První certifikační autorita, a.s.

Certifikační politika

vydávání komerčních certifikátů (algoritmus RSA)

Verze 1.00

OBSAH

tab. 1 - Vývoj dokumentu

Verze	Datum vydání	Schválil	Poznámka
1.00	29.03.2016	Ředitel společnosti První certifikační autorita, a.s.	První vydání.

1 ÚVOD

Kořenová kvalifikovaná certifikační autorita společnosti První certifikační autorita, a.s., dále též I.CA, vydala v souladu s požadavky technických standardů certifikát podřízené certifikační autoritě, provozované I.CA - dále též Autorita. Tato Autorita vydává koncovým uživatelům komerční certifikáty (dále též Certifikáty), jejichž vydávání se řídí touto certifikační politikou (dále též CP). Pro certifikační služby poskytované podle této CP je využíván algoritmus RSA.

Certifikáty vydávané podle této CP jsou určené pro ověřování elektronických podpisů, vytvářených fyzickými osobami, právnickými osobami nebo organizačními složkami státu (dále Organizacemi), pro autentizaci klienta a šifrování.

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

1.1 Přehled

Dokument **Certifikační politika vydávání komerčních certifikátů (algoritmus RSA)** vypracovaný společností První certifikační autorita, a. s., se zabývá skutečnostmi, vztahujícími se k procesům životního cyklu vydávaných Certifikátů a 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.

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

1.2 Název a jednoznačné určení dokumentu

Název a identifikace dokumentu:	Certifikační politika vydávání komerčních certifikátů (algoritmus RSA), verze 1.00
OID politiky:	1.3.6.1.4.1.23624.10.1.70.1.0

1.3 Participující subjekty

1.3.1 Certifikační autority (dále “CA”)

Certifikační autorita, provozovaná společností První certifikační autorita, a.s., vydávající Certifikáty koncovým uživatelům.

1.3.2 Registrační autority (dále “RA”)

Poskytování služeb společností První certifikační autorita, a.s., se realizuje prostřednictvím registračních autorit (stacionárních nebo mobilních), které jsou buď veřejné (poskytují služby veřejnosti), nebo klientské (poskytují služby svým zákazníkům). Tyto registrační autority:

- Přijímají žádosti o služby uvedené v této CP, zejména přijímají žádosti o vydání Certifikátu, zprostředkovávají předání Certifikátů a seznamů zneplatněných certifikátů, poskytují potřebné informace, přijímají reklamace atd.
- Jsou oprávněny z naléhavých provozních nebo technických důvodů pozastavit zcela nebo zčásti výkon své činnosti.
- Jsou zmocněny jménem I.CA uzavírat smlouvy o poskytování certifikační služby.
- Zajišťují zpoplatňování služeb I.CA poskytovaných prostřednictvím RA, pokud není stanoveno smlouvou jinak.
- V případě smluvní RA plní tato jménem I.CA obdobné funkce jako vlastní RA na základě písemné smlouvy mezi I.CA a provozovatelem smluvní RA.

1.3.3 Držitelé certifikátů a držitelé soukromého klíče

Držitelem Certifikátu je fyzická osoba nebo Organizace, která požádala o vydání Certifikátu a které byl Certifikát podle této CP vydán.

Držitelem soukromého klíče mohou být:

- soukromá fyzická osoba, resp. OSVČ, v tomto případě je držitel soukromého klíče shodný s držitelem Certifikátu,
- fyzická osoba zaměstnanec Organizace, držitelem Certifikátu je Organizace,
- Organizace, která je v tomto případě i držitelem Certifikátu.

1.3.4 Spoléhající se strany

Spoléhající se stranou jsou 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 a další, kterým to podle platné legislativy přísluší.

1.4 Použití certifikátu

1.4.1 Přípustné použití certifikátu

Certifikáty vydávané podle této CP lze využívat v procesech ověřování elektronického podpisu, pro šifrování komunikace nebo pro autentizaci klienta.

1.4.2 Omezení použití certifikátu

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

1.5 Správa politiky

1.5.1 Organizace spravující dokument

Tuto CP, resp. jí odpovídající CPS, spravuje společnost První certifikační autorita, a.s.

1.5.2 Kontaktní osoba

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

1.5.3 Osoba rozhodující o souladu CPS s certifikační politikou

Jedinou osobou, která je odpovědná za rozhodování o souladu postupů společnosti První certifikační autorita, a.s., uvedených v CPS s touto CP je ředitel společnosti První certifikační autorita, a.s.

1.5.4 Postupy při schvalování certifikační politiky

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

1.6 Přehled použitých pojmů a zkratek

tab. 2 - Pojmy

Pojem	Vysvětlení
bezpečné uživatelské zařízení	zařízení, na kterém je uložen soukromý klíč uživatele, chránící tento klíč a provádějící jménem uživatele podepisovací a dešifrovací operace
bit	z anglického *binary digit* - číslice dvojkové soustavy - základní a současně nejmenší jednotka informace v číslicové technice
Certifikát	v tomto dokumentu komerční certifikát
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)
elektronický podpis	v tomto dokumentu elektronický podpis, resp. zaručený elektronický podpis, tj. údaje v elektronické podobě, které jsou připojené k datové zprávě nebo jsou s ní logicky spojené, které slouží jako metoda k jednoznačnému ověření identity podepsané osoby ve vztahu k datové zprávě a které byly vytvořeny a připojeny k datové zprávě pomocí prostředků, které podepisující osoba může udržet pod svojí výhradní kontrolou
hashovací funkce	transformace, která jako vstup přijímá řetězec znaků o libovolné délce a výsledkem je řetězec znaků s pevnou délkou (hash)
infrastrukturní certifikát	certifikát sloužící v procesech vydávání certifikátů koncovým uživatelům, vydávání seznamů zneplatněných certifikátů a poskytování informací o stavu certifikátů
kořenová CA	certifikační autorita vydávající certifikáty podřízeným certifikačním autoritám
OCSP respondér	server poskytující protokolem OCSP údaje o stavu certifikátu veřejného klíče
Organizace	právnická osoba nebo organizační složka státu
párová data	soukromý a jemu odpovídající veřejný klíč
písemná smlouva	text smlouvy v elektronické, nebo listinné podobě
podepisující osoba	v tomto dokumentu - fyzická osoba, která drží prostředek pro vytváření elektronických podpisů, držitel soukromého klíče
podpisový certifikát	volitelně vydávaný certifikát jednoznačně související s Certifikátem
podřízená CA	pro účely tohoto dokumentu CA vydávající certifikáty koncovým uživatelům
Směrnice	SMĚRNICE EVROPSKÉHO PARLAMENTU A RADY 1999/93/ES ze dne 13. prosince 1999 o zásadách Společenství pro elektronické podpisy
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 využívaná v procesech vytváření elektronického podpisu, autentizace a dešifrování
spoléhající se strana	subjekt spoléhající se při své činnosti na certifikát
TWINS	obchodní produkt I.CA, obsahující dvojici certifikátů: ▪ kvalifikovaný certifikát – vydaný v souladu s legislativou týkající se elektronického podpisu, ▪ komerční certifikát – vydaný výhradně na základě smluvního vztahu mezi I.CA a koncovým uživatelem
veřejný klíč	jedinečná data využívaná v procesech ověřování elektronického podpisu, autentizace a šifrování
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

tab. 3 - Zkratky

Pojem	Vysvětlení
BIH	Bureau International de l'Heure, (anglicky The International Time Bureau), Mezinárodní časová služba
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
ČSN	označení českých technických norem
DER, PEM	způsoby zakódování (formáty) certifikátu
eIDAS	NAŘÍZENÍ EVROPSKÉHO PARLAMENTU A RADY (EU) č. 910/2014 ze dne 23. července 2014 o elektronické identifikaci a službách vytvářejících důvěru pro elektronické transakce na vnitřním trhu a o zrušení směrnice 1999/93/ES
EN	European Standard, typ ETSI standardu
EPS	elektrická požární signalizace
ESI	Electronic Signatures and Infrastructures
ETSI	European Telecommunications Standards Institute, evropský

	standardizační institut v oblasti informačních a komunikačních technologií
EZS	elektronická zabezpečovací signalizace
FIPS	Federal Information Processing Standard, označení standardů v oblasti informačních technologií pro nevojenské státní organizace ve Spojených státech
html	Hypertext Markup Language, značkovací jazyk pro vytváření hypertextových dokumentů
http	Hypertext Transfer Protocol, protokol pro výměnu textových dokumentů ve formátu html
https	Hypertext Transfer Protocol Secure, protokol pro zabezpečenou výměnu textových dokumentů ve formátu html
I.CA	První certifikační autorita, a.s.
ICA_OID	OID z prostoru přiděleného I.CA
IEC	International Electrotechnical Commission, světová organizace publikující standardy pro elektrotechniku, elektroniku, sdělovací techniku a příbuzné obory
ISMS	Information Security Management System, systém řízení bezpečnosti informací
ISO	International Organization for Standardization, mezinárodní organizace sdružující národní standardizační organizace, označení standardů
ITU	International Telecommunication Union
ITU-T	Telecommunication Standardization Sector of ITU
Microsoft_OID	OID z prostoru přiděleného Microsoftu
NCP	Normalized Certificate Policy, typ certifikační politiky nekvalifikovaných certifikátů, kvalitativně shodný s politikou vydávání kvalifikovaných certifikátů
NCP+	Extended Normalized Certificate Policy, certifikační politika NCP, soukromý klíč je umístěn na bezpečném uživatelském zařízení
OCSP	Online Certificate Status Protocol, protokol pro zjišťování stavu certifikátu veřejného klíče
OID	Object Identifier, objektový identifikátor, číselná identifikace objektu
OSVČ	osoba samostatně výdělečně činná
PCO	pult centrální ochrany
PDCA	Plan-Do-Check-Act, Plánování-Zavedení-Kontrola-Využití, Demingův cyklus, metoda neustálého zlepšování
PDS	PKI Disclosure Statement, zpráva pro uživatele
PKCS	Public Key Cryptography Standards, označení skupiny standardů pro kryptografii s veřejným klíčem

PKI	Public Key Infrastructure, infrastruktura veřejných klíčů
PUB	Publication, označení standardu FIPS
QESCD	Qualified Electronic Signature Creation Device, zařízení pro tvorbu kvalifikovaného elektronického podpisu (dle definice v eIDAS)
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
SSCD	Secure Signature Creation Device, bezpečné zařízení pro tvorbu elektronického podpisu (dle definice ve Směrnici)
TS	Technical Specification, typ ETSI standardu
UPN	User Principal Name, uživatelské jméno ve tvaru dle RFC 822
UPS	Uninterruptible Power Supply/Source, zdroj nepřerušovaného napájení
URI	Uniform Resource Identifier, textový řetězec s definovanou strukturou sloužící k přesné specifikaci zdroje informací
UTC	Universal Co-ordinated Time, standard přijatý 1.1.1972 pro světový koordinovaný čas - funkci „oficiálního časoměřiče" atomového času pro celý svět vykonává Bureau International de l'Heure (BIH)
X.501, X.509, X.520	standardy pro systémy založené na veřejném klíči
ZOOÚ	zákon č. 101/2000 Sb., o ochraně osobních údajů a o změně některých zákonů (zákon o ochraně osobních údajů), 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.

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 případě zneplatnění certifikátů sloužících v procesech vydávání Certifikátů koncovým uživatelům, vydávání seznamů zneplatněných certifikátů a poskytování informací o stavu certifikátů (dále též infrastrukturní certifikáty) oznámí I.CA tuto skutečnost na své internetové

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

2.3 Doba a periodicita zveřejňování informací

I.CA zveřejňuje informace s následující periodicitou:

- certifikační politika - po schválení a vydání nové verze,
- certifikační prováděcí směrnice - neprodleně,
- seznam vydaných Certifikátů - aktualizace při každém vydání nového Certifikátu,
- seznam zneplatněných certifikátů (CRL) - viz kapitola 4.9.7,
- informace o zneplatnění infrastrukturního certifikátu, s uvedením důvodu zneplatnění – bezodkladně,
- ostatní veřejné informace – není předem určeno, obecně však platí, že tyto informace musí reflektovat aktuální stav poskytovaných certifikačních služeb.

2.4 Řízení přístupu k jednotlivým typům úložišť

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

Neveřejné informace jsou dostupné pouze pověřeným zaměstnancům I.CA. 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

V procesu vydávání Certifikátu je vždy vyžadována významovost všech ověřitelných jmen, uvedených v položkách polí Subject, resp. SubjectAlternativeName. Podporované položky uvedených polí jsou uvedeny v kapitole 7.

3.1.3 Anonymita nebo používání pseudonymu

Certifikáty vydávané podle této CP nepodporují anonymitu, podporují používání pseudonymu.

3.1.4 Pravidla pro interpretaci různých forem jmen

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

3.1.5 Jedinečnost jmen

V každém Certifikátu vydaném podle této CP je uveden jedinečný identifikátor (pole serialNumber v položce Subject). Výskyt tohoto pole může být vícenásobný, povolené hodnoty jeho obsahu jsou uvedeny v kapitole 7.1. Jeden z výskytů položky serialNumber, určený k jednoznačné identifikaci držitele Certifikátu, resp. držitele soukromého klíče v systému Autority, je též uveden v rozšiřující položce Certifikátu, konkrétně v poli otherName položky SubjectAlternativeName.

3.1.6 Uznávání, ověřování a poslání obchodních značek

Certifikáty, vydávané podle této CP, mohou obsahovat pouze obchodní značky, jejichž vlastnictví nebo pronájem byly doloženy. Veškeré důsledky plynoucí z neoprávněného užívání ochranné známky nese držitel Certifikátu.

3.2 Počáteční ověření identity

Subjekty oprávněné podat žádost o vydání Certifikátu jsou vyjmenovány v kapitole 4.1.1 - jedná se jednak o fyzické osoby a dále Organizace. V následujících kapitolách jsou uvedena pravidla pro počáteční ověření jejich identity.

3.2.1 Ověřování vlastnictví soukromého klíče

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

3.2.2 Ověřování identity organizace

Musí být předložen:

- originál nebo úředně ověřená kopie výpisu z obchodního nebo jiného zákonem určeného rejstříku/registru, živnostenského listu, zřizovací listiny, resp. jiného dokladu stejné právní váhy, nebo
- vytištěný výtah z veřejně dostupných registrů, který předloží žadatel nebo jej vyhotoví operátor RA.

Tento dokument musí obsahovat úplné obchodní jméno, identifikační číslo (je-li přiřazeno), adresu sídla, jméno/jména osoby/osob oprávněné/oprávněných k zastupování (statutárních zástupců).

3.2.3 Ověřování identity fyzické osoby

Kapitola popisuje způsob ověřování identity fyzické osoby, tj.:

- fyzické osoby žádající o vydání Certifikátu pro sebe samu,
- fyzické osoby - zaměstnance Organizace,
- osoby zastupující Organizaci žádající o vydání Certifikátu.

Pro tyto tři kategorie fyzických osob je dále v textu používáno označení Osoba,

V procesu ověřování identity Osoby je vyžadován osobní doklad obsahující údaje uvedené níže v této kapitole. Osobním dokladem pro občany ČR musí být platný občanský průkaz nebo cestovní pas. Osobním dokladem pro cizince je platný cestovní pas, nebo jím v případě občanů členských států EU může být platný osobní doklad, sloužící k prokazování totožnosti na území příslušného státu.

Z tohoto dokladu jsou ověřovány následující údaje:

- celé občanské jméno,
- datum narození, nebo rodné číslo, je-li v dokladu uvedeno,
- číslo předloženého osobního dokladu,
- adresa trvalého bydliště (je-li v dokladu uvedena).

Pokud v předloženém osobním dokladu není uvedena adresa trvalého bydliště a tato v Certifikátu uvedena být má, musí být předložen také další doklad, který adresu trvalého bydliště obsahuje a který je s předloženým osobním dokladem jednoznačně svázán (rodné

číslo, číslo občanského průkazu atd.). Jinak nemůže být v žádosti o Certifikát a následně ve vydaném Certifikátu adresa trvalého bydliště uvedena.

V případě zaměstnance je dále vyžadováno potvrzení o zaměstnaneckém poměru k Organizaci. Toto potvrzení předloží žadatel na RA, může však být prokázáno způsobem definovaným v uzavřené smlouvě mezi I.CA a Organizací.

Pokud bude držitelem Certifikátu Organizace a osoba jednající za Organizaci není osobou ze zákona oprávněnou k zastupování Organizace, je dále požadována úředně ověřená plná moc k zastupování Organizace podepsaná statutárním zástupcem Organizace.

V případě že Osobu zastupuje na RA zmocněnec, je vyžadováno úředně ověřené zplnomocnění k jednání v zastoupení.

Pokud je fyzická osoba žádající o vydání Certifikátu pro sebe samu fyzickou osobou podnikající (OSVČ) a tato skutečnost má být v Certifikátu uvedena, platí dále relevantní požadavky kapitoly 3.2.2.

3.2.4 Neověřované informace o držiteli certifikátu, resp. držiteli soukromého klíče

Neověřovanými informacemi vztahujícími se k Osobě nebo Organizaci jsou:

- pseudonym,
- generační kvalifikátor,
- organizationalUnitName,
- title.

3.2.5 Ověřování kompetencí

Adresu elektronické pošty je možno umístit v rozšíření Certifikátu, konkrétně v poli rfc822Name položky SubjectAlternativeName, pouze tehdy, byla-li tato skutečnost v procesu vydání Certifikátu pro tuto žádost ověřena.

Příznak, že klíčový pár byl generován na bezpečném uživatelském zařízení lze do Certifikátu vložit pouze tehdy, byla-li tato skutečnost v procesu vydání certifikátu pro tuto žádost ověřena.

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 autorizace při požadavku na výměnu klíče

3.3.1 Identifikace a autorizace při běžném požadavku na výměnu klíče

Identifikace a autentizace při běžné výměně párových dat se prokazuje tak, že žádost o vydání následného certifikátu (viz kapitoly 4.7 a 4.8) ve struktuře PKCS#10 musí být:

- elektronicky podepsána soukromým klíčem, odpovídajícím veřejnému klíči obsaženému v platném Certifikátu, který je předmětem výměny, nebo

- obsažena v elektronické zprávě podepsané soukromým klíčem odpovídajícím veřejnému klíči v podpisovém certifikátu.

3.3.2 Identifikace a autorizace při požadavku na výměnu klíče po zneplatnění certifikátu

Není relevantní pro tento dokument, služba výměny veřejného klíče 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 autorizace při požadavku na zneplatnění certifikátu

V případě **osobního předání žádosti o zneplatnění Certifikátu na RA** musí být žádost o zneplatnění Certifikátu písemná a podepsaná Osobou, jejíž identita musí být řádně ověřena osobním dokladem.

V případě **předání žádosti o zneplatnění Certifikátu elektronickou cestou** jsou přípustné tyto způsoby identifikace a autentizace:

- prostřednictvím formuláře na webových stránkách společnosti (s využitím hesla pro zneplatnění Certifikátu),
- prostřednictvím nepodepsané elektronické zprávy obsahující heslo pro zneplatnění Certifikátu odeslané na adresu revoke@ica.cz,
- prostřednictvím podepsané elektronické zprávy, kde:
  - elektronický podpis musí být realizován soukromým klíčem příslušným k podpisovému certifikátu příslušnému k Certifikátu, který má být zneplatněn, nebo
  - elektronický podpis musí být realizován soukromým klíčem příslušným k zneplatňovanému Certifikátu,

  zpráva musí být odeslána na adresu revoke@ica.cz,
- prostřednictvím datové schránky I.CA (s využitím hesla pro zneplatnění Certifikátu),
- prostřednictvím definované osoby pověřené za Organizaci vystupovat ve smluvním vztahu s I.CA.

V případě použití **listovní zásilky pro předání žádosti o zneplatnění Certifikátu** s využitím hesla pro zneplatnění Certifikátu musí být tato zaslána doporučeně na adresu sídla společnosti I.CA.

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

O zneplatnění Certifikátu mohou požádat prostřednictvím oprávněného pracovníka i subjekty, jimž to umožňuje platná legislativa.

I.CA si vyhrazuje právo akceptování i jiných forem postupů při identifikaci a autentizaci požadavků na zneplatnění Certifikátu, které však nesmí být v rozporu s platnou legislativou.

4 POŽADAVKY NA ŽIVOTNÍ CYKLUS CERTIFIKÁTU

4.1 Žádost o vydání certifikátu

4.1.1 Kdo může požádat o vydání certifikátu

O vydání Certifikátu může požádat:

- fyzická osoba pro sebe samu jako držitele Certifikátu (fyzická osoba je držitelem Certifikátu i držitelem soukromého klíče),
- fyzická osoba, která je zaměstnancem Organizace (Organizace je držitelem Certifikátu, fyzická osoba je držitelem soukromého klíče),
- Organizace (Organizace je držitelem Certifikátu i držitelem soukromého klíče) prostřednictvím osoby zastupující Organizaci.

4.1.2 Registrační proces a odpovědnosti

Registrační proces (v případě prvotního certifikátu) zahajuje Osoba dostavením se s potřebnými dokumenty a případně s žádostí o Certifikát na pracoviště RA, kde probíhá zanesení údajů obsažených v předkládaných dokladech do informačního systému Autority a zpracování žádosti o Certifikát.

Osoby jsou povinny zejména:

- seznámit se s touto CP a smluvně se zavázat jednat podle ní,
- poskytovat pravdivé a úplné informace pro vydání Certifikátu,
- překontrolovat, zda údaje uvedené v žádosti o Certifikát a ve vydaném Certifikátu jsou správné a odpovídají požadovaným údajům,
- zvolit vhodné heslo pro zneplatnění Certifikátu (minimální/maximální délka hesla 6/32 znaků, povolené znaky 0..9, A..Z, a..z).

Poskytovatel je povinen zejména:

- před uzavřením smlouvy o vydání Certifikátu informovat Osobu o smluvních podmínkách,
- uzavírat s Osobou, resp. Organizací smlouvu o vydání Certifikátu obsahující náležitosti požadované technickými standardy,
- v procesu vydávání Certifikátu na RA ověřit všechny ověřitelné údaje uvedené v žádosti podle předložených dokladů,
- v případě, že soukromý klíč byl generován na bezpečném uživatelském zařízení, vyžadovat prokázání této skutečnosti,
- vydat Certifikát obsahující věcně správné údaje na základě informací, které jsou poskytovateli certifikačních služeb k dispozici v době vydávání tohoto Certifikátu,
- zveřejňovat veřejné informace v souladu s ustanoveními kapitoly 2.2,
- zveřejnit certifikáty Autority a kořenové CA,

- činnosti spojené s certifikační službou vydávání Certifikátů poskytovat v souladu s uzavřenou smlouvou, touto CP, příslušnou CPS, Systémovou bezpečnostní politikou CA a provozní dokumentací.

4.2 Zpracování žádosti o certifikát

4.2.1 Provádění identifikace a autentizace

Při vydávání **prvotního certifikátu** jsou identifikace a autentizace prováděny podle kapitoly 3.2.3, případně kapitoly 3.2.2), v případě vydávání **následného certifikátu** pak podle kapitoly 3.3.1).

4.2.2 Schválení nebo zamítnutí žádosti o certifikát

V procesu rozhodování o přijetí nebo zamítnutí žádosti o vydání **prvotního certifikátu** provádějí pracovnice/pracovníci, dále jen pracovníci, RA:

- vizuální kontrolu shody údajů obsažených v žádosti o Certifikát (struktura PKCS#10) s údaji obsaženými v předkládaných dokladech,
- vizuální kontrolu formální správnosti údajů.

Ověřování vlastnictví soukromého klíče, specifických práv a kontroly formální správnosti údajů jsou prováděny i programovým vybavením systému RA.

Pokud některá z uvedených kontrol skončí negativně, proces vydání Certifikátu je ukončen, v opačném případě je postupováno v souladu s ustanoveními kapitoly 4.3.

Postup vydání **následného certifikátu** je popsán v kapitole 4.3.

4.2.3 Doba zpracování žádosti o certifikát

Po kladném rozhodnutí o vydání Certifikátu je I.CA povinna neprodleně Certifikát vydat. Přibližné časové údaje pro vydání Certifikátu v pracovní dny a hodiny, není-li smluvně uvedeno jinak, jsou uvedeny v následujícím seznamu:

- prvotní certifikát - doba vydání je do 15 minut a jen ve výjimečných případech může být tato doba delší,
- následný certifikát - jednotky minut.

4.3 Vydání certifikátu

4.3.1 Úkony CA v průběhu vydávání certifikátu

V procesu vydávání Certifikátu provádějí operátorky/operátoři, dále jen operátoři, CA:

- vizuální kontrolu shody údajů obsažených v žádosti o Certifikát (struktura PKCS#10) a údajů doplněných pracovníkem RA,
- vizuální kontroly formální správnosti údajů.

Ověřování vlastnictví soukromého klíče (viz kapitola 3.2.1), specifických práv (viz kapitola 3.2.5) a kontroly formální správnosti údajů jsou prováděny jak programovým vybavením umístěným na pracovních stanicích operátorů CA, tak programovým vybavením jádra systému CA. Pokud některá z uvedených kontrol skončí negativně, proces vydání Certifikátu je ukončen.

4.3.2 Oznámení o vydání certifikátu držiteli certifikátu, resp. držiteli soukromého klíče certifikační autoritou

V procesu vydávání **prvotního certifikátu** je Osoba informována prostřednictvím pracovníka RA a Certifikát je zaslán na kontaktní e-mailovou adresu zadanou povinně při registraci.

V případě vydání **následného certifikátu** je tento Certifikát zaslán na kontaktní e-mailovou adresu zadanou povinně při registraci.

4.4 Převzetí vydaného certifikátu

4.4.1 Úkony spojené s převzetím certifikátu

Pokud byly splněny podmínky pro vydání Certifikátu, je povinností Osoby tento Certifikát přijmout. Jediným způsobem jak odmítnout převzetí Certifikátu je zažádat v souladu s touto CP o jeho zneplatnění.

I.CA může s Organizací sjednat postup odlišný od tohoto ustanovení CP. Tímto postupem však nesmí být dotčena příslušná ustanovení legislativních norem, které upravují oblast poskytování certifikačních služeb nebo obchodní činnosti s tímto spojené.

4.4.2 Zveřejňování certifikátů certifikační autoritou

I.CA zajistí zveřejnění jí vydaných Certifikátů, vyjma Certifikátů:

- obsahujících údaje, jejichž zveřejnění by bylo v rozporu s legislativou ČR (např. zákon o ochraně osobních údajů),
- u kterých si držitel Certifikátu vymínil, že nebudou zveřejněny.

4.4.3 Oznámení o vydání certifikátu certifikační autoritou jiným subjektům

Platí ustanovení kapitoly 4.4.2.

4.5 Použití párových dat a certifikátu

4.5.1 Použití soukromého klíče a certifikátu držitele certifikátu, resp. držitele soukromého klíče

Povinností Osob a držitelů Certifikátů je zejména:

- dodržovat veškerá relevantní ustanovení smlouvy o poskytování této certifikační služby,

- užívat soukromý klíč a odpovídající Certifikát vydaný podle této CP pouze pro účely stanovené v této CP,
- nakládat se soukromým klíčem, který odpovídá veřejnému klíči obsaženému v Certifikátu vydaném podle této CP, takovým způsobem, aby nemohlo dojít k jeho neoprávněnému použití,
- neprodleně uvědomit poskytovatele certifikačních služeb o skutečnostech, které vedou ke zneplatnění Certifikátu, zejména o podezření, že soukromý klíč byl zneužit, požádat o zneplatnění Certifikátu a ukončit používání příslušného soukromého klíče.

4.5.2 Použití veřejného klíče a certifikátu spoléhající se stranou

Spoléhající se strany jsou zejména povinny:

- získat certifikáty certifikačních autorit související s Certifikátem vydaným podle této CP, ověřit hodnoty jejich otisků a jejich platnost,
- provádět veškeré úkony potřebné k tomu, aby si ověřily, že Certifikát je platný,
- dodržovat veškerá ustanovení této CP.

4.6 Obnovení certifikátu

Službou obnovení Certifikátu je podle této CP míněno vydání následného certifikátu k ještě platnému Certifikátu, aniž by byl změněn veřejný klíč, nebo jiné informace v Certifikátu, nebo k zneplatněnému Certifikátu, nebo k expirovanému Certifikátu.

Služba obnovení Certifikátu není poskytována.

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

4.6.1 Podmínky pro obnovení certifikátu

Viz kapitola 4.6.

4.6.2 Kdo může žádat o obnovení

Viz kapitola 4.6.

4.6.3 Zpracování požadavku na obnovení certifikátu

Viz kapitola 4.6.

4.6.4 Oznámení o vydání nového certifikátu držiteli certifikátu, resp. držiteli soukromého klíče

Viz kapitola 4.6.

4.6.5 Úkony spojené s převzetím obnoveného certifikátu

Viz kapitola 4.6.

4.6.6 Zveřejňování obnovených certifikátů certifikační autoritou

Viz kapitola 4.6.

4.6.7 Oznámení o vydání certifikátu certifikační autoritou jiným subjektům

Viz kapitola 4.6.

4.7 Výměna veřejného klíče v certifikátu

Službou výměny veřejného klíče v Certifikátu je podle této CP míněno vydání nového Certifikátu s jiným veřejným klíčem, ale s totožným obsahem polí uvedených v položkách Subject nebo SubjectAlternativeName Certifikátu, jehož veřejný klíč je předmětem výměny.

V případě, že proces vydání nového Certifikátu probíhá výhradně elektronickou cestou, jedná se o službu výměny veřejného klíče v Certifikátu, tedy vydání **následného certifikátu** k Certifikátu, jehož veřejný klíč je předmětem výměny. Požadavky na identifikaci a autentizaci jsou uvedeny v kapitole 3.3.1, pokud splněny nejsou, jedná se o službu vydání **prvotního certifikátu**, počínající registračním procesem (viz kapitola 4.1.2).

4.7.1 Podmínky pro výměnu veřejného klíče v certifikátu

Žádost o vydání následného Certifikátu s vyměněným veřejným klíčem musí splňovat níže uvedené podmínky:

- položky polí Subject nebo SubjectAlternativeName musí být totožné jako v Certifikátu, který je předmětem výměny,
- veřejný klíč musí být jiný než v Certifikátu, který je předmětem výměny,
- ostatní položky žádosti zůstávají shodné s původními údaji v dokumentech předložených v procesu počátečního ověřování identity fyzické osoby,
- proces identifikace a autentizace je proveden v souladu s kapitolou 3.3.1.

4.7.2 Kdo může požádat o výměnu veřejného klíče v certifikátu

Výměnu veřejného klíče jsou oprávněny požadovat Osoby, resp. držitelé Certifikátů, jejichž veřejný klíč je předmětem výměny.

4.7.3 Zpracování požadavku na výměnu veřejného klíče v certifikátu

Pokud jsou splněny podmínky pro výměnu veřejného klíče je postupováno v souladu s kapitolou 4.3.1, v opačném případě je řízení k vydání Certifikátu ukončeno.

4.7.4 Oznámení o vydání nového certifikátu držiteli certifikátu, resp. držiteli soukromého klíče

Uvedeno v kapitole 4.3.2.

4.7.5 Úkony spojené s převzetím certifikátu s vyměněným veřejným klíčem

Uvedeno v kapitole 4.4.1.

4.7.6 Zveřejňování certifikátů s vyměněným veřejným klíčem certifikační autoritou

Uvedeno v kapitole 4.4.2.

4.7.7 Oznámení o vydání certifikátu certifikační autoritou jiným subjektům

Platí ustanovení kapitoly 4.4.2.

4.8 Změna údajů v certifikátu

Službou změny údajů v Certifikátu je podle této CP míněno vydání nového Certifikátu s minimálně jednou změnou v obsahu polí uvedených v položkách Subject nebo SubjectAlternativeName vztahujících se k Osobě, nebo s odebraným, nebo přidaným dalším polem, jehož obsah musí být ověřen. Veřejný klíč musí být jiný než v Certifikátu, který je předmětem výměny.

V případě, že proces vydání nového Certifikátu probíhá výhradně elektronickou cestou, jedná se o službu změny údajů v Certifikátu, tedy vydání **následného certifikátu** k Certifikátu, jehož údaje jsou předmětem výměny. Požadavky na identifikaci a autentizaci jsou uvedeny v kapitole 3.3.1, pokud splněny nejsou, jedná se o službu vydání **prvotního certifikátu**, počínající registračním procesem (viz kapitola 4.1.2).

4.8.1 Podmínky pro změnu údajů v certifikátu

Žádost o vydání Certifikátu (struktura PKCS#10) se změněnými údaji (následný certifikát) musí splňovat níže uvedené podmínky:

- měněná, resp. nově uvedená pole položek Subject nebo SubjectAlternativeName musí být řádným způsobem ověřena,
- ostatní položky žádosti zůstávají shodné s původními údaji v dokumentech předložených v procesu počátečního ověřování identity fyzické osoby,
- veřejný klíč musí být jiný než v původním Certifikátu,
- proces identifikace a autentizace je proveden v souladu s kapitolou 3.3.1.

4.8.2 Kdo může požádat o změnu údajů v certifikátu

Změnu údajů jsou oprávněny požadovat Osoby, resp. držitelé Certifikátů, jejichž údaje jsou předmětem změny.

4.8.3 Zpracování požadavku na změnu údajů v certifikátu

Pokud jsou splněny podmínky pro změnu údajů v Certifikátu je postupováno v souladu s kapitolou 4.2, v opačném případě je řízení k vydání Certifikátu ukončeno.

4.8.4 Oznámení o vydání certifikátu se změněnými údaji držiteli certifikátu, resp. držiteli soukromého klíče

Uvedeno v kapitole 4.3.2.

4.8.5 Úkony spojené s převzetím certifikátu se změněnými údaji

Uvedeno v kapitole 4.4.1.

4.8.6 Zveřejňování certifikátů se změněnými údaji

Uvedeno v kapitole 4.4.2.

4.8.7 Oznámení o vydání certifikátu certifikační autoritou jiným subjektům

Platí ustanovení kapitoly 4.4.2.

4.9 Zneplatnění a pozastavení platnosti certifikátu

Žádost o zneplatnění Certifikátu přijímá I.CA nepřetržitě pouze prostřednictvím předání žádosti elektronickou cestou a listovní zásilkou. Osobní předání na RA je možné pouze v pracovní době příslušné RA.

Službu pozastavení platnosti Certifikátu I.CA neposkytuje.

4.9.1 Podmínky pro zneplatnění

Certifikát musí být zneplatněn mj. na základě následujících okolností:

- dojde ke kompromitaci, resp. existuje důvodné podezření, že došlo ke kompromitaci, soukromého klíče,
- je porušeno ustanovení smlouvy o poskytování certifikační služby podle této CP ze strany Osoby, resp. držitele Certifikátu,
- pokud je veřejný klíč v žádosti o vydání Certifikátu duplicitní s veřejným klíčem v již vydaném Certifikátu.

I.CA si vyhrazuje právo akceptování i jiných podmínek na zneplatnění Certifikátu, které však nesmí být v rozporu s platnou legislativou.

4.9.2 Kdo může požádat o zneplatnění

Žádost o zneplatnění Certifikátu mohou podat:

- Osoba, resp. držitel Certifikátu,

- subjekt, který k tomu byl explicitně určen ve smlouvě o poskytování certifikační služby podle této CP,
- osoba oprávněná z pozůstalostního řízení Osoby, resp. držitele Certifikátu, pokud je držitelem Certifikátu fyzická osoba,
- osoba pověřená jednáním za právního nástupce původního subjektu, jemuž byl pro jeho zaměstnance Certifikát vydán,
- poskytovatel certifikačních služeb (oprávněným žadatelem o zneplatnění Certifikátu vydaného I.CA je v tomto případě ředitel I.CA):
  - v případě, že Certifikát byl vydán na základě nepravdivých údajů,
  - pokud prokazatelně zjistí, že soukromý klíč, patřící k veřejnému klíči uvedenému v Certifikátu, byl kompromitován,
  - dozví-li se prokazatelně, že Certifikát byl použit v rozporu s omezením definovaným v kapitole 1.4.2,
  - dozví-li se prokazatelně, že držitel soukromého klíče zemřel nebo zanikl, nebo soud jeho způsobilost k právním úkonům omezil, nebo pokud údaje, na jejichž základě byl Certifikát vydán, pozbyly pravdivosti,
  - pokud je veřejný klíč v žádosti o vydání Certifikátu duplicitní s veřejným klíčem v již vydaném certifikátu.

4.9.3 Postup při žádosti o zneplatnění

V případě osobního předání žádosti o zneplatnění Certifikátu na RA musí žádost obsahovat sériové číslo Certifikátu buď v dekadickém nebo hexadecimálním tvaru (uvozeno řetězcem „0x“), jméno, popř. jména a příjmení Osoby oprávněné žádat zneplatnění Certifikátu a heslo pro zneplatnění Certifikátu. Pokud Osoba heslo pro zneplatnění nezná, musí tuto skutečnost do písemné žádosti explicitně uvést, včetně čísla osobního dokladu předloženého při žádosti o vydání Certifikátu, nebo čísla nového primárního osobního dokladu, pokud byl původní nahrazen novým. Tímto osobním dokladem se musí pracovníkovi RA prokázat. Pracovník RA předá výše uvedenou žádost elektronickou cestou na provozní pracoviště Autority. Odpovědný pracovník CA rozhodne, zda je žádost oprávněná a rozhodnutí sdělí prostřednictvím pracovníka RA. V případě, že je žádost oprávněná, operátor CA Certifikát zneplatní - datum a čas zneplatnění Certifikátu jsou dány zpracováním tohoto požadavku. V případě, že žádost nelze akceptovat (nesprávné heslo pro zneplatnění, neprokazatelná identita Osoby), pokusí se pracovník RA v součinnosti s touto fyzickou osobou tyto skutečnosti napravit a pokud to z libovolného důvodu nebude možné, žádost o zneplatnění Certifikátu bude zamítnuta. Žadatel o zneplatnění Certifikátu je vždy o výsledku informován prostřednictvím pracovníka RA.

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

- Prostřednictvím formuláře na internetové informační adrese. Datum a čas zneplatnění Certifikátu jsou dány zpracováním platné žádosti o zneplatnění Certifikátu informačním systémem CA. O kladném vyřízení je žadatel informován.
- Elektronicky podepsaná zpráva - tělo zprávy musí obsahovat text (v českém nebo slovenském jazyce, s diakritikou nebo bez diakritiky, případně v jazyce anglickém):

  Zadam o zneplatneni certifikatu cislo = xxxxxxx,

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

Zpráva musí být elektronicky podepsána soukromým klíčem odpovídajícím veřejnému klíči v podpisovém certifikátu, nebo soukromým klíčem příslušným k veřejnému klíči ve zneplatňovaném Certifikátu.

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

  Zadam o zneplatneni certifikatu cislo = xxxxxxx

  Heslo pro zneplatneni = yyyyyy,

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

- Elektronicky podepsaná či ve zvláštních případech nepodepsaná zpráva odeslaná definovanou osobou pověřenou za Organizaci vystupovat ve smluvním vztahu s I.CA:

  Zadam o zneplatneni certifikatu cislo = xxxxxxx

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

Pozn.: Pokud žádost splňuje požadavky tří výše uvedených možností, odpovědný pracovník Certifikát v systému CA neprodleně zneplatní - datum a čas zneplatnění Certifikátu jsou dány zpracováním tohoto požadavku informačním systémem CA. O kladném vyřízení je žadatel informován.

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

Zadam o zneplatneni certifikatu cislo = xxxxxxx

Heslo pro zneplatneni = yyyyyy,

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

4.9.4 Prodleva při požadavku na zneplatnění certifikátu

Držitel Certifikátu musí o zneplatnění Certifikátu požádat bezodkladně po zjištění možnosti kompromitace soukromého klíče.

4.9.5 Doba zpracování žádosti o zneplatnění

Maximální doba mezi přijetím žádosti o zneplatnění Certifikátu a jeho zneplatněním je 24 hodin.

4.9.6 Povinnosti třetích stran při kontrole zneplatnění

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

4.9.7 Periodicita vydávání seznamu zneplatněných certifikátů

Seznam zneplatněných certifikátů je vydáván neprodleně po kladném zpracování žádosti o zneplatnění Certifikátu. Nedojde-li ke zneplatnění Certifikátu, je nový CRL vydáván zpravidla v intervalu 12 hodin, nejvýše však 24 hodin od vydání předchozího CRL.

4.9.8 Maximální zpoždění při vydávání seznamu zneplatněných certifikátů

CRL je vždy vydán nejvýše 24 hodin od vydání předchozího CRL.

4.9.9 Dostupnost ověřování stavu certifikátu on-line

Služba uvěřováni stavu Certifikátu s využitím protokolu OCSP je veřejně dostupná. Každý Certifikát, vydaný podle této CP, obsahuje odkaz na příslušný OCSP respondér.

OCSP odpovědi vyhovují normám RFC 2560 a RFC 5019. Certifikát OCSP respondéru obsahuje rozšíření typu id-pkix-ocsp-nocheck, jak je definováno v RFC 2560.

4.9.10 Požadavky na ověřování stavu certifikátu on-line

Viz kapitola 4.9.9.

4.9.11 Jiné možné způsoby oznamování zneplatnění

Není relevantní pro tento dokument.

4.9.12 Zvláštní postupy při kompromitaci klíče

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

4.9.13 Podmínky pro pozastavení platnosti certifikátu

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

4.9.14 Kdo může požádat o pozastavení platnosti

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

4.9.15 Postup při žádosti o pozastavení platnosti

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

4.9.16 Omezení doby pozastavení platnosti

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

4.10 Služby ověřování stavu 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.

Skutečnost, že Autorita poskytuje informace o stavu Certifikátu formou OCSP (služba OCSP), je uvedena ve vydaných Certifikátech.

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 služby OCSP.

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

Viz kapitola 5.8.

4.12 Úschova a obnova klíčů

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

4.12.1 Politika a postupy při úschově a obnově klíčů

Viz kapitola 4.12.

4.12.2 Politika a postupy při zapouzdřování a obnově šifrovacího klíče relace

Viz kapitola 4.12.

5 POSTUPY SPRÁVY, ŘÍZENÍ A PROVOZU

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 interních dokumentech. Uvedené dokumenty reflektují výsledky periodicky prováděné 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 sledování 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 podle potřeby vybavena čidly průniku vody pro případ zaplavení vodou z topení, nebo vodou ze střechy při prudkém dešti.

5.1.5 Protipožární prevence a ochrana

V objektech provozních pracovišť a pracovišť pro uchovávání informací 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 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 Procedurální postupy

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 pro jednotlivé činnosti

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

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

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

5.2.3 Identifikace a autentizace pro každou roli

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

5.2.4 Role vyžadující rozdělení povinností

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

5.3 Personální postupy

5.3.1 Požadavky na kvalifikaci, praxi a bezúhonnost

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

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

Ostatní zaměstnanci I.CA podílející se na zajištění certifikačních služeb jsou přijímáni na základě následujících kritérií:

- vysokoškolské vzdělání v rámci akreditovaného bakalářského, resp. magisterského studijního programu, nebo středoškolské vzdělání,
- základní orientace v oblasti infrastruktury veřejných klíčů a informační bezpečnosti.

5.3.2 Posouzení spolehlivosti osob

Zdrojem informací o všech zaměstnancích I.CA jsou:

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

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

5.3.3 Požadavky na 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 doškolování

Pro pracovníky RA je minimálně jednou za tři roky pořádáno školení zaměřené na procesy spojené s činností RA.

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

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 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 Postupy zpracování auditních záznamů

5.4.1 Typy zaznamenávaných událostí

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

Speciálním případem zaznamenávání událostí je událost generování párových dat Autority, 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 integritu těchto 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

Není-li stanoveno 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 provozní 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 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

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

5.5.1 Typy uchovávaných informací

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

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

5.5.2 Doba uchování uchovávaných informací

Informace vztahující se k certifikátům všech certifikačních autorit I.CA a jim odpovídajících OCSP respondérů, s výjimkou příslušných soukromých klíčů, jsou uchovávány po celou dobu existence I.CA. Ostatní informace a dokumentace jsou uchovávány v souladu s ustanoveními kapitoly 5.4.3.

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

5.5.3 Ochrana úložiště uchovávaných informací

Prostory, ve kterých se uchovávané informace a dokumentace nacházejí, jsou zabezpečeny způsobem vycházejícím z požadavků provedené analýzy rizik a ze 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

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

5.5.5 Požadavky na používání časových razítek při uchovávání informací

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

5.5.6 Systém shromažďování uchovávaných informací (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 získávání a ověřování uchovávaných informací

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 činným v trestním řízení a soudům, pokud je to právními normami vyžadováno.

O každém takto povoleném přístupu je pořizován písemný záznam.

5.6 Výměna klíče

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

Jak v případě standardních, tak nestandardních situací je výměna veřejného klíče v certifikátech certifikačních autorit veřejnosti s předstihem (je-li to možné) vhodnou formou sdělena.

5.7 Obnova po havárii nebo kompromitaci

5.7.1 Postup ošetření incidentu nebo kompromitace

V případě výskytu těchto 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, programového vybavení nebo dat

Viz kapitola 5.7.1.

5.7.3 Postup při kompromitaci soukromého klíče certifikační autority

V případě vzniku důvodné obavy z kompromitace soukromého klíče certifikačních autorit postupuje I.CA tak, že:

- ukončí jeho používání,
- okamžitě a trvale zneplatní příslušný certifikát a zničí jemu odpovídající soukromý klíč,
- zneplatní všechny platné Certifikáty,
- bezodkladně o této skutečnosti, včetně důvodu, informuje na své internetové informační adrese (viz kapitola 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, 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 kapitoly 2.2,
- pokud je součástí ukončení činnosti Autority ukončení platnosti jejího certifikátu, musí být součástí oznámení i tato informace včetně uvedení důvodu ukončení platnosti,
- ukončování činnosti je řízený proces probíhající podle předem připraveného plánu, jehož součástí je popis postupu uchovávání a zpřístupňování informací pro poskytování důkazů v soudním a správním řízení a pro účely zajištění kontinuity služeb,
- po dobu platnosti i jen jediného Certifikátu vydaného Autoritou musí Autorita či její nástupce v případě zániku zajistit alespoň služby zneplatňování Certifikátů a vydávání CRL,
- následně Autorita prokazatelně zničí svůj soukromý klíč a o tomto zničení provede záznam, který bude uchováván podle pravidel této CP, viz kapitola 5.4.

V případě ukončení činnosti poskytovatele certifikačních služeb bude postupováno v souladu s uzavřenými smlouvami, případně s příslušnými standardy nebo normami.

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

6 ŘÍZENÍ TECHNICKÉ BEZPEČNOSTI

6.1 Generování a instalace párových dat

6.1.1 Generování párových dat

Generování párových dat certifikačních autorit a jim odpovídajících OCSP respondérů, které probíhá v zabezpečené oblasti viz kapitola 5.1.1, podle předem připraveného scénáře, v souladu s požadavky kapitol 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 úroveň 3.

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

Generování párových dat vztahujících se k Certifikátům vydávaných podle této CP je prováděno na zařízeních, která jsou pod výhradní kontrolou příslušných držitelů Certifikátu, resp. držitelů soukromého klíče. Úložištěm těchto párových dat může být jak hardware, tak software.

6.1.2 Předávání soukromého klíče jeho držiteli

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

Služba generování párových dat Osobě, resp. držiteli Certifikátu není poskytována.

6.1.3 Předávání veřejného klíče vydavateli certifikátu

Veřejný klíč je Autoritě doručen v žádosti (formát PKCS#10) o vydání Certifikátu.

6.1.4 Poskytování veřejného klíče CA spoléhajícím se stranám

Veřejné klíče certifikačních autorit jsou obsaženy v certifikátech těchto certifikačních autorit, jejich získání je garantováno následujícími způsoby:

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

Získání ostatních veřejných klíčů formou získání certifikátů veřejných klíčů je popsáno v kapitole 2.2.

6.1.5 Délky párových dat

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

6.1.6 Parametry veřejného klíče a kontrola jeho kvality

Parametry algoritmů použitých při generování veřejných klíčů certifikačních autorit a jejich OCSP respondérů splňují požadavky uvedené v technických standardech nebo normách.

Parametry algoritmů použitých při generování veřejných klíčů koncových uživatelů musí tyto požadavky rovněž splňovat.

I.CA kontroluje povolenou délku klíčů a možný dvojí výskyt veřejného klíče ve vydávaných Certifikátech. V případě duplicitního výskytu jsou Osoba, resp. držitel Certifikátu požádáni o vygenerování nového veřejného klíče. Již vydaný Certifikát je neprodleně zneplatněn, Osoba, resp. držitel takového Certifikátu jsou o tomto neprodleně a vhodným způsobem informováni a vyzváni ke generování nových párových dat.

6.1.7 Účely použití veřejného klíče

Uvedeno v kapitole 1.4.

6.2 Ochrana soukromého klíče a technologie kryptografických modulů

6.2.1 Řízení a standardy kryptografických modulů

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

6.2.2 Soukromý klíč pod kontrolou více osoba (m z n)

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

6.2.3 Úschova soukromého klíče

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

6.2.4 Zálohování soukromého klíče

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

6.2.5 Uchovávání soukromého klíče

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

6.2.6 Transfer dat soukromého klíče do nebo z kryptografického modulu

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

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

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

O provedeném transferu je vždy pořízen písemný záznam.

6.2.7 Uložení soukromého klíče v kryptografickém modulu

Soukromé klíče certifikačních autorit a jejich OCSP respondérů jsou uloženy v kryptografickém modulu, splňujícím požadavky standardu FIPS PUB 140-2 úroveň 3.

6.2.8 Postup aktivace soukromého klíče

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

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

6.2.9 Postup deaktivace soukromého klíče

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

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

6.2.10 Postup ničení soukromého klíče

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

6.2.11 Hodnocení kryptografických modulů

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

6.3 Další aspekty správy párových dat

6.3.1 Uchovávání veřejných klíčů

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

6.3.2 Doba funkčnosti certifikátu a doba použitelnosti párových dat

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

6.4 Aktivační data

6.4.1 Generování a instalace aktivačních dat

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

6.4.2 Ochrana aktivačních dat

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

6.4.3 Ostatní aspekty aktivačních dat

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

6.5 Řízení počítačové bezpečnosti

6.5.1 Specifické technické požadavky na počítačovou bezpečnost

Úroveň bezpečnosti použitých komponent pro poskytování certifikačních služeb je definována v technických standardech nebo normách. Role přímo se podílející na vydání Certifikátů podle této CP používají dvoufaktorovou autentizaci.

6.5.2 Hodnocení počítačové bezpečnosti

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

- CWA 14167-1 - Security Requirements for Trustworthy Systems Managing Certificates for Electronic Signatures - Part 1: System Security Requirements /Bezpečnostní požadavky na důvěryhodné systémy spravující certifikáty pro elektronický podpis - část 1: Požadavky na bezpečnost systémů.
- ETSI TS 102 042 Electronic Signatures and Infrastructures (ESI); Policy requirements for certification authorities issuing public key certificates.
- ČSN ETSI EN 319 401 Elektronické podpisy a infrastruktury (ESI) - Obecné požadavky politiky na poskytovatele důvěryhodných služeb podporující elektronické podpisy.
- ETSI EN 319 401 Electronic Signatures and Infrastructures (ESI); General Policy Requirements for Trust Service Providers.
- ETSI EN 319 403 Electronic Signatures and Infrastructures (ESI); Trust Service Provider Conformity Assessment - Requirements for conformity assessment bodies assessing Trust Service Providers.
- ETSI EN 319 411-1 Electronic Signatures and Infrastructures (ESI); Policy and security requirements for Trust Service Providers issuing certificates; Part 1: General requirements.
- 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 EN 319 411-3 Electronic Signatures and Infrastructures (ESI); Policy and security requirements for Trust Service Providers issuing certificates; Part 3: Policy requirements for Certification Authorities issuing public key certificates.
- ETSI TS 119 312 Electronic Signatures and Infrastructures (ESI); Cryptographic Suites.
- ISO/IEC 17021 Conformity assessment -- Requirements for bodies providing audit and certification of management systems.
- ISO/IEC 17065 Conformity assessment -- Requirements for bodies certifying products, processes and services.

Činnost Autority se dále řídí požadavky technických norem a standardů:

- FIPS PUB 140-2 Requirements for Cryptographic Modules.
- ISO 3166-1 Codes for the representation of names of countries and their subdivisions - Part 1: Country codes.

- ITU-T - X.501 Information technology – Open Systems Interconnection – The Directory: Models.
- ITU-T - X.509 Information technology – Open Systems Interconnection – The Directory: Public-key and attribute certificate frameworks.
- ITU-T - X.520 Information technology – Open Systems Interconnection – The Directory: Selected attribute types.
- RSA Laboratories - PKCS#10: Certification Request Syntax Standard.
- RFC 2560 X.509 Internet Public Key Infrastructure Online Certificate Status Protocol - OCSP.
- RFC 3647 Internet X.509 Public Key Infrastructure Certificate Policy and Certification Practices Framework.
- RFC 5019 The Lightweight Online Certificate Status Protocol (OCSP) Profile for High-Volume Environments.
- RFC 5280 Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile.
- RFC 822 Standard for the Format of Arpa Internet Messages.
- ETSI EN 319 412-1 Electronic Signatures and Infrastructures (ESI); Certificate Profiles; Part 1: Overview and common data structures.
- ETSI EN 319 412-2 Electronic Signatures and Infrastructures (ESI); Certificate Profiles; Part 2: Certificate profile for certificates issued to natural persons.
- ETSI EN 319 412-5 Electronic Signatures and Infrastructures (ESI); Certificate Profiles; Part 5: QCStatements.

6.6 Technické řízení životního cyklu

6.6.1 Řízení vývoje systému

Při vývoji systému je postupováno v souladu s interní dokumentací.

6.6.2 Řízení správy bezpečnosti

Kontrola řízení bezpečnosti informací, včetně kontroly souladu se standardy, je prováděna formou interních a externích auditů systému řízení bezpečnosti informací (ISMS).

Bezpečnost informací se v I.CA řídí těmito normami:

- 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.

6.6.3 Řízení bezpečnosti životního cyklu

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

- vybudování - stanovení rozsahu a hranic, kterých se řízení bezpečnosti informací týká, určení bezpečnostní politiky, plánů a výběr bezpečnostních opatření v závislosti na vyhodnocených rizicích, to vše v souladu s celkovou bezpečnostní politikou,
- implementace a provoz - účelné a systematické prosazení vybraných bezpečnostních opatření,
- monitorování a přehodnocování - zajištění zpětné vazby, pravidelné sledování a hodnocení úspěšných i nedostatečných stránek řízení bezpečnosti informací, předávání poznatků vedení společnosti k posouzení,
- údržba a zlepšování - provádění opatření k nápravě a zlepšování, na základě rozhodnutí vedení organizace.

6.7 Řízení bezpečnosti sítě

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 Autority je vedena šifrovaně.

6.8 Označování časovými razítky

Řešení je uvedeno v kapitole 5.5.5.

7 PROFILY CERTIFIKÁTU, CRL A OCSP

7.1 Profil certifikátu

tab. 4 - Základní pole Certifikátu

Pole	Obsah
Version	v3 (0x2)
SerialNumber	jedinečné sériové číslo Certifikátu
SignatureAlgorithm	sha256withRSAEncryption
Issuer	vydavatel Certifikátu (Autorita)
Validity	
notBefore	počátek platnosti Certifikátu (UTC)
notAfter	konec platnosti Certifikátu (UTC)
Subject	viz tab. 5
SubjectPublicKeyInfo	
algorithm	rsaEncryption
subjectPublicKey	minimálně 2048 bitů
Extensions	viz tab. 6
Signature	elektronický podpis Autority

tab. 5 - Pole Subject

Všechny položky[1] pole Subject jsou převzaty ze žádosti o Certifikát s výjimkou položek vytvořených Autoritou. Povinné položky musí být v žádosti obsaženy.

Položka	Poznámka
countryName*	povinná, jediný výskyt, kód státu (ISO 3166)
givenName	fyzická osoba: povinná, jediný výskyt Organizace: nesmí být uvedena
surName	fyzická osoba: povinná, jediný výskyt Organizace: nesmí být uvedena
pseudonym	fyzická osoba: povinná v případě neuvedení položek givenName a surName, jediný výskyt Organizace: nesmí být uvedena
serialNumber (1. výskyt)	povinná, jednoznačná identifikace držitele soukromého klíče

[1] I.CA si vyhrazuje právo doplnit další položky, vyžadované aktualizacemi standardů ETSI, nebo třetími stranami (např. společnost Microsoft).

	v systému Autority (ICA – xxxxxxxx): ▪ v případě prvotního Certifikátu vytváří Autorita, ▪ v případě následného Certifikátu převzato ze žádosti
serialNumber (2. výskyt)	fyzická osoba: volitelná, jedna ze tří možností: ▪ IDCss-nnnnnnnn, ▪ PASss-nnnnnnnn, ▪ PNOss-yyyyyyyy (pouze pro občany Slovenské republiky), kde ss je kód státu (viz položka countryName), nnnnnnnn je číslo dokladu, yyyyyyyy je rodné číslo Organizace, OSVČ: nesmí být uvedena
organizationIdentifier	Organizace: volitelná, jedna ze tří možností: ▪ NTRss-id, ▪ VATss-id (pouze pro Organizace Slovenské republiky), ▪ SZ:ss-id (pouze pro Organizace Slovenské republiky), kde ss je kód státu, id je identifikační číslo fyzická osoba: nesmí být uvedena
commonName	fyzická osoba - povinná, jediný výskyt: ▪ v případě uvedení položek givenName a surName složeno z titulu před jménem givenName surName titulu za jménem ▪ v případě uvedení položky pseudonym složeno z jejího obsahu a doplněno řetězcem „ - PSEUDONYM“ Organizace: povinná, obsah musí být totožný s obsahem položky organizationName pro účely autentizace v rámci Slovenské republiky uvedena řetězcem „AUT “
initials	fyzická osoba: volitelná, jediný výskyt Organizace: nesmí být uvedena
emailAddress	v prvotním Certifikátu nesmí být uvedena
name	v prvotním Certifikátu nesmí být uvedena
generationQualifier	fyzická osoba: volitelná, jediný výskyt Organizace: nesmí být uvedena
organizationName	OSVČ, Organizace, zaměstnanec: povinná, jediný výskyt ostatní fyzické osoby: nesmí být uvedena
organizationalUnitName	OSVČ, Organizace, zaměstnanec: volitelná, možný vícenásobný výskyt ostatní fyzické osoby: nesmí být uvedena

title	OSVČ, zaměstnanec: volitelná, možný vícenásobný výskyt ostatní fyzické osoby, Organizace: nesmí být uvedena
stateOrProvinceName*	volitelná, jediný výskyt
localityName*	volitelná, jediný výskyt prvotní Certifikát: pokud bude uvedena musí být také streetAddress a postalCode.
streetAddress*	volitelná, jediný výskyt prvotní Certifikát: pokud bude uvedena musí být také localityName a postalCode.
postalCode*	volitelná, jediný výskyt prvotní Certifikát: pokud bude uvedena, musí být také localityName a streetAddress.

* položky countryName, stateOrProvinceName, localityName, streetAddress a postalCode se v případě Organizace vztahují k adrese sídla, nebo v případě fyzických osob k adrese jejich trvalého pobytu

7.1.1 Číslo verze

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

7.1.2 Rozšiřující položky v certifikátu

tab. 6 - Rozšiřují položky[2] Certifikátu

Položka	Obsah	Poznámka
CertificatePolicies		nekritická, vytváří Autorita
.PolicyInformation(1)		
policyIdentifier	viz kapitola 1.2	
[1.1]policyQualifiers PolicyQualifierInfo(1) cPSuri	http://www.ica.cz	
.PolicyInformation(2)		
policyIdentifier	jedna ze dvou možností: ▪ NCP: 0.4.0.2042.1.1, nebo ▪ NCP+: 0.4.0.2042.1.2 (pouze v případě soukromého klíče na bezpečném uživatelském	

[2] I.CA si vyhrazuje právo doplnit další položky, vyžadované aktualizacemi standardů ETSI, nebo třetími stranami (např. společnost Microsoft).

	zařízení)	
CRLDistributionPoints	http://scrldp1.ica.cz/pcaRR*_rsa.crl http://scrldp2.ica.cz/pcaRR_rsa.crl	nekritická, vytváří Autorita
authorityInformationAccess		nekritická, vytváří Autorita
id-ad-ocsp	http://ocsp.ica.cz/pcaRR_rsa	
id-ad-caIssuers	RSA:http://s.ica.cz/pcaRR_rsa.cer	
BasicConstraints		nekritická, vytváří Autorita
cA	False	
KeyUsage		kritická
	produkt TWINS: ▪ digitalSignature, ▪ dataEncipherment, ▪ keyEncipherment	vytváří Autorita
	na základě obsahu žádosti o Certifikát jakákoli kombinace z možností[3]: ▪ digitalSignature, ▪ nonRepudiation, ▪ keyEncipherment, ▪ dataEncipherment	v případě neuvedení položky KeyUsage v žádosti o Certifikát, vytváří Autorita (všechny čtyři možnosti, tedy digitalSignature, nonRepudiation, keyEncipherment, dataEncipherment)
ExtendedKeyUsage	na základě obsahu žádosti o Certifikát jakákoli kombinace z možností: ▪ id-kp-clientAuth, ▪ id-kp-emailProtection, ▪ Microsoft SmartCard Logon	nekritická
SubjectKeyIdentifier	hash veřejného klíče (subjectPublicKey) v Certifikátu (viz tab. 4)	nekritická, vytváří Autorita
AuthorityKeyIdentifier		nekritická, vytváří Autorita
KeyIdentifier	hash veřejného klíče Autority	

[3] V případě využití Certifikátu pouze pro elektronický podpis jedna z možností: nonRepudiation, nebo digitalSignature a nonRepudiation, nebo digitalSignature, nonRepudiation a keyEncipherment.

SubjectAlternativeName		nekritická
otherName (1. výskyt)	ICA_OID (1.3.6.1.4.1.23624.4.6): xxxxxxxx**	vytváří Autorita
otherName (2. výskyt)	Microsoft_OID (1.2.840.113556.1.4.656): UPN	volitelná, při uvedení v žádosti o Certifikát
rfc822Name	e-mail adresa	možný vícenásobný výskyt, volitelná, při uvedení emailové adresy v žádosti o Certifikát
nsComment	výrobní číslo bezpečného uživatelského zařízení	nekritická, vytváří Autorita v případě uložení soukromého klíče na bezpečném uživatelském zařízení
ICA_OID: 1.3.6.1.4.1.23624.4.3	číslo žádosti o Certifikát	nekritická, vytváří Autorita v případě produktu TWINS

* RR - poslední dvě číslice roku vydání certifikátu Autority

** viz tab. 5

7.1.3 Objektové identifikátory algoritmů

V procesu poskytování certifikačních služeb jsou využívány algoritmy v souladu s příslušnými technickými standardy.

7.1.4 Tvary jmen

V souladu s požadavkem RFC 5280 se obsah pole Issuer ve vydaném Certifikátu shoduje s polem Subject v certifikátu Autority. Déle platí ustanovení kapitoly 3.1.

Informace o držiteli Certifikátu, resp. držiteli soukromého klíče jsou uvedeny v poli Subject (viz tab. 5) a rozšiřující položce Certifikátu SubjectAlternativeName (viz tab. 6).

7.1.5 Omezení jmen

Jména a názvy uvedené v Certifikátu musí odpovídat údajům v dokumentech předkládaných v procesu registrace.

7.1.6 Objektový identifikátor certifikační politiky

Viz rozšiřující položky Certifikátu v kapitole 7.1.2 výše.

7.1.7 Použití položky Policy Constrainsts

Není relevantní pro tento dokument.

7.1.8 Syntaxe a sémantika kvalifikátorů politiky

Viz rozšiřující položky Certifikátu v kapitole 7.1.2 výše.

7.1.9 Zpracování sémantiky 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)
SignatureAlgorithm	sha256withRSAEncryption
Issuer	vydavatel CRL (Autorita)
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
Signature	elektronický podpis vydavatele CRL (Autority)

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, proto I.CA nepoužívá	nekritická
crlExtensions		
AuthorityKeyIdentifier		
KeyIdentifier	hash veřejného klíče vydavatele CRL	nekritická

	(Autority)	
CRLNumber	jedinečné číslo vydávaného CRL	nekritická

7.3 Profil OCSP

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

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

Bližší podrobnosti jsou uvedeny v odpovídající certifikační prováděcí směrnici.

7.3.1 Číslo verze

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

7.3.2 Rozšiřující položky OCSP

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

8 HODNOCENÍ SHODY A JINÁ HODNOCENÍ

8.1 Periodicita nebo okolnosti hodnocení

Periodicita hodnocení systému řízení bezpečnosti informací vychází z požadavků analogických požadavkům platné legislativy týkající se elektronického podpisu.

Periodicita hodnocení pro program Microsoft Trusted Root Certificate Program, včetně okolností pro provádění hodnocení, je striktně dána požadavky společnosti Microsoft.

8.2 Identita a kvalifikace hodnotitele

Kvalifikace externího auditora provádějícího hodnocení podle relevantních technických standardů je dána těmito standardy.

Požadavky na orgán provádějící hodnocení podle standardů ETSI (pro program Microsoft Trusted Root Certificate Program) jsou popsány ve standardu ETSI EN 319 403, resp. ve standardech odkazovaných.

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

Hodnocené oblasti jsou konkretizovány technickými standardy, podle 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 do doby, než budou tyto nedostatky odstraněny.

8.6 Sdělování výsledků hodnocení

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

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

Sdělování výsledků hodnocení taktéž podléhá požadavkům příslušných standardů, podle kterých je hodnocení prováděno.

9 OSTATNÍ OBCHODNÍ A PRÁVNÍ ZÁLEŽITOSTI

9.1 Poplatky

9.1.1 Poplatky za vydání nebo obnovení certifikátu

Poplatky za vydání Certifikátu jsou uvedeny v aktuálním ceníku služeb, který je k dispozici na internetové informační adrese I.CA nebo v případě uzavřeného smluvního vztahu mezi Organizací a I.CA v této smlouvě. Služba obnovení Certifikátu není poskytována.

9.1.2 Poplatky za přístup k certifikátu

Přístup elektronickou cestou k Certifikátům vydaným podle této CP I.CA nezpoplatňuje.

9.1.3 Zneplatnění nebo přístup k informaci o stavu certifikátu

Zneplatnění nebo přístup elektronickou cestou k informacím o zneplatněných certifikátech (CRL) a o stavech certifikátů (OCSP), I.CA v případě Certifikátů vydaných podle této CP nezpoplatňuje.

9.1.4 Poplatky za další služby

Není relevantní pro tento dokument.

9.1.5 Postup při refundování

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

Společnost První certifikační autorita, a.s., prohlašuje, že má k dispozici dostatečné finanční zdroje a jiná 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 Důvěrnost obchodních informací

9.3.1 Rozsah důvěrných informací

Důvěrnými informacemi I.CA jsou veškeré informace, které nejsou označeny jako veřejné a nejsou zveřejňovány způsobem uvedeným v kapitole 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 důvěrných informací

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

9.3.3 Odpovědnost za ochranu důvěrných informací

Žádný zaměstnanec I.CA, který přijde do styku s 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 Informace považované za osobní údaje

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

Zaměstnanci I.CA, případně subjekty definované platnou legislativou přicházející 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 Informace nepovažované za osobní údaje

Za citlivé údaje nejsou považovány údaje, které nejsou citlivými osobními údaji podle ZOOÚ.

9.4.4 Odpovědnost za ochranu osobních údajů

Za ochranu osobních údajů je odpovědný ředitel I.CA.

9.4.5 Oznámení o používání osobních údajů a souhlas s jejich zpracováním

Problematika oznamování o používání důvěrných informací a souhlasu s jejich zpracováním v I.CA řešena v souladu s požadavky příslušných zákonných norem.

9.4.6 Poskytování osobních údajů pro soudní či správní účely

Poskytování osobních údajů 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 podle požadavků příslušné legislativy.

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 certifikačních autorit pouze pro vydávání certifikátů koncovým uživatelům (vyjma kořenové CA), vydávání seznamů zneplatněných certifikátů a k vydávání certifikátů OCSP respondérů,
- použije soukromé klíče OCSP respondérů certifikačních autorit pouze v procesech poskytování odpovědí na stav certifikátu,
- Certifikáty vydávané koncovým uživatelům splňují náležitosti požadované relevantními technickými standardy,
- zneplatní vydané Certifikáty, pokud byla žádost o ukončení jejich platnosti podána způsobem definovaným v této CP.

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

- Osoba, resp. držitel Certifikátu neporušili povinnosti plynoucí jim ze smlouvy o poskytování certifikační služby a této CP,
- spoléhající se strana neporušila povinnosti této CP.

Osoba, resp. držitel Certifikátu vydaného podle této CP uplatňují záruku vždy u RA, která zpracovala jejich žádost o vydání tohoto Certifikátu.

I.CA vyjadřuje a poskytuje Osobám, držitelům Certifikátů a veškerým spoléhajícím se stranám záruky, že při vydávání Certifikátů a v průběhu doby jejich platnosti bude při jejich správě vyhovovat své CP a CPS.

Záruky zahrnují:

- kontrolu práva žádat o Certifikát,
- ověření informací uváděných v žádosti o vydání Certifikátu, včetně kontroly naplnění položek, obsažených v žádosti o Certifikát (formát PKCS#10) a identity,
- že smlouva o vydání Certifikátu odpovídá platným právním normám,
- že v režimu 24x7 je udržováno úložiště informací o stavu Certifikátu,
- že Certifikát může být zneplatněn z důvodů uvedených v této CP.

9.6.2 Zastupování a záruky RA

Určená RA:

- přejímá závazek za správnost jí poskytovaných služeb,
- nevyřídí kladně žádost, pokud se nepodařilo ověřit některou z položek žádosti, Osoba, resp. držitel Certifikátu odmítají potřebné údaje sdělit, nebo nejsou oprávněni k podání žádosti o Certifikát,
- v případě osobního podání žádosti o zneplatnění Certifikátu odpovídá za včasné předání této žádostí k vyřízení na pracoviště Autority,
- odpovídá za vyřizování připomínek a stížností.

9.6.3 Zastupování a záruky držitele certifikátu, resp. držitele soukromého klíče

Ve smlouvě mezi I.CA a Osobou, resp. držitelem Certifikátu je uvedeno, že jsou povinni řídit se ustanoveními této CP.

9.6.4 Zastupování a záruky spoléhajících se stran

Spoléhající se strany postupují podle této CP.

9.6.5 Zastupování a záruky ostatních zúčastněných subjektů

Není relevantní pro tento dokument.

9.7 Zřeknutí se záruk

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

9.8 Omezení odpovědnosti

Společnost První certifikační autorita, a.s., neodpovídá za škody způsobené spoléhajícím se stranám v případech, kdy nesplnily povinnosti, požadované touto CP, podle které byl

Certifikát vydán. Dále neodpovídá za škody vzniklé v důsledku porušení závazků I.CA z důvodu vyšší moci.

9.9 Záruky a odškodnění

Pro poskytování certifikačních služeb platí relevantní ustanovení platné legislativy týkající se vztahů mezi poskytovatelem spotřebitelem a dále takové záruky, které byly sjednány mezi společností První certifikační autorita, a.s., a žadatelem o certifikační službu. Smlouva musí být vždy v elektronické nebo listinné formě.

Společnost První certifikační autorita, a.s.:

- se zavazuje, že splní veškeré povinnosti definované uzavřenou smlouvou i příslušnými politikami,
- poskytuje výše uvedené záruky po celou dobu platnosti smlouvy o poskytování certifikačních služeb,
- souhlasí s tím, že dodavatelé aplikačního programového vybavení, se kterými má platnou smlouvu na distribuci kořenového certifikátu, nepřebírají žádné závazky nebo odpovědnosti, s výjimkou případů, kdy poškození či ztráta byly přímo způsobeny programovým vybavením tohoto dodavatele,
- další možné náhrady škody vycházejí z ustanovení příslušné legislativy a o jejich výši může rozhodnout soud.

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

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

Reklamaci je možné podat těmito způsoby:

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

Reklamující osoba (Osoba, resp. držitel Certifikátu nebo spoléhající se strana) je povinna uvést:

- co nejvýstižnější popis závady,
- sériové číslo reklamovaného produktu,
- požadovaný způsob vyřízení reklamace.

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

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

Nový Certifikát bude držiteli poskytnut zdarma v následujících případech:

- existuje-li důvodné podezření, že došlo ke kompromitaci soukromého klíče certifikační autority,
- na základě rozhodnutí členů vedení I.CA s přihlédnutím ke konkrétním okolnostem,
- v případě, že Autorita při příjmu žádosti o vydání Certifikátu zjistí, že existuje jiný Certifikát s duplicitním veřejným klíčem.

9.10 Doba platnosti, ukončení platnosti

9.10.1 Doba platnosti

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

9.10.2 Ukončení platnosti

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

9.10.3 Důsledky ukončení a přetrvání platnosti

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

9.11 Individuální upozorňování a komunikace se zúčastněnými subjekty

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

Komunikovat s I.CA lze taktéž způsoby uvedenými na internetové informační adrese.

9.12 Novelizace

9.12.1 Postup při novelizaci

Postup je realizován řízeným procesem popsaným v interním dokumentu.

9.12.2 Postup a periodicita oznamování

Vydání nové verze CP je vždy oznámeno formou zveřejňování informací.

9.12.3 Okolnosti, při kterých musí být změněn OID

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

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

9.13 Ustanovení o řešení sporů

V případě, že Osoba, resp. držitel Certifikátu nebo spoléhající se strana nesouhlasí s návrhem na vyřešení sporu, mohou použít následující stupně odvolání:

- odpovědný pracovník RA,
- odpovědný pracovník I.CA (nutné elektronické nebo listinné podání),
- ředitel I.CA (nutné elektronické nebo listinné podání).

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

9.14 Rozhodné právo

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

9.15 Shoda s platnými právními předpisy

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

9.16 Různá ustanovení

9.16.1 Rámcová dohoda

Není relevantní pro tento dokument.

9.16.2 Postoupení práv

Není relevantní pro tento dokument.

9.16.3 Oddělitelnost ustanovení

Pokud soud, nebo veřejnoprávní orgán, v jehož jurisdikci jsou aktivity pokryté touto CP, stanoví, že provádění některého povinného požadavku je nelegální, potom je rozsah tohoto požadavku omezen tak, aby požadavek byl platný a legální.

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, popř. výpadku komunikačního spojení.

9.17 Další ustanovení

Není relevantní pro tento dokument.

10 ZÁVĚREČNÁ USTANOVENÍ

Tato certifikační politika vydaná společností První certifikační autorita, a.s., nabývá platnosti a účinnosti dnem 29.03.2016.