

První certifikační autorita, a.s.



Certifikační politika

vydávání SSL certifikátů

(algoritmus RSA)

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

Verze 1.0

OBSAH

1	Úvod	11
1.1	Přehled	11
1.2	Název a identifikace dokumentu.....	12
1.3	Participující subjekty	12
1.3.1	Certifikační autority (dále „CA“)	12
1.3.2	Registrační autorita (dále „RA“)	12
1.3.3	Držitelé certifikátů	12
1.3.4	Spoléhající se strany	12
1.3.5	Jiné participující subjekty.....	13
1.4	Použití certifikátu.....	13
1.4.1	Přípustné použití certifikátu	13
1.4.2	Zakázané použití certifikátu	13
1.5	Správa politiky.....	13
1.5.1	Organizace spravující tento dokument.....	13
1.5.2	Kontaktní osoba	13
1.5.3	Osoba odpovědná za soulad CPS s touto politikou	13
1.5.4	Postupy při schvalování CPS.....	13
1.6	Pojmy a zkratky.....	14
1.6.1	Pojmy a zkratky	14
1.6.2	Použité normy a standardy	18
2	Odpovědnost za zveřejňování a úložiště informací a dokumentace.....	19
2.1	Úložiště informací a dokumentace.....	19
2.2	Zveřejňování informací a dokumentace.....	19
2.3	Periodicita zveřejňování informací.....	20
2.4	Řízení přístupu k jednotlivým typům úložišť	20
3	Identifikace a autentizace	21
3.1	Pojmenování	21
3.1.1	Typy jmen.....	21
3.1.2	Požadavek na významovost jmen	21
3.1.3	Anonymita a používání pseudonymu	21
3.1.4	Pravidla pro interpretaci různých forem jmen.....	21
3.1.5	Jedinečnost jmen.....	21
3.1.6	Obchodní značky.....	21
3.2	Počáteční ověřování identity	21

3.2.1	Metody ověřování vlastnictví soukromého klíče	21
3.2.2	Ověřování identity organizace a domény	22
3.2.3	Ověřování identity fyzické osoby	23
3.2.4	Neověřené informace vztahující se k držiteli certifikátu.....	23
3.2.5	Ověřování pravomoci	23
3.2.6	Kritéria pro interoperabilitu.....	23
3.3	Identifikace a autentizace při zpracování požadavků na výměnu veřejného klíče v certifikátu.....	23
3.3.1	Identifikace a autentizace při rutinní výměně soukromého klíče a jemu odpovídajícího veřejného klíče (dále „párová data“).....	23
3.3.2	Identifikace a autentizace při výměně párových dat po zneplatnění certifikátu.....	24
3.4	Identifikace a autentizace při zpracování požadavků na zneplatnění certifikátu.....	24
4	Požadavky na životní cyklus certifikátu.....	25
4.1	Žádost o vydání certifikátu	25
4.1.1	Subjekty oprávněné podat žádost o vydání certifikátu	25
4.1.2	Proces registrace a odpovědnosti.....	25
4.2	Zpracování žádosti o certifikát.....	25
4.2.1	Identifikace a autentizace	25
4.2.2	Přijetí nebo zamítnutí žádosti o certifikát	25
4.2.3	Doba zpracování žádosti o certifikát	26
4.3	Vydání certifikátu.....	26
4.3.1	Úkony CA v průběhu vydávání certifikátu	26
4.3.2	Oznámení o vydání certifikátu	26
4.4	Převzetí vydaného certifikátu	26
4.4.1	Úkony spojené s převzetím certifikátu	26
4.4.2	Zveřejňování vydaných certifikátů poskytovatelem	26
4.4.3	Oznámení o vydání certifikátu jiným subjektům	26
4.5	Použití párových dat a certifikátu.....	26
4.5.1	Použití soukromého klíče a certifikátu držitelem	26
4.5.2	Použití veřejného klíče a certifikátu spoléhající se stranou	27
4.6	Obnovení certifikátu	27
4.6.1	Podmínky pro obnovení certifikátu.....	27
4.6.2	Subjekty oprávněné požadovat obnovení certifikátu	27
4.6.3	Zpracování požadavku na obnovení certifikátu.....	27
4.6.4	Oznámení o vydání obnoveného certifikátu držiteli certifikátu.....	27
4.6.5	Úkony spojené s převzetím obnoveného certifikátu	28

4.6.6	Zveřejňování vydaných obnovených certifikátů poskytovatelem	28
4.6.7	Oznámení o vydání obnoveného certifikátu jiným subjektům.....	28
4.7	Výměna veřejného klíče v certifikátu	28
4.7.1	Podmínky pro výměnu veřejného klíče v certifikátu	28
4.7.2	Subjekty oprávněné požadovat výměnu veřejného klíče v certifikátu	28
4.7.3	Zpracování požadavku na výměnu veřejného klíče	28
4.7.4	Oznámení o vydání certifikátu s vyměněným veřejným klíčem	28
4.7.5	Úkony spojené s převzetím certifikátu s vyměněným veřejným klíčem.....	28
4.7.6	Zveřejnění vydaných certifikátů s vyměněným veřejným klíčem	28
4.7.7	Oznámení o vydání certifikátu s vyměněným veřejným klíčem jiným subjektům.....	28
4.8	Změna údajů v certifikátu	29
4.8.1	Podmínky pro změnu údajů v certifikátu	29
4.8.2	Subjekty oprávněné požadovat změnu údajů v certifikátu.....	29
4.8.3	Zpracování požadavku na změnu údajů v certifikátu	29
4.8.4	Oznámení o vydání certifikátu se změněnými údaji držiteli certifikátu.....	29
4.8.5	Úkony spojené s převzetím certifikátu se změněnými údaji	29
4.8.6	Zveřejnění vydaných certifikátů se změněnými údaji	29
4.8.7	Oznámení o vydání certifikátu se změněnými údaji jiným subjektům.....	29
4.9	Zneplatnění a pozastavení platnosti certifikátu	29
4.9.1	Podmínky pro zneplatnění certifikátu	30
4.9.2	Subjekty oprávněné žádat o zneplatnění certifikátu	31
4.9.3	Požadavek na zneplatnění certifikátu	31
4.9.4	Doba odkladu požadavku na zneplatnění certifikátu	32
4.9.5	Maximální doba, za kterou musí poskytovatel realizovat požadavek na zneplatnění certifikátu.....	32
4.9.6	Povinnosti spoléhajících se stran při ověřování, zda nebyl certifikát zneplatněn.....	33
4.9.7	Periodicita vydávání seznamu zneplatněných certifikátů (CRL).....	33
4.9.8	Maximální zpoždění při zveřejňování seznamu zneplatněných certifikátů.....	33
4.9.9	Možnost ověřování stavu certifikátu on-line („dále OCSP“).....	33
4.9.10	Požadavky při ověřování stavu pomocí OCSP	33
4.9.11	Jiné způsoby oznamování zneplatnění certifikátu	34

4.9.12	Případné odlišnosti postupu zneplatnění v případě kompromitace soukromého klíče	34
4.9.13	Podmínky pro pozastavení platnosti certifikátu	34
4.9.14	Subjekty oprávněné požadovat pozastavení platnosti certifikátu	34
4.9.15	Zpracování požadavku na pozastavení platnosti certifikátu	34
4.9.16	Omezení doby pozastavení platnosti certifikátu	34
4.10	Služby související s ověřováním statutu certifikátu	34
4.10.1	Funkční charakteristiky	34
4.10.2	Dostupnost služeb	34
4.10.3	Další charakteristiky služeb statutu certifikátu	35
4.11	Ukončení poskytování služeb pro držitele certifikátu	35
4.12	Úschova soukromého klíče u důvěryhodné třetí strany a jejich obnova	35
4.12.1	Politika a postupy při úschově a obnovování soukromého klíče	35
4.12.2	Politika a postupy při zapouzdřování a obnovování šifrovacího klíče pro relaci	35
5	Management, provozní a fyzická bezpečnost	36
5.1	Fyzická bezpečnost	36
5.1.1	Umístění a konstrukce	36
5.1.2	Fyzický přístup	36
5.1.3	Elektřina a klimatizace	36
5.1.4	Vlivy vody	36
5.1.5	Protipožární opatření a ochrana	36
5.1.6	Ukládání médií	37
5.1.7	Nakládání s odpady	37
5.1.8	Zálohy mimo budovu	37
5.2	Procesní bezpečnost	37
5.2.1	Důvěryhodné role	37
5.2.2	Počet osob požadovaných na zajištění jednotlivých činností	37
5.2.3	Identifikace a autentizace pro každou roli	37
5.2.4	Role vyžadující rozdělení povinností	38
5.3	Personální bezpečnost	38
5.3.1	Požadavky na kvalifikaci, zkušenosti a bezúhonnost	38
5.3.2	Posouzení spolehlivosti osob	38
5.3.3	Požadavky na přípravu pro výkon role, vstupní školení	38
5.3.4	Požadavky a periodicita školení	39
5.3.5	Periodicita a posloupnost rotace pracovníků mezi různými rolami	39
5.3.6	Postihy za neoprávněné činnosti zaměstnanců	39

5.3.7	Požadavky na nezávislé zhotovitele (dodavatele).....	39
5.3.8	Dokumentace poskytovaná zaměstnancům.....	39
5.4	Auditní záznamy (logy).....	39
5.4.1	Typy zaznamenávaných událostí.....	39
5.4.2	Periodicita zpracování záznamů	40
5.4.3	Doba uchování auditních záznamů.....	40
5.4.4	Ochrana auditních záznamů	40
5.4.5	Postupy pro zálohování auditních záznamů.....	40
5.4.6	Systém shromažďování auditních záznamů (interní nebo externí).....	40
5.4.7	Postup při oznamování události subjektu, který ji způsobil.....	40
5.4.8	Hodnocení zranitelnosti	40
5.5	Uchovávání informací a dokumentace	41
5.5.1	Typy informací a dokumentace, které se uchovávají	41
5.5.2	Doba uchování uchovávaných informací a dokumentace	41
5.5.3	Ochrana úložiště uchovávaných informací a dokumentace	41
5.5.4	Postupy při zálohování uchovávaných informací a dokumentace	41
5.5.5	Požadavky na používání časových razítek při uchovávání informací a dokumentace	41
5.5.6	Systém shromažďování uchovávaných informací a dokumentace (interní nebo externí)	41
5.5.7	Postupy pro získání a ověření uchovávaných informací a dokumentace.....	42
5.6	Výměna soukromého klíče v certifikátu poskytovatele.....	42
5.7	Obnova po havárii nebo kompromitaci	42
5.7.1	Postup v případě incidentu a kompromitace	42
5.7.2	Poškození výpočetních prostředků, softwaru nebo dat	42
5.7.3	Postup při kompromitaci soukromého klíče CA.....	42
5.7.4	Schopnost obnovit činnost po havárii.....	43
5.8	Ukončení činnosti CA nebo RA	43
6	Technická bezpečnost.....	44
6.1	Generování a instalace párových dat	44
6.1.1	Generování párových dat	44
6.1.2	Předání soukromých klíčů držiteli certifikátu	44
6.1.3	Předání veřejného klíče vydavateli certifikátu	44
6.1.4	Poskytování veřejného klíče CA spoléhajícím se stranám	44
6.1.5	Délky párových dat	44
6.1.6	Generování parametrů veřejného klíče a kontrola kvality.....	44

6.1.7	Využití klíčů	45
6.2	Ochrana soukromého klíče a bezpečnost kryptografických modulů.....	45
6.2.1	Standardy a podmínky používání kryptografických modulů	45
6.2.2	Sdílení tajemství	45
6.2.3	Úschova soukromého klíče.....	45
6.2.4	Zálohování soukromého klíče	45
6.2.5	Uchovávání soukromého klíče.....	45
6.2.6	Transfer soukromého klíče do kryptografického modulu nebo z kryptografického modulu.....	45
6.2.7	Uložení soukromého klíče v kryptografickém modulu	46
6.2.8	Postup při aktivaci soukromých klíčů	46
6.2.9	Postup při deaktivaci soukromých klíčů	46
6.2.10	Postup při zničení soukromých klíčů.....	46
6.2.11	Hodnocení kryptografických modulů.....	46
6.3	Další aspekty správy párových dat.....	46
6.3.1	Uchovávání veřejných klíčů	46
6.3.2	Maximální doba platnosti certifikátu vydaného držiteli certifikátu a párových dat.....	46
6.4	Aktivační data	47
6.4.1	Generování a instalace aktivačních dat	47
6.4.2	Ochrana aktivačních dat	47
6.4.3	Ostatní aspekty aktivačních dat	47
6.5	Počítačová bezpečnost	47
6.5.1	Specifické technické požadavky na počítačovou bezpečnost	47
6.5.2	Hodnocení počítačové bezpečnosti	47
6.6	Bezpečnost životního cyklu	48
6.6.1	Řízení vývoje systému.....	48
6.6.2	Kontroly řízení bezpečnosti	48
6.6.3	Řízení bezpečnosti životního cyklu.....	48
6.7	Síťová bezpečnost	48
6.8	Časová razítka	48
7	Profily certifikátu, seznamu zneplatněných certifikátů a OCSP	49
7.1	Profil certifikátu.....	49
7.1.1	Číslo verze	53
7.1.2	Rozšiřující položky v certifikátu.....	53
7.1.3	Objektové identifikátory (dále „OID“) algoritmů	56
7.1.4	Způsoby zápisu jmen a názvů	56

7.1.5	Omezení jmen a názvů.....	56
7.1.6	OID certifikační politiky	56
7.1.7	Rozšiřující položka „Policy Constraints“	57
7.1.8	Syntaxe a sémantika rozšiřující položky kvalifikátorů politiky „Policy Qualifiers“	57
7.1.9	Způsob zápisu kritické rozšiřující položky „Certificate Policies“.....	57
7.2	Profil seznamu zneplatněných certifikátů.....	57
7.2.1	Číslo verze	57
7.2.2	Rozšiřující položky seznamu zneplatněných certifikátů a záznamů v seznamu zneplatněných certifikátů	57
7.3	Profil OCSP.....	58
7.3.1	Číslo verze	58
7.3.2	Rozšiřující položky OCSP.....	58
8	Hodnocení shody a jiná hodnocení	59
8.1	Periodicita hodnocení nebo okolnosti pro provedení hodnocení.....	59
8.2	Identita a kvalifikace hodnotitele.....	59
8.3	Vztah hodnotitele k hodnocenému subjektu	59
8.4	Hodnocené oblasti	59
8.5	Postup v případě zjištění nedostatků.....	59
8.6	Sdělování výsledků hodnocení.....	59
8.7	Pravidelné samoaudity hodnocení kvality.....	60
9	Ostatní obchodní a právní záležitosti.....	61
9.1	Poplatky	61
9.1.1	Poplatky za vydání nebo obnovení certifikátu	61
9.1.2	Poplatky za přístup k certifikátu na seznamu vydaných certifikátů	61
9.1.3	Poplatky za informace o stavu certifikátu nebo o zneplatnění certifikátu	61
9.1.4	Poplatky za další služby	61
9.1.5	Jiná ustanovení týkající se poplatků (vč. refundací).....	61
9.2	Finanční odpovědnost	61
9.2.1	Krytí pojištěním.....	61
9.2.2	Další aktiva a záruky	62
9.2.3	Pojištění nebo krytí zárukou pro koncové uživatele	62
9.3	Citlivost obchodních informací.....	62
9.3.1	Výčet citlivých informací	62
9.3.2	Informace mimo rámec citlivých informací	62
9.3.3	Odpovědnost za ochranu citlivých informací.....	62

9.4	Ochrana osobních údajů	62
9.4.1	Politika ochrany osobních údajů	62
9.4.2	Osobní údaje	62
9.4.3	Údaje, které nejsou považovány za citlivé	63
9.4.4	Odpovědnost za ochranu osobních údajů.....	63
9.4.5	Oznámení o používání důvěrných informací a souhlas s používáním citlivých informací.....	63
9.4.6	Poskytování citlivých informací pro soudní či správní účely	63
9.4.7	Jiné okolnosti zpřístupňování osobních údajů.....	63
9.5	Práva duševního vlastnictví.....	63
9.6	Zastupování a záruky	63
9.6.1	Zastupování a záruky CA	63
9.6.2	Zastupování a záruky RA	64
9.6.3	Záruky držitele certifikátu.....	64
9.6.4	Záruky spoléhajících se stran	64
9.6.5	Zastupování a záruky ostatních zúčastněných subjektů	65
9.7	Zřeknutí se záruk	65
9.8	Omezení odpovědnosti	65
9.9	Odpovědnost za škodu, náhrada škody	65
9.10	Doba platnosti, ukončení platnosti.....	66
9.10.1	Doba platnosti	66
9.10.2	Ukončení platnosti.....	66
9.10.3	Důsledky ukončení a přetrvání závazků	66
9.11	Komunikace mezi zúčastněnými subjekty	66
9.12	Změny.....	67
9.12.1	Postup při změnách.....	67
9.12.2	Postup při oznamování změn	67
9.12.3	Okolnosti, při kterých musí být změněn OID.....	67
9.13	Řešení sporů.....	67
9.14	Rozhodné právo.....	67
9.15	Shoda s právními předpisy	67
9.16	Různé	67
9.16.1	Rámcová dohoda	67
9.16.2	Postoupení práv	68
9.16.3	Oddělitelnost požadavků	68
9.16.4	Zřeknutí se práv.....	68
9.16.5	Vyšší moc.....	68

9.17	Další opatření.....	68
10	Závěrečná ustanovení.....	69

tab. 1 – Vývoj dokumentu

Verze	Datum vydání	Schválil	Poznámka
1.0	15.07.2015	Ředitel společnosti První certifikační autorita, a.s.	První vydání

1 ÚVOD

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 pro vydávající certifikační autority. Všechny tyto autority provozuje I.CA a jednou nich je také autorita vydávající SSL certifikáty. Vydávané SSL certifikáty jsou dvou druhů podle typu politiky definované v příslušném technickém standardu, tzv. domain validated (DV), obsahující v příslušných položkách plně kvalifikovaná doménová jména a tzv. organization validated (OV), obsahující navíc informace o organizaci, které je certifikát vydáván. V procesu vydávání certifikátů je využíván algoritmus RSA, vydávání se řídí touto certifikační politikou (dále též CP).

Tento dokument definuje pravidla a postupy pro vydávání SSL certifikátů společností První certifikační autorita, a.s. SSL /TLS (Secure Socket Layer /Transport Layer Security) je šifrovací protokol, zajišťující zabezpečení přenášených dat, autentizaci serveru a /nebo klienta pomocí komerčních SSL certifikátů, fungujících na principu asymetrické kryptografie, tedy veřejných a soukromých klíčů.

Pozn.: Pokud jsou v textu uváděny odkazy na standardy či zákony, jedná se vždy buď přímo o uvedený standard či zákon, nebo o ten, který ho nahrazuje.

1.1 Přehled

Dokument **Certifikační politika vydávání SSL certifikátů (algoritmus RSA)**, vypracovaný společností První certifikační autorita, a. s., se zabývá skutečnostmi, vztahujícími se k procesům životního cyklu jí vydávaných SSL certifikátů a dodržuje strukturu, jejíž předlohou je osnova platného standardu RFC 3647 - Internet X.509 Public Key Infrastructure Certificate Policy and Certification Practices Framework, s přihlédnutím k platným standardům EU a k právu České 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 a úložiště informací, resp. dokumentace.
- Kapitola 3 popisuje procesy identifikace a autentizace žadatele o vydání certifikátu, resp. zneplatnění certifikátu, včetně definování typů a obsahů používaných jmen v žádostech, resp. vydávaných certifikátech.
- Kapitola 4 definuje procesy životního cyklu certifikátu, tzn. proces vydání certifikátu, 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 a jejich uchovávání, problematiku 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 vydávání certifikátů, poskytované společností První certifikační autorita, a.s., je možné považovat za důvěryhodné.

Bližší podrobnosti o naplnění položek certifikátů vydávaných podle této CP a o jejich správě jsou uvedeny v odpovídající Certifikační prováděcí směrnici.

1.2 Název a identifikace dokumentu

Název: Certifikační politika vydávání SSL certifikátů (algoritmus RSA)

OID: 1.3.1.6.4.1.23624.10.1.72.1.0

1.3 Participující subjekty

1.3.1 Certifikační autority (dále „CA“)

Veřejná certifikační autorita, provozovaná společností První certifikační autorita, a.s., vydávající SSL certifikáty koncovým uživatelům.

1.3.2 Registrační autorita (dále „RA“)

Přijímání žádostí o SSL certifikáty není delegováno na žádnou třetí stranu, fyzické přijímání žádostí a ověřování žadatele je možné pouze na určených RA provozovaných I.CA. Taková RA:

- přijímá žádosti o služby uvedené v této CP, zejména přijímá žádosti o SSL certifikáty, zprostředkovává předání certifikátů a seznamů zneplatněných certifikátů, poskytuje potřebné informace atd.,
- komunikuje se subjekty oprávněnými pro získání certifikátu,
- je oprávněna z naléhavých provozních nebo technických důvodů pozastavit zcela nebo zčásti výkon své činnosti - toto opatření je povinna neprodleně hlásit řediteli I.CA, který je potvrdí, zruší nebo změní,
- zajišťuje zpoplatňování služeb I.CA, pokud není stanoveno smlouvou jinak.

1.3.3 Držitelé certifikátů

SSL certifikáty jsou vydávány pouze organizacím, a to na základě smlouvy se společností První certifikační autorita, a.s., které požádaly o vydání certifikátu.

1.3.4 Spoléhající se strany

Spoléhající se stranou jsou subjekty spoléhající se při své činnosti na certifikát vydaný společností První certifikační autorita, a.s.

1.3.5 Jiné participující subjekty

Jinými participujícími subjekty mohou být orgány činné v trestním řízení a další, kterým to dle platných právních předpisů přísluší.

1.4 Použití certifikátu

1.4.1 Přípustné použití certifikátu

SSL certifikáty vydávané společností První certifikační autorita, a.s., podle této certifikační politiky smějí být používány k ověření serveru a k autentizaci. Certifikát smí být instalován pouze na serverech jejichž jména jsou uvedena v certifikátu.

1.4.2 Zakázané použití certifikátu

SSL certifikáty vydávané podle této certifikační politiky nesmějí být používány v rozporu s přípustným použitím popsáním v kapitole 1.4.1 a lze je využívat pouze pro legální účely a v souladu s platnými právními předpisy.

1.5 Správa politiky

1.5.1 Organizace spravující tento dokument

Tento dokument spravuje společnost První certifikační autorita, a.s.

1.5.2 Kontaktní osoba

Kontaktní osoba společnosti První certifikační autorita, a.s., odpovědná za správu tohoto dokumentu je uvedena na internetové adrese (viz kap. 2.2).

1.5.3 Osoba odpovědná za soulad CPS s touto politikou

Osobou odpovědná za soulad CPS s touto politikou je uvedena na internetové adrese (viz kap. 2.2).

1.5.4 Postupy při schvalování CPS

Soulad CPS s touto politikou posuzuje osoba uvedená v kap. 1.5.3, konečné rozhodnutí o souladu provádí ředitel společnosti První certifikační autorita, a.s.

1.6 Pojmy a zkratky

1.6.1 Pojmy a zkratky

tab. 2 - Pojmy a zkratky

Pojem	Vysvětlení
ASCII	American Standard Code for Information Interchange, kódová tabulka definující znaky anglické abecedy a jiné znaky používané v informatice
bit	z anglického <i>binary digit</i> - číslice dvojkové soustavy - je základní a současně nejmenší jednotkou informace používanou především v číslicové technice
CA	certifikační autorita
CA/Browser Forum	organizace, dobrovolné sdružení certifikačních autorit
CAA	DNS Resource záznam - viz RFC 6844
ccTLD	country code TLD, národní doména nejvyšší úrovně, internetová doména na nejvyšší úrovni stromu internetových domén obvykle používána, nebo rezervována pro země, svrchované státy, nebo závislá území, všechny v ASCII definované národní domény nejvyššího řádu jsou tvořeny dvěma znaky
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 ověření elektronické značky	jedinečná data, která se používají pro ověření elektronické značky
data pro ověření 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
DNS	Domain Name System, hierarchický systém doménových jmen, který je realizovaný DNS servery a DNS protokolem, kterým si vyměňují informace, hlavním úkolem jsou vzájemné převody doménových jmen na IP adresy uzlů sítě a obráceně

doménové jméno	označení přiřazené uzlu v doménovém jmenném systému
doménový jmenný prostor	množina všech možných doménových jmen, která jsou podřízena jednomu uzlu v doménovém jmenném systému
držitel certifikátu	žadatel o certifikát, kterému byl certifikát vydán
DV	Domain Validation, typ SSL 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	<p>údaje v elektronické podobě, které jsou připojené k datové zprávě nebo jsou s ní logicky spojené a které splňují následující požadavky:</p> <ul style="list-style-type: none"> • 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
EU	Evropská unie
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
FQDN	Fully Qualified Domain Name, plně kvalifikované doménové jméno, doménové jméno uvádějící označení všech nadřazených uzlů v internetovém doménovém jmenném systému
GET metoda	standardně preferovaná metoda zasílání http požadavků OCSP respondéru pomocí protokolu http, metoda umožňuje ukládání do mezipaměti (druhá metoda je POST)
gTLD	generic TLD, obecná doména nejvyššího řádu (např. .org pro neziskové organizace)
hash	transformace, která jako vstup přijímá řetězec znaků o libovolné délce a výsledkem je řetězec znaků s pevnou délkou

ICANN	Internet Corporation for Assigned Names and Numbers, organizace mj. přidělující a spravující doménová jména a IP adresy
IEC	International Electrotechnical Commission, světová organizace publikující standardy pro elektrotechniku, elektroniku, sdělovací techniku a příbuzné obory
IP	Internet Protocol, komunikační protokol pro přenos paketů a jejich směrování využívaný v Internetu
IT	Information Technology, informační technologie
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
následný certifikát	certifikát, který byl v souladu se smlouvou o poskytování certifikační služby, uzavřenou mezi žadatelem a I.CA, vydán žadateli na základě nové žádosti o certifikát v období platnosti certifikátu, ke kterému je tento následný certifikát vydáván
OCSP	Online Certificate Status Protocol, protokol pro zjišťování stavu certifikátu veřejného klíče
OCSP respondér	server poskytující protokolem OCSP údaje o stavu certifikátu veřejného klíče
OCSP stapling	způsob minimalizace dotazů na OCSP respondér, RFC 4366 - TLS Extensions; umožní TLS serveru vracet jednou získanou OCSP odpověď na stav svého certifikátu (po dobu její platnosti) všem koncovým uživatelům přistupujícím k TLS serveru
OV	Organization Validation, typ SSL certifikátu
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
phishing	podvodná technika používaná v elektronické komunikaci na Internetu k získávání citlivých údajů (hesla, čísla kreditních karet apod.)
PKCS	Public Key Cryptography Standards, označení skupiny standardů pro kryptografii s veřejným klíčem
PTC	Publicly-Trusted Certificate, certifikát, jehož certifikát kořenový je distribuován jako důvěryhodná kotva v běžně dostupném aplikačním programovém vybavení

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)
registrant doménového jména	někdy uváděn jako vlastník doménového jména, ale správněji osoby či entity registrované registrátorem doménového jména jako mající právo dohlížet na používání doménového jména, fyzická nebo právnická osoba vypisovaná jako "Registrant" příkazem WHOIS, nebo registrátorem doménového jména
registrátor doménového jména	osoba nebo entita, která registruje doménová jména z pověření nebo se souhlasem: <ul style="list-style-type: none"> internetové korporace pro přiřazování jmen a čísel (ICANN) - správce kořene DNS prostoru, správce TLD (např. .com) nebo ccTLD (např. .CZ, národního správce)
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
SSL	Secure Sockets Layer, komunikační protokol, resp. vrstva vložená mezi vrstvu transportní a aplikační, která poskytuje zabezpečení komunikace šifrováním a autentizací komunikujících stran
SSL certifikát	certifikát použitý pro identifikaci a šifrování v rámci komunikace prostřednictvím SSL /TLS protokolu
TLD	Top Level Domain, doména na nejvyšší úrovni stromu internetových domén (pod jeho kořenem), v doménovém jméně je doména nejvyšší úrovně uvedena na konci
TLS	Transport Layer Security, komunikační protokol, následovník SSL
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
vydávající CA	pro účely tohoto dokumentu: CA vydávající certifikáty koncovým uživatelům

WHOIS	databáze, která slouží k evidenci údajů o majitelích internetových domén a IP adres
X.501, X.509, X.520	standard popsany v dokumentu viz kap. 1.6.2
zákon o ochraně utajovaných informací	zákon č. 412/2005 Sb., o ochraně utajovaných informací a o bezpečnostní způsobilosti, ve znění pozdějších předpisů
zákoník práce	zákon č. 262/2006 Sb., zákoník práce, ve znění pozdějších předpisů
ZOOÚ	zákon č. 227/2000 Sb., o ochraně osobních údajů a o změně některých zákonů (zákon o ochraně osobních údajů), ve znění pozdějších předpisů
žadatel o SSL certifikát	právník osoba, která žádá o certifikát prostřednictvím statutárního zástupce společnosti nebo osoby pověřené k vyzvednutí certifikátu, jakmile je certifikát vydán, stává se žadatel držitelem certifikátu.

1.6.2 Použité normy a standardy

Tato CP a příslušná CPS zohledňují požadavky technických norem a standardů uvedených v kapitole 6.5.2 a dále:

- 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 4366 Transport Layer Security (TLS) Extensions.
- 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.
- RFC 6844 DNS Certification Authority Authorization (CAA) Resource Record.
- RFC 6962 Certificate Transparency.

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, jsou ssl@ica.cz, resp. info@ica.cz.

Na výše uvedené internetové adrese lze získat informace o:

- SSL 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.

I.CA provozuje testovací stránky umožňující nezávislým dodavatelům aplikačního programového vybavení testovat jejich software s různými stavy I.CA SSL certifikátů na adrese <https://test-ssl.ica.cz>.

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 kap. 4.9.7,
- zneplatnění certifikátu CA vydávající SSL certifikáty 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 (viz kapitoly 2.2 a 2.3) 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

Jména subjektů jsou konstruována v souladu se standardem X.501, resp. s navazujícím standardem X.520.

3.1.2 Požadavek na významovost jmen

Význam a obsah údajů, obsažených ve vydávaných SSL certifikátech, 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 procesu žádosti o SSL certifikát se do vydávaných certifikátů přenášejí ve tvaru, ve kterém jsou uvedeny v předkládaných dokladech.

3.1.5 Jedinečnost jmen

Jedinečnost jmen je zajištěna v průběhu ověřování údajů obsažených v žádosti o SSL certifikát (formát PKCS#10), požadovaných uvádět v polích Subject, resp. SubjectAlternativeName SSL certifikátu.

3.1.6 Obchodní značky

Všechna pole SSL certifikátu, které jsou v procesu vydání certifikátu ověřovány, mají předepsanou strukturu a musí být doložena jejich správnost, úplnost a oprávněnost použití - včetně obchodní značky.

3.2 Počáteční ověřování identity

3.2.1 Metody ověřování vlastnictví soukromého klíče

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 organizace a domény

Postup je popsán v následujících kapitolách.

3.2.2.1 Identita

I.CA ověřuje název a adresu organizace požadovanou uvést v subjektu certifikátu takto:

- primárně prostřednictvím elektronicky přístupného rejstříku provozovaného organizací státu, v jehož jurisdikci jsou založení, vznik, nebo uznání organizace žadatele (např. v ČR obchodní rejstřík),
- prostřednictvím předaného listinného výpisu z rejstříku provozovaného organizací státu, v jehož jurisdikci jsou založení, vznik, nebo uznání organizace žadatele (např. v ČR obchodní rejstřík), ověřeného notářem v tomto státě.

3.2.2.2 Ochranná známky

I.CA ověřuje ochrannou známku (v textovém tvaru) požadovanou uvést v subjektu certifikátu takto:

- primárně prostřednictvím elektronicky přístupného rejstříku provozovaného organizací státu, v jehož jurisdikci jsou založení, vznik, nebo uznání organizace žadatele (např. v ČR Úřad průmyslového vlastnictví),
- prostřednictvím předaného listinného výpisu z rejstříku provozovaného organizací státu, v jehož jurisdikci jsou založení, vznik, nebo uznání organizace žadatele (např. v ČR Úřad průmyslového vlastnictví), ověřeného notářem v tomto státě.

3.2.2.3 Ověření státu (country)

I.CA ověřuje požadovaný stát (country) v subjektu certifikátu takto:

- do pole Subject.country je uveden dvoupísmenný kód země odpovídající ISO 3166-1 lokality subjektu, která je ověřená podle kapitoly 3.2.2.1, nebo kód země spojený se subjektem a ověřený podle kapitoly 3.2.2.4,
- pokud země není reprezentována oficiálním kódem podle ISO 3166-1, CA vydávající SSL certifikáty volitelně může uvést uživatelsky přiřazený kód ISO 3166-1 s hodnotou XX ukazující, že oficiální ISO 3166-1 alpha-2 kód přiřazen nebyl.

3.2.2.4 Oprávnění registranta doménového jména

I.CA připouští pouze jedinou DNS doménu druhého řádu ve všech položkách SAN.dnsName a Subject.CN.

I.CA ověřuje DNS vlastnictví domény požadované žadatelem o certifikát v subjektu prostřednictvím údajů ve WHOIS registru provozovaném správcem TLD /ccTLD pro požadovaný stát.

Pokud žadatel není vlastníkem (registrantem) požadované domény, musí vlastník domény přímou komunikací s I.CA schválit položky žádosti o certifikát (zasláním autorizačního dokumentu domény).

3.2.2.5 Autentizace IP adresy

Není relevantní pro tento dokument - I.CA nepřipouští uvedení IP adresy v polích Subject nebo SAN certifikátu.

3.2.2.6 Ověření domény se zástupnými znaky

Není relevantní pro tento dokument - I.CA nepřipouští uvedení domény se zástupnými znaky v polích Subject nebo SAN certifikátu.

3.2.2.7 Přesnost zdroje dat

Při vzdáleném přístupu do elektronického rejstříku poskytovaného státní organizací a do databáze WHOIS poskytované správcem TLD /ccTLD je primárně používán zabezpečený protokol (https), pokud je poskytován.

3.2.3 Ověřování identity fyzické osoby

Není relevantní pro tento dokument - I.CA nevydává SSL certifikáty fyzickým osobám.

3.2.4 Neověřené informace vztahující se k držiteli certifikátu

Není relevantní pro tento dokument - všechny informace musí být řádným způsobem ověřeny.

3.2.5 Ověřování pravomoci

I.CA ověřuje pravost (autenticitu) žádosti o SSL certifikát předané zástupcem žadatele takto:

- pomocí spolehlivých kontaktních údajů zjištěných při ověření podle kap. 3.2.2.1 nebo 3.2.2.4 kontaktuje zástupce žadatele nebo autoritativní zdroj v organizaci žadatele (hlavní kancelář firmy, správní oddělení, oddělení lidských zdrojů, IT oddělení) a ověří pravost původu žádosti o SSL certifikát a její obsah,
- žadatel může volitelně I.CA předat písemný seznam osob, včetně jejich e-mailových adres, (s ověřenými podpisy statutárních zástupců), které jediné mohou předkládat žádosti o vydání nebo zneplatnění SSL certifikátu pro danou organizaci a doménový prostor.

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 veřejného klíče v certifikátu

3.3.1 Identifikace a autentizace při rutinní výměně soukromého klíče a jemu odpovídajícího veřejného klíče (dále „párová data“)

Vždy se jedná o vydání nového certifikátu s novým veřejným klíčem. I.CA může použít pro vydání tohoto certifikátu (pro stejného žadatele a doménu) informace získané při předchozím ověřování podle kap. 3.2 za předpokladu, že nejsou starší 39 měsíců.

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.

3.4 Identifikace a autentizace při zpracování požadavků na zneplatnění certifikátu

Možné způsoby identifikace a autentizace jsou následující:

- prostřednictvím formuláře na webových stránkách společnosti (s využitím hesla pro zneplatnění certifikátu),
- prostřednictvím nepodepsané elektronické zprávy (obsahující heslo pro zneplatnění certifikátu), odeslaná na adresu ssl@ica.cz,
- prostřednictvím podepsané elektronické zprávy (elektronický podpis musí být realizován soukromým klíčem příslušným k předmětnému certifikátu, jenž má být zneplatněn), odeslaná na adresu ssl@ica.cz,
- prostřednictvím datové schránky (s využitím hesla pro zneplatnění certifikátu),
- prostřednictvím doporučené listovní zásilky na adresu sídla I.CA (s využitím hesla pro zneplatnění certifikátu).

Údaje, které musí žádost o zneplatnění certifikátu obsahovat, jsou uvedeny v kapitole 4.9.3.

I.CA si vyhrazuje právo akceptování i jiných forem postupů pro identifikaci a autentizaci zpracování požadavku na zneplatnění certifikátu.

4 POŽADAVKY NA ŽIVOTNÍ CYKLUS CERTIFIKÁTU

4.1 Žádost o vydání certifikátu

4.1.1 Subjekty oprávněné podat žádost o vydání certifikátu

SSL certifikáty jsou vydávány pouze organizacím na základě smlouvy se společností První certifikační autorita, a.s - viz kap. 1.3.3.

I.CA udržuje záznamy o dříve odmítnutých žádostech z důvodů podezření na phishing nebo podvod o certifikátech zneplatněných ze strany I.CA ze stejných důvodů, a používá je pro kontrolu následně předkládaných žádostí.

4.1.2 Proces registrace a odpovědnosti

Před zasláním žádosti o SSL certifikát musí mít žadatel se společností První certifikační autorita, a.s uzavřenu smlouvu, jejíž součástí je definování podmínek užití certifikátu.

Až poté zástupce žadatele může zaslat na e-mailovou adresu ssl@ica.cz žádost o SSL certifikát, jejímž obsahem bude žádost o SSL certifikát ve formátu PKCS#10 a prohlášení, že všechny informace uvedené v žádosti jsou pravdivé.

4.2 Zpracování žádosti o certifikát

4.2.1 Identifikace a autentizace

Při zpracování žádosti je prováděno:

- ověření pravosti původu žádosti,
- ověření vlastnictví soukromého klíče,
- ověření identity organizace,
- ověření oprávnění užívat uvedené jméno domény druhého řádu.

Před schválením žádosti o SSL certifikát RA prověřuje:

- záznamy o žádostech odmítnutých dříve z důvodů podezření na phishing nebo podvod a záznamy o certifikátech zneplatněných ze strany I.CA ze stejných důvodů - viz kap. 4.1.1,
- požadované doménové jméno proti seznamu phishingových stránek,
- další interní kritéria pro odhalení podvodných žádostí.

Kontrola CAA DNS záznamů není aktuálně prováděna.

4.2.2 Přijetí nebo zamítnutí žádosti o certifikát

I.CA nevydává certifikáty pro gTLD domény. Pokud některá z ověření viz kap. 4.2.1 skončí negativně, proces vydání certifikátu je ukončen. V opačném případě pracovník RA vydání SSL certifikátu schválí.

4.2.3 Doba zpracování žádosti o certifikát

Pokud se podaří ověřit všechny položky žádosti, bude certifikát vydán do 5 pracovních dnů.

4.3 Vydání certifikátu

4.3.1 Úkony CA v průběhu vydávání certifikátu

V procesu vydávání certifikátu provádějí operátoři CA vydávající SSL certifikáty kontroly na shodnost údajů, obsažených v žádosti o certifikát (struktura PKCS#10) a údajů, doplněných pracovníkem RA. Kontroly na formální správnost údajů jsou taktéž prováděny programovým vybavením informačního systému CA.

Vydání certifikátu je provedeno na základě vědomého příkazu k provedení operace podpisu vydávaného SSL certifikátu oprávněným operátorem CA.

4.3.2 Oznámení o vydání certifikátu

Vydaný certifikát je automaticky zaslán na kontaktní e-mailovou adresu žadatele.

4.4 Převzetí vydaného certifikátu

4.4.1 Úkony spojené s převzetím certifikátu

Pokud byly splněny podmínky pro vydání certifikátu, je povinností žadatele o certifikát tento certifikát přijmout a přesvědčit se o přesnosti a správnosti údajů v něm uvedených. Jediným způsobem, jakým může žadatel o certifikát postupovat v případě, že tento certifikát nemá zájem převzít, je zažádat v souladu s touto CP o jeho zneplatnění.

4.4.2 Zveřejňování vydaných certifikátů poskytovatelem

I.CA je povinna zajistit neprodlené zveřejnění jí vydaných certifikátů, vyjma certifikátů:

- obsahujících údaje, jejichž zveřejnění by bylo v rozporu s legislativou ČR,
- u kterých si žadatel o certifikát vymínil, že nebudou zveřejněny.

4.4.3 Oznámení o vydání certifikátu jiným subjektům

Oznámení o vydání certifikátu získá pouze žadatel o certifikát.

4.5 Použití párových dat a certifikátu

4.5.1 Použití soukromého klíče a certifikátu držitelem

Povinností držitelů certifikátů je zejména:

- bez zbytečného odkladu podávat přesné, pravdivé a úplné informace I.CA ve vztahu k vydanému certifikátu,
- dodržovat veškerá relevantní ustanovení smlouvy o poskytování této certifikační služby,
- zacházet s prostředky, jakož i se soukromým klíčem s náležitou péčí tak, aby nemohlo dojít k jejich neoprávněnému použití,
- uvědomit neprodleně I.CA o tom, že hrozí nebezpečí zneužití jejich soukromého klíče odpovídajícího veřejnému klíči v SSL certifikátu,
- využívat soukromý klíč související s vydaným certifikátem v souladu s ustanoveními této CP.

4.5.2 Použití veřejného klíče a certifikátu spoléhající se stranou

Spoléhající se strany jsou zejména povinny:

- získat certifikáty CA související s certifikátem vydaným dle této CP a ověřit hodnoty jejich otisků,
- provádět veškeré úkony potřebné k tomu, aby si ověřily, že elektronický podpis certifikátu vydaného dle této CP je platný a tento certifikát, včetně certifikátů CA souvisejících s tímto vydaným certifikátem, nebyl zneplatněn,
- dodržovat veškerá relevantní ustanovení této CP.

4.6 Obnovení certifikátu

Vždy se jedná o vydání nového certifikátu s novým veřejným klíčem, kdy všechny informace musí být řádným způsobem ověřeny. I.CA postupuje při ověřování vlastnictví soukromého klíče odpovídajícího veřejnému klíči v žádosti o certifikát v souladu s kapitolou 3.2.1. V procesu ověřování ostatních údajů (pro stejného žadatele a doménu) může použít informace získané při předchozím ověřování za předpokladu, že nejsou starší 39 měsíců, v opačném případě je postupováno podle kap. 3.2.2. Pro vydání certifikátu dále platí požadavky kapitol 4.1 až 4.4.

4.6.1 Podmínky pro obnovení certifikátu

Viz kap 4.6.

4.6.2 Subjekty oprávněné požadovat obnovení certifikátu

Viz kap 4.6.

4.6.3 Zpracování požadavku na obnovení certifikátu

Viz kap 4.6.

4.6.4 Oznámení o vydání obnoveného certifikátu držiteli certifikátu

Viz kap 4.6.

4.6.5 Úkony spojené s převzetím obnoveného certifikátu

Viz kap 4.6.

4.6.6 Zveřejňování vydaných obnovených certifikátů poskytovatelem

Viz kap 4.6.

4.6.7 Oznámení o vydání obnoveného certifikátu jiným subjektům

Viz kap 4.6.

4.7 Výměna veřejného klíče v certifikátu

Službou výměny veřejného klíče je v kontextu této CP míněno vydání certifikátu s novým veřejným klíčem, aniž by byly změněny jiné informace v certifikátu. Pro vydání takového certifikátu platí požadavky kapitol 3.3.1 a 4.1 až 4.4.

4.7.1 Podmínky pro výměnu veřejného klíče v certifikátu

Viz kap 4.7.

4.7.2 Subjekty oprávněné požadovat výměnu veřejného klíče v certifikátu

Viz kap 4.7.

4.7.3 Zpracování požadavku na výměnu veřejného klíče

Viz kap 4.7.

4.7.4 Oznámení o vydání certifikátu s vyměněným veřejným klíčem

Viz kap 4.7.

4.7.5 Úkony spojené s převzetím certifikátu s vyměněným veřejným klíčem

Viz kap 4.7.

4.7.6 Zveřejnění vydaných certifikátů s vyměněným veřejným klíčem

Viz kap 4.7.

4.7.7 Oznámení o vydání certifikátu s vyměněným veřejným klíčem jiným subjektům

Viz kap 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. I.CA postupuje při ověřování vlastnictví soukromého klíče odpovídajícího veřejnému klíči v žádosti o certifikát v souladu s kapitolou 3.2.1. V procesu ověřování ostatních údajů (pro stejného žadatele a doménu) může použít informace získané při předchozím ověřování za předpokladu, že nejsou starší 39 měsíců, v opačném případě je postupováno podle kap. 3.2.2. Pro vydání certifikátu dále platí požadavky kapitol 4.1 až 4.4.

4.8.1 Podmínky pro změnu údajů v certifikátu

Viz kap 4.8.

4.8.2 Subjekty oprávněné požadovat změnu údajů v certifikátu

Viz kap 4.8.

4.8.3 Zpracování požadavku na změnu údajů v certifikátu

Viz kap 4.8.

4.8.4 Oznámení o vydání certifikátu se změněnými údaji držiteli certifikátu

Viz kap 4.8.

4.8.5 Úkony spojené s převzetím certifikátu se změněnými údaji

Viz kap 4.8.

4.8.6 Zveřejnění vydaných certifikátů se změněnými údaji

Viz kap 4.8.

4.8.7 Oznámení o vydání certifikátu se změněnými údaji jiným subjektům

Viz kap 4.8.

4.9 Zneplatnění a pozastavení platnosti certifikátu

Žádosti o zneplatnění certifikátu přijímá I.CA nepřetržitě prostřednictvím předání žádosti elektronickou cestou a listovní zásilkou.

Službu pozastavení platnosti certifikátu I.CA neposkytuje.

4.9.1 Podmínky pro zneplatnění certifikátu

4.9.1.1 Důvody zneplatnění uživatelského certifikátu

I.CA zneplatní certifikát během 24 hodin, pokud nastane jeden nebo více z následujících důvodů:

- držitel certifikátu podal písemnou žádost o zneplatnění certifikátu,
- držitel certifikátu oznámil certifikační autoritě, že původní žádost o certifikát byla neoprávněná a že zpětně neudělí autorizaci,
- I.CA získá důkaz, že soukromý klíč držitele certifikátu odpovídající klíči veřejnému v certifikátu byl kompromitován (viz také kapitola 10.2.4), nebo že dále nevyhovuje požadovaným kryptografickým algoritmům, držitel certifikátu je v takovém případě povinen řídit se pokyny CA vydávající SSL certifikáty,
- I.CA získá důkaz, že certifikát byl zneužit,
- I.CA je uvědoměna, že držitel certifikátu porušil jednu nebo více ze svých důležitých povinností plynoucích ze smlouvy o vydání certifikátu nebo smlouvy o podmínkách používání certifikátu,
- I.CA je uvědoměna o okolnostech indikujících, že plně kvalifikované jméno domény (FQDN) nebo IP adresa nejsou dále ze zákona povoleny (tj. soud nebo arbitráž odňaly registrantovi právo používat doménové jméno, zrušily relevantní smlouvu, smlouva o licenci nebo službě mezi registrantem doménového jména a žadatelem o certifikát byla zrušena, nebo se registrantovi doménového jména nepodařilo doménové jméno obnovit),
- I.CA je uvědoměna, že došlo k podstatným změnám informací obsažených v certifikátu,
- I.CA je uvědoměna, že certifikát nebyl vydán v souladu s CP, nebo CPS
- I.CA zjistí, že některá informace v certifikátu je nepřesná nebo zavádějící,
- I.CA z nějakého důvodu zastavila činnost a nemá připravený postup, aby zneplatňování jejich certifikátů převzala jiná CA,
- oprávnění I.CA vydávat certifikáty podle této CP vypršelo, bylo zneplatněno, nebo ukončeno a I.CA nepřipravila způsob jak udržovat CRL /OCSP úložiště,
- I.CA je uvědoměna o možné kompromitaci soukromého klíče autority vydávající SSL certifikáty,
- zneplatnění je vyžadováno CP nebo CPS,
- technický obsah nebo formát certifikátu představují neakceptovatelné riziko (např. daný kryptografický /podepisovací algoritmus nebo délka klíče).

4.9.1.2 Důvody zneplatnění certifikátu CA vydávající SSL certifikáty

I.CA zneplatní certifikát CA vydávající SSL certifikáty během sedmi dnů, pokud nastane některý z uvedených případů:

- CA vydávající SSL certifikáty požádá písemně o zneplatnění,
- že soukromý klíč CA vydávající SSL certifikáty odpovídající klíči veřejnému z jejího certifikátu byl kompromitován, nebo nadále nesplňuje požadavky na kryptografické algoritmy,

- kořenová CA, nebo pořízená CA vydávající SSL certifikáty, ukončily z nějakého důvodu činnost a nepřevedly podporu zneplatňování na jinou CA,
- právo kořenové CA nebo CA vydávající SSL certifikáty vydávat certifikáty podle relevantních CP vypršelo, nebo bylo odvoláno či ukončeno, pokud kořenová CA nezajistila pro CA vydávající SSL certifikáty pokračující správu úložiště CRL /OCSP,
- zneplatnění je vyžádáno CP a /nebo CPS kořenové CA,
- technický obsah nebo formát certifikátu představují neakceptovatelné riziko (např. daný kryptografický /podepisovací algoritmus nebo délka klíče).

4.9.2 Subjekty oprávněné žádat o zneplatnění certifikátu

Žádost o zneplatnění mohou podat:

- držitel certifikátu,
- subjekt, který k tomu byl explicitně určen ve smlouvě o poskytování certifikační služby,
- poskytovatel certifikačních služeb (oprávněným žadatelem o zneplatnění certifikátu vydaného I.CA je v tomto případě ředitel I.CA).

Držitel je povinen v případě podání žádosti o zneplatnění SSL certifikátu okamžitě přestat používat tento certifikát i odpovídající soukromý klíč.

4.9.3 Požadavek na zneplatnění certifikátu

4.9.3.1 Požadavek na zneplatnění certifikátu držitelem certifikátu

V případě předání žádosti o zneplatnění certifikátu elektronickou cestou jsou přípustné následující možnosti:

- Prostřednictvím formuláře na k tomuto účelu vyhrazené internetové informační adrese <http://www.ica.cz>. Datum a čas zneplatnění certifikátu je určen okamžikem přijetí platné žádosti o zneplatnění certifikátu informačním systémem CA. O kladném vyřízení je žadatel informován.
- Elektronicky podepsaná zpráva - tělo zprávy musí obsahovat text (v českém nebo slovenském jazyce, s diakritikou nebo bez diakritiky, případně v jazyce anglickém):

Zadam o zneplatneni certifikatu cislo = xxxxxxxx,

kde „xxxxxxx“ je sériové číslo certifikátu a musí být buď v dekadickém nebo hexadecimálním tvaru (uvozeno řetězcem „0x“).

- Elektronicky nepodepsaná elektronická zpráva - tělo zprávy musí obsahovat text (v českém nebo slovenském jazyce, s diakritikou nebo bez diakritiky, případně v jazyce anglickém):

Zadam o zneplatneni certifikatu cislo = xxxxxxxx

Heslo pro zneplatneni = yyyyyy,

kde „xxxxxxx“ je sériové číslo certifikátu a „yyyyyy“ je heslo pro zneplatnění. Sériové číslo musí být buď v dekadickém nebo hexadecimálním tvaru (uvozeno řetězcem „0x“).

Pozn.: Pokud žádost splňuje požadavky dvou výše uvedených možností, odpovědný pracovník RA certifikát v systému CA daný certifikát neprodleně zneplatní - datum

a čas zneplatnění certifikátu je určen přijetím tohoto požadavku informačním systémem CA. O kladném vyřízení je žadatel informován.

V případě použití doporučené listovní zásilky žádosti o zneplatnění certifikátu musí být v zásilce uvedena žádost v následujícím tvaru (v českém nebo slovenském jazyce, s diakritikou nebo bez diakritiky, případně v jazyce anglickém):

Zadam o zneplatneni certifikatu cislo = xxxxxxxx

Heslo pro zneplatneni = yyyyyy,

kde „xxxxxx“ je sériové číslo certifikátu a „yyyyyy“ je heslo pro zneplatnění. Sériové číslo je buď v dekadickém nebo hexadecimálním tvaru (uvozeno řetězcem „0x“). V případě, že žádost uvedené požadavky splňuje, odpovědný pracovník I.CA certifikát v informačním systému CA zneplatní - datum a čas zneplatnění certifikátu je určen přijetím tohoto požadavku informačním systémem CA. V případě, že žádost nelze akceptovat (nesprávné heslo pro zneplatnění) bude žádost o zneplatnění certifikátu zamítnuta. O vyřízení žádosti je žadatel informován doporučeným dopisem na poštovní adresu uvedenou jako adresa odesílatele.

4.9.3.2 Podezření na kompromitaci klíče a zneužití certifikátu

Oznámení o podezření na kompromitaci klíče a zneužití certifikátu je možné zaslat na adresu ssl@ica.cz, případně doporučenou listovní zásilkou, nebo podat prostřednictvím datové schránky.

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

4.9.5.1 Požadavek na zneplatnění certifikátu držitelem certifikátu

Požadavek na zneplatnění certifikátu pocházející od držitele certifikátu je realizován bezodkladně po přijetí oprávněné žádosti o zneplatnění. CRL obsahující sériové číslo zneplatněného certifikátu je vydán neprodleně po zneplatnění tohoto certifikátu.

4.9.5.2 Hlášení problémů s certifikáty

I.CA zahájí vyšetřování každého hlášeného problému s certifikátem během 24 hodin po přijetí hlášení a rozhodne, zda je nutné zneplatnění, nebo jiný odpovídající postup, na základě alespoň těchto kritérií:

- povaha údajného problému,
- počet obdržených hlášení o problému s certifikátem vztahujících se k jednotlivému certifikátu, nebo k držiteli certifikátu,
- kdo si stěžuje (např. hlášení od organizace prosazující právo, že stránka provozuje ilegální aktivity, má větší závažnost, než stížnost od zákazníka uvádějícího, že nedostal objednané zboží),
- relevantní legislativa.

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

Spoléhající se strany jsou povinny provádět veškeré úkony, uvedené v kapitole 4.5.2.

4.9.7 Periodicita vydávání seznamu zneplatněných certifikátů (CRL)

4.9.7.1 Stav SSL certifikátů

Seznam zneplatněných SSL certifikátů (CRL autority vydávající SSL certifikáty) je vydáván:

- neprodleně po zneplatnění každého certifikátu,
- a nejvýše 24 hodin od vydání předchozího CRL.

4.9.7.2 Stav certifikátu CA vydávající SSL certifikáty

Seznam zneplatněných certifikátů kořenové CA je vydáván:

- do 24 hodin od zneplatnění certifikátu CA vydávající SSL certifikáty,
- a nejméně 1x ročně.

Doba platnosti CRL je maximálně 12 měsíců.

4.9.8 Maximální zpoždění při zveřejňování seznamu zneplatněných certifikátů

Seznam zneplatněných certifikátů je zveřejňován neprodleně po jeho vydání.

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

Služba uvěřování stavu certifikátu s využitím protokolu OCSP je veřejně dostupná.

OCSP odpovědi vyhovují normám RFC 2560 a RFC 5019. OCSP odpovědi jsou podepsány OCSP respondérem, jehož certifikát je podepsán CA vydávající SSL certifikáty. Certifikát OCSP respondéru obsahuje rozšíření typu id-pkix-ocsp-nocheck, jak je definováno v RFC 2560.

4.9.10 Požadavky při ověřování stavu pomocí OCSP

OCSP umožňuje dotazy využívající GET metodu.

4.9.10.1 Stav SSL certifikátů

I.CA aktualizuje informaci poskytovanou prostřednictvím OCSP nejméně jednou za čtyři dny. OCSP odpovědi mají dobu platnosti maximálně deset dnů.

4.9.10.2 Stav certifikátu pořízené CA vydávající SSL certifikáty

I.CA aktualizuje informaci poskytovanou prostřednictvím OCSP:

- do 24 hodin po zneplatnění certifikátu CA vydávající SSL certifikáty,
- a nejméně každých dvanáct měsíců.

4.9.11 Jiné způsoby oznamování zneplatnění certifikátu

I.CA smluvně zavazuje držitele SSL certifikátu webových serverů, aby provedli konfiguraci serverů k provádění OCSP stapling dle RFC 4366 pro distribuci OCSP odpovědí.

4.9.12 Případné odlišnosti postupu zneplatnění v případě kompromitace soukromého klíče

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

4.10.1 Funkční charakteristiky

Seznamy veřejných SSL certifikátů jsou poskytovány formou zveřejňování informací, seznamy zneplatněných SSL certifikátů jsou poskytovány jak formou zveřejňování informací, tak uvedením distribučních míst CRL ve vydaných SSL certifikátech. OCSP odpovědi OCSP respondéru CA vydávající SSL certifikáty poskytují informaci o stavu certifikátu vydaného touto CA.

Záznamy o zneplatnění na CRL nebo v OCSP odpovědi jsou udržovány až do doby konce platnosti odvolaného certifikátu.

4.10.2 Dostupnost služeb

I.CA garantuje zajištění nepřetržité dostupnosti (7 dní v týdnu, 24 hodin denně) a integrity seznamu jí vydaných certifikátů a seznamu zneplatněných certifikátů (platné CRL), a dále dostupnost služeb OCSP.

Doba odpovědi na žádost o stav certifikátu s využitím CRL nebo OCSP je za normálních provozních podmínek kratší než 10 vteřin.

I.CA udržuje prostřednictvím mailové adresy `ssl@ica.cz`, své datové schránky a doporučenou listovní zásilkou nepřetržitou 24x7 dostupnost tak, aby interně zareagovala na hlášení závažného problému s certifikátem a, pokud je to nutné, přeposlala takové hlášení příslušnému orgánu nebo zneplatnila certifikát, který je předmětem hlášení.

4.10.3 Další charakteristiky služeb statutu certifikátu

Není relevantní pro tento dokument - další charakteristiky služeb stavu certifikátu nejsou poskytovány.

4.11 Ukončení poskytování služeb pro držitele certifikátu

I.CA ukončí poskytování služeb držiteli certifikátu ve chvíli, kdy dojde k ukončení smluvního vztahu mezi První certifikační autoritou, a.s., a organizací (držitelem certifikátu).

4.12 Úschova soukromého klíče u důvěryhodné třetí strany a jejich obnova

Není relevantní pro tento dokument - služba úschovy soukromého klíče a jeho obnovy není poskytována.

4.12.1 Politika a postupy při úschově a obnovování soukromého klíče

Není relevantní pro tento dokument - služba úschovy soukromého klíče a jeho obnovy není poskytována.

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

Není relevantní pro tento dokument - služba zapouzdřování a obnovování šifrovacího klíče pro relaci není poskytována.

5 MANAGEMENT, PROVOZNÍ A FYZICKÁ BEZPEČNOST

Oblasti managementu provozní a fyzické bezpečnosti jsou řešeny jak v základních dokumentech Celková bezpečnostní politika, Systémová bezpečnostní politika CA, 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, pracovišť 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 $20^{\circ}\text{C} \pm 5^{\circ}\text{C}$. 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 stoukou 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 ukládat, 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

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

- generování párových dat CA, využívaných v procesech vydávání SSL certifikátů a seznamů zneplatněných SSL certifikátů,
- ničení soukromých klíčů výše uvedených párových dat,
- zálohování /obnovu soukromých klíčů výše uvedených párových dat,
- aktivace 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 definované 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 3 roky praxe v oblasti informačních a komunikačních technologií, nebo středoškolské vzdělání a nejméně 5 let praxe v oblasti informačních a komunikačních technologií, přičemž z toho nejméně 1 rok v oblasti poskytování certifikačních služeb,
- znalost v oblasti infrastruktury veřejných klíčů a informační bezpečnosti,
- v jednotlivých případech lze zkrátit délku uvedené praxe až o jednu třetinu stanovené délky na základě přezkoušení, při němž pracovník prokáže dostatečné znalosti k výkonu své funkce.

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, které 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 uvedeným v interních dokumentech společnosti a řídicím se zákoníkem práce (tento proces nebrání případnému trestnímu stíhání, pokud tomu odpovídá závažnost zjištěné neautorizované činnosti).

5.3.7 Požadavky na nezávislé zhotovitele (dodavatele)

I.CA může nebo musí některé činnosti zajišťovat smluvně. Tyto obchodně právní vztahy jsou ošetřeny bilaterálními obchodními smlouvami. Jedná se o např. o smluvní registrační autority, zhotovitele programového aplikačního vybavení, dodavatele hardware, systémového programového vybavení, externí auditory atd. Tyto subjekty jsou povinny se řídit odpovídajícími veřejnými certifikačními politikami, relevantními částmi interní dokumentace, 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 pro vydání SSL certifikátů, mj. o životním cyklu SSL certifikátů, certifikátů CA vydávající SSL certifikáty a OCSP respondérů, využívaných v procesu ověřování stavu těchto SSL certifikátů.

Speciálním případem zaznamenávání událostí je událost generování párových dat CA vydávající SSL certifikáty, 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)

Auditní záznamy jsou shromažďovány v rámci jednotlivých subsystémů.

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, včetně vydaných certifikátů,
- případný videozáznam průběhu generování párových dat CA vydávající SSL certifikáty,
- další záznamy potřebné pro služby CA vydávající SSL certifikáty (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 vydávající SSL certifikáty, s výjimkou příslušných soukromých klíčů, jsou uchovávány po celou dobu existence I.CA. Ostatní informace a dokumentace dle kap. 5.5.1 jsou uchovávány v souladu s kap. 5.4.3.

Postupy při uchovávání informací a dokumentace jsou upraveny interní dokumentací.

5.5.3 Ochrana úložiště uchovávaných informací a dokumentace

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

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

5.5.4 Postupy při zálohování uchovávaných informací a dokumentace

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

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 směrnici. 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 soukromého klíče v certifikátu poskytovatele

V případě standardních situací (uplynutí platnosti certifikátu) je výměna s dostatečným časovým předstihem (minimálně jeden rok před uplynutím doby platnosti tohoto certifikátu) prováděna formou vydání nového certifikátu poskytovatele. V případě nestandardních situací (např. dojde-li k takovému vývoji kryptoanalytických metod, že by mohla být ohrožena bezpečnost certifikačních služeb, 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 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 plán obnovy a případně s další relevantní interní dokumentací.

5.7.2 Poškození výpočetních prostředků, softwaru nebo dat

Viz kap. 5.7.1.

5.7.3 Postup při kompromitaci soukromého klíče CA

V případě vzniku důvodné obavy z kompromitace soukromého klíče CA vydávající SSL certifikáty postupuje I.CA 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 soukromým klíčem elektronicky podepsány,
- bezodkladně o této skutečnosti, včetně důvodu, informuje v souladu s kap. 2.2, pro zpřístupnění této informace je využit i příslušný seznam zneplatněných certifikátů.

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 procesu vydávání certifikátů a poskytování informací o stavu certifikátů.

5.7.4 Schopnost obnovit činnost po havárii

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

5.8 Ukončení činnosti CA nebo RA

V případě plánovaného ukončení vydávání SSL certifikátů, tzn. z jiných důvodů, než jsou mimořádné události, jakými jsou stávky, občanské nepokoje, válečný stav, přírodní katastrofy celostátního rozsahu nebo jiné výsledky působení vyšší moci, zajistí I.CA provedení následujících činností:

- zpřístupní informaci o ukončení vydávání SSL certifikátů na své internetové adrese,
- vynaloží veškeré možné úsilí pro to, aby evidence o vydaných SSL certifikátech byla převzata jiným poskytovatelem certifikačních služeb - tuto informaci zahrne do zprávy odeslané všem svým klientům, kteří jsou držiteli platných smluv o vydání SSL certifikátu, pokud toto bude známo nejméně 2 měsíce před plánovaným ukončením činnosti,
- po uplynutí platnosti posledního vydaného SSL certifikátu prokazatelně zničí soukromý klíč CA vydávající SSL certifikáty.

6 TECHNICKÁ BEZPEČNOST

6.1 Generování a instalace párových dat

6.1.1 Generování párových dat

Generování párových dat CA vydávající SSL certifikáty, které probíhá v zabezpečené zóně podle předem připraveného scénáře, v souladu s požadavky kap. 5.2 a 5.4.1 a o jehož průběhu je vyhotoven písemný protokol, je prováděno v kryptografickém modulu, který byl hodnocen podle FIPS PUB 140-2 Level 3.

Generování párových dat, vztahujících se k SSL certifikátům, je prováděno na zařízeních, která jsou pod výhradní kontrolou žadatelů o certifikát. Úložištěm těchto párových dat může být jak hardware, tak software.

6.1.2 Předání soukromých klíčů držiteli certifikátu

Pro problematiku soukromého klíče CA vydávající SSL certifikáty není relevantní - soukromý klíč je uložen v kryptografickém modulu, který je pod výhradní kontrolou I.CA.

Služba generování párových dat vztahujících se k SSL certifikátům koncových uživatelů a tedy předání soukromého klíče držiteli certifikátu není neposkytována.

6.1.3 Předání veřejného klíče vydavateli certifikátu

Veřejný klíč žadatele o certifikát je vydavateli certifikátu doručen v žádosti o vydání certifikátu.

6.1.4 Poskytování veřejného klíče CA spoléhajícím se stranám

Získání veřejného klíče CA vydávající SSL certifikáty obsaženého v jejím certifikátu je garantováno následujícími způsoby:

- prostřednictvím internetových informačních adres I.CA,
- každý žadatel obdrží certifikát CA vydávající SSL certifikáty při získání SSL certifikátu.

6.1.5 Délky párových dat

V procesu poskytování certifikačních služeb v oblasti SSL certifikátů využívá I.CA asymetrický algoritmus RSA. Mohutnost klíčů CA vydávající SSL certifikáty (resp. parametrů daného algoritmu) je minimálně 2048 bitů, mohutnost klíčů (resp. parametrů daného algoritmu) na straně držitele SSL certifikátu je 2048 bitů. Ve vydávaných certifikátech je používán hashovací algoritmus SHA-256. V žádosti o SSL certifikát je povolen hashovací algoritmus SHA-256. I.CA si vyhrazuje právo podpory i dalších hashovacích algoritmů, splňujících požadavky platných standardů na problematiku hashovacích funkcí.

6.1.6 Generování parametrů veřejného klíče a kontrola kvality

Parametry veřejného klíče odpovídají požadavkům platných technických standardů.

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

6.1.7 Využití klíčů

CA pro vydávání SSL certifikátů je součástí hierarchické struktury certifikačních autorit provozovaných I.CA. Soukromý klíč kořenové CA není používán pro podepisování certifikátů vydávaných koncovým uživatelům.

Použití SSL certifikátu je popsáno v kap. 1.4.

6.2 Ochrana soukromého klíče a bezpečnost kryptografických modulů

6.2.1 Standardy a podmínky používání kryptografických modulů

Generování párových dat CA vydávající SSL certifikáty a uložení tohoto soukromého klíče, probíhá v kryptografickém modulu, který splňuje požadavky standardu FIPS PUB 140-2 Level 3.

6.2.2 Sdílení tajemství

Ochrana sdílením tajemství je realizována prostředky kryptografického modulu. Při provádění citlivých činností (viz kap. 6.1.1 a 6.2.10) je nezbytná přítomnost tří zaměstnanců I.CA, z nichž dva znají každý jednu část kódu k provedení těchto činností.

6.2.3 Úschova soukromého klíče

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

6.2.4 Zálohování soukromého klíče

Kryptografický modul použitý pro správu párových dat umožňuje zálohování soukromého klíče. Záloha databáze kryptografického modulu je prováděna s využitím jeho nativních prostředků v zašifrované podobě.

6.2.5 Uchovávání soukromého klíče

Po uplynutí doby platnosti soukromého klíče je tento včetně záloh zničen.

6.2.6 Transfer soukromého klíče do kryptografického modulu nebo z kryptografického modulu

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

6.2.7 Uložení soukromého klíče v kryptografickém modulu

Soukromé klíče jsou uložena bezpečným způsobem v kryptografickém modulu splňujícím požadavky standardu FIPS PUB 140-2 Level 3.

6.2.8 Postup při aktivaci soukromých klíčů

Aktivaci soukromých klíčů, vygenerovaných v kryptografickém modulu, provádí dva členové vedení I.CA prostřednictvím vlastní aktivace kryptografického modulu a aktivační čipové karty podle přesně určeného postupu, který je upraven interní dokumentací. Po aktivaci je systém připraven k činnosti, aktivační čipová karta se vyjme.

6.2.9 Postup při deaktivaci soukromých klíčů

Deaktivaci soukromých klíčů provádí dva členové vedení I.CA prostřednictvím kryptografického modulu a 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 soukromých klíčů

Soukromé klíče jsou uloženy v kryptografickém modulu. Ničení těchto klíčů je realizováno prostředky kryptografického modulu. Zálohy soukromých klíčů uložených v zašifrované podobě na externích médiích jsou rovněž zničeny. Ničení spočívá ve fyzické destrukci těchto nosičů. Postup ničení soukromých klíčů je přesně určen a popsán v interní dokumentaci.

6.2.11 Hodnocení kryptografických modulů

Kryptografický modul použitý byl certifikován na shodu s požadavky standardu FIPS PUB 140-2 Level 3.

6.3 Další aspekty správy párových dat

6.3.1 Uchovávání veřejných klíčů

Veřejných klíče, využívané v procesu vydávání SSL certifikátů jsou uchovávány po celou dobu existence I.CA.

6.3.2 Maximální doba platnosti certifikátu vydaného držiteli certifikátu 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 jsou vytvářena v průběhu generování párových dat CA vydávající SSL certifikáty.

6.4.2 Ochrana aktivačních dat

Aktivační data jsou chráněna způsobem uvedeným v interní dokumentaci.

6.4.3 Ostatní aspekty aktivačních dat

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

6.5 Počítačová bezpečnost

6.5.1 Specifické technické požadavky na počítačovou bezpečnost

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

6.5.2 Hodnocení počítačové bezpečnosti

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

- CWA 14167-1 - Security Requirements for Trustworthy Systems Managing Certificates for Electronic Signatures - Part 1: System Security Requirements /Bezpečnostní požadavky na důvěryhodné systémy spravující certifikáty pro elektronický podpis - část 1: Požadavky na bezpečnost systémů.
- ČSN ETSI EN 319 401 Elektronické podpisy a infrastruktury (ESI) - Obecné požadavky politiky na poskytovatele důvěryhodných služeb podporující elektronické podpisy.
- 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.
- CA/Browser Forum - Baseline Requirements for the Issuance and Management of Publicly-Trusted Certificates (Baseline Requirements).
- 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.
- ČSN ISO/IEC 27006 Informační technologie - Bezpečnostní techniky - Požadavky na orgány provádějící audit a certifikaci systémů řízení bezpečnosti informací.
- ISO/IEC 17021 Conformity assessment -- Requirements for bodies providing audit and certification of management systems.

6.6 Bezpečnost životního cyklu

6.6.1 Řízení vývoje systému

Při vývoji systému je postupováno v souladu s interní dokumentací.

6.6.2 Kontroly řízení bezpečnosti

Soulad se standardy (viz kap. 6.5.2) je ověřován pravidelnými audity systému managementu bezpečnosti informací, prováděnými auditory kvalifikovanými v souladu s relevantními technickými standardy.

6.6.3 Řízení bezpečnosti životního cyklu

Řízení bezpečnosti životního cyklu je v I.CA 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 kapitole 5.5.5.

7 PROFILY CERTIFIKÁTU, SEZNAMU ZNEPLATNĚNÝCH CERTIFIKÁTŮ A OCSP

7.1 Profil certifikátu

tab. 3 - Základní položky certifikátu kořenové CA

Pole	Obsah	Poznámka
Version	v3 (0x2)	
SerialNumber	jedinečné sériové číslo certifikátu	
SignatureAlgorithm	Sha512WithRSAEncryption	
Issuer		
commonName	I.CA Root CA/RSA	
organizationName	První certifikační autorita, a.s.	
Country	CZ	
serialNumber	NTRCZ-26439395	
Validity		
NotBefore	datum vydání	UTC
NotAfter	datum vydání + 25 let	UTC
Subject		
commonName	I.CA Root CA/RSA	
organizationName	První certifikační autorita, a.s.	
Country	CZ	
serialNumber	NTRCZ-26439395	
SubjectPublicKeyInfo		
Algorithm	rsaEncryption	
subjectPublicKey	veřejný klíč (4096 bitů)	
Extensions	rozšíření certifikátu	viz tab. 7
Signature	elektronická značka vydavatele certifikátu	

tab. 4 - Základní položky certifikátu CA vydávající SSL certifikáty

Položka	Obsah položky	Poznámka
Version	v3 (0x2)	
SerialNumber	jedinečné sériové číslo certifikátu	
SignatureAlgorithm	Sha256WithRSAEncryption	

Issuer	vydavatel tohoto certifikátu	viz tab. 3
Validity		
NotBefore	datum vydání	UTC
NotAfter	datum vydání+10 let	UTC
Subject		
commonName	I.CA SSL CA/RSA MM/RRRR*	
organizationName	První certifikační autorita, a.s.	
Country	CZ	
serialNumber	NTRCZ-26439395	
SubjectPublicKeyInfo		
Algorithm	rsaEncryption	
subjectPublicKey	veřejný klíč (4096 bitů)	
Extensions	rozšíření certifikátu	viz tab. 8
Signature	elektronická značka vydavatele certifikátu	

* měsíc a rok vydání certifikátu

tab. 5 - Základní položky certifikátu OCSP respondéru CA vydávající SSL certifikáty

Pole	Obsah	Poznámka
Version	v3 (0x2)	
SerialNumber	jedinečné sériové číslo certifikátu	
SignatureAlgorithm	Sha256WithRSA	
Issuer	vydavatel tohoto certifikátu	viz pole Subject v tab. 4
Validity	110 dnů	
Subject		
commonName	I.CA SSL CA/RSA MM/RRRR* OCSP responder	
organizationName	První certifikační autorita, a.s.	
countryName	CZ	
serialNumber	NTRCZ-26439395	
SubjectPublicKeyInfo		
Algorithm	RSA	
subjectPublicKey	2048	
Extensions	rozšíření certifikátu	viz tab. 9
Signature	elektronický podpis vydávající CA	

* měsíc a rok vydání certifikátu CA vydávající SSL certifikáty

tab. 6 - Základní položky SSL certifikátu typu OV

Pole	Obsah	Poznámka
Version	v3 (0x2)	
SerialNumber	jednoznačné sériové číslo certifikátu	
SignatureAlgorithm	Sha256WithRSAEncryption	
Issuer	vydavatel tohoto certifikátu	viz pole Subject v tab. 4
Validity		
notBefore	datum vydání	UTC
notAfter	datum vydání + 1 rok	UTC
Subject		
commonName	pokud uvedeno, MUSÍ se jednat o plně kvalifikované doménové jméno serveru, obsažené v první položce SAN.dnsName (viz tab. 11)	volitelná položka
organizationName	ověřené jméno nebo obchodní jméno subjektu (organizace vlastníci SSL /TLS server)	povinná položka
organizationalUnitName	ověřené jméno, obchodní jméno, obchodní značku, adresu, lokalitu nebo jiný text vztahující se k subjektu	volitelná položka
streetAddress	ověřená adresa ulice subjektu	volitelná položka
localityName	ověřená informace o lokalitě subjektu	volitelná položka, jedna z položek localityName, stateOrProvinceName MUSÍ být vyplněna
stateOrProvinceName	ověřená informace o státu či kraji subjektu	volitelná položka, jedna z položek localityName, stateOrProvinceName MUSÍ být vyplněna
postalCode	ověřená informace o poštovním směrovacím čísle subjektu	volitelná položka
countryName	dvoupísmenný kód země odpovídající ISO 3166-1 lokality subjektu	povinná položka
serialNumber	řetězec jednoznačně identifikující daný subjekt v informačním systému I.CA	povinná položka, generuje CA

SubjectPublicKeyInfo		
algorithm	RSAEncryption	
subjectPublicKey	2048	
Extensions	rozšíření vydávaného certifikátu	viz tab. 10
Signature	elektronický podpis vydavatele certifikátu	

tab. 7 - Základní položky SSL certifikátu typu DV

Pole	Obsah	Poznámka
Version	v3 (0x2)	
SerialNumber	jednoznačné sériové číslo	
SignatureAlgorithm	Sha256WithRSAEncryption	
Issuer	vydavatel tohoto certifikátu	viz pole Subject v tab. 4
Validity		
notBefore	datum vydání	UTC
notAfter	datum vydání + 1rok	UTC
Subject		
commonName	pokud je uvedeno, MUSÍ se jednat o plně kvalifikované doménové jméno serveru, obsažené v první položce SAN.dnsName (viz tab. 11)	volitelná položka
countryName	dvoupísmenný kód země odpovídající ISO 3166-1 lokality subjektu	volitelná položka, musí být shodná s ccTLD v požadovaných dnsName v názvu serverů v CN a SAN
serialNumber	řetězec, jednoznačně identifikující daný subjekt v informačním systému I.CA	povinná položka, generuje CA
SubjectPublicKeyInfo		
algorithm	RSAEncryption	
subjectPublicKey	2048	
Extensions	rozšíření vydávaného certifikátu	viz tab. 11
Signature	elektronický podpis vydavatele certifikátu	

7.1.1 Číslo verze

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

7.1.2 Rozšiřující položky v certifikátu

7.1.2.1 Kořenová CA

tab. 8 - Rozšíření certifikátu kořenové CA

Pole	Obsah	Poznámka
CertificatePolicies		nekritická
policyIdentifier	2.5.29.32.0 (anyPolicy)	
userNotice	Tento kvalifikovaný systémový certifikát byl vydán podle zákona 227/2000 Sb. v platném znění/This qualified system certificate was issued according to Act No. 227/2000 Coll.	
BasicConstraints		kritická
cA	True	
KeyUsage	keyCertSign, cRLSign	kritická
SubjectKeyIdentifier		nekritická
KeyIdentifier	hash veřejného klíče kořenové certifikační autority	

7.1.2.2 CA vydávající SSL certifikáty a její OCSP respondér

tab. 9 - Rozšíření certifikátu CA vydávající SSL certifikáty

Položka	Obsah položky	Poznámka
CertificatePolicies		nekritická
.PolicyInformation(1)		
policyIdentifier	2.5.29.32.0 (anyPolicy)	
[1.1]policyQualifiers .PolicyQualifierInfo(1) userNotice	Tento kvalifikovaný systémový certifikát byl vydán podle zákona 227/2000 Sb. v platném znění/This qualified system certificate was issued according to Act No. 227/2000 Coll.	
BasicConstraints		kritická
cA	True	
pathLen	0	
KeyUsage	keyCertSign, cRLSign	kritická

SubjectKeyIdentifier	hash veřejného klíče ve vydávaném certifikátu	nekritická
AuthorityKeyIdentifier	hash veřejného klíče vydavatele certifikátu	nekritická
CRLDistributionPoints	http://qcrlp1.ica.cz/rcaRR_rsa.crl* http://qcrlp2.ica.cz/rcaRR_rsa.crl* http://qcrlp3.ica.cz/rcaRR_rsa.crl*	nekritická
authorityInformationAccess		nekritická
accessMethod id-ad-ocsp	http://ocsp.ica.cz/rcaRR_rsa*	http URI OCSP respondéru kořenové CA
accessMethod id-ad-calssuers	http://rca.ica.cz/rcaRR_rsa.cer*	http URI certifikátu kořenové CA

* *RR* - poslední dvě číslice roku vydání certifikátu kořenové CA

tab. 10 - Rozšíření certifikátu OCSP respondéru CA vydávající SSL certifikáty

Položka	Obsah	Poznámka
CertificatePolicies.		nekritická
.PolicyInformation(1)		
policyIdentifier	1.3.6.1.4.1.23624.10.1.80.1.0	
authorityInformationAccess		nekritická
accessMethod id-ad-calssuers	http://s.ica.cz/scaRR_rsa.cer*	nekritická, http URI certifikátu vydávající CA
BasicConstraints		nekritická
cA	False	
KeyUsage	digitalSignature	kritická
ExtendedKeyUsage	id-kp-OCSPSigning	kritická
id-pkix-ocsp-nocheck	NULL	nekritická
SubjectKeyIdentifier	hash veřejného klíče ve vydávaném certifikátu	nekritická
AuthorityKeyIdentifier	hash veřejného klíče vydavatele certifikátu	nekritická

* *RR* - poslední dvě číslice roku vydání certifikátu CA vydávající SSL certifikáty

7.1.2.3 SSL certifikát

tab. 11 - Rozšíření SSL certifikátu typů OV i DV

Pole	Příklad naplnění	Poznámka
CertificatePolicies.		nekritická

.PolicyInformation(1)		
policyIdentifier	1.3.6.1.4.1.23624.10.1.72.1.0	
[1.1]policyQualifiers .PolicyQualifierInfo(1) cPSuri	http://www.ica.cz	
.PolicyInformation(2)		
policyIdentifier	DV: 2.23.140.1.2.1 OV: 2.23.140.1.2.2	identifikátor politiky dle požadavků Microsoft
CRLDistributionPoints	http://scrlp1.ica.cz/scaRR_rsa.crl* http://scrlp2.ica.cz/scaRR_rsa.crl*	nekritická
authorityInformationAccess		nekritická
accessMethod id-ad-ocsp	http://ocsp.ica.cz/scaRR_rsa*	URI (http) na OCSP responder vydávající CA
accessMethod id-ad-calssuers	http://s.ica.cz/scaRR_rsa.cer*	URI (http) souboru, který obsahuje certifikát vydávající CA
BasicConstraints		nekritická
cA	False	
KeyUsage	digitalSignature, keyEncipherment	kritická
ExtendedKeyUsage ¹	id-kp-serverAuth , id-kp-clientAuth , id-kp-emailProtection	nekritická
SubjectKeyIdentifier	hash veřejného klíče ve vydávaném certifikátu	nekritická
AuthorityKeyIdentifier	hash veřejného klíče vydavatele certifikátu	nekritická
SubjectAlternativeName. dNSName	Obsah první položky dnsName MUSÍ být totožný s obsahem položky Subject.commonName, pokud je commonName uvedeno (viz tab. 6 a 7 - commonName)	nekritická platí: <ul style="list-style-type: none"> • přípustné max. 10 položek dnsName, • u všech položek dnsName je přípustná pouze jediná doména 2.řádu, • SSL certifikáty pro domény se zástupnými znaky

¹ Jedná se o podporovanou množinu, konkrétní EKU je přebíráno ze žádosti o certifikát.

		(např. *.firma.cz) NESMĚJÍ být vydávány, • SSL certifikáty pro nové generické domény nejvyššího řádu NESMĚJÍ být vydávány , • NESMÍ se jednat o interní jméno
--	--	--

* RR - poslední dvě číslice roku vydání certifikátu CA vydávající SSL certifikáty

I.CA si vyhrazuje právo doplnit další OID politik dle standardu ETSI.

7.1.2.4 Všechny certifikáty

Ostatní pole a rozšíření jsou nastavena v souladu s RFC 5280. CA vydávající SSL certifikáty nevydá certifikát obsahující příznak keyUsage, hodnotu extendedKeyUsage, rozšíření certifikátu nebo další data nspecifikovaná v této kapitole 7.1.2, pokud nemá pro vložení takových dat do certifikátu důvod.

CA vydávající SSL certifikáty rovněž nevydá certifikáty:

- s rozšířeními, která jsou nerelevantní v kontextu veřejného Internetu,
- se sémantikou, která, pokud by byla zahrnuta, uvede v omyl spoléhající se stranu.

7.1.2.5 Aplikace RFC 5280

„Předcertifikát“, jak je popsán v RFC 6962 – Certificate Transparency, není považován za certifikát splňující požadavky RFC 5280.

7.1.3 Objektové identifikátory (dále „OID“) algoritmů

V procesu poskytování certifikačních služeb jsou využívány algoritmy, uvedené v příslušných technických standardech a ve shodě s Baseline Requirements.

7.1.4 Způsoby zápisu jmen a názvů

V souladu s požadavkem RFC 5280 se obsah pole Issuer ve vydaném SSL certifikátu shoduje s polem Subject v certifikátu CA vydávající SSL certifikáty. Déle platí ustanovení kapitoly 3.1.

Informace o subjektu jednotlivých certifikátů - viz tabulky kap. 7.1.

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

Viz rozšiřující položky v profilu certifikátů v kapitole 7.1.2 výše.

7.1.7 Rozšiřující položka „Policy Constraints“

Není relevantní pro tento dokument.

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

Viz rozšiřující položky v profilu certifikátů v kapitole 7.1.2 výše.

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. 12 - Profil CRL

Položka	Obsah
Version	v2(0x1)
SignatureAlgorithm	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. 13
crlExtensions	rozšíření CRL - viz tab. 13
SignatureAlgorithm	Sha256WithRSAEncryption
Signature	elektronický podpis vydavatele CRL

7.2.1 Číslo verze

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

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

tab. 13 - Rozšiřující položky CRL

Položka	Obsah	Poznámka
crlEntryExtensions		
CRLReason	důvod zneplatnění certifikátu; důvod	nekritická

	certificateHold je nepřipustný, nepoužívá se	
crlExtensions		
AuthorityKeyIdentifier		
KeyIdentifier	hash veřejného klíče vydavatele CRL	nekritická
CRLNumber	jedinečné číslo vydávaného CRL	nekritická

7.3 Profil OCSP

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 v souladu se standardy viz kap. 4.9.9.

8 HODNOCENÍ SHODY A JINÁ HODNOCENÍ

8.1 Periodicita hodnocení nebo okolnosti pro provedení hodnocení

Periodicity hodnocení, včetně okolností pro provádění hodnocení, jsou striktně dány požadavky standardů, dle kterých je hodnocení prováděno. Doba činnosti CA vydávající SSL certifikáty je rozdělena do nepřerušené posloupnosti auditních period, přičemž auditní perioda nepřekračuje jeden rok.

8.2 Identita a kvalifikace hodnotitele

Orgán provádějící audit je akreditován oficiálním akreditačním orgánem evropské kooperace pro akreditaci - viz <http://www.european-accreditation.org>, nebo mezinárodního akreditačního fóra - viz <http://www.iaf.nu>, jako vyhovující normě ISO/IEC 17021. Dále je akreditován národním akreditačním orgánem v souladu s ISO 27006 k provádění auditů podle ISO 27001.

8.3 Vztah hodnotitele k hodnocenému subjektu

Hodnotitel je nezávislý na společnosti První certifikační autorita, a.s.

8.4 Hodnocené oblasti

Hodnocené oblasti jsou dány standardem ETSI TS 102 042, podle kterého je hodnocení prováděno.

8.5 Postup v případě zjištění nedostatků

Se zjištěními všech typů prováděných hodnocení je seznámen bezpečnostní manažer I.CA, který je povinen zajistit odstranění případných nedostatků. Pokud by byly zjištěny nedostatky, které by zásadním způsobem znemožňovaly poskytovat certifikační služby v souladu s příslušným standardem, přeruší I.CA vydávání SSL certifikátů do doby, než budou tyto nedostatky odstraněny.

8.6 Sdělování výsledků hodnocení

Sdělování výsledků hodnocení je prováděno formou písemné závěrečné zprávy, která je hodnotícím subjektem předána řediteli, resp. bezpečnostnímu manažerovi I.CA.

V nejbližším možném termínu svolá bezpečnostní manažer I.CA schůzi bezpečnostního výboru, na které musí být přítomni členové vedení společnosti, které s obsahem závěrečné zprávy seznámí.

Sdělování výsledků hodnocení taktéž podléhá požadavkům příslušných standardů, dle kterých je hodnocení prováděno, závěrečný výrok auditora je veřejně dostupný.

8.7 Pravidelné samoaudity hodnocení kvality

Zaměstnanec I.CA provádí alespoň čtvrtletně, na náhodně vybraném vzorku o velikosti alespoň jednoho SSL certifikátu, nejméně však tři procent SSL certifikátů vydaných v době bezprostředně následující po té, kdy byl vybrán vzorek pro minulý samoaudit, kontrolu souladu s CP a CPS.

9 OSTATNÍ OBCHODNÍ A PRÁVNÍ ZÁLEŽITOSTI

9.1 Poplatky

9.1.1 Poplatky za vydání nebo obnovení certifikátu

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

9.1.2 Poplatky za přístup k certifikátu na seznamu vydaných certifikátů

Přístup elektronickou cestou k veřejným SSL certifikátům vydaným podle této CP I.CA nezpoblatňuje.

9.1.3 Poplatky za informace o stavu certifikátu nebo o zneplatnění certifikátu

Přístup elektronickou cestou k informacím o zneplatněných certifikátech (CRL) nebo stavech certifikátů (OCSP) vydaných dle této CP I.CA nezpoblatňuje.

9.1.4 Poplatky za další služby

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

Poplatky za nadstandardní služby jsou stanovovány smluvně.

9.1.5 Jiná ustanovení týkající se poplatků (vč. refundací)

I.CA je oprávněna stanovit pro individuálně uzavřené smlouvy odlišnou výši poplatku za vydání SSL certifikátu.

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 kap. 2.2, zejména:

- veškeré soukromé klíče, sloužící v procesu poskytování certifikačních služeb,
- obchodní informace I.CA,
- veškeré interní informace a dokumentace, týkající se poskytování certifikačních služeb,
- 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 kap. 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 nespádají 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 Poskytování 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:

- použije soukromé klíče příslušné certifikátům CA pouze v procesech vydávání certifikátů koncovým uživatelům a seznamů zneplatněných certifikátů,
- použije soukromé klíče příslušné OCSP respondérům příslušných CA pouze v procesech poskytování odpovědí na stav certifikátu vydaného touto CA,

- koncovým uživatelům vydávané SSL certifikáty splňují náležitosti požadované příslušným standardem,
- zneplatní vydané SSL certifikáty, pokud byla žádost o ukončení jejich platnosti podána způsobem definovaným v této CP.

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

- držitel certifikátu neporušil povinnosti plynoucí mu ze smlouvy o poskytování certifikační služby a této CP,
- spoléhající se strana neporušila povinnosti této CP.

Držitel SSL certifikátu, vydaného dle této CP, uplatňuje záruku vždy u RA, která zpracovala jeho žádost o vydání certifikátu.

I.CA vyjadřuje a poskytuje příjemcům SSL certifikátu, tj. držitelům, dodavatelům aplikačního programového vybavení, se kterými má uzavřenou smlouvu o zahrnutí kořenového certifikátu do jejich produktů a veškerým spoléhajícím se stranám záruku, že při vydávání SSL certifikátu a v průběhu doby platnosti při jeho správě bude vyhovovat své CP a CPS.

Záruky zahrnují:

- kontrolu práva užívat doménové jméno uváděné v SSL certifikátu,
- kontrolu práva žádat o certifikát jménem subjektu,
- ověření informací uváděných v žádosti o vydání SSL certifikátu, včetně kontroly obsahu položky organizační jednotky, případně identity žadatele,
- že smlouva o vydání SSL certifikátu odpovídá platným právním normám,
- že v režimu 24x7 je udržováno úložiště informací o stavu certifikátu,
- že SSL certifikát může být zneplatněn v souladu s důvody uvedenými v této CP.

9.6.2 Zastupování a záruky RA

Určená RA (viz kap. 1.3.2):

- přejímá závazek za správnost jí poskytovaných služeb,
- nevyřídí kladně žádost, pokud se nepodařilo ověřit některou z položek žádosti, žadatel odmítá potřebné údaje sdělit nebo není oprávněn k podání žádosti o certifikát,
- odpovídá za včasné předání žádostí o zneplatnění vydaných certifikátů k vyřízení na pracoviště CA,
- odpovídá za vyřizování připomínek a stížností klientů.

9.6.3 Záruky držitele certifikátu

Ve smlouvě mezi organizací a I.CA je uvedeno, že držitel je povinen řídit se ustanoveními této CP.

9.6.4 Záruky spoléhajících se stran

Spoléhající se strany postupují v souladu s touto CP.

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 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 touto certifikační politikou, dle které byl certifikát vydán.

9.9 Odpovědnost za škodu, náhrada škody

V procesu poskytování certifikačních služeb platí vždy takové záruky, které byly sjednány mezi společností První certifikační autorita, a.s., a žadatelem o konkrétní certifikační službu. Smlouva nesmí být v rozporu s platnou legislativou a musí být vždy v písemné formě.

Společnost První certifikační autorita, a.s.:

- se zavazuje, že splní veškeré povinnosti definované jak příslušnými právními předpisy, tak příslušnými certifikačními politikami,
- poskytuje výše uvedené záruky po celou dobu platnosti smlouvy o poskytování certifikačních služeb,
- souhlasí s tím, že dodavatelé aplikačního programového vybavení, kteří mají platnou smlouvu na distribuci kořenového certifikátu, nepřebírají žádné závazky nebo potenciální odpovědnost CA ve smyslu této CP s výjimkou případů, kde poškození či ztráta byly přímo způsobeny programovým vybavením tohoto dodavatele,
- jiné záruky, než výše uvedené, neposkytuje.

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

Společnost První certifikační autorita, a.s., neodpovídá:

- za vady poskytnutých služeb vzniklé z důvodu nesprávného nebo neoprávněného využívání služeb poskytnutých v rámci plnění smlouvy o poskytování certifikačních služeb držitelem, zejména za provozování v rozporu s podmínkami uvedenými v certifikační politice, jakož i za vady vzniklé z důvodu vyšší moci, včetně dočasného výpadku telekomunikačního spojení aj.,
- za škodu vyplývající z použití certifikátu v období po podání žádosti o jeho zneplatnění, pokud společnost První certifikační autorita, a.s., dodrží definovanou lhůtu pro zveřejnění zneplatněného certifikátu na seznamu zneplatněných certifikátů (CRL).

Reklamací je možné podat těmito způsoby:

- e-mailem na adresu reklamace@ica.cz,
- prostřednictvím datové schránky I.CA,
- doporučenou poštovní zásilkou na adresu sídla společnosti,

- osobně v sídle společnosti.

Reklamující osoba (držitel certifikátu) je povinna uvést:

- co nejvýstižnější popis závad a jejich projevů,
- sériové číslo reklamovaného produktu.

O reklamaci rozhodne I.CA nejpozději do tří pracovních dnů od doručení reklamace a vyrozumí o tom reklamujícího (formou elektronické pošty, nebo doporučenou zásilkou), pokud se strany nedohodnou jinak.

Reklamace, včetně vady, bude vyřízena bez zbytečných odkladů, a to nejpozději do jednoho měsíce ode dne uplatnění reklamace, pokud se strany nedohodnou jinak.

Nový certifikát bude držiteli poskytnut zdarma v následujících případech:

- existuje-li důvodné podezření, že došlo ke kompromitaci soukromého klíče, využívaného CA v procesu vydávání certifikátu koncovému uživateli a seznamů zneplatněných certifikátů, nabídne I.CA držitelům bezplatné vydání nového certifikátu - případné náklady na vydání nových certifikátů hradí I.CA, která po dobu zablokování certifikátů nese veškerou odpovědnost za případné škody vzniklé v souvislosti se zneužitím těchto certifikátů,
- v případě, že CA při příjmu žádosti o vydání certifikátu zjistí, že existuje jiný certifikát se stejným veřejným klíčem, je žadatel o certifikát vyzván k vygenerování nové žádosti a tedy i nových párových dat - držitel již existujícího certifikátu, který vlastní veřejný klíč stejný jako žadatel o vydání certifikátu, je vyzván k vygenerování nových párových dat, jeho původní certifikát je okamžitě zneplatněn a držitel je o této skutečnosti informován.

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 SSL certifikátu.

9.10.2 Ukončení platnosti

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

Jedinou osobou, která je oprávněna schvalovat ukončení platnosti této CP, a to v případě jejího nahrazení novou verzí, nebo ukončení poskytování služeb CA, vydávají certifikáty dle 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.

9.11 Komunikace mezi zúčastněnými subjekty

Pro individuální oznámení a komunikaci se zúčastněnými subjekty může I.CA využít jimi dodané e-mailové adresy, poštovní adresy, telefonní čísla, osobní jednání atd.

Komunikovat s I.CA lze taktéž způsoby uvedenými na adrese <http://www.ica.cz/>.

9.12 Změny

9.12.1 Postup při změnách

Postup je realizován řízeným procesem popsáním v interním dokumentu.

9.12.2 Postup při oznamování změn

Vydání nové verze certifikační politiky je vždy oznámeno formou zveřejnění informací (viz kap. 2.2).

9.12.3 Okolnosti, při kterých musí být změněn OID

V případě vydání nové verze tohoto dokumentu je pro tento dokument přiděleno nové OID.

9.13 Řešení sporů

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

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

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

9.14 Rozhodné právo

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

9.16.1 Rámcová dohoda

Není relevantní pro tento dokument.

9.16.2 Postoupení práv

Není relevantní pro tento dokument.

9.16.3 Oddělitelnost požadavků

Pokud soud, nebo veřejnoprávní orgán, v jehož jurisdikci jsou aktivity pokryté touto CP, stanoví, že provádění některého povinného požadavku je nelegální, potom je rozsah tohoto požadavku omezen tak, aby požadavek byl platný a legální. To platí pouze pro provozní činnosti a vydávání certifikátů podle legislativy daného státu. I,.CA o této skutečnosti informuje CA/Browser Forum.

9.16.4 Zřeknutí se práv

Není relevantní pro tento dokument.

9.16.5 Vyšší moc

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

9.17 Další opatření

Není relevantní pro tento dokument.

10 ZÁVĚREČNÁ USTANOVENÍ

Tato certifikační politika vydaná společností První certifikační autorita, a.s. nabývá platnosti a účinnosti dnem 15.07.2015.