První certifikační autorita, a.s.

Certifikační politika

kořenové kvalifikované certifikační autority

(algoritmus RSA)

Verze 1.0

OBSAH

tab. 1 - Vývoj dokumentu

Verze	Datum vydání	Schválil	Poznámka
1.0	18.05.2015	Ředitel společnosti První certifikační autorita, a.s.	První vydání.

1 ÚVOD

Tento dokument byl vypracován na základě požadavků platné legislativy vztahující se k problematice využívání kryptografických algoritmů v procesu poskytování certifikačních služeb. Kořenová kvalifikovaná certifikační autorita (algoritmus RSA) společnosti První certifikační autorita, a.s., (dále též Autorita), vydává v hierarchické dvoustupňové struktuře certifikačních autorit, v souladu s platnou legislativou a s požadavky technických standardů, kvalifikovaný systémový certifikát s algoritmem RSA kořenové certifikační autority, certifikáty s algoritmem RSA pro podřízené certifikační autority a certifikát svého OCSP respondéru s algoritmem RSA.

1.1 Přehled

Dokument **Certifikační politika kořenové kvalifikované certifikační autority (algoritmus RSA)**, dále též CP, vypracovaný společností První certifikační autorita, a. s., (dále též I.CA) se zabývá skutečnostmi, vztahujícími se k procesům životního cyklu jí vydávaných certifikátů a striktně dodržuje strukturu, jejíž předlohou je osnova platného standardu RFC, s přihlédnutím k platným standardům Evropské unie 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 informací, resp. dokumentace.
- Kapitola 3 popisuje procesy identifikace a autentizace žadatele o vydání certifikátu, resp. zneplatnění certifikátu, včetně definování typů a obsahů používaných jmen ve vydávaných certifikátech.
- Kapitola 4 definuje procesy životního cyklu jí vydávaných certifikátů, tzn. žádost o vydání a vlastní vydání certifikátu, žádost o zneplatnění a vlastní zneplatnění certifikátu, služby související s ověřováním stavu certifikátu, ukončení poskytování certifikačních služeb atd.
- Kapitola 5 zahrnuje problematiku fyzické, procesní a personální bezpečnosti, včetně definování množiny zaznamenávaných událostí, uchovávání těchto záznamů a reakce po haváriích nebo kompromitaci.
- Kapitola 6 je zaměřena na technickou bezpečnost typu generování veřejných a soukromých klíčů, ochrany soukromých klíčů, včetně počítačové a síťové ochrany.
- Kapitola 7 definuje profil vydávaných certifikátů a seznamů zneplatněných certifikátů.
- Kapitola 8 je zaměřena na problematiku hodnocení poskytovaných certifikačních služeb.
- Kapitola 9 zahrnuje problematiku obchodní a právní.

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

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

1.2 Název a jednoznačné určení dokumentu

Název tohoto dokumentu:	Certifikační politika kořenové kvalifikované certifikační autority (algoritmus RSA)
OID politiky:	1.3.6.1.4.1.23624.10.1.10.1.0

1.3 Participující subjekty

1.3.1 Certifikační autority (dále “CA”)

Kořenová kvalifikovaná certifikační autorita (algoritmus RSA), tj. Autorita, vydává v hierarchické dvoustupňové struktuře certifikačních autorit, v souladu s platnou legislativou a s požadavky technických standardů, certifikáty s algoritmem RSA pro podřízené certifikační autority a pro OCSP respondér Autority.

Autorita je ve stavu off-line a v žádném okamžiku tedy nemá propojení s externí sítí. Ve stavu on-line je pouze její OCSP respondér. Fyzicky je informační systém Autority realizován vyhrazenými počítači, HSM modul obsahující soukromý klíč je k informačnímu systému Autority připojen prostřednictvím vyhrazeného zabezpečeného rozhraní.

1.3.2 Registrační autority (dále “RA”)

Na procesech životního cyklu Autoritou vydávaných certifikátů se podílí speciální registrační autorita ve vlastnictví I.CA.

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

Certifikáty jsou vydávány výhradně pro certifikační autority provozované společností I.CA a pro OCSP respondér Autority. Oprávněným žadatelem a následně držitelem certifikátů je I.CA jako právnická osoba.

1.3.4 Spoléhající se strany

Spoléhající se stranou jsou subjekty spoléhající se při své činnosti na certifikát vydaný podle této CP.

1.3.5 Jiné participující subjekty

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

1.4 Použití certifikátu

1.4.1 Přípustné použití certifikátu

Certifikáty vydávané Autoritou podle této CP smějí být používány výhradně pro ověřování:

- elektronických značek jí vydaných certifikátů, seznamů zneplatněných certifikátů Autority (CRL) a OCSP odpovědí respondéru Autority,
- elektronických značek certifikátů a seznamů zneplatněných certifikátů (CRL) vydaných podřízenými certifikačními autoritami a OCSP odpovědí vydaných OCSP respondéry podřízených certifikačních autorit.

1.4.2 Omezení použití certifikátu

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

1.5 Správa politiky

1.5.1 Organizace spravující certifikační politiku nebo certifikační prováděcí směrnici

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

1.5.2 Kontaktní osoba organizace spravující certifikační politiku nebo certifikační prováděcí směrnici

Kontaktní osoba společnosti První certifikační autorita, a.s., v souvislosti s touto CP, resp. s odpovídající CPS, je uvedena na internetové adrese viz kap. 2.2.

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

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

1.5.4 Postupy při schvalování souladu podle bodu 1.5.3

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

1.6 Přehled použitých pojmů a zkratek

tab. 2 - Pojmy a zkratky

Pojem	Vysvětlení
bit	z anglického *binary digit* - číslice dvojkové soustavy je základní a současně nejmenší jednotkou informace používanou především v číslicové a výpočetní technice
CA	certifikační autorita
CRL (Certificate Revocation List)	seznam zneplatněných certifikátů obsahující certifikáty, které, již nelze pokládat za platné, někdy se pro seznam zneplatněných certifikátů certifikačních autorit užívá pojem Authority Revocation List (ARL)
držitel certifikátu	fyzická osoba, právnická osoba nebo organizační složka státu, která požádala o vydání certifikátu pro sebe nebo pro podepisující osobu a které byl certifikát vydán (v případě této CP První certifikační autorita, a.s.)
elektronický podpis, resp. elektronická značka	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 elektronickou značkou údaje v elektronické podobě, které jsou připojené k datové zprávě nebo jsou s ní logicky spojené a které splňují následující požadavky: • jsou jednoznačně spojené s označující osobou a umožňují její identifikaci prostřednictvím kvalifikovaného systémového certifikátu, • byly vytvořeny a připojeny k datové zprávě pomocí prostředků pro vytváření elektronických značek, které označující osoba může udržet pod svou výhradní kontrolou, • jsou k datové zprávě, ke které se vztahují, připojeny takovým způsobem, že je možné zjistit jakoukoli následnou změnu dat,
hash	transformace, která jako vstup přijímá řetězec znaků o libovolné délce a výsledkem je řetězec znaků s pevnou délkou
kořenový certifikát	self-signed (viz vysvětlení dále) certifikát certifikační autority na vrcholu hierarchické struktury certifikačních autorit
kvalifikovaný certifikát, kvalifikovaný systémový certifikát	certifikát, který má náležitosti podle platné legislativy ČR
OCSP respondér	server, obvykle provozovaný vydavatelem certifikátu, poskytující podepsané odpovědi, v jakém stavu je certifikát specifikovaný v dotazu
off-line	nepřipojený k počítači, počítačové síti, nebo Internetu

on-line	připojený k počítači, počítačové síti, nebo Internetu
označující osoba	fyzická osoba, právnická osoba nebo organizační složka státu, která drží prostředek pro vytváření elektronických značek a označuje datovou zprávu elektronickou značkou (v případě této CP První certifikační autorita, a.s.)
párová data	jedinečná data pro vytváření elektronického podpisu, resp. elektronické značky, spolu s odpovídajícími daty pro ověřování elektronického podpisu, resp. elektronické značky
podepisující osoba	fyzická osoba, která je držitelem prostředku pro vytváření elektronických podpisů a jedná jménem svým nebo jménem jiné fyzické či právnické osoby
MVČR	Ministerstvo vnitra České republiky
RA	registrační autorita
self-signed certifikát	certifikát veřejného klíče podepsaný soukromým klíčem tvořícím s tímto veřejným klíčem párová data
soukromý klíč	jedinečná data pro vytváření elektronického podpisu, resp. elektronické značky
spoléhající se strana	subjekt, spoléhající se při své činnosti na certifikát vydaný I.CA
veřejný klíč	jedinečná data pro ověřování elektronického podpisu, resp. elektronické značky
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. 101/2000 Sb., o ochraně osobních údajů a o změně některých zákonů (zákon o ochraně osobních údajů), ve znění pozdějších předpisů
ZoEP	zákon č. 227/2000 Sb., o elektronickém podpisu a o změně některých dalších zákonů (zákon o elektronickém podpisu), ve znění pozdějších předpisů

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, na nichž lze nalézt veřejné informace o společnosti První certifikační autorita, a.s., případně odkazy pro zjištění dalších informací, jsou:

a) adresa sídla společnosti:

   První certifikační autorita, a.s.

   Podvinný mlýn 2178/6

   190 00 Praha 9

   Česká republika

b) internetová adresa http://www.ica.cz,

c) sídla registračních autorit.

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

a) sídla registračních autorit,

b) elektronická poštovní adresa info@ica.cz.

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

Na výše uvedené internetové adrese lze získat informace o certifikátech vydaných podle této CP a o seznamech zneplatněných certifikátů (CRL).

V případech odejmutí akreditace, nebo vzniku důvodné obavy ze zneužití soukromého klíče Autority, oznámí I.CA tuto skutečnost na výše uvedené internetové adrese a prostřednictvím celostátně distribuovaného deníku Hospodářské noviny, nebo Mladá fronta Dnes.

2.3 Periodicita zveřejňování informací

Autorita zveřejňuje informace s následující periodicitou:

- certifikační politika - po ověření kořenového kvalifikovaného systémového certifikátu Autority, resp. po ověření jí vydaného kvalifikovaného systémového certifikátu podřízené certifikační autority poskytující kvalifikované certifikační služby dozorovým orgánem,
- certifikační prováděcí směrnice - neprodleně (jsou-li určeny ke zveřejnění),
- seznam vydaných certifikátů - aktualizace při každém vydání nového certifikátu určeného ke zveřejnění,
- seznam zneplatněných certifikátů - po každé změně a dále v pravidelných intervalech (nejméně jednou ročně),

- informace požadované platnou legislativou - bezodkladně,
- ostatní veřejné informace - není předem určeno, obecně však platí, že tyto informace musí reflektovat aktuální stav poskytovaných služeb.

2.4 Řízení přístupu k jednotlivým typům úložišť

Veškeré veřejné informace (viz kap. 2.2 a 2.3) zpřístupňuje I.CA bezplatně bez omezení.

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

3 IDENTIFIKACE A AUTENTIZACE

3.1 Pojmenování

3.1.1 Typy jmen

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

3.1.2 Požadavek na významovost jmen

U všech certifikátů musí jména vyjadřovat účel, ke kterému je certifikát vydáván (název podřízené certifikační autority, označení OCSP respondéru).

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 certifikát se do vydávaných certifikátů přenášejí ve tvaru, ve kterém jsou uvedeny v předkládaných dokumentech.

3.1.5 Jedinečnost jmen

Jména (položky Subject a Issuer) musí být jedinečná. Společnost První certifikační autorita, a.s., zaručuje jedinečnost těchto položek v certifikátech vydávaných dle této CP.

3.1.6 Obchodní značky

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

3.2 Počáteční ověření identity

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

Soulad dat se ověřuje tak, že je žádost o příslušný certifikát ve formátu PKCS#10, obsahující veřejný klíč, podepsána soukromým klíčem, který odpovídá veřejnému klíči, obsaženému v předkládané žádosti. Tímto způsobem žadatel o certifikát dokazuje, že v době tvorby žádosti o certifikát vlastnil soukromý klíč, odpovídající veřejnému klíči, který je v této žádosti obsažen.

3.2.2 Ověřování identity právnické osoby nebo organizační složky státu

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

3.2.3 Ověřování identity fyzické osoby

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

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

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

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

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

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

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

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

Všechny informace musí být řádným způsobem ověřeny.

3.2.5 Ověřování specifických práv

Není relevantní pro tento dokument.

3.2.6 Kritéria pro interoperabilitu

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

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

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

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

3.3.2 Identifikace a autentizace při výměně párových dat po zneplatnění certifikátu

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

3.4 Identifikace a autentizace při zpracování požadavků na zneplatnění certifikátu

Oprávněnou osobou žádat o zneplatnění certifikátu Autority i certifikátu jí vydaného je ředitel I.CA.

Žadatelem o zneplatnění certifikátu Autority může být taktéž představitel úřadu, který společnost První certifikační autorita, a.s., akreditoval. Žádost od úřadu musí být písemná, nebo musí být doručena do datové schránky.

Samotnému procesu zneplatnění certifikátu Autority musí být ředitel I.CA vždy osobně přítomen.

4 POŽADAVKY NA ŽIVOTNÍ CYKLUS CERTIFIKÁTU

4.1 Žádost o vydání certifikátu

4.1.1 Subjekty oprávněné podat žádost o vydání certifikátu

Žádost o vydání certifikátu Autoritou je oprávněn podat ředitel I.CA.

4.1.2 Registrační proces a odpovědnosti poskytovatele a žadatele

Písemná žádost o vydání certifikátu je předkládána vedení společnosti První certifikační autorita, a.s., prostřednictvím jejího ředitele a musí obsahovat název a OID této certifikační politiky (viz kapitola 1.2), včetně uvedení požadovaného jména CA (tzv. commonName, viz kapitola 7). Žádost musí být podepsána ředitelem I.CA.

4.1.2.1 Odpovědnost žadatele

Žadatel je povinen zejména:

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

4.1.2.2 Odpovědnost poskytovatele

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

4.2 Zpracování žádosti o certifikát

4.2.1 Identifikace a autentizace

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

4.2.2 Přijetí nebo zamítnutí žádosti o certifikát

Na základě písemné žádosti (viz kap. 4.1.2) rozhodne vedení společnosti První certifikační autorita, a.s., o vydání certifikátu CA s příslušným jménem, případně o zamítnutí žádosti. Výsledek je dokumentován.

4.2.3 Doba zpracování žádosti o certifikát

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

4.3 Vydání certifikátů

4.3.1 Úkony CA v průběhu vydávání certifikátu

Po kladném vyřízení žádosti o certifikát (viz kap. 4.2) následuje proces vydávání certifikátu, v jehož průběhu jsou prováděny nezbytné kontroly (formální správnost údajů obsažených v žádosti, řádné naplnění položek žádosti), zejména ověření:

- identity právnické osoby (viz kap. 3.2.2),
- identity fyzické osoby žadatele o certifikát (viz kap. 3.2.3),
- dalších údajů obsažených v písemné žádosti,
- souladu údajů obsažených v žádosti o certifikát ve formátu PKCS#10 s údaji obsaženými v předkládaných dokumentech,
- vlastnictví příslušného soukromého klíče (viz kap. 3.2.1),

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

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

Žadatel o certifikát je osobně přítomen vydání certifikátu.

4.4 Převzetí vydaného certifikátu

4.4.1 Úkony spojené s převzetím certifikátu

Žadatel o certifikát, nebo jím určený pracovník, je povinen překontrolovat, zda jsou údaje obsažené ve vydaném certifikátu v souladu s údaji uvedenými v žádosti a v předkládaných dokumentech.

4.4.2 Zveřejňování vydaných certifikátů poskytovatelem

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

Certifikát kořenové kvalifikované certifikační autority a certifikáty podřízených certifikačních autorit související s kvalifikovanými certifikačními službami jsou předány dozorovému orgánu.

4.4.3 Oznámení o vydání certifikátu jiným subjektům

Platí ustanovení kap. 4.4.2 a požadavky platné legislativy.

4.5 Použití párových dat a certifikátu

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

Povinností označující osoby mj. je:

- používat soukromý klíč a jemu odpovídající veřejný klíč obsažený ve vydaném certifikátu v souladu s touto CP,
- nakládat se soukromým klíčem, odpovídajícím veřejnému klíči v certifikátu vydaném podle této CP, tak, aby nemohlo dojít k jeho neoprávněnému použití,
- v případě kompromitace, nebo podezření na kompromitaci, soukromého klíče odpovídajícího veřejnému klíči v certifikátu certifikační autority vydaném podle této CP, o této skutečnosti okamžitě informovat v souladu s platnou legislativou (ZoEP) a zároveň ukončit jeho používání.

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

Spoléhající se strany jsou zejména povinny:

- získat z bezpečného zdroje certifikát kořenové Autority (internetová adresa uvedená v kap. 2.2, internetová adresa dozorového orgánu, pracoviště RA) a ověřit kontrolní součet tohoto certifikátu,
- provádět veškeré úkony potřebné k tomu, aby si ověřily, že certifikát vydaný Autoritou nebyl zneplatněn, mj. ověřit platnost:
  - kořenového certifikátu,
  - jí vydaného certifikátu podřízené certifikační autority.

4.6 Obnovení certifikátu

Je nutné vydat nový certifikát s novým veřejným klíčem. Platí stejné požadavky jako v případě počátečního ověření identity - viz kap. 3.2.

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, podepisující nebo označující osobě

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

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

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

Viz kap. 4.7.

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

Viz kap. 4.7.

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

Viz kap. 4.7.

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

Viz kap. 4.7.

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

Viz kap. 4.7.

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

Viz kap. 4.7.

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

Viz kap. 4.7.

4.8 Změna údajů v certifikátu

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

4.8.1 Podmínky pro změnu údajů v certifikátu

Viz 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 podepisující nebo označující osobě

Viz kap. 4.8.

4.8.5 Úkony spojené s převzetím certifikátu se změněnými údaji

Viz kap. 4.8.

4.8.6 Zveřejňování 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

4.9.1 Podmínky pro zneplatnění certifikátu

Certifikát může být zneplatněn na základě následujících okolností:

- dojde ke kompromitaci, resp. existuje důvodné podezření, že došlo ke kompromitaci, soukromého klíče, odpovídajícího veřejnému klíči tohoto certifikátu,
- žádost ředitele I.CA,
- nastanou-li skutečnosti uvedené v ZoEP.

4.9.2 Subjekty oprávněné žádat o zneplatnění certifikátu

Žádost o zneplatnění mohou podat:

- ředitel I.CA,
- další subjekty definované ZoEP.

4.9.3 Požadavek na zneplatnění certifikátu

Viz kap 3.4.

4.9.4 Doba odkladu požadavku na zneplatnění certifikátu

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

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

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

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

Spoléhající se strany jsou povinny postupovat v souladu s kap. 4.5.2.

4.9.7 Periodicita vydávání seznamu zneplatněných certifikátů

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

4.9.8 Maximální zpoždění při vydávání seznamu zneplatněných certifikátů

Seznam zneplatněných certifikátů je zveřejňován neprodleně po jeho vydání.

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

Služba ověřováni stavu certifikátu vydaného Autoritou s využitím protokolu OCSP je veřejně dostupná.

4.9.10 Požadavky při ověřování statutu certifikátu on-line

Viz kap. 4.9.9.

4.9.11 Jiné způsoby oznamování zneplatnění certifikátu

Není relevantní pro tento dokument, jiná služba oznamování zneplatnění certifikátu není poskytována.

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

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

4.9.13 Podmínky pro pozastavení platnosti certifikátu

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

4.9.14 Subjekty oprávněné požadovat pozastavení platnosti certifikátu

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

4.9.15 Zpracování požadavku na pozastavení platnosti certifikátu

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

4.9.16 Omezení doby pozastavení platnosti certifikátu

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

4.10 Služby související s ověřováním statutu certifikátu

4.10.1 Funkční charakteristiky

Seznamy veřejných certifikátů vydaných Autoritou jsou poskytovány formou zveřejňování informací, seznamy zneplatněných certifikátů Autoritou vydaných certifikátů jsou poskytovány jak formou zveřejňování informací, tak uvedením distribučních míst CRL ve

vydaných certifikátech. OCSP odpovědi OCSP respondéru Autority poskytují informaci o stavu certifikátu vydaného Autoritou.

4.10.2 Dostupnost služeb

Autorita 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.

4.10.3 Další charakteristiky služeb statutu certifikátu

Další charakteristiky služeb stavu certifikátu nejsou poskytovány.

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

Viz kap. 5.8.

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

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

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

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

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

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

5 MANAGEMENT, PROVOZNÍ A FYZICKÁ BEZPEČNOST

Management bezpečnosti je zaměřen především na:

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

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

5.1 Fyzická bezpečnost

5.1.1 Umístění a konstrukce

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

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

5.1.2 Fyzický přístup

Požadavky na fyzický přístup do jednotlivých vyhrazených prostor (chráněných mechanickými a elektronickými prostředky) provozních pracovišť jsou uvedeny v interní dokumentaci společnosti. Ochrana objektů je řešena elektronickým zabezpečovacím systémem (EZS), připojením na pult centrální ochrany (PCO) a případně speciálním systémem pro snímání, přenos a zobrazování pohybu osob a dopravních prostředků.

5.1.3 Elektřina a klimatizace

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

5.1.4 Vlivy vody

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

5.1.5 Protipožární opatření a ochrana

V objektech provozních pracovišť je instalována elektronická požární signalizace (EPS). Vstupní dveře vyhrazených prostor, ve kterých jsou umístěna zařízení, určená k výkonu

hlavních certifikačních služeb, jsou opatřeny protipožární vložkou. V samotných prostorách se nachází hasicí přístroj.

5.1.6 Ukládání médií

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

Papírová média, která je nutno, mj. dle ZoEP, archivovat, jsou skladována v jiné geografické lokalitě, než je umístěno provozní pracoviště.

5.1.7 Nakládání s odpady

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

5.1.8 Zálohy mimo budovu

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

5.2 Procesní bezpečnost

5.2.1 Důvěryhodné role

Pro vybrané činnosti jsou ve společnosti 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

V rámci Autority jsou pro procesy poskytování certifikačních služeb definovány činnosti, které musí být vykonány za účasti více než jediné osoby. Jedná se zejména o:

- generování párových dat Autority,
- ničení soukromého klíče Autority,
- zálohování /obnovu soukromého klíče Autority,
- aktivace kryptografického modulu, obsahujícího soukromý klíč Autority.

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

5.2.3 Identifikace a autentizace pro každou roli

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

5.2.4 Role vyžadující rozdělení povinností

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

5.3 Personální bezpečnost

5.3.1 Požadavky na kvalifikaci, zkušenosti a bezúhonnost

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

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

5.3.3 Požadavky na přípravu pro výkon role, vstupní školení

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

5.3.4 Požadavky a periodicita školení

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

5.3.5 Periodicita a posloupnost rotace pracovníků mezi různými rolemi

Z důvodů možné zastupitelnosti v mimořádných případech jsou zaměstnanci I.CA motivováni k získávání znalostí potřebných pro zastávání jiné role v I.CA.

5.3.6 Postihy za neoprávněné činnosti zaměstnanců

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

5.3.7 Požadavky na nezávislé zhotovitele (dodavatele)

I.CA může nebo musí některé činnosti zajišťovat smluvně. Tyto obchodně právní vztahy jsou ošetřeny bilaterálními obchodními smlouvami. Jedná se o např. o smluvní registrační autority, zhotovitele programového aplikačního vybavení, dodavatele hardware, systémového programového vybavení, externí auditory atd. Tyto subjekty jsou povinny se řídit odpovídajícími veřejnými certifikačními politikami, relevantními částmi interní dokumentace I.CA, které jim budou poskytnuty a předepsanými normativními dokumenty. V případě porušení povinností stanovených v uvedených dokumentech jsou vyžadovány smluvní pokuty, případně je s dodavatelem okamžitě ukončena smlouva.

5.3.8 Dokumentace poskytovaná zaměstnancům

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

5.4 Auditní záznamy (logy)

5.4.1 Typy zaznamenávaných událostí

Zaznamenávány jsou veškeré události požadované ZoEP a technickými standardy, mj. o životním cyklu vydávaných certifikátů, nakládání se soukromým klíčem Autority a o dalších událostech, jako je např. ukončení činnosti Autority.

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.

Speciálním případem zaznamenávání událostí je událost generování párových dat Autority. Celý proces probíhá v souladu se ZoEP a platnými technickými standardy, přičemž minimálně platí, že:

- je prováděn podle připraveného scénáře ve fyzicky zabezpečeném prostředí,
- dále:
  - je mu osobně přítomen auditor kvalifikovaný v souladu s platnými technickými standardy, nebo
  - je pořizován videozáznam, podle možnosti je generování přítomen notář, který o průběhu sepíše osvědčení,
- na základě osobní přítomnosti, nebo videozáznamu a případného osvědčení vystaví auditor, kvalifikovaný v souladu s platnými technickými standardy, zprávu, že Autorita při generování párových dat postupovala v souladu s připraveným scénářem a o opatřeních pro zajištění integrity a důvěrnosti.

5.4.2 Periodicita zpracování záznamů

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

5.4.3 Doba 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 bezpečnostní dokumentaci.

5.4.5 Postupy pro zálohování auditních záznamů

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

5.4.6 Systém shromažďování auditních záznamů (interní nebo externí)

Systém shromažďování auditních záznamů je z pohledu informačních systémů Autority interní.

5.4.7 Postup při oznamování události subjektu, který ji způsobil

Subjekt není o zapsání události do auditního záznamu informován.

5.4.8 Hodnocení zranitelnosti

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

5.5 Uchovávání informací a dokumentace

Uchovávání informací a dokumentace je u I.CA prováděno dle požadavků ZoEP a 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 v oblasti vydávání certifikátů, zejména:

- videozáznam průběhu generování párových dat Autority,
- případné osvědčení notáře o průběhu generování párových dat Autority,
- zprávu auditora o průběhu generování párových dat Autority,
- dokumenty a záznamy související s životním cyklem vydaných certifikátů,
- vydané certifikáty,
- další záznamy požadované ZoEP (např. seznamy zneplatněných certifikátů),
- aplikační programové vybavení a veškerou dokumentaci společnosti, která je nutná pro provádění kontrol,
- záznam o manipulaci (např. převzetí, předání, uložení, kontrola, konverze do elektronické podoby atp.) s informacemi,
- provozní a bezpečnostní dokumentace.

5.5.2 Doba uchování uchovávaných informací a dokumentace

Informace, vztahující se k certifikátům vydaným Autoritou, s výjimkou příslušných soukromých klíčů, jsou uchovávány po celou dobu existence I.CA.

Uchovávání ostatních informací a dokumentace dle kap. 5.5.1 je prováděno v souladu kap. 5.4.3.

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

5.5.3 Ochrana úložiště uchovávaných informací a dokumentace

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

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

5.5.4 Postupy při zálohování uchovávaných informací a dokumentace

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

5.5.5 Požadavky na používání časových razítek při uchovávání informací a dokumentace

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

5.5.6 Systém shromažďování uchovávaných informací a dokumentace (interní nebo externí)

Informace a dokumentace jsou ukládány na místo určené ředitelem I.CA.

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

5.5.7 Postupy pro získání a ověření uchovávaných informací a dokumentace

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

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

O každém takto povoleném přístupu je pořizován písemný záznam.

5.6 Výměna dat pro ověřování elektronických značek v nadřízeném kvalifikovaném systémovém certifikátu poskytovatele

V případě standardních situací (uplynutí platnosti certifikátu) je výměna s dostatečným časovým předstihem (minimálně jeden rok před uplynutím doby platnosti tohoto certifikátu) prováděna formou vydání nového certifikátu poskytovatele. V případě nestandardních situací (např. dojde-li k takovému vývoji kryptoanalytických metod, že by mohla být ohrožena bezpečnost procesu vytváření elektronických značek, tzn. změny kryptografických algoritmů, délky klíčů atd.) je tato činnost prováděna v adekvátním časovém období.

Jak v případě standardních situací, tak nestandardních situací je výměna veřejného klíče v nadřízeném kvalifikovaném systémovém certifikátu poskytovatele veřejnosti s předstihem (je-li to možné) vhodnou formou sdělena.

5.7 Obnova po havárii nebo kompromitaci

5.7.1 Postup v případě incidentu a kompromitace

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

5.7.2 Poškození výpočetních prostředků, softwaru nebo dat

Viz kap. 5.7.1.

5.7.3 Postup při kompromitaci dat pro vytváření elektronických značek poskytovatele

V případě vzniku důvodné obavy z kompromitace soukromého klíče Autority postupuje Autorita tak, že:

- ukončí jeho používání,
- okamžitě a trvale zneplatní příslušný certifikát a zničí jemu odpovídající soukromý klíč,
- zneplatní všechny platné certifikáty, které byly výše uvedeným klíčem elektronicky označeny,
- bezodkladně o této skutečnosti, včetně důvodu, informuje na své internetové informační adrese (viz kap. 2.2), pro zpřístupnění této informace je využit i seznam zneplatněných certifikátů,
- oznámí dozorovému orgánu informaci o zneplatnění příslušného certifikátu s uvedením důvodu.

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

5.7.4 Schopnost obnovit činnost po havárii

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

5.8 Ukončení činnosti CA nebo RA

Pro ukončování činnosti Autority platí následující pravidla:

- ukončení činnosti Autority musí být písemně oznámeno všem držitelům platných certifikátů, dozorovému orgánu určenému ZoEP a subjektům, které mají uzavřenou smlouvu přímo se vztahující k poskytování certifikačních služeb,
- ukončení činnosti Autority musí být zveřejněno na internetové adrese podle kap. 2.2,
- pokud je součástí ukončení činnosti Autority ukončení platnosti jejího certifikátu, musí být součástí oznámení i tato informace včetně uvedení důvodu ukončení platnosti,
- po dobu platnosti jediného certifikátu vydaného Autoritou musí Autorita zajistit alespoň funkce zneplatňování certifikátu a vydávání CRL,

- následně Autorita prokazatelně zničí svůj soukromý klíč a o tomto zničení provede záznam, který bude uchováván v souladu s pravidly této CP, viz kap. 5.4.

V případě ukončení činnosti poskytovatele certifikačních služeb bude postupováno v souladu s příslušnými ustanoveními ZoEP.

V případě odnětí akreditace:

- informace o odnětí akreditace musí být písemně nebo elektronicky oznámena všem držitelům platných certifikátů a subjektům, které mají uzavřenou smlouvu přímo se vztahující k poskytování certifikačních služeb,
- informace o odnětí akreditace musí být zveřejněna v souladu s kap. 2.2 a na všech pracovištích registračních autorit; součástí informace bude i sdělení, že kvalifikované systémové certifikáty nelze nadále používat podle ustanovení platné legislativy,¨
- o dalším postupu rozhodne ředitel I.CA na základě rozhodnutí dozorového orgánu dle ZoEP.

Ukončení činnosti RA není relevantní pro tento dokument.

6 TECHNICKÁ BEZPEČNOST

6.1 Generování a instalace párových dat

6.1.1 Generování párových dat

Generování párových dat Autority, které probíhá v zóně zabezpečené v souladu se ZoEP a o jehož průběhu je vyhotovena písemná zpráva - viz kap. 5.4.1, je prováděno v kryptografickém modulu, který byl hodnocen podle FIPS 140-2 Level 3 a tedy splňuje požadavky ZoEP. Procesu generování:

- je přítomen auditor,
- nebo je z průběhu pořízen videozáznam a může být přítomen notář, který o průběhu sepíše osvědčení,

podrobnosti viz kap. 5.4.1).

Generování párových dat OCSP respondéru Autority, které probíhá v zóně zabezpečené v souladu se ZoEP, je prováděno v kryptografickém modulu, který byl hodnocen podle FIPS 140-2 Level 3.

Veškeré požadavky na proces generování těchto párových dat jsou popsány v interní bezpečnostní dokumentaci.

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

Není relevantní pro tento dokument, soukromý klíč Autority je uložen v kryptografickém modulu.

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

Veřejný klíč je Autoritě doručován jako součást žádosti o vydání certifikátu.

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

Získání veřejného klíče Autority obsaženého v jejím certifikátu je garantováno následujícími způsoby:

- obdržením na RA,
- prostřednictvím internetových informačních adres I.CA a příslušného dozorového orgánu, případně prostřednictvím věstníku příslušného dozorového orgánu,
- každý žadatel o certifikát obdrží kořenový certifikát Autority při získání svého prvotního certifikátu.

Získání veřejného klíče OCSP respondéru Autority obsaženého v jeho certifikátu je garantováno následujícími způsoby:

- obdržením na RA,

- prostřednictvím internetových informačních adres I.CA.

6.1.5 Délky párových dat

Autorita využívá asymetrický algoritmus RSA. Mohutnost klíčů (resp. parametrů daného algoritmu) Autority je 4096 bitů, mohutnost klíčů (resp. parametrů daného algoritmu) jí vydávaných certifikátů je minimálně 2048 bitů.

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

Algoritmy použité pro generování celočíselných hodnot nutných pro vytváření elektronické značky (např. testy prvočíselnosti atd.), mají parametry uvedené v platné legislativě (ZoEP), resp. v ní odkazovaných technických standardech.

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

Uvedeno v kap. 1.4.

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

6.2.1 Standardy a podmínky používání kryptografických modulů

Generování párových dat Autority a uložení odpovídajícího soukromého klíče probíhá v kryptografickém modulu, který splňuje požadavky standardu FIPS PUB 140-2 úroveň 3 a platné legislativy (ZoEP).

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 dat pro vytváření elektronických podpisů nebo dat pro vytváření elektronických značek

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

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

Kryptografický modul použitý pro správu párových dat Autority, umožňuje zálohování soukromého klíče. Klíč je zálohován s využitím nativních prostředků konkrétního kryptografického modulu v zašifrované podobě.

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

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

6.2.6 Transfer dat pro vytváření elektronických značek 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 dat pro vytváření elektronických značek v kryptografickém modulu

Soukromý klíč je uložen bezpečným způsobem v kryptografickém modulu splňujícím požadavky standardu FIPS PUB 140-2 úroveň 3 a platné legislativy (ZoEP).

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

Aktivaci soukromého klíče, vygenerovaného v kryptografickém modulu, provádějí 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 elektronickému označování vydávaných certifikátů a seznamů zneplatněných certifikátů, aktivační čipová karta se vyjme. Po aktivaci je zařízení přístupné pouze určeným odpovědným zaměstnancům I.CA.

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

Deaktivaci soukromého klíče Autority provádějí 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 dat pro vytváření elektronických podpisů nebo dat pro vytváření elektronických značek

Soukromý klíč Autority je uložen v kryptografickém modulu. Ničení tohoto klíče je realizováno prostředky kryptografického modulu. Zálohy soukromého klíče uložené v zašifrované podobě na externích médiích jsou rovněž zničeny. Ničení spočívá ve fyzické destrukci těchto nosičů. Postup ničení soukromého klíče je přesně určen a popsán v interní bezpečnostní dokumentaci.

6.2.11 Hodnocení kryptografických modulů

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

6.3 Další aspekty správy párových dat

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

Problematika uchovávání veřejného klíče Autority je řešena v souladu se ZoEP.

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

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

6.4 Aktivační data

6.4.1 Generování a instalace aktivačních dat

Aktivační data jsou vytvářena v průběhu generování párových dat Autority.

6.4.2 Ochrana aktivačních dat

Aktivační data Autority jsou chráněna způsobem popsaným v interní bezpečnostní dokumentaci.

6.4.3 Ostatní aspekty aktivačních dat

Aktivační data Autority 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 ZoEP a technickými standardy.

6.5.2 Hodnocení počítačové bezpečnosti

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

- CWA 14167-1 - Security Requirements for Trustworthy Systems Managing Certificates for Electronic Signatures - Part 1: System Security Requirements /Bezpečnostní požadavky na důvěryhodné systémy spravující certifikáty pro elektronický podpis - část 1: Požadavky na bezpečnost systémů.
- ČSN ETSI TS 101 456 - Elektronické podpisy a infrastruktury - Požadavky na postupy certifikační autority vydávající kvalifikované certifikáty.
- ČSN ETSI EN 319 411-2 Elektronické podpisy a infrastruktury (ESI) - Požadavky politiky a bezpečnosti na poskytovatele důvěryhodných služeb vydávající certifikáty - Část 2: Požadavky politiky na certifikační autority vydávající kvalifikované certifikáty.

- ČSN ETSI EN 319 411-3 Elektronické podpisy a infrastruktury (ESI) - Požadavky politiky a bezpečnosti na poskytovatele důvěryhodných služeb vydávající certifikáty - Část 3: Požadavky politiky na certifikační autority vydávající certifikáty veřejného klíče.
- ETSI TS 119 312 Electronic Signatures and Infrastructures (ESI); Cryptographic Suites.
- ČSN ISO/IEC 27000 Informační technologie - Bezpečnostní techniky - Systémy řízení bezpečnosti informací - Přehled a slovník.
- ČSN ISO/IEC 27001 Informační technologie - Bezpečnostní techniky - Systémy řízení bezpečnosti informací - Požadavky.
- ČSN ISO/IEC 27002 Informační technologie - Bezpečnostní techniky - Soubor postupů pro opatření bezpečnosti informací.
- ČSN EN ISO 19011 Směrnice pro auditování systému managementu.

6.6 Bezpečnost životního cyklu

6.6.1 Řízení vývoje systému

Při vývoji systému je postupováno v souladu s interní dokumentací.

6.6.2 Kontroly řízení bezpečnosti

Kontrola řízení bezpečnosti je prováděna pravidelnými audity (interními a externími) systému managementu bezpečnosti informací a kontrolami bezpečnostní shody (interními).

6.6.3 Řízení bezpečnosti životního cyklu

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

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

6.7 Síťová bezpečnost

Informační systém Autority je ve stavu off-line a není tedy propojen s žádnou externí síti, ve stavu on-line je pouze OCSP respondér Autority. Ten je, stejně jako zbývající síťová infrastruktura provozního pracoviště, chráněn komerčním produktem typu firewall. Detailní řešení řízení síťové bezpečnosti je popsáno v interní dokumentaci.

6.8 Časová razítka

Řešení je uvedeno v kap. 5.5.5.

7 PROFILY CERTIFIKÁTU, SEZNAMU ZNEPLATNĚNÝCH CERTIFIKÁTŮ A OCSP

7.1 Profil certifikátu

Kořenová certifikační autorita

tab. 3 - Certifikát kořenové CA

Pole	Obsah	Poznámka
Version	v3 (0x2)	
SerialNumber	jedinečné sériové číslo vydávaného 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. 6
Signature	elektronická značka vydavatele certifikátu	

Podřízená certifikační autorita

tab. 4 - Certifikát podřízené certifikační autority

Položka	Obsah položky	Poznámka
Version	v3 (0x2)	

SerialNumber	jedinečné sériové číslo vydávaného certifikátu	
SignatureAlgorithm	Sha256WithRSAEncryption	
Issuer	vydavatel certifikátu	viz tab. 3
Validity		
NotBefore	datum vydání	UTC
NotAfter	datum vydání+10 let	UTC
Subject		
commonName	jméno podřízené certifikační autority	
organizationName	První certifikační autorita, a.s.	
Country	CZ	
serialNumber	NTRCZ-26439395	
SubjectPublicKeyInfo		
Algorithm	rsaEncryption	
subjectPublicKey	veřejný klíč (minimálně 2048 bitů)	
Extensions	rozšíření certifikátu	viz tab. 7
Signature	elektronická značka vydavatele certifikátu	

OCSP respondér kořenové certifikační autority

tab. 5 - Certifikát OCSP respondéru kořenové certifikační autority

Pole	Obsah	Poznámka
Version	v3 (0x2)	
SerialNumber	jedinečné sériové číslo vydávaného certifikátu	
SignatureAlgorithm	Sha256WithRSAEncryption	
Issuer	vydavatel certifikátu	viz tab. 3
Validity		
NotBefore	datum vydání	UTC
NotAfter	datum vydání + maximálně 380 dnů	UTC
Subject		
commonName	I.CA Root CA/RSA OCSP responder	
organizationName	První certifikační autorita, a.s.	
countryName	CZ	
serialNumber	NTRCZ-26439395	
SubjectPublicKeyInfo		

algorithm	rsaEncryption	
subjectPublicKey	veřejný klíč (minimálně 2048 bitů)	
Extensions	rozšíření certifikátu	viz tab. 8
Signature	elektronická značka vydavatele certifikátu	

7.1.1 Číslo verze

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

7.1.2 Rozšiřující položky v certifikátu

Kořenová certifikační autorita

tab. 6 - Rozšíření certifikátu kořenové certifikační autority

Pole	Obsah	Poznámka
CertificatePolicies		nekritické
policyIdentifier	2.5.29.32.0 (anyPolicy)	
userNotice	Tento kvalifikovany systemovy certifikat byl vydan podle zakona 227/2000 Sb. v platnem zneni/This qualified system certificate was issued according to Act No. 227/2000 Coll.	
BasicConstraints		kritické
cA	True	
KeyUsage	keyCertSign, cRLSign	kritické
SubjectKeyIdentifier		nekritické
KeyIdentifier	hash veřejného klíče kořenové certifikační autority (tj. této certifikační autority)	

Podřízená certifikační autorita

tab. 7 - Rozšíření certifikátu podřízené certifikační autority

Položka	Obsah položky	Poznámka
CertificatePolicies		nekritické
policyIdentifier	2.5.29.32.0 (anyPolicy)	
userNotice	Tento kvalifikovany systemovy certifikat byl vydan podle zakona 227/2000 Sb. v platnem zneni/This qualified system certificate was issued according to Act No. 227/2000 Coll.	
BasicConstraints		kritické

cA	True	
pathLenConstraint	0	
KeyUsage	keyCertSign, cRLSign	kritické
SubjectKeyIdentifier		nekritické
KeyIdentifier	hash veřejného klíče této podřízené certifikační autority	
AuthorityKeyIdentifier		nekritické
KeyIdentifier	hash veřejného klíče vydavatele certifikátu (tj. kořenové certifikační autority)	
CRLDistributionPoints	http://qcrldp1.ica.cz/rca*RR*_rsa.crl* http://qcrldp2.ica.cz/rca*RR*_rsa.crl* http://qcrldp3.ica.cz/rca*RR*_rsa.crl*	nekritické
AuthorityInformationAccess		nekritické
id-ad-ocsp	http://ocsp.ica.cz/rca*RR*_rsa*	URI (http) na OCSP respondér kořenové CA
id-ad-caIssuers	http://r.ica.cz/rca*RR*_rsa.cer*	URI (http) na certifikát kořenové CA

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

Certifikát OCSP respondéru kořenové certifikační autority

tab. 8 - Rozšíření certifikátu OCSP respondéru kořenové certifikační autority

Položka	Obsah	Poznámka
CertificatePolicies		nekritické
policyIdentifier	viz kap. 1.2	
userNotice	Tento kvalifikovany systemovy certifikat byl vydan podle zakona 227/2000 Sb. v platnem zneni/This qualified system certificate was issued according to Act No. 227/2000 Coll.	
AuthorityInformationAccess		nekritické
id-ad-caIssuers	http://r.ica.cz/rca*RR*_rsa.cer*	URI (http) na certifikát kořenové CA
BasicConstraints		nekritická
cA	False	

KeyUsage	digitalSignature, nonRepudation	kritické
ExtendedKeyUsage	id-kp-OCSPSigning	kritické
id-pkix-ocsp-nocheck	NULL	nekritické
SubjectKeyIdentifier		nekritické
KeyIdentifier	hash veřejného klíče tohoto OCSP respodéru	
AuthorityKeyIdentifier		nekritické
KeyIdentifier	hash veřejného klíče vydavatele certifikátu (tj. kořenové certifikační autority)	

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

7.1.3 Objektové identifikátory (dále “OID”) algoritmů

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

7.1.4 Způsoby zápisu jmen a názvů

Uvedeno v kap. 3.1.

7.1.5 Omezení jmen a názvů

Pro jména, uváděná v položkách polí Issuer a Subject vydávaného certifikátu, není žádné omezení s výjimkou omezení vyplývajících z kap. 3.1.2.

7.1.6 OID certifikační politiky

OID tohoto dokumentu /politiky je uveden v kap. 1.2. V certifikátech certifikačních autorit je uvedeno speciální označení politiky anyPolicy, jehož OID je 2.5.29.32.0.

7.1.7 Rozšiřující položka „Policy Constrainsts“

Není relevantní pro tento dokument, není aplikováno.

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

Rozšiřující položka „Policy Qualifiers“ obsahuje informaci, že certifikát byl v souladu se ZoEP vydán jako kvalifikovaný systémový certifikát (viz userNotice v tab. 6, tab. 7, tab. 8).

7.1.9 Způsob zápisu kritické rozšiřující položky „Certificate Policies“

Viz tab. 6, tab. 7 a tab. 8. Položka není kritická.

7.2 Profil seznamu zneplatněných certifikátů

tab. 9 - Profil CRL

Položka	Obsah
Version	v2(0x1)
Signature Algorithm	Sha512WithRSAEncryption
Issuer	vydavatel CRL
thisUpdate	datum vydání
nextUpdate	datum vydání + maximálně 365 dní
revokedCertificates	seznam zneplatněných certifikátů
userCertificate	sériové číslo zneplatněného certifikátu
revocationDate	datum a čas zneplatnění certifikátu
crlEntryExtensions	rozšíření položky seznamu - viz tab. 10
crlExtensions	rozšíření CRL - viz tab. 10
SignatureAlgorithm	Sha512WithRSAEncryption
Signature	elektronická značka vydavatele CRL

7.2.1 Číslo verze

Seznamy zneplatněných certifikátů jsou vydávány dle X509 verze 2.

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

tab. 10 - Rozšíření CRL

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

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 standardem pro protokol OCSP.

8 HODNOCENÍ SHODY A JINÁ HODNOCENÍ

8.1 Periodicita hodnocení nebo okolnosti pro provedení hodnocení

Periodicita hodnocení systému řízení bezpečnosti informací a kontroly bezpečnostní shody, je dána požadavky ZoEP.

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

8.2 Identita a kvalifikace hodnotitele

Kvalifikace externího auditora je dána požadavky ZoEP, resp. jím odkazovanými technickými standardy.

8.3 Vztah hodnotitele k hodnocenému subjektu

V případě interního hodnotitele platí, že tento není ve vztahu podřízenosti vůči organizační jednotce, která zajišťuje provoz Autority.

V případě externího hodnotitele platí, že se jedná o subjekt, který není s I.CA majetkově ani organizačně svázán.

8.4 Hodnocené oblasti

V případě provádění hodnocení požadovaného ZoEP jsou hodnocené oblasti konkretizovány touto legislativou, v ostatních případech jsou hodnocené oblasti dány standardy, dle kterých je hodnocení prováděno.

8.5 Postup v případě zjištění nedostatků

Se zjištěními všech typů prováděných hodnocení je seznámen bezpečnostní manažer, který je povinen zajistit odstranění případných nedostatků. V případě zjištění nedostatků, které závažně ovlivní schopnost Autority dostát svým závazkům, resp. požadavkům vyplývajícím ze ZoEP, případně z relevantních technických standardů, přeruší Autorita vydávání certifikátů do doby, než budou nedostatky odstraněny.

8.6 Sdělování výsledků hodnocení

Sdělování výsledků hodnocení je prováděno formou danou ZoEP, případně technickými standardy, obvykle formou písemné závěrečné zprávy, která je hodnotícím subjektem předána řediteli I.CA, resp. bezpečnostnímu manažerovi společnosti.

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

9 OSTATNÍ OBCHODNÍ A PRÁVNÍ ZÁLEŽITOSTI

9.1 Poplatky

9.1.1 Poplatky za vydání nebo obnovení certifikátu

Provozovatelem všech certifikačních autorit a OCSP respondéru, jejichž certifikáty byly vydány dle této CP, je společnost První certifikační autorita, a.s. Poplatky za vydávání certifikátů kořenovou certifikační autoritou nejsou účtovány.

9.1.2 Poplatky za přístup k certifikátu na seznamu vydaných certifikátů

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

9.1.3 Poplatky za informace o statutu certifikátu nebo o zneplatnění certifikátu

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

9.1.4 Poplatky za další služby

Provozovatelem všech certifikačních autorit i OCSP respondéru, jejichž certifikáty byly vydány dle této CP, je společnost První certifikační autorita, a.s. Poplatky za další služby nejsou účtovány.

9.1.5 Jiná ustanovení týkající se poplatků (vč. refundací)

Žádná jiná ustanovení týkající se poplatků nejsou.

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 provoz v souladu s požadavky uvedenými v ZoEP a s ohledem na riziko vzniku odpovědnosti za škodu.

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

9.2.3 Pojištění nebo krytí zárukou pro koncové uživatele

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 označeny jako veřejné a nejsou zveřejňovány způsobem uvedeným v kap. 2.2, zejména:

- veškeré soukromé klíče, sloužící v procesu poskytování certifikačních služeb,
- ostatní kryptograficky podstatné informace, týkající se 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 pracovník, který přijde do styku s citlivými a důvěrnými informacemi, je nesmí bez souhlasu ředitele I.CA poskytnout třetí straně.

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

9.4 Ochrana osobních údajů

9.4.1 Politika ochrany osobních údajů

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

9.4.2 Osobní údaje

Osobními informacemi jsou veškeré osobní údaje klientů, uživatelů či pracovníků podléhající ochraně ve smyslu příslušných zákonných norem.

9.4.3 Údaje, které nejsou považovány za citlivé

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

9.4.4 Odpovědnost za ochranu osobních údajů

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

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

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

9.4.6 Poskytnutí citlivých informací pro soudní či správní účely

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

9.4.7 Jiné okolnosti zpřístupňování osobních údajů

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

9.5 Práva duševního vlastnictví

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

9.6 Zastupování a záruky

9.6.1 Zastupování a záruky CA

I.CA zaručuje, že:

- použije soukromé klíče příslušné certifikátům Autority pouze k elektronickému označování vydávaných certifikátů a seznamů zneplatněných certifikátů,
- certifikáty vydávané Autoritou splňují náležitosti požadované ZoEP,
- zneplatní certifikáty vydané Autoritou, pokud byla žádost o ukončení jejich platnosti podána způsobem definovaným v této CP.

9.6.2 Zastupování a záruky RA

Není relevantní pro tento dokument, viz bod 1.3.2

9.6.3 Zastupování a záruky držitele certifikátu, podepisující nebo označující osoby

Držitel certifikátu nebo podepisující osoba postupují v souladu s ZoEP a relevantními technickými standardy a ručí za správnost jimi uváděných informací v celém životním cyklu využívání poskytované certifikační služby.

9.6.4 Zastupování a záruky spoléhajících se stran

Spoléhající se strany postupují v souladu s ZoEP a relevantními technickými standardy.

9.6.5 Zastupování a záruky ostatních zúčastněných subjektů

Služba není poskytována.

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 certifikační politikou, dle které byl certifikát vydán.

9.9 Odpovědnost za škodu, náhrada škody

Není relevantní pro tento dokument, je řešeno v politikách autorit vydávajících certifikáty koncovým klientům.

9.10 Doba platnosti, ukončení platnosti

9.10.1 Doba platnosti

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

9.10.2 Ukončení platnosti

Jedinou osobou, která je oprávněna schvalovat ukončení platnosti této CP, a to v případě jejího nahrazení novou verzí, nebo ukončení poskytování služeb Autority, 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

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

9.12 Změny

9.12.1 Postup při změnách

Postup je realizován řízeným procesem popsaným v interním dokumentu.

9.12.2 Postup při oznamování změn

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

9.12.3 Okolnosti, při kterých musí být změněn OID

V případě jakékoliv změny v této CP je změněn i její OID (viz kap. 1.2).

9.13 Řešení sporů

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

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 požadavky ZoEP a s relevantními technickými standardy.

9.16 Další ustanovení

9.16.1 Rámcová dohoda

Není relevantní pro tento dokument.

9.16.2 Postoupení práv

V případě ukončení činnosti kvalifikovaného poskytovatele certifikačních služeb postupuje společnost První certifikační autorita, a.s., v souladu se ZoEP.

9.16.3 Oddělitelnost ustanovení

Není relevantní pro tento dokument.

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 vyplývající 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 18.05.2015.