon, resp. standard či zákon, který ho nahrazuje. Pokud by byla tato politika v rozporu se standardy nebo zákony, které nahradí dosud platné, bude vydána její nová verze.

1.1 Přehled

Dokument **Certifikační politika vydávání certifikátů OCSP respondérů (algoritmus RSA)**, dále též CP, vypracovaný společností První certifikační autorita, a. s., se zabývá skutečnostmi, vztahujícími se k procesům životního cyklu vydávaných certifikátů dodržuje strukturu, jejíž předlohou je osnova platného standardu RFC 3647, s přihlédnutím k platným standardům Evropské unie a k právu České republiky a Slovenské republiky v dané oblasti (jednotlivé kapitoly jsou proto v tomto dokumentu zachovány i v případě, že jsou ve vztahu k ní irelevantní). Dokument je rozdělen do devíti základních kapitol, jejichž stručný popis je uveden v následujícím seznamu:

- Kapitola 1 identifikuje tento dokument přiřazeným jedinečným identifikátorem, obecně popisuje subjekty, které participují na poskytování této certifikační služby a definuje přípustné využívání vydávaných certifikátů.
- Kapitola 2 popisuje problematiku odpovědností za zveřejňování informací, resp. dokumentace.
- Kapitola 3 popisuje procesy identifikace a autentizace žadatele o vydání certifikátu, resp. zneplatnění certifikátu, včetně definování typů a obsahů používaných jmen ve vydávaných certifikátech.
- Kapitola 4 definuje procesy životního cyklu jí vydávaných certifikátů, tzn. žádost o vydání a vlastní vydání certifikátu, žádost o zneplatnění a vlastní zneplatnění certifikátu, služby související s ověřováním stavu certifikátu, ukončení poskytování certifikačních služeb atd.
- Kapitola 5 zahrnuje problematiku fyzické, procesní a personální bezpečnosti, včetně definování množiny zaznamenávaných událostí, uchovávání těchto záznamů a reakce po haváriích nebo kompromitaci.
- Kapitola 6 je zaměřena na technickou bezpečnost typu generování veřejných a soukromých klíčů, ochrany soukromých klíčů, včetně počítačové a síťové ochrany.
- Kapitola 7 definuje profil vydávaných certifikátů a seznamů zneplatněných certifikátů.
- Kapitola 8 je zaměřena na problematiku hodnocení poskytovaných certifikačních služeb.

- Kapitola 9 zahrnuje problematiku obchodní a právní.

Tento dokument může být mimo jiné využit nezávislými institucemi (např. auditorskými společnostmi) jako základ pro potvrzení toho, že certifikační služby v oblasti vydávaní certifikátů, poskytované společností První certifikační autorita, a.s., je možné považovat za důvěryhodné.

OCSP respondéry, provozované společností První certifikační autorita, a. s., jsou autorizovanými respondéry v souladu se standardem RFC 2560, tzn. certifikát veřejného klíče OCSP respondéru je vydán tou certifikační autoritou, která vydala certifikát koncovému uživateli, na jehož stav tento OCSP respondér odpovídá.

Bližší podrobnosti o naplnění položek certifikátů vydávaných podle této politiky a o jejich správě mohou být uvedeny v odpovídající certifikační prováděcí směrnici (dále CPS).

1.2 Název a jednoznačné určení dokumentu

Název a identifikace dokumentu:	Certifikační politika vydávání certifikátů OCSP respondérů (algoritmus RSA), verze 1.10
OID politiky:	1.3.6.1.4.1.23624.10.1.80.1.1

1.3 Participující subjekty

1.3.1 Certifikační autority (dále „CA")

Veřejné certifikační autority, provozované společností První certifikační autorita, a.s., vydávající certifikáty koncovým uživatelům. Ty mohou provozovat svoje OCSP respondéry.

1.3.2 Registrační autority (dále „RA")

Na procesech životního cyklu certifikátů vydávaných dle této CP se podílí registrační autorita ve vlastnictví I.CA.

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

Certifikáty, vydávané dle této CP, jsou určeny výhradně pro OCSP respondéry certifikačních autorit provozovaných I.CA, vydávajících certifikáty koncovým uživatelům. Oprávněným žadatelem a následně držitelem certifikátů je I.CA jako právnická osoba.

1.3.4 Spoléhající se strany

Spoléhající se stranou jsou v případě této CP subjekty spoléhající se při své činnosti na certifikáty, vydávané podle této CP.

1.3.5 Jiné participující subjekty

Jinými participujícími subjekty jsou orgány činné v trestním řízení, případně orgány dozoru a další, kterým to dle platné legislativy přísluší.

1.4 Použití certifikátu

1.4.1 Přípustné použití certifikátu

Certifikáty vydávané podle této CP smějí být používány výhradně pro ověřování OCSP odpovědí na stav certifikátu koncového uživatele.

1.4.2 Omezení použití certifikátu

Certifikáty vydávané podle této CP nesmějí být používány v rozporu s přípustným použitím popsaným v kapitola 1.4.1 a dále pro jakékoliv nelegální účely.

1.5 Správa politiky

1.5.1 Organizace spravující certifikační politiku nebo certifikační prováděcí směrnici

Tuto CP, resp. jí odpovídající certifikační prováděcí směrnici (dále též CPS), spravuje společnost První certifikační autorita, a.s.

1.5.2 Kontaktní osoba organizace spravující certifikační politiku nebo certifikační prováděcí směrnici

Kontaktní osoba společnosti První certifikační autorita, a.s., v souvislosti s touto CP, resp. s odpovídající CPS, je uvedena na internetové 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 společnosti První certifikační autorita, a.s., s postupy jiných poskytovatelů certifikačních služeb, je ředitel společnosti První certifikační autorita, a.s.

1.5.4 Postupy při schvalování souladu podle bodu 1.5.3

V případě, že je potřebné provést změny v této CP s ohledem na soulad dle kapitoly 1.5.3 a vytvořit její novou verzi, určuje ředitel společnosti První certifikační autorita, a.s., osobu, která je oprávněna tyto změny provést. Nabytí platnosti nové verze CP předchází její schválení ředitelem společnosti První certifikační autorita, a.s. Dále platí požadavky kapitoly 9.12.

1.6 Přehled použitých pojmů a zkratek

1.6.1 Použité pojmy a zkratky

tab. 2 - Pojmy a zkratky

Pojem	Vysvětlení
bit	z anglického *binary digit* - číslice dvojkové soustavy - je základní a současně nejmenší jednotkou informace používanou především v číslicové technice
CA	certifikační autorita
CEN	European Committee for Standardization, asociace sdružující národní standardizační orgány
CP	certifikační politika
CPS	certifikační prováděcí směrnice
CRL	Certificate Revocation List, seznam zneplatněných certifikátů obsahující certifikáty, které již nelze pokládat za platné
CWA	CEN Workshop Agreement, referenční dokument CEN
ČR	Česká republika
data pro ověřování elektronické značky	jedinečná data, která se používají pro ověření elektronické značky
data pro ověřování elektronického podpisu	jedinečná data, která se používají pro ověření elektronického podpisu
data pro vytváření elektronické značky	jedinečná data, která označující osoba používá k vytváření elektronické značky
data pro vytváření elektronického podpisu	jedinečná data, která podepisující osoba používá k vytváření elektronického podpisu
DER, PEM	způsoby zakódování (formáty) certifikátu
dvoufaktorová autentizace	autentizace využívající dvou ze tří faktorů - něco vím (heslo), něco mám (např. čipová karta, hardwarový token) nebo něco jsem (otisky prstů, snímání oční sítnice či duhovky)
elektronická značka	údaje v elektronické podobě, které jsou připojené k datové zprávě nebo jsou s ní logicky spojené a které splňují následující požadavky: ▪ jsou jednoznačně spojené s označující osobou a umožňují její identifikaci prostřednictvím kvalifikovaného systémového certifikátu, ▪ byly vytvořeny a připojeny k datové zprávě pomocí prostředků pro vytváření elektronických značek, které označující osoba může udržet pod svou výhradní kontrolou, ▪ jsou k datové zprávě, ke které se vztahují, připojeny takovým způsobem, že je možné zjistit jakoukoli následnou změnu dat

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
EN	European Standard, typ ETSI standardu
ETSI	the European Telecommunications Standards Institute, evropský standardizační institut v oblasti informačních a komunikačních technologií
FIPS	Federal Information Processing Standard, označení standardů v oblasti informačních technologií pro nevojenské státní organizace ve Spojených státech
hash	transformace, která jako vstup přijímá řetězec znaků o libovolné délce a výsledkem je řetězec znaků s pevnou délkou
IEC	International Electrotechnical Commission, světová organizace publikující standardy pro elektrotechniku, elektroniku, sdělovací techniku a příbuzné obory
ITU	International Telecommunication Union
ITU-T	Telecommunication Standardization Sector of ITU
ISO	International Organization for Standardization, mezinárodní organizace sdružující národní standardizační organizace, označení standardů
kořenová CA	CA, vydávající certifikáty vydávajícím CA
kvalifikovaný systémový certifikát	certifikát, který má náležitosti podle platné legislativy
OCSP	Online Certificate Status Protocol, protokol pro zjišťování stavu certifikátu veřejného klíče
OCSP respondér	server poskytují protokolem OCSP údaje o stavu certifikátu veřejného klíče
označující osoba	fyzická osoba, právnická osoba nebo organizační složka státu, která drží prostředek pro vytváření elektronických značek a označuje datovou zprávu elektronickou značkou
párová data	jedinečná data pro vytváření elektronického podpisu /elektronické značky spolu s odpovídajícími daty pro ověřování elektronického podpisu /elektronické značky
PKCS	Public Key Cryptography Standards, označení skupiny standardů pro kryptografii s veřejným klíčem
PUB	Publication, označení standardu FIPS
RA	registrační autorita
RFC	Request for Comments, označení řady standardů a dalších dokumentů popisujících internetové protokoly, systémy apod.
RSA	šifra s veřejným klíčem pro podepisování a šifrování (iniciály původních autorů Rivest, Shamir a Adleman)

SHA	typ hashovací funkce
smluvní partner	poskytovatel vybraných certifikačních služeb, který zajišťuje na základě písemné smlouvy pro I.CA certifikační služby nebo jejich části - nejčastěji se jedná o smluvní RA
soukromý klíč	jedinečná data pro vytváření elektronického podpisu /elektronické značky
spoléhající se strana	subjekt, spoléhající se při své činnosti na certifikát vydaný CA
SSCD	Secure Signature Creation Device, bezpečné zařízení pro tvorbu elektronického podpisu (dle definice ve Směrnici)
TS	Technical Specification, typ ETSI standardu
URI	Uniform Resource Identifier, textový řetězec s definovanou strukturou sloužící k přesné specifikaci zdroje informací
veřejný klíč	jedinečná data pro ověřování elektronického podpisu /elektronické značky
podřízená CA	pro účely tohoto dokumentu: CA vydávající certifikáty koncovým uživatelům
X.501, X.509, X.520	standardy pro systémy založené na veřejném klíči
zákon o ochraně utajovaných informací	zákon České republiky č. 412/2005 Sb., o ochraně utajovaných informací a o bezpečnostní způsobilosti, ve znění pozdějších předpisů
zákoník práce	zákon České republiky č. 262/2006 Sb., zákoník práce, ve znění pozdějších předpisů
ZoEP	▪ zákon České republiky č. 227/2000 Sb., o elektronickém podpisu a o změně některých dalších zákonů (zákon o elektronickém podpisu), ve znění pozdějších předpisů, ▪ zákon Slovenské republiky č. 215/2002 Z.z. o elektronickom podpise a o zmene a doplnení niektorých zákonov
ZOOÚ	▪ zákon České republiky č. 4101/2000 Sb., o ochraně osobních údajů a o změně některých zákonů (zákon o ochraně osobních údajů), ve znění pozdějších předpisů, ▪ zákon Slovenské republiky č. 122/2013 Z.z. o ochrane osobných údajov a o zmene a doplnení niektorých zákonov

2 ODPOVĚDNOST ZA ZVEŘEJŇOVÁNÍ A ÚLOŽIŠTĚ INFORMACÍ A DOKUMENTACE

2.1 Úložiště informací a dokumentace

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

2.2 Zveřejňování informací a dokumentace

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

- adresa sídla společnosti:

  První certifikační autorita, a.s.

  Podvinný mlýn 2178/6

  190 00 Praha 9

  Česká republika
- internetová adresa http://www.ica.cz,
- sídla registračních autorit.

Elektronické adresy, které slouží pro kontakt veřejnosti s I.CA, je info@ica.cz.

Na výše uvedené internetové adrese lze získat informace o:

- certifikátech - přímo se zveřejňují následující informace (ostatní informace lze získat z certifikátu):
  - číslo certifikátu,
  - obsah položky Obecné jméno (commonName),
  - údaj o počátku platnosti (s uvedením hodiny, minuty a sekundy),
  - odkazy na místo, kde lze certifikát získat v určených formátech (DER, PEM, TXT),
- seznamech zneplatněných certifikátů (CRL) - přímo 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).

Povolenými protokoly pro přístup k veřejným informacím jsou http a https. I.CA může bez udání důvodu přístup k některým informacím zrušit nebo pozastavit.

V případech vzniku důvodné obavy ze zneužití soukromých klíčů, sloužících v procesech vydávání certifikátů koncovým uživatelům, vydávání seznamů zneplatněných certifikátů, nebo poskytování informací o stavu certifikátů, oznámí I.CA tuto skutečnost na své

internetové informační adrese a prostřednictvím celostátně distribuovaného deníku Hospodářské noviny nebo Mladá fronta Dnes.

2.3 Periodicita zveřejňování informací

I.CA zveřejňuje informace s následující periodicitou:

- certifikační politika - po schválení a vydání nové verze,
- certifikační prováděcí směrnice - neprodleně (je-li určena ke zveřejnění),
- seznam vydaných certifikátů – aktualizace při každém vydání nového certifikátu,
- seznam zneplatněných certifikátů (CRL) - viz kapitola 4.9.7,
- zneplatnění certifikátu CA vydávající certifikáty koncovým uživatelů, s uvedením důvodu zneplatnění – bezodkladně,
- ostatní veřejné informace – není předem určeno, obecně však platí, že tyto informace musí reflektovat 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 zaměstnancům I.CA, nebo subjektům definovaným platnou legislativou. Přístup k těmto informacím je řízen pravidly uvedenými v interní dokumentaci.

3 IDENTIFIKACE A AUTENTIZACE

3.1 Pojmenování

3.1.1 Typy jmen

Veškerá jména jsou konstruována v souladu se standardem X.501, resp. s navazujícím standardem X.520.

3.1.2 Požadavek na významovost jmen

U všech certifikátů musí jména vyjadřovat účel, ke kterému je certifikát vydáván (OCSP respondér) a identifikaci certifikační autority, ve jménu které OCSP respondér vydává OCSP odpovědi.

Význam a obsah údajů, obsažených ve vydávaných certifikátech OCSP respondérů, je uveden v kapitole 7.

3.1.3 Anonymita a používání pseudonymu

Není relevantní pro tento dokument, není podporováno.

3.1.4 Pravidla pro interpretaci různých forem jmen

Údaje uváděné v žádosti o OCSP respondérů (formát PKCS#10) se do položky Subject, resp. SubjectAlternativeName ve vydávaných certifikátech OCSP respondéru přenášejí ve tvaru, ve kterém jsou uvedeny v předkládané žádosti.

3.1.5 Jedinečnost jmen

Společnost První certifikační autorita, a.s., zaručuje jedinečnost pole Subject v Certifikátu.

3.1.6 Obchodní značky

Certifikáty vydávané podle této CP mohou obsahovat pouze obchodní značky vlastněné společností První certifikační autorita, a.s.

3.2 Počáteční ověření identity

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

Vlastnictví soukromého klíče odpovídajícího veřejnému klíči v žádosti o certifikát se prokazuje předložením žádosti ve formátu PKCS#10. Ta je zmíněným soukromým klíčem

elektronicky podepsána a žadatel o certifikát tak prokazuje, že v době tvorby elektronického podpisu soukromý klíč vlastnil.

3.2.2 Ověřování identity právnické osoby nebo organizační složky státu

Certifikáty vydávané dle této CP jsou vydávány pouze pro právnickou osobu I.CA. Její identita se prokazuje výpisem z Obchodního rejstříku.

3.2.3 Ověřování identity fyzické osoby

Fyzickou osobou, která může ve jménu společnosti První certifikační autorita, a.s., žádat o vydání certifikátu dle této CP, je výhradně vedoucí provozního pracoviště.

V procesu ověřování identity jsou vyžadovány dva doklady, obsahující následující údaje.

Primárním osobním dokladem pro občany ČR musí být občanský průkaz. Primárním osobním dokladem pro cizince je platný cestovní pas, popř. obdobný doklad stejné právní váhy. Z tohoto dokladu jsou ověřovány následující údaje:

- celé občanské jméno,
- datum a místo narození (nebo rodné číslo u občanů České republiky, resp. Slovenské republiky),
- číslo předloženého primárního osobního dokladu,
- adresa trvalého bydliště (je-li v primárním dokladu uvedena).

Sekundární osobní doklad musí být vydán orgánem veřejné moci nebo jinou organizací, jejíž existenci lze doložit, a musí obsahovat celé občanské jméno fyzické osoby vyřizující žádost a dále nejméně jeden z následujících údajů:

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

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

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

Všechny informace musí být řádným způsobem ověřeny.

3.2.5 Ověřování specifických práv

Není relevantní pro tento dokument.

3.2.6 Kritéria pro interoperabilitu

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

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

3.3.1 Identifikace a autentizace při rutinní výměně dat pro vytváření elektronických podpisů nebo dat pro vytváření elektronických značek a jim odpovídajících dat pro ověřování elektronických podpisů nebo 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

Není relevantní pro tento dokument, služba výměny párových dat po zneplatnění certifikátu není podporována. 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

Oprávněnou osobou žádat o zneplatnění certifikátu OCSP respondéru je ředitel I.CA. Pro identifikaci a autentizaci platí požadavky kapitol 3.2.2 a 3.2.3.

4 POŽADAVKY NA ŽIVOTNÍ CYKLUS CERTIFIKÁTU

4.1 Žádost o vydání certifikátu

4.1.1 Subjekty oprávněné podat žádost o vydání certifikátu

Žádost o vydání certifikátu OCSP respondéru je oprávněn podat vedoucí provozního pracoviště.

4.1.2 Registrační proces a odpovědnosti poskytovatele a žadatele

Písemná žádost o prvotní vydání certifikátu OCSP respondéru je předkládána vedení společnosti První certifikační autorita, a.s., prostřednictvím vedoucího provozního pracoviště a musí obsahovat název a OID této certifikační politiky, včetně uvedení jména CA, která certifikát OCSP respondéru vydá. Žádost musí být vedoucím provozního pracoviště podepsána.

Další žádosti o vydání nového certifikátu témuž OCSP respondéru podává vedoucí provozního pracoviště přímo registrační autoritě.

4.1.2.1 Odpovědnost žadatele

Žadatel je povinen zejména:

- poskytovat pravdivé a úplné informace při registraci žádosti o vydání certifikátu,
- seznámit se s CP, podle které mu bude vydán certifikát.

4.1.2.2 Odpovědnost poskytovatele

Poskytovatel certifikačních služeb je zejména povinen certifikační služby poskytovat v souladu s příslušnou CP a CPS, Systémovou bezpečnostní politikou CA a provozní dokumentací.

4.2 Zpracování žádosti o certifikát

4.2.1 Identifikace a autentizace

Žadatel o certifikát se identifikuje a autentizuje způsobem, uvedeným v kapitolách 3.2.2 a 3.2.3.

4.2.2 Přijetí nebo zamítnutí žádosti o certifikát

Na základě písemné žádosti rozhodne vedení společnosti První certifikační autorita, a.s., o vydání prvotního certifikátu OCSP respondéru s příslušným jménem, případně o zamítnutí žádosti. Výsledek je dokumentován.

4.2.3 Doba zpracování žádosti o certifikát

Doba zpracování písemné žádosti o vydání certifikátu nepřekročí pět pracovních dnů ode dne předložení žádosti vedení společnosti.

4.3 Vydání certifikátů

4.3.1 Úkony CA v průběhu vydávání certifikátu

Po kladném vyřízení prvotní žádosti o certifikát, resp. v případě žádosti o vydání dalšího certifikátu téhož OCSP respondéru, následuje proces vydávání certifikátu, v jehož průběhu jsou prováděny nezbytné kontroly (formální správnost údajů obsažených v žádosti, řádné naplnění položek žádosti), zejména ověření:

- vlastnictví příslušného soukromého klíče,
- identity právnické osoby,
- identity fyzické osoby žadatele o certifikát,
- údajů obsažených v písemné žádosti,
- souladu údajů obsažených v žádosti o certifikát ve formátu PKCS#10 s údaji obsaženými v předkládaných dokumentech.

Pokud některá z výše uvedených ověření skončí negativně, proces vydání certifikátu je ukončen.

4.3.2 Oznámení o vydání certifikátu držiteli certifikátu, podepisující nebo označující osobě

Vedoucí provozního pracoviště je osobně přítomen vydání certifikátu.

4.4 Převzetí vydaného certifikátu

4.4.1 Úkony spojené s převzetím certifikátu

Vedoucí provozního pracoviště je povinen překontrolovat, zda jsou údaje obsažené ve vydaném certifikátu v souladu s údaji uvedenými v žádosti a v předkládaných dokumentech.

4.4.2 Zveřejňování vydaných certifikátů poskytovatelem

Certifikáty vydané podle této CP jsou zveřejněny způsobem podle bodu 2.2.

4.4.3 Oznámení o vydání certifikátu jiným subjektům

Platí ustanovení kapitoly 4.4.2.

4.5 Použití párových dat a certifikátu

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

Povinností označující /podepisující osoby je zejména:

- používat soukromý klíč a jemu odpovídající veřejný klíč obsažený ve vydaném certifikátu v souladu s touto CP,
- nakládat se soukromým klíčem, odpovídajícím veřejnému klíči v certifikátu vydaném podle této CP, tak, aby nemohlo dojít k jeho neoprávněnému použití.

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

Spoléhající se strany jsou zejména povinny ověřit certifikát OCSP respondéru a celou certifikační cestu podle platných standardů.

4.6 Obnovení certifikátu

Vždy se jedná o vydání nového certifikátu s novým veřejným klíčem, kdy všechny informace musí být řádným způsobem ověřeny. Platí stejné požadavky jako v případě počátečního ověření identity - viz kapitola 3.2.

4.6.1 Podmínky pro obnovení certifikátu

Viz kapitola 4.6.

4.6.2 Subjekty oprávněné požadovat obnovení certifikátu

Viz kapitola 4.6.

4.6.3 Zpracování požadavku na obnovení certifikátu

Viz kapitola 4.6.

4.6.4 Oznámení o vydání obnoveného certifikátu držiteli certifikátu, podepisující nebo označující osobě

Viz kapitola 4.6.

4.6.5 Úkony spojené s převzetím obnoveného certifikátu

Viz kapitola 4.6.

4.6.6 Zveřejňování vydaných obnovených certifikátů poskytovatelem

Viz kapitola 4.6.

4.6.7 Oznámení o vydání obnoveného certifikátu jiným subjektům

Viz kapitola 4.6.

4.7 Výměna dat pro ověřování elektronických podpisů nebo dat pro ověřování elektronických značek v certifikátu

Vždy se jedná o vydání nového certifikátu s novým veřejným klíčem, kdy všechny informace musí být řádným způsobem ověřeny. Platí stejné požadavky jako v případě počátečního ověření identity - viz kapitola 3.2.

4.7.1 Podmínky pro výměnu dat pro ověřování elektronických podpisů nebo dat pro ověřování elektronických značek v certifikátu

Viz kapitola 4.7.

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

Viz kapitola 4.7.

4.7.3 Zpracování požadavku na výměnu dat pro ověřování elektronických podpisů nebo dat pro ověřování elektronických značek

Viz kapitola 4.7.

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

Viz kapitola 4.7.

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

Viz kapitola 4.7.

4.7.6 Zveřejnění vydaných certifikátů s vyměněnými daty pro ověřování elektronických podpisů nebo daty pro ověřování elektronických značek

Viz kapitola 4.7.

4.7.7 Oznámení o vydání certifikátu s vyměněnými daty pro ověřování elektronických podpisů nebo daty pro ověřování elektronických značek jiným subjektům

Viz kapitola 4.7.

4.8 Změna údajů v certifikátu

Vždy se jedná o vydání nového certifikátu s novým veřejným klíčem, kdy všechny informace musí být řádným způsobem ověřeny. Platí stejné požadavky jako v případě počátečního ověření identity - viz kapitola 3.2.

4.8.1 Podmínky pro změnu údajů v certifikátu

Viz kapitola 4.8.

4.8.2 Subjekty oprávněné požadovat změnu údajů v certifikátu

Viz kapitola 4.8.

4.8.3 Zpracování požadavku na změnu údajů v certifikátu

Viz kapitola 4.8.

4.8.4 Oznámení o vydání certifikátu se změněnými údaji podepisující nebo označující osobě

Viz kapitola 4.8.

4.8.5 Úkony spojené s převzetím certifikátu se změněnými údaji

Viz kapitola 4.8.

4.8.6 Zveřejňování vydaných certifikátů se změněnými údaji

Viz kapitola 4.8.

4.8.7 Oznámení o vydání certifikátu se změněnými údaji jiným subjektům

Viz kapitola 4.8.

4.9 Zneplatnění a pozastavení platnosti certifikátu

Zneplatnění certifikátu OCSP respondéru znamená, že do doby vydání certifikátu nového je služba tohoto OCSP respondéru pozastavena.

Službu pozastavení platnosti certifikátu I.CA neposkytuje.

4.9.1 Podmínky pro zneplatnění certifikátu

Certifikát může být zneplatněn na základě následujících okolností:

- existuje důvodné podezření, že došlo ke kompromitaci, soukromého klíče, odpovídajícího veřejnému klíči tohoto certifikátu,
- žádost ředitele I.CA,
- technický obsah nebo formát certifikátu představují neakceptovatelné riziko (např. daný kryptografický /podepisovací algoritmus nebo délka klíče),
- pokud se jedná o kvalifikovaný systémový certifikát, nastanou-li skutečnosti uvedené v ZoEP.

4.9.2 Subjekty oprávněné žádat o zneplatnění certifikátu

Žádost o zneplatnění mohou podat:

- ředitel I.CA,
- pokud se jedná o kvalifikovaný systémový certifikát další subjekty definované ZoEP.

4.9.3 Požadavek na zneplatnění certifikátu

Viz kapitola 3.4.

4.9.4 Doba odkladu požadavku na zneplatnění certifikátu

Není relevantní pro tento dokument, služba odkladu požadavku na zneplatnění certifikátu není poskytována.

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

Požadavek na zneplatnění certifikátu musí být realizován bezodkladně po přijetí oprávněné žádosti o zneplatnění. CRL obsahující sériové číslo zneplatněného certifikátu OCSP respondéru musí být vydán neprodleně po zneplatnění tohoto certifikátu.

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

Není relevantní pro tento dokument, zneplatnění certifikátu OCSP respondéru není ověřováno.

4.9.7 Periodicita vydávání seznamu zneplatněných certifikátů

Seznam zneplatněných certifikátů, vydaných dle této CP, je vydáván po každém zneplatnění certifikátu OCSP respondéru a dále v pravidelných intervalech, nejvýše čtyřiadvacet hodin od vydání předchozího CRL.

4.9.8 Maximální zpoždění při vydávání seznamu zneplatněných certifikátů

Seznam zneplatněných certifikátů je zveřejňován neprodleně po jeho vydání.

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

Není relevantní pro tento dokument, stav certifikátu OCSP respondéru není ověřován.

4.9.10 Požadavky při ověřování statutu certifikátu on-line

Viz kapitola 4.9.9.

4.9.11 Jiné způsoby oznamování zneplatnění certifikátu

Viz kapitola 4.9.9.

4.9.12 Případné odlišnosti postupu zneplatnění v případě kompromitace dat pro vytváření elektronických podpisů nebo dat pro vytváření elektronických značek

Postup pro zneplatnění certifikátu v případě kompromitace soukromého klíče není odlišný od výše popsaného postupu pro zneplatnění certifikátu.

4.9.13 Podmínky pro pozastavení platnosti certifikátu

Není relevantní pro tento dokument, služba pozastavení platnosti certifikátu není poskytována.

4.9.14 Subjekty oprávněné požadovat pozastavení platnosti certifikátu

Není relevantní pro tento dokument, služba pozastavení platnosti certifikátu není poskytována.

4.9.15 Zpracování požadavku na pozastavení platnosti certifikátu

Není relevantní pro tento dokument, služba pozastavení platnosti certifikátu není poskytována.

4.9.16 Omezení doby pozastavení platnosti certifikátu

Není relevantní pro tento dokument, služba pozastavení platnosti certifikátu není poskytována.

4.10 Služby související s ověřováním statutu certifikátu

Není relevantní pro tento dokument, stav certifikátu OCSP respondéru není ověřován.

4.10.1 Funkční charakteristiky

Viz kapitola 4.10.

4.10.2 Dostupnost služeb

Viz kapitola 4.10.

4.10.3 Další charakteristiky služeb statutu certifikátu

Viz kapitola 4.10.

4.11 Ukončení poskytování služeb pro držitele certifikátu, podepisující nebo označující osobu

Viz kapitola 5.8.

4.12 Úschova dat pro vytváření elektronických podpisů nebo pro vytváření elektronických značek u důvěryhodné třetí strany a jejich obnova

Není relevantní pro tento dokument, služba úschovy soukromého klíče není poskytována.

4.12.1 Politika a postupy při úschově a obnovování dat pro vytváření elektronických podpisů nebo dat pro vytváření elektronických značek

Viz kapitola 4.12.

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

Viz kapitola 4.12.

5 MANAGEMENT, PROVOZNÍ A FYZICKÁ BEZPEČNOST

Management bezpečnosti je zaměřen především na:

- systémy poskytovaných certifikačních služeb,
- veškeré procesy podporující poskytování certifikačních služeb.

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

5.1 Fyzická bezpečnost

5.1.1 Umístění a konstrukce

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

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

5.1.2 Fyzický přístup

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 Vlivy vody

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

5.1.5 Protipožární opatření a ochrana

V objektech provozních pracovišť 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. dle ZoEP, 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 popsaném v interní dokumentaci.

5.2 Procesní bezpečnost

5.2.1 Důvěryhodné role

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

5.2.2 Počet osob požadovaných na zajištění jednotlivých činností

Pro procesy související s párovými daty certifikačních autorit a OCSP respondérů jsou definovány činnosti, které musí být vykonány za účasti více než jediné osoby. Jedná se zejména o:

- generování párových dat veškerých certifikačních autorit a OCSP respondéru kořenové certifikační autority,
- ničení soukromých klíčů veškerých certifikačních autorit a OCSP respondéru kořenové certifikační autority,
- zálohování soukromých klíčů kvalifikovaných certifikačních autorit včetně kořenové certifikační autority,
- obnovu soukromých klíčů veškerých certifikačních autorit a jejich OCSP respondérů,
- aktivaci kryptografického modulu, obsahujícího soukromé klíče výše uvedených párových dat.

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

5.2.3 Identifikace a autentizace pro každou roli

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

5.2.4 Role vyžadující rozdělení povinností

Role vyžadující rozdělení povinností, včetně popisu náplně jejich činnosti, jsou popsány v interní dokumentaci.

5.3 Personální bezpečnost

5.3.1 Požadavky na kvalifikaci, zkušenosti a bezúhonnost

Zaměstnanci I.CA v důvěryhodných rolích jsou vybíráni a přijímáni na základě dále popsaných personálních kritérií:

- naprostá občanská bezúhonnost - prokazováno tím, že tyto osoby nemají žádný záznam v rejstříku trestů (výpis z rejstříku trestů, nebo čestné prohlášení),
- vysokoškolské vzdělání v rámci akreditovaného bakalářského nebo magisterského studijního programu a nejméně tři roky praxe v oblasti informačních a komunikačních technologií, nebo středoškolské vzdělání a nejméně pět let praxe v oblasti informačních a komunikačních technologií, přičemž z toho nejméně jeden rok v oblasti poskytování certifikačních služeb,
- znalost v oblasti infrastruktury veřejných klíčů a informační bezpečnosti.

Ostatní zaměstnanci I.CA podílející se na zajištění certifikačních služeb 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 o všech zaměstnancích I.CA jsou:

- sami tito zaměstnanci,
- osoby, které tyto zaměstnance znají,
- veřejné zdroje informací.

Zaměstnanci poskytují prvotní informace osobním pohovorem při přijímání do pracovního poměru, ty jsou aktualizovány při periodických pohovorech s nadřízeným pracovníkem v průběhu pracovního poměru.

5.3.3 Požadavky na přípravu pro výkon role, vstupní školení

Zaměstnanci 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 zaměstnance I.CA pořádá vedení společnosti 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 zaměstnanci I.CA motivováni k získávání znalostí potřebných pro zastávání jiné role v I.CA.

5.3.6 Postihy za neoprávněné činnosti zaměstnanců

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

5.3.7 Požadavky na nezávislé zhotovitele (dodavatele)

I.CA může nebo musí některé činnosti zajišťovat smluvně, za činnost nezávislých dodavatelů plně odpovídá. 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 povinností stanovených v uvedených dokumentech jsou vyžadovány smluvní pokuty, případně je s dodavatelem okamžitě ukončena smlouva.

5.3.8 Dokumentace poskytovaná zaměstnancům

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

5.4 Auditní záznamy (logy)

5.4.1 Typy zaznamenávaných událostí

Zaznamenávány jsou veškeré události požadované technickými standardy, mj. o životním cyklu certifikátů OCSP respondérů a jim odpovídajících certifikátů CA.

Speciálním případem zaznamenávání událostí je událost generování párových dat CA vydávající certifikáty OCSP respondérů, přičemž minimálně platí, že:

- je prováděno podle připraveného scénáře ve fyzicky zabezpečeném prostředí,
- podle možností je pořizován videozáznam.

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 auditních dat, rezervování dostatečného prostoru pro auditní data, automatické nepřepisování auditního souboru, prezentaci auditních záznamů pro uživatele vhodným způsobem a omezení přístupu k auditnímu souboru pouze pro definované uživatele.

5.4.2 Periodicita zpracování záznamů

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

5.4.3 Doba uchování auditních záznamů

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

5.4.4 Ochrana auditních záznamů

Auditní záznamy v elektronické a papírové podobě jsou uloženy způsobem, zajišťujícím ochranu před jejich změnami, krádeží a zničením (ať již úmyslným, nebo neúmyslným).

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

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

Ochrana výše uvedených typů auditních záznamů je popsána v interní dokumentaci.

5.4.5 Postupy pro zálohování auditních záznamů

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

5.4.6 Systém shromažďování auditních záznamů (interní nebo externí)

Systém shromažďování auditních záznamů je z pohledu informačních systémů CA vydávající certifikáty OCSP respondéru interní.

5.4.7 Postup při oznamování události subjektu, který ji způsobil

Subjekt není o zapsání události do auditního záznamu informován.

5.4.8 Hodnocení zranitelnosti

Hodnocení zranitelnosti je ve společnosti První certifikační autorita, a.s., prováděno v periodických intervalech jako součást analýzy rizik. Sledování zranitelnosti zařízení a programového vybavení souvisejících s certifikačními službami je popsáno v interní dokumentaci.

5.5 Uchovávání informací a dokumentace

Uchovávání informací a dokumentace je u I.CA prováděno dle interní dokumentace.

5.5.1 Typy informací a dokumentace, které se uchovávají

I.CA uchovává níže uvedené typy informací a dokumentaci (v elektronické nebo listinné podobě), které souvisejí s poskytovanými certifikačními službami, zejména:

- dokumenty a záznamy související s životním cyklem vydaných certifikátů OCSP respondérů, včetně těchto certifikátů a certifikátů s nimi souvisejících,
- případný videozáznam průběhu generování párových dat CA vydávající certifikáty OCSP respondéru,
- další záznamy potřebné pro služby CA vydávající certifikáty OCSP respondéru (např. seznamy zneplatněných certifikátů),
- záznam o manipulaci s informacemi (např. převzetí, předání, uložení, kontrola, konverze do elektronické podoby atd.),
- aplikační programové vybavení, provozní a bezpečnostní dokumentace.

5.5.2 Doba uchování uchovávaných informací a dokumentace

Informace, vztahující se k certifikátům CA vydávajících certifikáty OCSP respondéru, s výjimkou příslušných soukromých klíčů, jsou uchovávány po celou dobu existence I.CA. Ostatní informace a dokumentace dle kapitoly 5.5.1 jsou uchovávány v souladu s kapitolou 5.4.3.

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

5.5.3 Ochrana úložiště uchovávaných informací a dokumentace

Prostory, ve kterých se uchovávané informace a dokumentace nacházejí, jsou zabezpečeny formou opatření, vycházejících z požadavků objektové a fyzické bezpečnosti a zákona o ochraně utajovaných informací.

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

5.5.4 Postupy při zálohování uchovávaných informací a dokumentace

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

5.5.5 Požadavky na používání časových razítek při uchovávání informací a dokumentace

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

5.5.6 Systém shromažďování uchovávaných informací a dokumentace (interní nebo 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. Shromažďování uchovávaných informací je evidováno.

5.5.7 Postupy pro získání a ověření uchovávaných informací a dokumentace

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

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

O každém takto povoleném přístupu je pořizován písemný záznam.

5.6 Výměna dat pro ověřování elektronických značek v nadřízeném 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 nadřízeném 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 uvedených událostí postupuje I.CA v souladu s interním plánem pro zvládání krizových situací a plánem obnovy a případně s další relevantní interní dokumentací.

5.7.2 Poškození výpočetních prostředků, softwaru nebo dat

Viz kapitola 5.7.1.

5.7.3 Postup při kompromitaci dat pro vytváření elektronických značek poskytovatele

V případě vzniku důvodné obavy z kompromitace soukromého klíče vydávající certifikační autority postupuje tato certifikační autorita tak, že:

- ukončí jeho používání,
- okamžitě a trvale zneplatní příslušný certifikát a zničí jemu odpovídající soukromý klíč,
- zneplatní všechny platné certifikáty, které byly výše uvedeným klíčem elektronicky označeny,
- bezodkladně o této skutečnosti, včetně důvodu, informuje na své internetové informační adrese, pro zpřístupnění této informace je využit i seznam zneplatněných certifikátů,
- případně oznámí dozorovému orgánu informaci o zneplatnění příslušného certifikátu s uvedením důvodu.

Obdobný postup bude uplatněn i v případě, že dojde k takovému vývoji kryptoanalytických metod (např. změny kryptografických algoritmů, délky klíčů atd.), že by mohla být bezprostředně ohrožena bezpečnost certifikačních služeb.

5.7.4 Schopnost obnovit činnost po havárii

V případě havárie postupuje I.CA v souladu s interním plánem pro zvládání krizových situací a plánem obnovy a s další relevantní interní dokumentací.

5.8 Ukončení činnosti CA nebo RA

Ukončení činnosti certifikační autority je popsáno v certifikační politice této certifikační autority (vydávající certifikáty koncovým uživatelům).

6 TECHNICKÁ BEZPEČNOST

6.1 Generování a instalace párových dat

6.1.1 Generování párových dat

Generování párových dat certifikačních autorit a jim odpovídajících OCSP respondérů probíhá v zabezpečené oblasti a je prováděno v kryptografickém modulu, který byl hodnocen podle FIPS PUB 140-2 úroveň 3. O generování je pořízen písemný záznam.

Generování párových dat pracovníků podílejících se na vydávání SSL koncovým uživatelům je prováněno na čipových kartách, splňujících požadavky na SSCD. Soukromé klíče těchto párových dat jsou na čipové kartě uloženy v neexportovatelném tvaru a k jejich použití je nutné zadat PIN.

6.1.2 Předání dat pro vytváření elektronických podpisů nebo dat pro vytváření elektronických značek podepisující nebo označující osobě

Pro problematiku soukromých klíčů certifikačních autorit a jim odpovídajících OCSP respondérů není relevantní - soukromé klíče jsou uloženy v kryptografickém modulu, který je pod výhradní kontrolou I.CA.

6.1.3 Předání dat pro ověřování elektronických podpisů nebo dat pro ověřování elektronických značek poskytovateli certifikačních služeb

Veřejný klíč je vydávající certifikační autoritě doručen v žádosti (formát PKCS#10) o vydání certifikátu.

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

Veřejný klíč OCSP respondéru je obsažen v jeho OCSP odpovědi.

6.1.5 Délky párových dat

Pro certifikační služby poskytované podle této CP je výhradně využíván asymetrický algoritmus RSA. Mohutnost klíče (resp. parametrů daného algoritmu) kořenové certifikační autority I.CA je 4096 bitů, mohutnost klíčů (resp. parametrů daného algoritmu) v jí vydávaných certifikátech a certifikátech OCSP respondérů je minimálně 2048 bitů.

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

Parametry algoritmů použitých při generování veřejných klíčů certifikačních autorit a jejich OCSP respondérů splňují požadavky, uvedené v platné legislativě týkající se elektronického podpisu, resp. v ní odkazovaných technických standardech nebo normách.

6.1.7 Omezení pro použití dat pro ověřování elektronických podpisů nebo dat pro ověřování elektronických značek

Uvedeno v kapitole 1.4.

6.2 Ochrana dat pro vytváření elektronických podpisů nebo dat pro vytváření elektronických značek a bezpečnost kryptografických modulů

6.2.1 Standardy a podmínky používání kryptografických modulů

Generování párových dat a uložení soukromých klíčů certifikačních autorit a jejich OCSP respondérů probíhá v kryptografickém modulu, který splňuje požadavky platné legislativy týkající se elektronického podpisu, tedy standardu FIPS PUB 140-2 úroveň 3.

6.2.2 Sdílení tajemství

Při provádění citlivých činností, tj. generování párových dat certifikačních autorit, OCSP respondéru kořenové certifikační autority, transferu dat z kryptografického modulu kvalifikovaných certifikačních autorit a při transferu dat do kryptografických modulů je nezbytná přítomnost dvou členů vedení I.CA, z nichž každý zná část kódu k provedení těchto činností.

6.2.3 Úschova dat pro vytváření elektronických podpisů nebo dat pro vytváření elektronických značek

Není relevantní pro tento dokument, služba úschovy soukromého klíče není poskytována.

6.2.4 Zálohování dat pro vytváření elektronických podpisů nebo dat pro vytváření elektronických značek

Kryptografický modul použitý pro správu párových dat certifikačních autorit a jejich OCSP respondérů umožňuje zálohování soukromých klíčů. Soukromé klíče jsou zálohovány s využitím nativních prostředků kryptografického modulu v zašifrované podobě.

6.2.5 Uchovávání dat pro vytváření elektronických podpisů nebo dat pro vytváření elektronických značek

Po uplynutí doby platnosti soukromých klíčů certifikačních autorit a jejich OCSP respondérů jsou tyto včetně záloh zničeny. Uchovávání těchto soukromých klíčů představuje bezpečnostní riziko, proto je u I.CA zakázáno.

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

Transfer soukromých klíčů kvalifikovaných certifikačních autorit z a do kryptografického modulu probíhá za přímé osobní účasti nejméně dvou členů vedení I.CA.

Transfer soukromých klíčů ostatních certifikačních autorit a všech OCSP respondérů z kryptografického modulu provádí jeden člen vedení I.CA.

Transfer soukromých klíčů ostatních certifikačních autorit a všech OCSP respondérů do kryptografického modulu probíhá za přímé osobní účasti nejméně dvou členů vedení I.CA.

O provedeném transferu je vždy pořízen písemný záznam.

6.2.7 Uložení dat pro vytváření elektronických značek v kryptografickém modulu

Soukromé klíče certifikačních autorit a jejich OCSP respondérů jsou uloženy v kryptografickém modulu, splňujícím požadavky platné legislativy týkající se elektronického podpisu, tedy standardu FIPS PUB 140-2 úroveň 3.

6.2.8 Postup při aktivaci dat pro vytváření elektronických podpisů nebo dat pro vytváření elektronických značek

Aktivace soukromých klíčů certifikačních autorit a OCSP respondéru kořenové certifikační autority uložených v kryptografickém modulu je prováděna za přímé osobní účasti nejméně dvou členů vedení I.CA s využitím aktivační čipové karty podle přesně určeného postupu, který je upraven interní dokumentací. O provedené aktivaci je pořízen písemný záznam.

Aktivace soukromých klíčů OCSP respondéru ostatních certifikačních autorit uložených v kryptografickém modulu je prováděna za přímé osobní účasti jednoho člena vedení I.CA s využitím aktivační čipové karty podle přesně určeného postupu, který je upraven interní dokumentací. O provedené aktivaci je pořízen písemný záznam.

6.2.9 Postup při deaktivaci dat pro vytváření elektronických podpisů nebo dat pro vytváření elektronických značek

Deaktivace soukromých klíčů certifikačních autorit a OCSP respondéru kořenové certifikační autority uložených v kryptografickém modulu je prováděna za přímé osobní účasti nejméně dvou členů vedení I.CA s využitím aktivační čipové karty podle přesně určeného postupu, který je upraven interní dokumentací. O provedené deaktivaci je pořízen písemný záznam.

Deaktivace soukromých klíčů OCSP respondérů ostatních certifikačních autorit uložených v kryptografickém modulu je prováděna za přímé osobní účasti jednoho člena vedení I.CA s využitím aktivační čipové karty podle přesně určeného postupu, který je upraven interní dokumentací. O provedené deaktivaci je pořízen písemný záznam.

6.2.10 Postup při zničení dat pro vytváření elektronických podpisů nebo dat pro vytváření elektronických značek

Soukromé klíče certifikačních autorit a jejich OCSP respondérů jsou uloženy v kryptografickém modulu. Ničení těchto klíčů je realizováno nativními prostředky kryptografického modulu. Zálohy soukromých klíčů na externích médiích jsou rovněž zničeny. Ničení spočívá ve fyzické destrukci těchto nosičů. Postup ničení soukromého klíče je přesně určen a popsán v interní dokumentaci.

6.2.11 Hodnocení kryptografických modulů

Kryptografické moduly sloužící ke generování párových dat a uložení soukromých klíčů certifikačních autorit a jejich OCSP respondérů byly certifikovány na shodu s požadavky standardu FIPS PUB 140-2 úroveň 3. Bezpečnost modulů je sledována po celou dobu jejich využívání.

6.3 Další aspekty správy párových dat

6.3.1 Uchovávání dat pro ověřování elektronických podpisů nebo dat pro ověřování elektronických značek

Veřejné klíče certifikačních autorit a jejich OCSP respondérů jsou uchovávány po celou dobu existence I.CA.

6.3.2 Maximální doba platnosti certifikátu vydaného podepisující nebo označující osobě a párových dat

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

6.4 Aktivační data

6.4.1 Generování a instalace aktivačních dat

Aktivační data certifikačních autorit a jejich OCSP respondérů jsou vytvářena v průběhu generování odpovídajících párových dat.

6.4.2 Ochrana aktivačních dat

Aktivační data certifikačních autorit a jejich OCSP respondérů jsou chráněna způsobem popsaným v interní dokumentaci.

6.4.3 Ostatní aspekty aktivačních dat

Aktivační data certifikačních autorit a jejich OCSP respondérů jsou určena výhradně pro procesy poskytování certifikačních služeb a nesmí být použita k jiným účelům, ani přenášena nebo uchovávána v otevřené podobě. Veškeré aspekty jsou popsány v interní dokumentaci.

6.5 Počítačová bezpečnost

6.5.1 Specifické technické požadavky na počítačovou bezpečnost

Úroveň bezpečnosti použitých komponent pro poskytování certifikačních služeb je definována technickými standardy. Role přímo se podílející na vydání certifikátu OCSP respondéru používají dvoufaktorovou autentizaci.

6.5.2 Hodnocení počítačové bezpečnosti

Hodnocení počítačové bezpečnosti I.CA je založeno na požadavcích uvedených v mezinárodních a národních standardech, zejména:

- CWA 14167-1 - Security Requirements for Trustworthy Systems Managing Certificates for Electronic Signatures - Part 1: System Security Requirements /Bezpečnostní požadavky na důvěryhodné systémy spravující certifikáty pro elektronický podpis - část 1: Požadavky na bezpečnost systémů.
- ČSN ETSI TS 101 456 - Elektronické podpisy a infrastruktury - Požadavky na postupy certifikační autority vydávající kvalifikované certifikáty.
- ČSN ETSI EN 319 411-2 Elektronické podpisy a infrastruktury (ESI) - Požadavky politiky a bezpečnosti na poskytovatele důvěryhodných služeb vydávající certifikáty - Část 2: Požadavky politiky na certifikační autority vydávající kvalifikované certifikáty.
- ČSN ETSI EN 319 411-3 Elektronické podpisy a infrastruktury (ESI) - Požadavky politiky a bezpečnosti na poskytovatele důvěryhodných služeb vydávající certifikáty - Část 3: Požadavky politiky na certifikační autority vydávající certifikáty veřejného klíče.
- ETSI TS 102 042 Electronic Signatures and Infrastructures (ESI); Policy requirements for certification authorities issuing public key certificates.
- ETSI TS 119 312 Electronic Signatures and Infrastructures (ESI); Cryptographic Suites.
- ČSN ISO/IEC 27000 Informační technologie - Bezpečnostní techniky - Systémy řízení bezpečnosti informací - Přehled a slovník.
- 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.

Činnost certifikační autority se dále řídí požadavky technických norem a standardů:

- FIPS PUB 140-2 Requirements for Cryptographic Modules.
- ISO 3166-1 Codes for the representation of names of countries and their subdivisions - Part 1: Country codes.
- ITU-T - X.501 Information technology – Open Systems Interconnection – The Directory: Models.
- ITU-T - X.509 Information technology – Open Systems Interconnection – The Directory: Public-key and attribute certificate frameworks.
- ITU-T - X.520 Information technology – Open Systems Interconnection – The Directory: Selected attribute types.
- RSA Laboratories - PKCS#10: Certification Request Syntax Standard.
- RFC 2560 X.509 Internet Public Key Infrastructure Online Certificate Status Protocol - OCSP.
- RFC 3647 Internet X.509 Public Key Infrastructure Certificate Policy and Certification Practices Framework.
- RFC 5019 The Lightweight Online Certificate Status Protocol (OCSP) Profile for High-Volume Environments.

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

6.6 Bezpečnost životního cyklu

6.6.1 Řízení vývoje systému

Při vývoji systému je postupováno v souladu s interní dokumentací.

6.6.2 Kontroly řízení bezpečnosti

Kontrola řízení bezpečnosti informací, včetně kontroly souladu se standardy, je prováděna v případě kvalifikovaných služeb v rámci periodických kontrol bezpečnostní shody podle platné legislativy týkající se elektronického podpisu a dále formou interních a externích auditů systému řízení bezpečnosti informací (ISMS).

6.6.3 Řízení bezpečnosti životního cyklu

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

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

6.7 Síťová bezpečnost

V prostředí I.CA nejsou prostředky provádějící vlastní certifikační služby přímo dostupné z veřejné sítě Internet. Informační systém je mimo jiné chráněn komerčním produktem typu firewall. Veškerá komunikace mezi RA a provozním pracovištěm CA je vedena šifrovaně.

6.8 Časová razítka

Řešení je uvedeno v kapitola 5.5.5.

7 PROFILY CERTIFIKÁTU, SEZNAMU ZNEPLATNĚNÝCH CERTIFIKÁTŮ A OCSP

7.1 Profil certifikátu

tab. 3 - Základní pole certifikátu OCSP respondéru podřízené CA

Pole	Obsah
Version	v3 (0x2)
SerialNumber	jedinečné sériové číslo vydávaného certifikátu
SignatureAlgorithm	Sha256WithRSAEncryption
Issuer	vydavatel certifikátu
Validity	
NotBefore	datum vydání (UTC)
NotAfter	datum vydání + maximálně 110 dnů (UTC)
Subject[1]	
commonName*	jméno OCSP respondéru
organizationName	První certifikační autorita, a.s.
countryName	CZ
serialNumber**	NTRCZ-26439395
SubjectPublicKeyInfo	
algorithm	rsaEncryption
subjectPublicKey	veřejný klíč (minimálně 2048 bitů)
Extensions	viz tab. 4
Signature	elektronická značka/podpis/pečeť

* obsahující jméno vydávající certifikační autority vydávající certifikát OCSP respondéru následované řetězcem „OCSP responder“

** lze nahradit položkou organizationIdentifier

7.1.1 Číslo verze

Vydávané certifikáty jsou v souladu se standardem X.509 ve verzi 3.

[1] I.CA si vyhrazuje právo upravit množinu položek a obsah pole Subject, vyžadovanou aktualizacemi standardů ETSI, nebo třetími stranami (např. společnost Microsoft).

7.1.2 Rozšiřující položky v certifikátu

tab. 4 - Rozšíření certifikátu[2] OCSP respondéru podřízené CA

Položka	Obsah	Poznámka
CertificatePolicies		nekritická, vytváří CA
.PolicyInformation(1)		
policyIdentifier	viz kapitola 1.2	
[1.1]policyQualifiers .PolicyQualifierInfo(1) userNotice	Tento kvalifikovany systemovy certifikat byl vydan podle zakona 227/2000 Sb. v platnem zneni/This qualified system certificate was issued according to Act No. 227/2000 Coll.	viz kapitola 7.1.8
.PolicyInformation(2)*		
policyIdentifier	1.3.158.36061701.0.0.0.1.2.2	
AuthorityInformationAccess		nekritická, vytváří CA
id-ad-caIssuers**	{http://q.ica.cz/qcaRR_rsa.cer| http://s.ica.cz/pcaRR_rsa.cer| http://s.ica.cz/scaRR_rsa.cer| http://q.ica.cz/2qcaRR_rsa.cer}	
BasicConstraints		nekritická, vytváří CA
cA	False	
KeyUsage	digitalSignature, nonRepudiation***	kritická, vytváří CA
ExtendedKeyUsage	id-kp-OCSPSigning	kritická, vytváří CA
id-pkix-ocsp-nocheck	NULL	nekritická, vytváří CA
SubjectKeyIdentifier	hash veřejného klíče (subjectPublicKey) v certifikátu (viz tab. 3)	nekritická, vytváří CA
AuthorityKeyIdentifier		nekritická, vytváří CA
keyIdentifier	hash veřejného klíče vydavatele certifikátu	

* může být obsažen v certifikátu OCSP respondéru, splňujícím požadavky legislativy Slovenské republiky

[2] I.CA si vyhrazuje právo upravit množinu a obsah rozšíření Certifikátu, vyžadovanou aktualizacemi standardů ETSI, nebo třetími stranami (např. společnost Microsoft).

** RR - poslední dvě číslice roku vydání certifikátu CA vydávající certifikát OCSP respondéru

*** nonRepudiation – volitelně v případě, že se jedná o certifikát OCSP respondéru certifikační autority, vydávající kvalifikované certifikáty

7.1.3 Objektové identifikátory (dále „OID") algoritmů

V procesu poskytování certifikačních služeb jsou využívány algoritmy, uvedené v příslušných technických standardech.

7.1.4 Způsoby zápisu jmen a názvů

V souladu s požadavkem RFC 5280 se obsah pole Issuer ve vydaném certifikátu OCSP respondéru shoduje s polem Subject v certifikátu CA vydávající tento certifikát. Dále platí ustanovení kapitoly 3.1.

Informace o držiteli certifikátu jsou uvedeny v poli Subject (viz tab. 3).

7.1.5 Omezení jmen a názvů

Jména a názvy uvedené v certifikátu musí, je-li to možné, přesně odpovídat údajům v dokumentech, kterými se žadatel o certifikát nebo držitel certifikátu prokazoval v procesu registrace.

7.1.6 OID certifikační politiky

OID certifikační politiky, resp. politik jsou uvedeny v položce CertificatePolicies (viz tab. 4).

7.1.7 Rozšiřující položka „Policy Constrainsts"

Není relevantní pro tento dokument.

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

Rozšiřující položka certifikátu OCSP respondéru může obsahovat „PolicyQualifiers" pouze v případě, že tento byl vydán jako kvalifikovaný systémový certifikát.

Certifikáty vydávané po datu ukončení platnosti zákona České republiky č. 227/2000 Sb. tento kvalifikátor neobsahovat nesmí.

7.1.9 Způsob zápisu kritické rozšiřující položky „Certificate Policies"

Není relevantní pro tento dokument - položka není označena jako kritická.

7.2 Profil seznamu zneplatněných certifikátů

tab. 3 - Profil CRL[3]

Položka	Obsah
Version	v2(0x1)
Signature Algorithm	Sha256WithRSAEncryption
Issuer	označení vydavatele CRL
thisUpdate	datum a čas vydání CRL (UTC)
nextUpdate	datum a předpokládaný čas vydání následujícího CRL (UTC)
revokedCertificates	seznam zneplatněných certifikátů
userCertificate	sériové číslo zneplatněného certifikátu
revocationDate	datum a čas zneplatnění certifikátu
crlEntryExtensions	rozšíření položky seznamu - viz tab. 4
crlExtensions	rozšíření CRL - viz tab. 4
SignatureAlgorithm	Sha256WithRSAEncryption
Signature	elektronická značka/podpis/pečeť vydavatele CRL

7.2.1 Číslo verze

Seznamy zneplatněných certifikátů jsou vydávány dle X.509 verze 2.

7.2.2 Rozšíření CRL a záznamů CRL

tab. 4 - Rozšíření CRL[4]

Položka	Obsah	Poznámka
crlEntryExtensions		
CRLReason	důvod zneplatnění certifikátu; důvod certificateHold je nepřípustný, nepoužívá se	nekritická
crlExtensions		
AuthorityKeyIdentifier		
KeyIdentifier	hash veřejného klíče vydavatele CRL	nekritická
CRLNumber	jedinečné číslo vydávaného CRL	nekritická

[3] I.CA si vyhrazuje právo upravit množinu polí a obsah CRL, vyžadovanou aktualizacemi standardů ETSI, nebo třetími stranami (např. společnost Microsoft).

[4] I.CA si vyhrazuje právo upravit množinu a obsah rozšíření CRL, vyžadovanou aktualizacemi standardů ETSI, nebo třetími stranami (např. společnost Microsoft).

7.3 Profil OCSP

Profily OCSP žádosti i odpovědi jsou v souladu s RFC 6960 a RFC 5019.

OCSP odpovědi jsou typu BasicOCSPResponse a obsahují všechna povinná pole. V případě odvolaného certifikátu je uvedeno volitelné pole revocationReason. Pro certifikáty nevydané příslušnou CA je vrácena odpověď unAuthorized. Jako přenosový protokol je používáno pouze http.

Bližší podrobnosti jsou uvedeny v odpovídající certifikační prováděcí směrnici.

7.3.1 Číslo verze

V žádosti a odpovědi na stav certifikátu s využitím protokolu OCSP je uvedena verze 1.

7.3.2 Rozšiřující položky OCSP

Konkrétní rozšiřující položky uváděné v žádosti a odpovědi na stav certifikátu s využitím protokolu OCSP jsou uvedeny v odpovídající certifikační prováděcí směrnici.

8 HODNOCENÍ SHODY A JINÁ HODNOCENÍ

Hodnocení shody je popsáno v certifikační politice konkrétní certifikační služby, využívající OCSP respondér.

8.1 Periodicita hodnocení nebo okolnosti pro provedení hodnocení

Viz kapitola 8.

8.2 Identita a kvalifikace hodnotitele

Viz kapitola 8.

8.3 Vztah hodnotitele k hodnocenému subjektu

Viz kapitola 8.

8.4 Hodnocené oblasti

Viz kapitola 8.

8.5 Postup v případě zjištění nedostatků

Viz kapitola 8.

8.6 Sdělování výsledků hodnocení

Viz kapitola 8.

9 OSTATNÍ OBCHODNÍ A PRÁVNÍ ZÁLEŽITOSTI

9.1 Poplatky

9.1.1 Poplatky za vydání nebo obnovení certifikátu

Provozovatelem OCSP respondérů vydávajících certifikačních autorit je společnost První certifikační autorita, a.s., poplatky za vydávání certifikátů OCSP respondérů nejsou účtovány. Služba obnovení certifikátu OCSP respondéru není poskytována.

9.1.2 Poplatky za přístup k certifikátu na seznamu vydaných certifikátů

Přístup elektronickou cestou k certifikátům vydaným dle této CP I.CA nezpoplatňuje.

9.1.3 Poplatky za informace o statutu certifikátu nebo o zneplatnění certifikátu

Přístup elektronickou cestou k informacím o zneplatněných certifikátech (CRL) nebo stavech certifikátů (OCSP) I.CA nezpoplatňuje.

9.1.4 Poplatky za další služby

Není relevantní pro tento dokument.

9.1.5 Jiná ustanovení týkající se poplatků (vč. refundací)

Není relevantní pro tento dokument.

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.

Společnost První certifikační autorita, a.s., sjednala pro všechny zaměstnance pojištění odpovědnosti za škody způsobené zaměstnavateli v rozsahu, určeném představenstvem společnosti.

9.2.2 Další aktiva a záruky

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

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

9.2.3 Pojištění nebo krytí zárukou pro koncové uživatele

Není relevantní pro tento dokument, služba není poskytována.

9.3 Citlivost obchodních informací

9.3.1 Výčet citlivých informací

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

- veškeré soukromé klíče, sloužící v procesu poskytování certifikačních služeb,
- obchodní informace I.CA,
- veškeré interní informace a dokumentace,
- veškeré osobní údaje.

9.3.2 Informace mimo rámec citlivých informací

Za veřejné se považují pouze informace označené jako veřejné včetně těch, které jsou zveřejňovány způsobem uvedeným v kapitole 2.2.

9.3.3 Odpovědnost za ochranu citlivých informací

Žádný zaměstnanec I.CA, který přijde do styku s citlivými a důvěrnými informacemi, je nesmí bez souhlasu ředitele I.CA poskytnout třetí straně.

9.4 Ochrana osobních údajů

9.4.1 Politika ochrany osobních údajů

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

9.4.2 Osobní údaje

Osobními informacemi jsou veškeré osobní údaje podléhající ochraně ve smyslu příslušných zákonných norem.

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

9.4.3 Údaje, které nejsou považovány za citlivé

Za citlivé nejsou považovány údaje, které nespadají do působnosti ZOOÚ.

9.4.4 Odpovědnost za ochranu osobních údajů

Za ochranu osobních údajů je odpovědný ředitel I.CA.

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

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

9.4.6 Poskytnutí citlivých informací pro soudní či správní účely

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

9.4.7 Jiné okolnosti zpřístupňování osobních údajů

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

9.5 Práva duševního vlastnictví

Tato CP, veškeré související dokumenty, obsah webových stránek 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 v případě certifikátů vydaných dle této CP:

- použije soukromé klíče certifikačních autorit pouze pro vydávání certifikátů koncovým uživatelům (vyjma kořenové CA), vydávání seznamů zneplatněných certifikátů a k vydávání certifikátů OCSP respondérů,
- použije soukromé klíče příslušné OCSP respondérům příslušných CA pouze v procesech poskytování odpovědí na stav certifikátu vydaného příslušnou CA,
- zneplatní certifikáty OCSP respondérů, pokud byla žádost o jejich zneplatnění podána způsobem definovaným v této CP.

9.6.2 Zastupování a záruky RA

RA:

- přejímá závazek za správnost jí poskytovaných služeb,
- nevyřídí kladně žádost, pokud se nepodařilo ověřit některou z položek žádosti nebo žadatel není oprávněn k podání žádosti o certifikát.

9.6.3 Zastupování a záruky držitele certifikátu, podepisující nebo označující osoby

Není relevantní pro tento dokument.

9.6.4 Zastupování a záruky spoléhajících se stran

Záruky spoléhajících se stran jsou popsány v certifikační politice konkrétní certifikační služby, využívající OCSP respondér.

9.6.5 Zastupování a záruky ostatních zúčastněných subjektů

Není relevantní pro tento dokument.

9.7 Zřeknutí se záruk

Společnost První certifikační autorita, a.s., poskytuje pouze záruky, uvedené v kapitole 9.6.

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 konkrétní certifikační služby, využívající OCSP respondér. Dále neodpovídá za škody vzniklé v důsledku porušení závazků I.CA z důvodu vyšší moci.

9.9 Odpovědnost za škodu, náhrada škody

Není relevantní pro tento dokument, je uvedeno v certifikační politice konkrétní certifikační služby, využívající OCSP respondér.

9.10 Doba platnosti, ukončení platnosti

9.10.1 Doba platnosti

Tato CP nabývá platnosti dnem uvedeným v kapitole 10 a platí minimálně po dobu platnosti posledního podle ní vydaného certifikátu.

9.10.2 Ukončení platnosti

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

9.10.3 Důsledky ukončení a přetrvání závazků

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

Po ukončení platnosti této CP přetrvávají z ní vyplývající závazky I.CA, a to po dobu platnosti posledního podle ní vydaného certifikátu OCSP respondéru.

9.11 Komunikace mezi zúčastněnými subjekty

Komunikace mezi subjekty, které jsou organizačnímu částmi I.CA, se řídí interními pravidly I.CA.

Způsob komunikace se spoléhajícími se stranami je vždy uveden v certifikační politice konkrétní certifikační služby, využívající OCSP respondér.

9.12 Změny

9.12.1 Postup při změnách

Postup je realizován řízeným procesem popsaným v interním dokumentu.

9.12.2 Postup při oznamování změn

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

9.12.3 Okolnosti, při kterých musí být změněn OID

OID politiky musí být změněn v případě významných změn ve způsobu poskytování této certifikační služby.

V případě jakýchkoliv změn v tomto dokumentu je vždy změněna jeho verze.

9.13 Řešení sporů

Řešení sporů mezi organizačnímu částmi I.CA se řídí interními pravidly I.CA.

Řešení sporů se spoléhajícími se stranami je vždy popsáno v certifikační politice konkrétní certifikační služby, využívající OCSP respondér.

9.14 Rozhodné právo

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

9.15 Shoda s právními předpisy

Systém poskytování certifikačních služeb je provozován ve shodě s legislativními požadavky a dále s relevantními mezinárodními standardy.

9.16 Další ustanovení

Vždy popsáno v certifikační politice konkrétní certifikační služby, využívající OCSP respondér.

9.16.1 Rámcová dohoda

Viz kapitola 9.16.

9.16.2 Postoupení práv

Viz kapitola 9.16.

9.16.3 Oddělitelnost ustanovení

Viz kapitola 9.16.

9.16.4 Zřeknutí se práv

Viz kapitola 9.16.

9.16.5 Vyšší moc

Viz kapitola 9.16.

9.17 Další opatření

Není relevantní pro tento dokument.

10 ZÁVĚREČNÁ USTANOVENÍ

Tato certifikační politika vydaná společností První certifikační autorita, a.s., nabývá platnosti a účinnosti dnem 2.11.2015.