První certifikační autorita, a.s.

Certifikační politika

vydávání certifikátů pro systém TSA (algoritmus RSA)

Verze 1.1

OBSAH

tab. 1 - Vývoj dokumentu

Verze	Datum vydání	Schválil	Poznámka
1.0	15.07.2015	Ředitel společnosti První certifikační autorita, a.s.	První vydání.
1.1	02.11.2015	Ředitel společnosti První certifikační autorita, a.s.	Úprava profilu certifikátu.

1 ÚVOD

Tento dokument byl vypracován na základě požadavků platných standardů vztahujících se k problematice poskytování certifikačních služeb. Kořenová kvalifikovaná certifikační autorita (algoritmus RSA) společnosti První certifikační autorita, a.s., dále též I.CA, vydala v hierarchické dvoustupňové struktuře certifikačních autorit, v souladu s požadavky technických standardů a platné legislativy kvalifikovaný systémový certifikát (dále též certifikát) s algoritmem RSA pro vydávající kvalifikovanou certifikační autoritu provozovanou I.CA. Tato kvalifikovaná certifikační autorita vydává mj. certifikáty pro jednotlivé servery vydávající kvalifikovaná časová razítka tvořící systém TSA, provozovaný I.CA. Vydávání těchto certifikátů se řídí touto certifikační politikou.

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

1.1 Přehled

Dokument **Certifikační politika vydávání certifikátů pro systém TSA (algoritmus RSA)**, dále též CP, vypracovaný společností První certifikační autorita, a. s., se zabývá skutečnostmi, vztahujícími se k procesům životního cyklu vydávaných certifikátů dodržuje strukturu, jejíž předlohou je osnova platného standardu RFC 3647, s přihlédnutím k platným standardům Evropské unie a k právu České republiky 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 mohou uvedeny v odpovídající certifikační prováděcí směrnici (dále CPS).

1.2 Název a jednoznačné určení dokumentu

Název tohoto dokumentu:	Certifikační politika vydávání certifikátů pro systém TSA (algoritmus RSA)
OID politiky:	1.3.6.1.4.1.23624.10.1.32.1.1

1.3 Participující subjekty

1.3.1 Certifikační autority (dále „CA")

Kvalifikovaná certifikační autorita, provozovaná společností První certifikační autorita, a.s., vydávající kvalifikované certifikáty koncovým uživatelům.

1.3.2 Registrační autority (dále „RA")

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

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

Certifikáty, vydávané dle této CP, jsou určeny pro servery vydávající kvalifikovaná časová razítka systému TSA, provozovaného I.CA.

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

1.3.4 Spoléhající se strany

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

1.3.5 Jiné participující subjekty

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

1.4 Použití certifikátu

1.4.1 Přípustné použití certifikátu

Certifikáty vydávané podle této CP smějí být používány výhradně v procesu ověřování elektronické značky kvalifikovaných časových razítek, vydávaných I.CA.

1.4.2 Omezení použití certifikátu

Certifikáty vydávané 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

1.6.1 Použité pojmy a zkratky

tab. 2 - Pojmy a zkratky

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

elektronický podpis	údaje v elektronické podobě, které jsou připojené k datové zprávě nebo jsou s ní logicky spojené a které slouží jako metoda k jednoznačnému ověření identity podepsané osoby ve vztahu k datové zprávě
EN	European Standard, typ ETSI standardu
ETSI	the European Telecommunications Standards Institute, evropský standardizační institut v oblasti informačních a komunikačních technologií
FIPS	Federal Information Processing Standard, označení standardů v oblasti informačních technologií pro nevojenské státní organizace ve Spojených státech
hash	transformace, která jako vstup přijímá řetězec znaků o libovolné délce a výsledkem je řetězec znaků s pevnou délkou
IEC	International Electrotechnical Commission, světová organizace publikující standardy pro elektrotechniku, elektroniku, sdělovací techniku a příbuzné obory
ISO	International Organization for Standardization, mezinárodní organizace sdružující národní standardizační organizace, označení standardů
ITU	International Telecommunication Union
ITU-T	Telecommunication Standardization Sector of ITU
kořenová CA	CA, vydávající certifikáty vydávajícím CA
kvalifikovaný systémový certifikát	certifikát, splňující požadavky zákona č. 227/2000 Sb., o elektronickém podpisu a o změně některých dalších zákonů (zákon o elektronickém podpisu), ve znění pozdějších předpisů
OCSP	Online Certificate Status Protocol, protokol pro zjišťování stavu certifikátu veřejného klíče
OCSP respondér	server poskytují protokolem OCSP údaje o stavu certifikátu veřejného klíče
označující osoba	fyzická osoba, právnická osoba nebo organizační složka státu, která drží prostředek pro vytváření elektronických značek a označuje datovou zprávu elektronickou značkou
párová data	jedinečná data pro vytváření elektronického podpisu /elektronické značky spolu s odpovídajícími daty pro ověřování elektronického podpisu /elektronické značky
PKCS	Public Key Cryptography Standards, označení skupiny standardů pro kryptografii s veřejným klíčem
PUB	Publication, označení standardu FIPS
RA	registrační autorita
RFC	Request for Comments, označení řady standardů a dalších dokumentů popisujících internetové protokoly, systémy apod.

RSA	šifra s veřejným klíčem pro podepisování a šifrování (iniciály původních autorů Rivest, Shamir a Adleman)
SHA	typ hashovací funkce
smluvní partner	poskytovatel vybraných certifikačních služeb, který zajišťuje na základě písemné smlouvy pro I.CA certifikační služby nebo jejich části - nejčastěji se jedná o smluvní RA
soukromý klíč	jedinečná data pro vytváření elektronického podpisu /elektronické značky
spoléhající se strana	subjekt, spoléhající se při své činnosti na certifikát vydaný CA
TS	Technical Specification, typ ETSI standardu
TSA	Time Stamping Authority, autorita časových razítek, obsahující více serverů, vydávajících časová razítka, kdy každý z nich disponuje jedinečným soukromým klíčem a odpovídajícím certifikátem
TSS	Time Stamp Service, služba časových razítek
TSU	Time Stamp Unit, server vydávající časová razítka
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
X.501, X.509, X.520	standard popsaný 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
ZoEP	zákon č. 227/2000 Sb., o elektronickém podpisu a o změně některých dalších zákonů (zákon o elektronickém podpisu), 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

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.
- ITU-T - X.501 Information technology – Open Systems Interconnection – The Directory: Models.
- ITU-T - X.509 Information technology – Open Systems Interconnection – The Directory: Public-key and attribute certificate frameworks.

- ITU-T - X.520 Information technology – Open Systems Interconnection – The Directory: Selected attribute types.
- RSA Laboratories - PKCS#10: Certification Request Syntax Standard.
- RFC 2560 X.509 Internet Public Key Infrastructure Online Certificate Status Protocol - OCSP.
- RFC 3647 Internet X.509 Public Key Infrastructure Certificate Policy and Certification Practices Framework.
- RFC 5019 The Lightweight Online Certificate Status Protocol (OCSP) Profile for High-Volume Environments.
- RFC 5280 Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile.

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.

Elektronická adresa, která slouží pro kontakt veřejnosti s I.CA, je info@ica.cz.

Na výše uvedené internetové adrese lze získat informace o:

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

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

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

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

2.3 Periodicita zveřejňování informací

I.CA zveřejňuje informace s následující periodicitou:

- certifikační politika - po schválení a vydání nové verze,
- certifikační prováděcí směrnice - neprodleně (je-li určena ke zveřejnění),
- seznam vydaných certifikátů – aktualizace při každém vydání nového certifikátu,
- seznam zneplatněných certifikátů (CRL) - viz kap. 4.9.7,
- zneplatnění certifikátu CA vydávající certifikáty koncovým uživatelů, s uvedením důvodu zneplatnění – bezodkladně,
- ostatní veřejné informace – není předem určeno, obecně však platí, že tyto informace musí reflektovat aktuální stav poskytovaných certifikačních služeb.

2.4 Řízení přístupu k jednotlivým typům úložišť

Veškeré veřejné informace (viz kap. 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

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. Význam a obsah údajů, obsažených v certifikátech pro servery vydávajících kvalifikovaná časová razítka systému TSA, 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 certifikát pro TSU systému TSA se do vydávaných certifikátů přenášejí ve tvaru, ve kterém jsou uvedeny v předkládaných dokladech.

3.1.5 Jedinečnost jmen

Jména, uváděná v položce Subject, musí být jedinečná. Společnost První certifikační autorita, a.s., zaručuje jedinečnost této položky v certifikátech.

3.1.6 Obchodní značky

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

3.2 Počáteční ověření identity

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

Vlastnictví soukromého klíče odpovídajícího veřejnému klíči v žádosti o certifikát se prokazuje předložením žádosti ve formátu PKCS#10. Ta je zmíněným soukromým klíčem elektronicky podepsána a žadatel o certifikát tak prokazuje, že v době tvorby elektronického podpisu soukromý klíč vlastnil.

3.2.2 Ověřování identity právnické osoby nebo organizační složky státu

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

3.2.3 Ověřování identity fyzické osoby

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

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

Není relevantní pro tento dokument, služba výměny párových dat po zneplatnění certifikátu není podporována. Je nutné vydat nový certifikát s novým veřejným klíčem. Platí stejné požadavky, jako v případě počátečního ověření identity.

3.4 Identifikace a autentizace při zpracování požadavků na zneplatnění certifikátu

Oprávněnou osobou žádat o zneplatnění certifikátu pro TSU systému TSA je ředitel I.CA. Pro identifikaci a autentizaci platí požadavky kap. 3.2.2 a 3.2.3.

4 POŽADAVKY NA ŽIVOTNÍ CYKLUS CERTIFIKÁTU

4.1 Žádost o vydání certifikátu

4.1.1 Subjekty oprávněné podat žádost o vydání certifikátu

Žádost o vydání certifikátu pro TSU systému TSA je oprávněn podat ředitel I.CA.

4.1.2 Registrační proces a odpovědnosti poskytovatele a žadatele

Písemná žádost o vydání certifikátu pro TSU systému TSA je předkládána vedení společnosti První certifikační autorita, a.s., prostřednictvím ředitele a musí obsahovat název a OID této certifikační politiky (viz kapitola 1.2). Žádost musí být ředitelem I.CA podepsána.

4.1.2.1 Odpovědnost žadatele

Žadatel je povinen zejména:

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

4.1.2.2 Odpovědnost poskytovatele

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

4.2 Zpracování žádosti o certifikát

4.2.1 Identifikace a autentizace

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

4.2.2 Přijetí nebo zamítnutí žádosti o certifikát

Na základě písemné žádosti (viz kap. 4.1.2) rozhodne vedení společnosti První certifikační autorita, a.s., o vydání certifikátu pro TSU systému TSA, 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:

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

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

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

Ředitel I.CA je osobně přítomen vydání certifikátu.

4.4 Převzetí vydaného certifikátu

4.4.1 Úkony spojené s převzetím certifikátu

Ředitel I.CA, resp. jím pověřený 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.

4.4.3 Oznámení o vydání certifikátu jiným subjektům

Platí ustanovení kap. 4.4.2.

4.5 Použití párových dat a certifikátu

Platnost certifikátu systému TSA vydaného dle této CP je uvedena v tomto certifikátu. Platnost párových dat (veřejný a soukromý klíč) pro tvorbu elektronické značky/podpisu, resp. ověřování elektronické značky/podpisu časových razítek, je omezena platností tohoto certifikátu (obvykle na dobu šesti let).

V prvním roce po vygenerování párových dat a vydání certifikátu veřejného klíče je klíč soukromý používán pro tvorbu elektronické značky/podpisu časového razítka. Před koncem tohoto období jsou vygenerována nová párová data a vydán certifikát příslušného veřejného klíče. K tvorbě elektronické značky/podpisu časových razítek je dále využíván nejnovější soukromý klíč. Veřejné klíče, staré i nejnovější, jsou využívány k ověřování elektronických značek/podpisů vytvořených odpovídajícím soukromým klíčem.

V případě nestandardních situací (např. dojde-li k takovému vývoji kryptoanalytických metod, které by mohly ohrozit bezpečnost procesu tvorby elektronických podpisů/značek a je nutná změna kryptografických algoritmů, délky klíčů atd.) je generování nových párových dat a vydání příslušného certifikátu provedeno neprodleně.

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 je zejména:

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

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

Spoléhající se strany jsou zejména povinny ověřit certifikát TSU systému TSA a celou certifikační cestu podle platných standardů.

4.6 Obnovení certifikátu

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

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

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

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

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

Zneplatnění certifikátu konkrétního TSU systému TSA znamená, že do doby vydání certifikátu nového je činnost tohoto TSU pozastavena.

Službu pozastavení platnosti certifikátu I.CA neposkytuje.

4.9.1 Podmínky pro zneplatnění certifikátu

Certifikát může být zneplatněn na základě následujících okolností:

- existuje důvodné podezření, že došlo ke kompromitaci, soukromého klíče, odpovídajícího veřejnému klíči tohoto certifikátu,
- žádost ředitele I.CA,
- technický obsah nebo formát certifikátu představují neakceptovatelné riziko (např. daný kryptografický /podepisovací algoritmus nebo délka klíče),
- 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 TSU systému TSA musí být vydán neprodleně po zneplatnění tohoto certifikátu.

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

Není relevantní pro tento dokument, je popsáno v politice vydávání kvalifikovaných časových razítek.

4.9.7 Periodicita vydávání seznamu zneplatněných certifikátů

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

4.9.8 Maximální zpoždění při vydávání seznamu zneplatněných certifikátů

Seznam zneplatněných certifikátů je zveřejňován neprodleně po jeho vydání.

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

Skutečnost, zda kvalifikovaná certifikační autorita, která certifikát pro TSU systému TSA vydala, poskytuje službu OCSP ověřování stavu certifikátu, je uvedena v CPS kvalifikované certifikační autority.

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.

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 jsou poskytovány formou zveřejňování informací, seznamy zneplatněných certifikátů jsou poskytovány jak formou zveřejňování informací, tak uvedením distribučních míst CRL ve vydaných certifikátech TSU systému TSA.

Skutečnost, zda kvalifikovaná certifikační autorita, která certifikáty pro systém TSA vydává, službu OCSP poskytuje, je uvedena v CPS této kvalifikované certifikační autority. OCSP odpovědi OCSP respondéru CA vydávající certifikáty pro TSU systému TSA potom poskytují informaci o stavu takového certifikátu vydaného touto CA.

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). Pokud je poskytována služba OCSP garantuje I.CA její dostupnost.

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, 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

Viz kap. 4.12.

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

Viz kap. 4.12.

5 MANAGEMENT, PROVOZNÍ A FYZICKÁ BEZPEČNOST

Management bezpečnosti je zaměřen především na:

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

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

5.1 Fyzická bezpečnost

5.1.1 Umístění a konstrukce

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

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

5.1.2 Fyzický přístup

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

5.1.3 Elektřina a klimatizace

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

5.1.4 Vlivy vody

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

5.1.5 Protipožární opatření a ochrana

V objektech provozních pracovišť je instalována elektronická požární signalizace (EPS). Vstupní dveře vyhrazených prostor, ve kterých jsou umístěna zařízení, určená k výkonu hlavních certifikačních služeb, jsou opatřeny protipožární vložkou. V samotných prostorách se nachází hasicí přístroj.

5.1.6 Ukládání médií

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

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

5.1.7 Nakládání s odpady

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

5.1.8 Zálohy mimo budovu

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

5.2 Procesní bezpečnost

5.2.1 Důvěryhodné role

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

5.2.2 Počet osob požadovaných na zajištění jednotlivých činností

V rámci certifikační autority vydávající certifikáty pro TSU systému TSA jsou definovány činnosti, které musí být vykonány za účasti více než jediné osoby. Jedná se zejména o:

- generování klíčového páru certifikační autority a TSU systému TSA,
- zálohování /obnovu soukromého klíče certifikační autority a TSU systému TSA,
- aktivace soukromého klíče certifikační 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 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 technickými standardy, mj. o životním cyklu certifikátů TSU systému TSA a jim odpovídajících certifikátů CA.

Speciálním případem zaznamenávání událostí je událost generování párových dat CA vydávající certifikáty TSU systému TSA, přičemž minimálně platí, že:

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

Všechny auditní záznamy jsou v nutné míře pořizovány, uchovávány a zpracovávány se zachováním prokazatelnosti původu, integrity, dostupnosti, důvěrnosti a časové autentičnosti.

Auditní systém je navržen a provozován způsobem, který zaručuje udržování auditních dat, rezervování dostatečného prostoru pro auditní data, automatické nepřepisování auditního souboru, prezentaci auditních záznamů pro uživatele vhodným způsobem a omezení přístupu k auditnímu souboru pouze pro definované uživatele.

5.4.2 Periodicita zpracování záznamů

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

5.4.3 Doba uchování auditních záznamů

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

5.4.4 Ochrana auditních záznamů

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

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

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

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

5.4.5 Postupy pro zálohování auditních záznamů

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

5.4.6 Systém shromažďování auditních záznamů (interní nebo externí)

Systém shromažďování auditních záznamů je z pohledu informačních systémů CA vydávající certifikáty pro systém TSA interní.

5.4.7 Postup při oznamování události subjektu, který ji způsobil

Subjekt není o zapsání události do auditního záznamu informován.

5.4.8 Hodnocení zranitelnosti

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

5.5 Uchovávání informací a dokumentace

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

5.5.1 Typy informací a dokumentace, které se uchovávají

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

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

5.5.2 Doba uchování uchovávaných informací a dokumentace

Informace, vztahující se k certifikátům CA vydávajících certifikáty TSU systému TSA, 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. Totéž platí pro certifikáty TSU systému TSA.

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 certifikační autority vydávající certifikáty pro TSU systému TSA postupuje tato certifikační autorita tak, že:

- ukončí jeho používání,
- okamžitě a trvale zneplatní příslušný certifikát a zničí jemu odpovídající soukromý klíč,
- zneplatní všechny platné certifikáty, které byly výše uvedeným klíčem elektronicky označeny,
- bezodkladně o této skutečnosti, včetně důvodu, informuje na své internetové informační adrese (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 vydávající certifikační autority platí následující pravidla:

- ukončení činnosti autority musí být písemně oznámeno všem držitelům platných certifikátů, subjektům, které mají uzavřenou smlouvu přímo se vztahující k poskytování certifikačních služeb, případně dozorovému orgánu,
- 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 uzavřenými smlouvami, případně s příslušnými legislativními normami.

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.

V případě ukončení činnosti konkrétního pracoviště RA je tato skutečnost oznámena na internetové adrese http://www.ica.cz.

6 TECHNICKÁ BEZPEČNOST

6.1 Generování a instalace párových dat

6.1.1 Generování párových dat

Generování párových dat CA vydávající certifikáty pro TSU systému TSA, které probíhá v zabezpečené oblasti viz kap. 5.1.1, 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 TSU systému TSA rovněž probíhá v zabezpečené oblasti a je prováděno v kryptografickém modulu, který byl hodnocen podle FIPS PUB 140-2 Level 3 a který je součástí tohoto TSU.

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 TSU systému TSA je generován a uložen v kryptografickém modulu, který je součástí TSU systému TSA a je pod výhradní kontrolou I.CA.

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

Veřejný klíč, odpovídající soukromému klíči konkrétního TSU systému TSA, je vydávající certifikační autoritě doručen v žádosti o vydání tohoto certifikátu.

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

Získání veřejného klíče CA vydávající certifikát pro TSU systému TSA obsaženého v jejím certifikátu je garantováno následujícími způsoby:

- obdržením na RA,
- prostřednictvím internetových informačních adres I.CA,
- prostřednictvím příslušného dozorového orgánu, resp. prostřednictvím věstníku příslušného dozorového orgánu.

Získání veřejného klíče TSU systému TSA obsaženého v certifikátu tohoto TSU je garantováno stejnými, výše uvedenými, způsoby.

Certifikát veřejného klíče TSU systému TSA je taktéž obsažen ve vydaném časovém razítku.

6.1.5 Délky párových dat

Hierarchická struktura certifikačních autorit využívá asymetrický algoritmus RSA. Mohutnost klíče (resp. parametrů daného algoritmu) kořenové certifikační autority je 4096 bitů,

mohutnost klíčů (resp. parametrů daného algoritmu) v jí vydávaných certifikátech je minimálně 2048 bitů. Mohutnost klíčů v certifikátech TSU systému TSA je minimálně 2048 bitů.

6.1.6 Generování parametrů dat pro ověřování elektronických podpisů nebo dat pro ověřování 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 a uložení odpovídajícího soukromého klíče probíhá v kryptografickém modulu, který splňuje požadavky standardu FIPS PUB 140-2 Level 3.

6.2.2 Sdílení tajemství

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

Není relevantní pro párová data TSU systému TSA.

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

Kryptografické moduly použité pro správu párových dat umožňují zálohování soukromého klíče. Záloha databáze kryptografického modulu vydávající certifikační autority je prováděna s využitím jeho nativních prostředků v zašifrované podobě. S využitím nativních prostředků kryptografického modulu a v zašifrované podobě je rovněž zálohován soukromý klíč TSU systému TSA.

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 vydávající certifikační autority 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.

Vkládání soukromého klíče do kryptografického modulu TSU systému TSA v případě, že se jedná o jeho obnovení ze šifrované zálohy, provádí vedoucí provozního pracoviště.

6.2.7 Uložení dat pro vytváření elektronických značek v kryptografickém modulu

Soukromé klíče jsou uloženy bezpečným způsobem v kryptografických modulech splňujících požadavky standardu FIPS PUB 140-2 Level 3.

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

Aktivaci soukromého klíče TSU systému TSA vygenerovaného v kryptografickém modulu provádí vedoucí provozního pracoviště vložením příslušného certifikátu.

Aktivaci soukromého klíče CA 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 činnosti, aktivační čipová karta se vyjme.

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

Deaktivace původního soukromého klíče TSU systému TSA je prováděna vložením nového certifikátu.

Deaktivaci soukromého klíče CA 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 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 dokumentaci.

6.2.11 Hodnocení kryptografických modulů

Kryptografické moduly byly certifikovány na shodu s požadavky standardu FIPS PUB 140-2 Level 3.

6.3 Další aspekty správy párových dat

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

Veřejné klíče CA a TSU systému TSA jsou uchovávány po celou dobu existence I.CA.

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

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.

6.4.2 Ochrana aktivačních dat

Aktivační data jsou chráněna způsobem popsaným 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 generování párových dat a vydávání certifikátu TSU systému TSA používají dvoufaktorovou autentizaci.

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 102 042 Electronic Signatures and Infrastructures (ESI); Policy requirements for certification authorities issuing public key certificates.
- ETSI TS 119 312 Electronic Signatures and Infrastructures (ESI); Cryptographic Suites.
- ČSN ISO/IEC 27000 Informační technologie - Bezpečnostní techniky - Systémy řízení bezpečnosti informací - Přehled a slovník.
- ČSN ISO/IEC 27001 Informační technologie - Bezpečnostní techniky - Systémy řízení bezpečnosti informací - Požadavky.
- ČSN ISO/IEC 27002 Informační technologie - Bezpečnostní techniky - Soubor postupů pro opatření bezpečnosti informací.
- 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 je vytvářeno procesním přístupem typu „Plánování-Zavedení-Kontrola-Využití“ (Plan-Do-Check-Act, PDCA), který se skládá z navazujících procesů:

- vybudování - definování bezpečnostní politiky, plánů, cílů, procesů a postupů s ohledem na řízení rizik a bezpečnost informací tak, aby byly v souladu s celkovou bezpečnostní politikou,

- implementace a provoz - bezpečnostní politiky, plánů, cílů, procesů a postupů,
- monitorování a přehodnocování - posouzení procesu s ohledem na bezpečnostní politiku a předání poznatků vedení společnosti k posouzení,
- využití - na základě rozhodnutí vedení organizace provedení nápravných opatření.

6.7 Síťová bezpečnost

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

6.8 Časová razítka

Řešení je uvedeno v kap. 5.5.5.

7 PROFILY CERTIFIKÁTU, SEZNAMU ZNEPLATNĚNÝCH CERTIFIKÁTŮ A OCSP

7.1 Profil certifikátu

Vydávající certifikační autorita

tab. 3 - Certifikát vydávající certifikační autority

Položka	Obsah položky	Poznámka
Version	v3 (0x2)	
SerialNumber	jedinečné sériové číslo vydávaného certifikátu	
SignatureAlgorithm	Sha256WithRSAEncryption	
Issuer	vydavatel certifikátu	
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+10 let	UTC
Subject		
commonName	I.CA Qualified CA/RSA MM/RRRR*	
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. 5
Signature	elektronická značka/podpis vydavatele certifikátu	

* měsíc a rok vydání certifikátu

TSU systému TSA

tab. 4 - Certifikát TSU systému TSA

Položka	Obsah položky	Poznámka
Version	v3 (0x2)	
SerialNumber	jedinečné sériové číslo vydávaného certifikátu	
SignatureAlgorithm	Sha256WithRSAEncryption	
Issuer	vydavatel certifikátu	viz pole Subject v tab. 3
Validity		
NotBefore	počátek platnosti certifikátu	UTC
NotAfter	konec platnosti certifikátu	UTC
Subject		
commonName	I.CA Time Stamping Authority TSS/TSU X MM/RRRR*	
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. 5
Signature	elektronická značka vydavatele certifikátu	

* X – číslo TSU, MM/RRRR – měsíc a rok vydání certifikátu, mezi X a MM/RRRR je jedna mezera

7.1.1 Číslo verze

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

7.1.2 Rozšiřující položky v certifikátu

Vydávající certifikační autorita

tab. 5 - Rozšíření certifikátu vydávající certifikační autority

Položka	Obsah položky	Poznámka
CertificatePolicies		nekritická
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		kritická
cA	True	
pathLenConstraint	0	
KeyUsage	keyCertSign, cRLSign	kritická
SubjectKeyIdentifier		nekritická
KeyIdentifier	hash veřejného klíče této vydávající certifikační autority	
AuthorityKeyIdentifier		nekritická
KeyIdentifier	hash veřejného klíče vydavatele certifikátu (tj. kořenové certifikační autority)	
CRLDistributionPoints	http://qcrldp1.ica.cz/rcaRR_rsa.crl* http://qcrldp2.ica.cz/rcaRR_rsa.crl* http://qcrldp3.ica.cz/rcaRR_rsa.crl*	nekritická
AuthorityInformationAccess		nekritická
id-ad-ocsp	http://ocsp.ica.cz/rcaRR_rsa*	URI (http) na OCSP respondér kořenové CA
id-ad-caIssuers	http://r.ica.cz/rcaRR_rsa.cer*	URI (http) na certifikát kořenové CA

* RR - poslední dvě číslice roku vydání certifikátu kořenové CA

Certifikát TSU systému TSA

tab. 6 - Rozšíření certifikátu TSU systému TSA

Položka	Obsah	Poznámka
CertificatePolicies		nekritická
.PolicyInformation(1)		
policyIdentifier	viz kap. 1.2	
[1.1]policyQualifiers .PolicyQualifierInfo(1) userNotice	Tento kvalifikovany systemovy certifikat byl vydan podle zakona 227/2000 Sb. v platnem zneni/This qualified system certificate was issued according to Act No. 227/2000 Coll.	
.PolicyInformation(2)		

policyIdentifier	1.3.158.36061701.0.0.0.1.2.2	
CRLDistributionPoints	http://qcrldp1.ica.cz/qcaRR_rsa.crl* http://qcrldp2.ica.cz/qcaRR_rsa.crl* http://qcrldp3.ica.cz/qcaRR_rsa.crl*	nekritická
AuthorityInformationAccess		nekritická
id-ad-caIssuers	http://q.ica.cz/qcaRR_rsa.p7c	URI (http) p7c souboru, který obsahuje certifikáty vydavatele certifikátu TSU
BasicConstraints		nekritická
cA	False	
KeyUsage	digitalSignature, nonRepudiation	kritická
ExtendedKeyUsage	id-kp-timeStamping	kritická
SubjectKeyIdentifier		nekritická
KeyIdentifier	hash veřejného klíče v tomto certifikátu	
AuthorityKeyIdentifier		nekritická
KeyIdentifier	hash veřejného klíče vydavatele certifikátu	

* RR - poslední dvě číslice roku vydání certifikátu CA vydávající certifikáty TSU systému TSA

I.CA si vyhrazuje právo doplnit další položky, vyžadované aktualizacemi standardů ETSI.

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

V souladu s požadavkem RFC 5280 se obsah pole Issuer ve vydaném certifikátu TSU systému TSA shoduje s polem Subject v certifikátu CA vydávající tento certifikát. Dále 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 Constrainsts“

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. 7 - Profil CRL

Položka	Obsah
Version	v2(0x1)
Signature Algorithm	Sha256WithRSAEncryption
Issuer	označení vydavatele CRL
thisUpdate	datum a čas vydání CRL (UTC)
nextUpdate	datum a předpokládaný čas vydání následujícího CRL (UTC)
revokedCertificates	seznam zneplatněných certifikátů
userCertificate	sériové číslo zneplatněného certifikátu
revocationDate	datum a čas zneplatnění certifikátu
crlEntryExtensions	rozšíření položky seznamu - viz tab. 8
crlExtensions	rozšíření CRL - viz tab. 8
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. 8 - Rozšíření CRL

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

7.3 Profil OCSP

7.3.1 Číslo verze

Bude-li využíván protokol OCSP, pak v žádosti a odpovědi na stav certifikátu s využitím protokolu OCSP bude uvedena verze 1.

7.3.2 Rozšiřující položky OCSP

Bude-li využíván protokol OCSP, pak konkrétní rozšiřující položky uváděné v žádosti a odpovědi na stav certifikátu s využitím protokolu OCSP budou v souladu se standardy RFC 2560 a RFC 5019. Certifikát OCSP respondéru bude obsahovat rozšíření typu id-pkix-ocsp-nocheck, jak je definováno v RFC 2560.

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 a standardy ETSI.

8.2 Identita a kvalifikace hodnotitele

Kvalifikace externího auditora provádějícího hodnocení podle ZoEP, je dána tímto zákonem, resp. jím odkazovanými technickými standardy.

Orgán provádějící audit podle standardů ETSI 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

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

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 I.CA, který je povinen zajistit odstranění případných nedostatků. Pokud by byly zjištěny nedostatky, které by zásadním způsobem znemožňovaly poskytovat konkrétní certifikační službu, přeruší I.CA tuto službu, 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.

9 OSTATNÍ OBCHODNÍ A PRÁVNÍ ZÁLEŽITOSTI

9.1 Poplatky

9.1.1 Poplatky za vydání nebo obnovení certifikátu

Provozovatelem systému TSA je společnost První certifikační autorita, a.s., poplatky za vydávání certifikátů pro TSU systému TSA nejsou účtovány. Služba obnovení certifikátu TSU systému TSA není poskytována.

9.1.2 Poplatky za přístup k certifikátu na seznamu vydaných certifikátů

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

9.1.3 Poplatky za informace o statutu certifikátu nebo o zneplatnění certifikátu

Přístup elektronickou cestou k informacím o zneplatněných certifikátech (CRL), případně o stavech certifikátů (OCSP), pokud je tato služba poskytována, I.CA nezpoplatňuje.

9.1.4 Poplatky za další služby

Není relevantní pro tento dokument.

9.1.5 Jiná ustanovení týkající se poplatků (vč. refundací)

Není relevantní pro tento dokument.

9.2 Finanční odpovědnost

9.2.1 Krytí pojištěním

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

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

9.2.2 Další aktiva a záruky

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

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

9.2.3 Pojištění nebo krytí zárukou pro koncové uživatele

Není relevantní pro tento dokument, služba není poskytována.

9.3 Citlivost obchodních informací

9.3.1 Výčet citlivých informací

Citlivými a důvěrnými informacemi I.CA jsou veškeré informace, které nejsou označeny jako veřejné a 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,
- 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 nespadají do působnosti ZOOÚ.

9.4.4 Odpovědnost za ochranu osobních údajů

Za ochranu osobních údajů je odpovědný ředitel I.CA.

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

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

9.4.6 Poskytnutí citlivých informací pro soudní či správní účely

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

9.4.7 Jiné okolnosti zpřístupňování osobních údajů

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

9.5 Práva duševního vlastnictví

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

9.6 Zastupování a záruky

9.6.1 Zastupování a záruky CA

I.CA zaručuje, že:

- použije soukromé klíče příslušné certifikátům certifikačních autorit pouze k elektronickému označování vydávaných certifikátů a seznamů zneplatněných certifikátů,
- použije soukromé klíče příslušné certifikátům pro TSU systému TSA pouze k elektronickému označování vydávaných časových razítek,
- zneplatní certifikáty TSU systému TSA, pokud byla žádost o jejich zneplatnění podána způsobem definovaným v této CP.

9.6.2 Zastupování a záruky RA

RA:

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

9.6.3 Zastupování a záruky držitele certifikátu, podepisující nebo označující osoby

Není relevantní pro tento dokument.

9.6.4 Zastupování a záruky spoléhajících se stran

Záruky spoléhajících se stran jsou popsány v politice vydávání kvalifikovaných časových razítek.

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 CP, nebo politikou vydávání kvalifikovaných časových razítek.

9.9 Odpovědnost za škodu, náhrada škody

Není relevantní pro tento dokument, je uvedeno v politice vydávání kvalifikovaných časových razítek.

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 systému TSA, 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

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

Způsob komunikace se spoléhajícími se stranami je uveden v politice vydávání kvalifikovaných časových razítek.

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

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

Způsob řešení sporů mezi I.CA a uživatelem příslušné certifikační služby a je uveden politice této služby.

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

Popsáno v politice vydávání kvalifikovaných časových razítek.

9.16.1 Rámcová dohoda

Viz kap. 9.16.

9.16.2 Postoupení práv

Viz kap. 9.16.

9.16.3 Oddělitelnost ustanovení

Viz kap. 9.16.

9.16.4 Zřeknutí se práv

Viz kap. 9.16.

9.16.5 Vyšší moc

Viz kap. 9.16.

9.17 Další opatření

Není relevantní pro tento dokument.

10 ZÁVĚREČNÁ USTANOVENÍ

Tato certifikační politika vydaná společností První certifikační autorita, a.s., nabývá platnosti a účinnosti dnem 02.11.2015.