První certifikační autorita, a.s.

Certifikační prováděcí směrnice

(algoritmus RSA)

Verze 1.3

OBSAH

tab. 1 - Vývoj dokumentu

Verze	Datum vydání	Schválil	Poznámka
1.0	15.07.2015	Ředitel společnosti První certifikační autorita, a.s.	První vydání.
1.1	02.11.2015	Ředitel společnosti První certifikační autorita, a.s.	Aktualizace OID certifikačních politik (TSA, OCSP).
1.2	29.03.2016	Ředitel společnosti První certifikační autorita, a.s.	Aktualizace OID certifikační politiky SSL.
1.3	06.04.2016	Ředitel společnosti První certifikační autorita, a.s.	Rozšíření podporovaných CP.

1 ÚVOD

Kořenová kvalifikovaná certifikační autorita (algoritmus RSA) společnosti První certifikační autorita, a.s., vydává v hierarchické dvoustupňové struktuře certifikačních autorit, v souladu s platnou legislativou a s požadavky technických standardů, kvalifikovaný systémový certifikát s algoritmem RSA kořenové certifikační autority, certifikáty s algoritmem RSA pro vydávající certifikační autority a certifikát svého OCSP respondéru s algoritmem RSA. Tyto vydávající certifikační autority potom vydávají certifikáty pro TSS systému TSA, certifikáty svých OCSP respondérů, pokud je služba OCSP poskytována a certifikáty koncovým uživatelům.

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 prováděcí směrnice (algoritmus RSA)**, dále též CPS, vypracovaný společností První certifikační autorita, a. s., (dále též I.CA) 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). Týká se certifikačních politik uvedených v kap. 1.2.

Dokument je rozdělen do devíti základních kapitol, jejichž stručný popis je uveden v následujícím seznamu:

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

- Kapitola 9 zahrnuje problematiku obchodní a právní.

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

1.2 Název a jednoznačné určení dokumentu

Název tohoto dokumentu: Certifikační prováděcí směrnice (algoritmus RSA)

OID dokumentu: není přiřazeno

Tato CPS se vztahuje k následujícím CP:

OID	CP
1.3.6.1.4.1.23624.10.1.10.1.0	Certifikační politika kořenové kvalifikované certifikační autority (algoritmus RSA)
1.3.1.6.4.1.23624.10.1.72.1.1	Certifikační politika vydávání SSL certifikátů (algoritmus RSA), verze 1.10
1.3.6.1.4.1.23624.10.1.80.1.1	Certifikační politika vydávání certifikátů OCSP respondérů (algoritmus RSA), verze 1.10
1.3.6.1.4.1.23624.10.1.32.1.1	Certifikační politika vydávání certifikátů pro systém TSA (algoritmus RSA), verze 1.1
1.3.6.1.4.1.23624.10.1.30.1.0	Certifikační politika vydávání kvalifikovaných certifikátů pro elektronické podpisy (algoritmus RSA) , verze 1.00
1.3.6.1.4.1.23624.10.1.33.1.0	Certifikační politika vydávání systémových certifikátů (algoritmus RSA), verze 1.00
1.3.6.1.4.1.23624.10.1.70.1.0	Certifikační politika vydávání komerčních certifikátů (algoritmus RSA), verze 1.00
1.3.6.1.4.1.23624.10.1.71.1.0	Certifikační politika vydávání technologických (komerčních serverových) certifikátů (algoritmus RSA), verze 1.00
1.3.6.1.4.1.23624.10.1.73.1.0	Certifikační politika vydávání komerčních certifikátů pro elektronické pečetě (algoritmus RSA), verze 1.00
1.3.6.1.4.1.23624.10.1.90.1.0	Certifikační politika vydávání kvalifikovaných certifikátů SK pro elektronické podpisy (algoritmus RSA), verze 1.00
1.3.6.1.4.1.23624.10.1.91.1.0	Certifikační politika vydávání kvalifikovaných systémových certifikátů SK (algoritmus RSA), verze 1.00
1.3.6.1.4.1.23624.10.1.92.1.0	Certifikační politika vydávání kvalifikovaných mandátních certifikátů SK (algoritmus RSA), verze 1.00

1.3 Participující subjekty

1.3.1 Certifikační autority (dále “CA”)

1.3.1.1 Kořenová certifikační autorita

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

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

1.3.1.2 Vydávající certifikační autority

Veřejné certifikační autority, provozované společností První certifikační autorita, a.s., poskytující certifikační služby koncovým uživatelům.

1.3.2 Registrační autority (dále “RA”)

Registrační autority, využívané v procesech životního cyklu certifikátů, vydávaných koncovým uživatelům. Tyto RA mohou být stacionární nebo mobilní.

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

1.3.3.1 Certifikáty poskytovatele (I.CA)

Certifikáty jsou vydávány výhradně pro certifikační autority, jejich OCSP respondéry a pro TSS systému TSA, vše provozované I.CA. Oprávněným žadatelem a následně držitelem certifikátů je I.CA jako právnická osoba.

1.3.3.2 Certifikáty koncových uživatelů

Certifikáty jsou vydávány koncovým uživatelům, využívajícím certifikační služby I.CA.

1.3.4 Spoléhající se strany

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

1.3.5 Jiné participující subjekty

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

1.4 Použití certifikátu

1.4.1 Přípustné použití certifikátu

Certifikáty kořenové CA smějí být používány výhradně pro ověřování jí vydaných certifikátů, seznamů jí zneplatněných certifikátů (CRL, resp. ARL) a OCSP odpovědí vydaných jejím OCSP respondérem.

Certifikáty vydávajících certifikačních autorit smějí být používány výhradně pro ověřování certifikátů a seznamů zneplatněných certifikátů (CRL) vydaných těmito vydávajícími certifikačními autoritami a OCSP odpovědí vydaných OCSP respondéry (jsou-li implementovány) těchto vydávajících certifikačních autorit.

Certifikáty TSS systému TSA smějí být používány výhradně pro ověřování časových razítek vydaných těmito TSS.

Certifikáty koncových uživatelů smějí být používány obecně v procesech PKI, tedy ověřování elektronických podpisů /elektronických značek/ elektronických pečetí, identifikace, autentizace a šifrování.

1.4.2 Omezení použití certifikátu

Certifikáty vydávané v souladu s konkrétní CP nesmějí být používány v rozporu s použitím popsaným v této CP a dále pro jakékoliv nelegální účely.

1.5 Správa politiky

1.5.1 Organizace spravující certifikační politiku nebo certifikační prováděcí směrnici

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

1.5.2 Kontaktní osoba organizace spravující certifikační politiku nebo certifikační prováděcí směrnici

Kontaktní osoba společnosti První certifikační autorita, a.s., v souvislosti touto CPS a odpovídajícími certifikačními politikami, je uvedena na internetové adrese (viz kap. 2.2).

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

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

1.5.4 Postupy při schvalování souladu podle bodu 1.5.3

V případě, že je potřebné provést změny v této CPS, nebo některé certifikační politice 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 /CPS předchází její schválení ředitelem společnosti První certifikační autorita, a.s. Dále platí požadavky kap. 9.12.

1.6 Přehled použitých pojmů a zkratek

tab. 2 - Pojmy

Pojem	Vysvětlení
bit	z anglického *binary digit* - číslice dvojkové soustavy - základní a současně nejmenší jednotka informace v číslicové technice
Certifikát	v tomto dokumentu kvalifikovaný certifikát pro elektronický podpis
dozorový orgán	orgán dozoru nad dodržováním legislativy týkající se elektronického podpisu
dvoufaktorová autentizace	autentizace využívající dvou ze tří faktorů - něco vím (heslo), něco mám (např. čipová karta, hardwarový token) nebo něco jsem (otisky prstů, snímání oční sítnice či duhovky)
elektronická pečeť	v tomto dokumentu elektronická pečeť, resp. zaručená elektronická pečeť dle platné legislativy týkající se elektronického podpisu
elektronická značka	v tomto dokumentu elektronická značka dle platné legislativy týkající se elektronického podpisu
elektronický podpis	v tomto dokumentu elektronický podpis, resp. zaručený elektronický podpis, resp. uznávaný elektronický podpis, resp. kvalifikovaný elektronický podpis dle platné legislativy týkající se elektronického podpisu
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
kvalifikovaný certifikát, kvalifikovaný systémový certifikát, nadřízený kvalifikovaný systémový certifikát, systémový certifikát	certifikát, který má náležitosti podle platné legislativy týkající se elektronického podpisu
kvalifikovaný prostředek pro vytváření elektronických podpisů	prostředek pro vytváření elektronických podpisů, který splňuje požadavky stanovené v příloze II eIDAS
legislativa týkající se elektronického podpisu	aktuálně platná legislativa České republika a Slovenské republiky vztahující se k elektronickému podpisu a nařízení

	eIDAS
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	fyzická osoba, která drží prostředek pro vytváření elektronických podpisů
vydávající, podřízená CA	pro účely tohoto dokumentu CA vydávající certifikáty koncovým uživatelům
prostředek pro vytváření elektronických podpisů	v tomto dokumentu - technické zařízení nebo programové vybavení, které se používá k vytváření elektronických podpisů, resp. konfigurované programové vybavení nebo technické zařízení, které se používá k vytváření elektronických podpisů;
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 pro vytváření elektronické podpisu
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 pro ověřování elektronické podpisu
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
EU	Evropská unie
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

MPSV	Ministerstvo práce a sociálních věcí
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
TSA	Time Stamping Authority, autorita časových razítek, obsahující více serverů, vydávajících časová razítka, kdy každý z nich disponuje jedinečným soukromým klíčem a tedy i kvalifikovaným systémovým certifikátem
TSS	Time Stamp Server, server vytvářející časová razítka
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, ▪ zákon Slovenské republiky č. 122/2013 Z.z. o ochrane osobných údajov a o zmene a doplnení niektorých zákonov

2 ODPOVĚDNOST ZA ZVEŘEJŇOVÁNÍ A ÚLOŽIŠTĚ INFORMACÍ A DOKUMENTACE

2.1 Úložiště informací a dokumentace

Společnost První certifikační autorita, a.s., zřizuje a provozuje úložiště informací a dokumentace.

2.2 Zveřejňování informací a dokumentace

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

- 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.

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

- sídla registračních autorit,
- elektronická poštovní adresa info@ica.cz.

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

Na výše uvedené internetové adrese lze získat informace o:

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

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

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

2.3 Periodicita zveřejňování informací

Viz kapitola 2.3 konkrétní CP.

2.4 Řízení přístupu k jednotlivým typům úložišť

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

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

- „Operátor CA“,
- „Směrnice pro pracovníky RA I.CA“,
- „Řízení bezpečnosti informací“,
- „Příručka administrátora“,
- „Bezpečnostní incidenty“,
- „HSM/Private Server“,
- „Správa TSS“,
- „Dokumenty agendy certifikačních služeb“,
- „Dílčí spisový a skartační řád pro agendy certifikačních služeb“,
- „Dílčí spisový a skartační plán pro agendy certifikačních služeb“.

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. Konkrétní obsah jmen je definován v konkrétní CP.

3.1.3 Anonymita a používání pseudonymu

Viz kapitola 3.1.3 konkrétní CP.

3.1.4 Pravidla pro interpretaci různých forem jmen

Údaje uváděné v procesu žádosti o certifikát se do vydávaných certifikátů přenášejí ve tvaru, ve kterém jsou uvedeny v předkládaných dokumentech.

3.1.5 Jedinečnost jmen

Uvedeno v konkrétní politice.

3.1.6 Obchodní značky

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

3.2 Počáteční ověření identity

Postup ověřování identity je uveden v konkrétní CP a dále upřesněn v interním dokumentu:

- „Směrnice pro pracovníky RA I.CA“.

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

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

3.2.2 Ověřování identity právnické osoby nebo organizační složky státu

Identita se prokazuje výpisem z Obchodního rejstříku. Blíže je postup popsán v interním dokumentu:

- „Směrnice pro pracovníky RA I.CA“.

3.2.3 Ověřování identity fyzické osoby

Postup je popsán v konkrétní CP a dále v interním dokumentu:

- „Směrnice pro pracovníky RA I.CA“.

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

Neověřované informace jsou vždy uvedeny v konkrétní CP..

3.2.5 Ověřování specifických práv

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 certifikovaném zařízení typu SSCD/QESCD lze do Certifikátu vložit pouze tehdy, byla-li tato skutečnost v procesu vydání Certifikátu pro tuto žádost ověřena.

Postup ověřování dalších specifických práv je opsán v konkrétní CP.

3.2.6 Kritéria pro interoperabilitu

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

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

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

Vždy je nutné vydat nový certifikát s novým veřejným klíčem. Konkrétní požadavky jsou uvedeny v konkrétní CP.

3.3.1.1 Certifikáty poskytovatele (I.CA)

Jedná se o vydání prvotního certifikátu, kdy platí stejné požadavky, jako v případě počátečního ověření identity.

3.3.1.2 Certifikáty koncových uživatelů

V případě SSL certifikátů se vždy jedná o vydání prvotního certifikátu, kdy platí stejné požadavky, jako v případě počátečního ověření identity.

Pro ostatní typy certifikátů lze vydat tzv. následný certifikát, kdy je standardní žádost o certifikát (s novým veřejným klíčem) předávná ke zpracování elektronicky podepsána /označena/opatřena elektronickou pečetí vytvořenou soukromým klíčem, náležícím veřejnému klíči v platném certifikátu, ke kterému je vydáván tento následný certifikát. V tomto případě není vyžadována fyzická přítomnost žadatele o certifikát na RA a žadatel o certifikát tímto podpisem /značkou/ pečetí potvrzuje, že údaje o subjektu nebyly změněny.

3.3.2 Identifikace a autentizace při výměně párových dat po zneplatnění certifikátu

I.CA nepodporuje výměnu párových dat již zneplatněného certifikátu. Jediný způsob, jak získat nový certifikát, je získání nového certifikátu s novým veřejným klíčem.

3.4 Identifikace a autentizace při zpracování požadavků na zneplatnění certifikátu

Konkrétní způsoby identifikace a autentizace při zpracování požadavků na zneplatnění certifikátu jsou uvedeny v konkrétní CP.

3.4.1 Certifikáty poskytovatele (I.CA)

Oprávněnou osobou žádat o zneplatnění certifikátu:

- kořenové certifikační autority i jí vydaného certifikátu OCSP respondéru,
- vydávající certifikační autority i jí vydaného certifikátu OCSP respondéru,
- TSS systému TSA,

je ředitel I.CA.

Žadatelem o zneplatnění certifikátu kořenové certifikační autority, popř. certifikátu, souvisejícího s kvalifikovanými certifikačními službami, může být taktéž představitel úřadu, který společnost První certifikační autorita, a.s., akreditoval. Žádost od úřadu musí být písemná, nebo být doručena do datové schránky I.CA. Samotnému procesu zneplatnění takového certifikátu musí být ředitel I.CA vždy osobně přítomen.

3.4.2 Certifikáty koncových uživatelů

Možné způsoby identifikace a autentizace jsou následující:

- osobně na RA,
- prostřednictvím formuláře na webových stránkách společnosti (s využitím hesla pro zneplatnění certifikátu),
- prostřednictvím nepodepsané elektronické zprávy (obsahující heslo pro zneplatnění certifikátu),
- prostřednictvím elektronicky podepsané /elektronicky označené /opatřené elektronickou pečetí elektronické zprávy (realizovány soukromým klíčem příslušným k předmětnému certifikátu, jenž má být zneplatněn, nebo soukromým klíčem z podpisového certifikátu),
- prostřednictvím datové schránky (s využitím hesla pro zneplatnění certifikátu),
- prostřednictvím doporučené listovní zásilky na adresu sídla I.CA (s využitím hesla pro zneplatnění certifikátu).

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

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

4 POŽADAVKY NA ŽIVOTNÍ CYKLUS CERTIFIKÁTU

4.1 Žádost o vydání certifikátu

4.1.1 Subjekty oprávněné podat žádost o vydání certifikátu

Žádost o vydání certifikátu může podat fyzická osoba nebo organizace. Subjekty oprávněné podat žádost o vydání certifikátu jsou uvedeny v konkrétní CP.

4.1.2 Registrační proces a odpovědnosti poskytovatele a žadatele

Procesy prováděné v průběhu registračního procesu jsou uvedeny v konkrétní CP.

4.1.2.1 Odpovědnost žadatele

Žadatel je povinen zejména:

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

4.1.2.2 Odpovědnost poskytovatele

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

4.2 Zpracování žádosti o certifikát

Proces zpracování žádosti o certifikát je popsaný v interní dokumentaci:

- „Směrnice pro pracovníky RA I.CA“,
- „Operátor CA“.

4.2.1 Identifikace a autentizace

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

4.2.2 Přijetí nebo zamítnutí žádosti o certifikát

V případě vydávání certifikátů poskytovatele rozhodne vedení společnosti První certifikační autorita, a.s., na základě písemné žádosti o vydání certifikátu, případně o zamítnutí žádosti. Výsledek je dokumentován.

Pokud některá z ověření, prováděna pracovníkem RA skončí negativně, proces vydání certifikátu je ukončen. V opačném případě pracovník RA vydání certifikátu schválí.

Postupy pro přijetí nebo odmítnutí žádosti o certifikát jsou uvedeny v konkrétní CP a v interní dokumentaci:

- „Směrnice pro pracovníky RA I.CA“.

4.2.3 Doba zpracování žádosti o certifikát

V případě vydávání certifikátů poskytovatele doba zpracování písemné žádosti o vydání certifikátu nepřekročí pět pracovních dnů ode dne předložení žádosti vedení společnosti.

Certifikáty koncových uživatelů jsou vydávány obratem po ověření žádosti na RA, v případě následného certifikátu po kontrole operátorem CA. Výjimku tvoří SSL certifikáty, kdy doba zpracování žádosti o certifikát zpravidla nepřekročí pět pracovních dnů (z důvodu ověřování údajů v žádosti).

4.3 Vydání certifikátů

4.3.1 Úkony CA v průběhu vydávání certifikátu

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

Postupy jsou uvedeny v konkrétní CP a upřesněny v interní dokumentaci:

- „Směrnice pro pracovníky RA I.CA“,
- „Operátor CA“.

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

V případě, že žadatel o certifikát je osobně přítomen vydání certifikátu, získá oznámení o jeho vydání od pracovníka RA. Vydaný certifikát je vždy automaticky zaslán na kontaktní e-mailovou adresu žadatele.

Uvedené postupy jsou detailně popsány v interní dokumentaci:

- „Směrnice pro pracovníky RA I.CA“,
- „Operátor CA“.

4.4 Převzetí vydaného certifikátu

4.4.1 Úkony spojené s převzetím certifikátu

Úkony spojené s převzetím certifikátu jsou vždy popsány v konkrétní CP.

Proces je detailně popsán v interní dokumentaci:

- „Směrnice pro pracovníky RA I.CA“,
- „Operátor CA“.

4.4.2 Zveřejňování vydaných certifikátů poskytovatelem

Certifikáty poskytovatele jsou zveřejňovány na webových stránkách I.CA, certifikáty související s kvalifikovanými certifikačními službami jsou navíc předány dozorovému orgánu.

Veřejné certifikáty koncových uživatelů jsou zveřejněny způsobem podle bodu 2.2.

4.4.3 Oznámení o vydání certifikátu jiným subjektům

Platí ustanovení kap. 4.4.2.

4.5 Použití párových dat a certifikátu

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

Povinností držitele certifikátu, resp. držitele soukromého klíče mj. je:

- bez zbytečného odkladu podávat přesné, pravdivé a úplné informace společnosti I.CA ve vztahu k vydanému certifikátu,
- v případě koncového uživatele dodržovat veškerá relevantní ustanovení smlouvy o poskytování této certifikační služby,
- používat soukromý klíč a jemu odpovídající veřejný klíč obsažený ve vydaném certifikátu v souladu s konkrétní CP,
- nakládat se soukromým klíčem, odpovídajícím veřejnému klíči v certifikátu, tak, aby nemohlo dojít k jeho neoprávněnému použití,
- pokud hrozí nebezpečí zneužití soukromého klíče odpovídajícího veřejnému klíči v certifikátu, požádat neprodleně o zneplatnění tohoto certifikátu.

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

Spoléhající se strany jsou zejména povinny ověřit elektronický podpis /elektronickou značku/ elektronickou pečeť dokumentu, byl-li tento elektronicky podepsán /elektronicky označen/ opatřen elektronickou pečetí, tj.:

- získat z bezpečného zdroje certifikát kořenové certifikační autority a ověřit kontrolní součet tohoto certifikátu,
- provádět veškeré úkony potřebné k tomu, aby si ověřily, že certifikát vydaný kořenovou certifikační autoritou nebyl zneplatněn, mj. ověřit platnost:
  - kořenového certifikátu,
  - jí vydaného certifikátu,
- provádět veškeré úkony potřebné k tomu, aby si ověřily, že elektronický podpis / elektronická značka/ elektronická pečeť certifikátu koncového uživatele jsou platné.

4.6 Obnovení certifikátu

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

4.6.1 Podmínky pro obnovení certifikátu

Viz kap. 4.6.

4.6.2 Subjekty oprávněné požadovat obnovení certifikátu

Viz kap. 4.6.

4.6.3 Zpracování požadavku na obnovení certifikátu

Viz kap. 4.6.

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

Viz kap. 4.6.

4.6.5 Úkony spojené s převzetím obnoveného certifikátu

Viz kap. 4.6.

4.6.6 Zveřejňování vydaných obnovených certifikátů poskytovatelem

Viz kap. 4.6.

4.6.7 Oznámení o vydání obnoveného certifikátu jiným subjektům

Viz kap. 4.6.

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

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

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

Viz kap. 4.7.

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

Viz kap. 4.7.

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

Viz kap. 4.7.

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

Viz kap. 4.7.

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

Viz kap. 4.7.

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

Viz kap. 4.7.

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

Viz kap. 4.7.

4.8 Změna údajů v certifikátu

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

4.8.1 Podmínky pro změnu údajů v certifikátu

Viz kap. 4.8.

4.8.2 Subjekty oprávněné požadovat změnu údajů v certifikátu

Viz kap. 4.8.

4.8.3 Zpracování požadavku na změnu údajů v certifikátu

Viz kap. 4.8.

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

Viz kap. 4.8.

4.8.5 Úkony spojené s převzetím certifikátu se změněnými údaji

Viz kap. 4.8.

4.8.6 Zveřejňování vydaných certifikátů se změněnými údaji

Viz kap. 4.8.

4.8.7 Oznámení o vydání certifikátu se změněnými údaji jiným subjektům

Viz kap. 4.8.

4.9 Zneplatnění a pozastavení platnosti certifikátu

4.9.1 Podmínky pro zneplatnění certifikátu

Kromě podmínek uvedených v následujících podkapitolách si I.CA vyhrazuje právo akceptování i jiných okolností podmínek na zneplatnění certifikátu.

4.9.1.1 Certifikáty poskytovatele (I.CA)

Certifikát může být zneplatněn na základě následujících okolností:

- dojde ke kompromitaci, resp. existuje důvodné podezření, že došlo ke kompromitaci, soukromého klíče,
- žádost ředitele I.CA,
- nastanou-li skutečnosti uvedené v platné legislativě týkající se elektronického podpisu.

4.9.1.2 Certifikáty koncových uživatelů

Certifikát může být zneplatněn na základě následujících okolností:

- žádost držitele certifikátu nebo držitele soukromého klíče osoby,
- žádost ředitele I.CA, pokud byla zjištěna duplicita veřejného klíče s veřejným klíčem v jiné žádosti, nebo bylo ze strany držitele certifikátu nebo držitele soukromého klíče porušeno ustanovení smlouvy o poskytování certifikační služby,
- nastanou-li skutečnosti uvedené v platné legislativě týkající se elektronického podpisu.

4.9.2 Subjekty oprávněné žádat o zneplatnění certifikátu

4.9.2.1 Certifikáty poskytovatele (I.CA)

Žádost o zneplatnění mohou podat:

- ředitel I.CA,
- další subjekty definované platnou legislativou týkající se elektronického podpisu.

4.9.2.2 Certifikáty koncových uživatelů

Žádost o zneplatnění mohou podat:

- držitel certifikátu nebo držitel soukromého klíče, nebo subjekt, který k tomu byl explicitně určen ve smlouvě o poskytování certifikační služby,
- osoba oprávněná z pozůstalostního řízení,
- ředitel I.CA,
- další subjekty definované platnou legislativou týkající se elektronického podpisu.

4.9.3 Požadavek na zneplatnění certifikátu

Způsob podání žádosti o zneplatnění certifikátu koncového uživatele je vždy popsán v konkrétní CP.

Požadavky na identifikaci a autentizaci jsou uvedeny v kap 3.4.

4.9.4 Doba odkladu požadavku na zneplatnění certifikátu

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

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

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

Detailní postupy jsou uvedeny v interním dokumentu:

- „Operátor CA“.

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

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

4.9.7 Periodicita vydávání seznamu zneplatněných certifikátů

Periodicita vydávání seznamu zneplatněných certifikátů je uvedena v konkrétní CP.

Činnosti operátorů CA v procesu vytváření a vydávání CRL jsou popsány v interním dokumentu:

- „Operátor CA“.

4.9.8 Maximální zpoždění při vydávání seznamu zneplatněných certifikátů

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

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

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 při ověřování statutu certifikátu on-line

Viz kap. 4.9.9.

4.9.11 Jiné způsoby oznamování zneplatnění certifikátu

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

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

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

4.9.13 Podmínky pro pozastavení platnosti certifikátu

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

4.9.14 Subjekty oprávněné požadovat pozastavení platnosti certifikátu

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

4.9.15 Zpracování požadavku na pozastavení platnosti certifikátu

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

4.9.16 Omezení doby pozastavení platnosti certifikátu

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

4.10 Služby související s ověřováním statutu certifikátu

4.10.1 Funkční charakteristiky

Seznamy veřejných certifikátů jsou poskytovány formou zveřejňování informací, seznamy zneplatněných certifikátů jsou poskytovány jak formou zveřejňování informací, tak uvedením distribučních míst CRL ve vydaných certifikátech. OCSP odpovědi, pokud je služba OCSP poskytována - viz kap. 4.9.9, poskytují informaci o stavu certifikátu.

4.10.2 Dostupnost služeb

I.CA garantuje zajištění nepřetržité dostupnosti (7 dní v týdnu, 24 hodin denně) a integrity seznamu jí vydaných certifikátů a seznamů zneplatněných certifikátů (platné CRL), a dále dostupnost služby OCSP, pokud je tato poskytována - viz kap. 4.9.9.

Postup je uveden v interních dokumentech I.CA, zejména:

- „Operátor CA“,
- „Příručka administrátora“,
- „Obnova komponenty provozního pracoviště“,
- „Přemístění provozního pracoviště“.

4.10.3 Další charakteristiky služeb statutu certifikátu

Další charakteristiky služeb stavu certifikátu nejsou poskytovány.

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

I.CA ukončí poskytování služeb koncovému uživateli (držiteli certifikátu, resp. držiteli soukromého klíče) ve chvíli, kdy:

- skončila platnost certifikátu, aniž by bylo v souladu s relevantní CP požádáno o vydání následného certifikátu,
- dojde k ukončení smlouvy o poskytování certifikačních služeb mezi držitelem certifikátu a I.CA s výjimkou služby zneplatnění certifikátu, která je poskytována po celou dobu platnosti tohoto certifikátu.

Postup v případě ukončení činnosti CA nebo RA je popsán v kap. 5.8.

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

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

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

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

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

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

5 MANAGEMENT, PROVOZNÍ A FYZICKÁ BEZPEČNOST

Management bezpečnosti je zaměřen především na:

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

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

5.1 Fyzická bezpečnost

Problematika fyzické bezpečnosti je detailně uvedena v interní dokumentaci, zejména:

- „Řízení fyzického přístupu do místností I.CA“,
- „Požární bezpečnost“,
- „Kontrolní činnost, bezúhonnost a odbornost“,
- „Bezpečnostní incidenty“,
- „Obnova komponenty provozního pracoviště“,
- „Přemístění provozního pracoviště“,
- „Kamerový systém – provozní pracoviště“,
- projekty fyzické bezpečnosti jednotlivých provozních pracovišť.

5.1.1 Umístění a konstrukce

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

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

5.1.2 Fyzický přístup

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

5.1.3 Elektřina a klimatizace

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

5.1.4 Vlivy vody

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

5.1.5 Protipožární opatření a ochrana

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

5.1.6 Ukládání médií

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

Papírová média, která je nutno, mj. dle platné legislativy týkající se elektronického podpisu, archivovat, jsou skladována v jiné geografické lokalitě, než je umístěno provozní pracoviště.

5.1.7 Nakládání s odpady

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

5.1.8 Zálohy mimo budovu

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

5.2 Procesní bezpečnost

5.2.1 Důvěryhodné role

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

- „Systémová bezpečnostní politika CA“,
- „Řízení bezpečnosti informací“.

- „Příručka administrátora“.

5.2.2 Počet osob požadovaných na zajištění jednotlivých činností

Pro procesy poskytování certifikačních služeb jsou vždy definovány činnosti, které musí být vykonány za účasti více než jediné osoby. Jedná se např. o generování párových dat, ničení soukromého klíče poskytovatele, jeho zálohování a obnovu, případně o aktivace kryptografického modulu, obsahujícího tento soukromý klíč. Podrobné informace jsou vždy uvedeny v konkrétní CP a v interní dokumentaci:

- „Příručka administrátora“,
- „Hierarchická struktura - Postupy generování klíčů a certifikátů CA“,
- „HSM/Private Server“.

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. Problematika je upravena v interní dokumentaci, zejména:

- „Směrnice pro pracovníky RA I.CA“,
- „Operátor CA“,
- „Příručka administrátora“.

5.2.4 Role vyžadující rozdělení povinností

Role vyžadující rozdělení povinností, včetně popisu náplně jejich činnosti, jsou popsány v interním dokumentu:

- „Systémová bezpečnostní politika CA“.

5.3 Personální bezpečnost

5.3.1 Požadavky na kvalifikaci, zkušenosti a bezúhonnost

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

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

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

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

Problematika je detailně popsána v interním dokumentu:

- „Kontrolní činnost, bezúhonnost a odbornost“.

5.3.2 Posouzení spolehlivosti osob

Zdrojem informací o všech zaměstnancích I.CA jsou:

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

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

5.3.3 Požadavky na přípravu pro výkon role, vstupní školení

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

Problematika je detailně popsána v interním dokumentu:

- „Kontrolní činnost, bezúhonnost a odbornost“.

5.3.4 Požadavky a periodicita školení

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

Problematika je detailně popsána v interním dokumentu:

- „Kontrolní činnost, bezúhonnost a odbornost“.

5.3.5 Periodicita a posloupnost rotace pracovníků mezi různými rolemi

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

5.3.6 Postihy za neoprávněné činnosti zaměstnanců

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

Problematika je detailně popsána v interním dokumentu:

- „Pracovní řád“.

5.3.7 Požadavky na nezávislé zhotovitele (dodavatele)

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

5.3.8 Dokumentace poskytovaná zaměstnancům

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

5.4 Auditní záznamy (logy)

Zaznamenávány jsou veškeré události požadované v případě kvalifikovaných certifikačních služeb platnou legislativou týkající se elektronického podpisu a jí odkazovanými technickými standardy, v ostatních případech relevantními technickými standardy, mj. o životním cyklu vydávaných certifikátů, nakládání se soukromými klíči poskytovatele a o dalších událostech, jako je např. ukončení činnosti certifikační autority.

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

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

Problematika spojená s vytvářením, zpracováním a uchováváním auditních logů (viz kapitoly 5.4.1 až 5.4.8) je detailně řešena v interní dokumentaci, zejména:

- „Příručka administrátora“,
- „Příprava uchovávaných informací“,
- „Záloha dat provozních systémů“,
- „Dokumenty agendy certifikačních služeb“,
- „Dílčí spisový a skartační řád pro agendy certifikačních služeb“,
- „Dílčí spisový a skartační plán pro agendy certifikačních služeb“.

5.4.1 Typy zaznamenávaných událostí

Speciálním případem zaznamenávání událostí je událost generování párových dat kořenové certifikační autority. Celý proces probíhá v souladu s platnou legislativou týkající se elektronického podpisu a relevantními technickými standardy, přičemž minimálně platí, že:

- je prováděn podle připraveného scénáře ve fyzicky zabezpečeném prostředí,

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

S ohledem na požadavky relevantních technických standardů a platné legislativy týkající se elektronického podpisu jsou v důvěryhodných systémech I.CA do elektronického auditního logu zaznamenávány následující bezpečnostně relevantní provozní události:

- z hlediska systému významné události prostředí a klíčového hospodářství,
- spuštění a ukončení funkcí auditu,
- změny parametrů auditu,
- akce, prováděné při chybách úložiště auditních záznamů,
- všechny pokusy přístupu k systému
- všechny události vztahující se k životnímu cyklu párových dat a certifikátů CA.
- záznam o registraci žadatele,
- záznam o pokus neoprávněné registrace žadatele (s maximem dosažitelných informací o neoprávněném žadateli),
- záznam o zrušení registrace žadatele (údaje o žadateli se uchovávají),
- vše, co souvisí s životním cyklem certifikátu koncového uživatele:
  - záznam o požadavku RA na vydání certifikátu včetně výsledku,
  - záznam o neoprávněném požadavku na vydání certifikátu včetně výsledku,
  - záznam o požadavku na vydání následného certifikátu včetně výsledku,
  - záznam o neoprávněném požadavku na vydání následného certifikátu včetně výsledku,
  - záznam o požadavku na zneplatnění certifikátu včetně údajů o žádající osobě a výsledku,
  - záznam o neoprávněném požadavku na zneplatnění certifikátu včetně údajů o žádající osobě a výsledku,
  - záznam o oznámení možné kompromitace dat pro vytváření elektronických podpisů, resp. značek podepisující /označující osobou,
  - záznam o zneplatnění certifikátu,
  - záznam o pokusu neoprávněného přístupu do systému,
  - záznam o zveřejnění certifikátu, včetně výsledku,
  - záznam o zanesení zneplatněného certifikátu do CRL,
  - záznam o zveřejnění CRL.

Všechny záznamy v auditním souboru obsahují následující parametry:

- datum (rok, měsíc, den) a čas (hodina, minuta, sekunda) události,
- typ události,
- identitu entity, která je za akci odpovědná,
- úspěšnost /neúspěšnost auditované události.

5.4.2 Periodicita zpracování záznamů

Auditní záznamy jsou kontrolovány a vyhodnocovány v intervalech definovaných v interní bezpečnostním dokumentu:

- „Příručka administrátora“,

v případě bezpečnostního incidentu okamžitě.

5.4.3 Doba uchování auditních záznamů

Auditní záznamy jsou uchovávány po dobu definovanou platnou legislativou týkající se elektronického podpisu.

5.4.4 Ochrana auditních záznamů

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

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

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

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 interní.

5.4.7 Postup při oznamování události subjektu, který ji způsobil

Subjekt není o zapsání události do auditního záznamu informován.

5.4.8 Hodnocení zranitelnosti

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

5.5 Uchovávání informací a dokumentace

Uchovávání informací a dokumentace je u I.CA prováděno dle požadavků platné legislativy týkající se elektronického podpisu, ve shodě s dalšími relevantními právními předpisy (např. zákona o archivnictví a spisové službě), a dle interní dokumentace:

- „Řízení fyzického přístupu do místností I.CA“,
- „Příprava uchovávaných informací“,
- „Záloha dat provozních systémů“,
- „Příručka administrátora“,
- „Dokumenty agendy certifikačních služeb“,
- „Dílčí spisový a skartační řád pro agendy certifikačních služeb“,
- „Dílčí spisový a skartační plán pro agendy certifikačních služeb“.

5.5.1 Typy informací a dokumentace, které se uchovávají

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

- videozáznam průběhu generování párových dat kořenové certifikační autority,
- případné osvědčení notáře o průběhu generování párových dat kořenové certifikační autority,
- zprávu auditora o průběhu generování párových dat kořenové certifikační autority,
- smlouvy o poskytování certifikačních služeb (včetně žádostí o poskytování certifikačních služeb),
- v případě kvalifikovaných certifikačních služeb kopie předložených osobních dokladů žadatele o certifikát, popř. zmocněnce, na jejichž základě byla ověřena identita žadatele o certifikát, popř. zmocněnce,
- potvrzení o převzetí certifikátu držitelem, popř. zmocněncem, případně jeho souhlas se zveřejněním certifikátu v seznamu vydaných certifikátů
- prohlášení držitele certifikátu o tom, že mu byly před uzavřením smlouvy o poskytování certifikačních služeb poskytnuty písemné informace o přesných podmínkách pro využívání těchto služeb, včetně případných omezení pro jejich použití, o podmínkách reklamací a řešení vzniklých sporů, a v případě kvalifikovaných certifikačních služeb o tom, zda je, či není poskytovatel certifikačních služeb akreditován,
- dokumenty a záznamy související s životním cyklem vydaných certifikátů,
- vydané certifikáty,
- v případě kvalifikovaných certifikačních služeb další záznamy požadované platnou legislativou týkající se elektronického podpisu (např. seznamy zneplatněných certifikátů),
- aplikační programové vybavení a veškerou dokumentaci společnosti, která je nutná pro provádění kontrol,
- záznam o manipulaci (např. převzetí, předání, uložení, kontrola, konverze do elektronické podoby atp.) s informacemi,

- provozní a bezpečnostní dokumentace.

5.5.2 Doba uchování uchovávaných informací a dokumentace

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

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

Postupy při zálohování uchovávaných informací a dokumentace jsou upraveny interní dokumentací - viz kap 5.5.

5.5.3 Ochrana úložiště uchovávaných informací a dokumentace

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

Postupy při ochraně úložiště uchovávaných informací a dokumentace jsou upraveny interní dokumentací - viz kap 5.5.

5.5.4 Postupy při zálohování uchovávaných informací a dokumentace

Postupy při zálohování uchovávaných informací a dokumentace jsou upraveny interní dokumentací - viz kap 5.5.

5.5.5 Požadavky na používání časových razítek při uchovávání informací a dokumentace

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

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

Informace a dokumentace jsou ukládány na místo určené ředitelem I.CA. Registrační autority jsou povinny provést předarchivaci dokumentů v určených termínech a předat je určeným pracovníkům I.CA.

Samotná problematika přípravy a způsobu ukládání informací a dokumentace v elektronické i písemné podobě je upravena interním dokumentací - viz kap 5.5. Shromažďování uchovávaných informací je evidováno.

5.5.7 Postupy pro získání a ověření uchovávaných informací a dokumentace

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

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

O každém takto povoleném přístupu je pořizován písemný záznam.

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

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

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

5.7 Obnova po havárii nebo kompromitaci

5.7.1 Postup v případě incidentu a kompromitace

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

- „Plán pro zvládání krizových situací a plán obnovy“,
- „Obnova komponenty provozního pracoviště“,
- „Přemístění provozního pracoviště“,
- „Bezpečnostní incidenty“.

5.7.2 Poškození výpočetních prostředků, softwaru nebo dat

Viz kap. 5.7.1.

5.7.3 Postup při kompromitaci dat pro vytváření elektronických značek poskytovatele

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

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

- v případě kvalifikovaných certifikačních služeb 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:

- „Plán pro zvládání krizových situací a plán obnovy“,
- „Obnova komponenty provozního pracoviště“,
- „Přemístění provozního pracoviště“.

5.8 Ukončení činnosti CA nebo RA

Pro ukončování činnosti CA platí následující pravidla:

- ukončení činnosti CA musí být písemně oznámeno všem držitelům platných certifikátů, subjektům, které mají uzavřenou smlouvu přímo se vztahující k poskytování certifikačních služeb a v případě kvalifikovaných certifikačních služeb dozorovému orgánu určenému platnou legislativou týkající se elektronického podpisu,
- ukončení činnosti CA musí být zveřejněno na internetové adrese podle kap. 2.2,
- pokud je součástí ukončení činnosti CA ukončení platnosti jejího certifikátu, musí být součástí oznámení i tato informace včetně uvedení důvodu ukončení platnosti,
- po dobu platnosti jediného certifikátu vydaného certifikační autoritou musí tato zajistit alespoň funkce zneplatňování certifikátu a vydávání CRL,
- následně CA prokazatelně zničí svůj soukromý klíč a o tomto zničení provede záznam, který bude uchováván v souladu s pravidly této CP, viz kap. 5.4.

V případě ukončení činnosti poskytovatele kvalifikovaných certifikačních služeb bude postupováno v souladu s příslušnými ustanoveními platné legislativy týkající se elektronického podpisu. Problematika plánovaného ukončení činnosti I.CA jako kvalifikovaného poskytovatele certifikačních služeb v oblasti vydávání certifikátů je detailně uvedena v interním dokumentu:

- „Ukončení činnosti služeb I.CA“.

V případě odnětí akreditace dle platné legislativy týkající se elektronického podpisu::

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

V případě ukončení činnosti konkrétního pracoviště RA je tato skutečnost oznámena na internetové adrese http://www.ica.cz, případně před skutečným uzavřením formou vývěsky na pracovišti této RA.

6 TECHNICKÁ BEZPEČNOST

6.1 Generování a instalace párových dat

6.1.1 Generování párových dat

Pro generování párových dat všech certifikačních autorit, jejich případných OCSP respondérů a TSS systému TSA platí, že probíhá v zóně zabezpečené v souladu s platnou legislativou týkající se elektronického podpisu, resp. se zákonem o ochraně utajovaných informací, je prováděno v kryptografickém modulu, který byl hodnocen podle FIPS PUB 140-2 Level 3 a průběh je dokumentován. Bližší podrobnosti jsou vždy popsány v konkrétní CP.

Veškeré požadavky na proces generování párových dat jsou popsány v interní dokumentaci:

- „Řízení fyzického přístupu do místností I.CA“,
- „HSM/Private Server“,
- „Správa TSS“,
- „Hierarchická struktura - Postupy generováním klíčů a certifikátů CA“.

Protokol o průběhu generování párových dat obsahuje minimálně:

- jmenný seznam přítomných zaměstnanců,
- datum a čas zahájení a ukončení generace párových dat s přesností minimálně na minuty,
- místo, kde bylo generování prováděno,
- popis zařízení, na kterém bylo generování prováděno, umožňující jednoznačnou identifikaci tohoto zařízení,
- datum vyhotovení protokolu,
- vlastnoruční podpisy všech pracovníků, kteří generování párových dat prováděli.

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.

I.CA neposkytuje službu generování párových dat koncového uživatele na svých zařízeních. Koncový uživatel je povinen používat taková zařízení, která splňují v případě kvalifikovaných certifikačních služeb požadavky platné legislativy týkající se elektronického - viz konkrétní CP.

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

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

Služba generování párových dat podepisující osobě není poskytována.

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

Veřejné klíče (formát PKCS#10) (formát PKCS#10) jsou doručovány jako součást žádosti o vydání certifikátu.

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

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

Mohutnost klíče (resp. parametrů algoritmu) kořenové certifikační autority využívající algoritmus RSA je 4096 bitů. Mohutnost klíčů (resp. parametrů algoritmu) ostatních vydávaných certifikátů je vždy uvedena v konkrétní CP.

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

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

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 je podepisující osoba požádána o vygenerování nového veřejného klíče. Již vydaný Certifikát je neprodleně zneplatněn, podepisující osoba nebo držitel takového Certifikátu jsou o tomto neprodleně a vhodným způsobem informováni a vyzváni ke generování nových párových dat.

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

Uvedeno v kap. 1.4.

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

Konkrétní postupy ochrany soukromého klíče poskytovatele (kapitoly 6.2.1 až 6.2.10) jsou popsány v interní dokumentaci:

- „Řízení fyzického přístupu do místností I.CA“,
- „HSM/Private Server“,
- „Hierarchická struktura - Postupy generováním klíčů a certifikátů CA“,
- „Správa TSS“.

6.2.1 Standardy a podmínky používání kryptografických modulů

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

6.2.2 Sdílení tajemství

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

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

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

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

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

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

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

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

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

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

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

O provedeném transferu je vždy pořízen písemný záznam.

6.2.7 Uložení dat pro vytváření elektronických značek v kryptografickém modulu

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

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

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

Aktivace soukromých klíčů OCSP 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.

Postup je přesně upraven interní dokumentací:

- „HSM/Private Server“,
- „Správa TSS“.

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

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

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

Postup je upraven interním dokumentem:

- „HSM/Private Server“.

O provedené deaktivaci je pořízen písemný záznam.

Deaktivace původního soukromého klíče TSS systému TSA je prováděna vložením nového certifikátu, postup je popsán v interním dokumentu:

- „Správa TSS“.

O provedené deaktivaci je pořízen písemný záznam.

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

Soukromé klíče certifikačních autorit, jejich OCSP respondérů a TSS serverů 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:

- „HSM/Private Server“,
- „Správa TSS“.

6.2.11 Hodnocení kryptografických modulů

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

6.3 Další aspekty správy párových dat

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

Veškeré veřejné klíče poskytovatele jsou uchovávány po celou dobu existence I.CA.

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

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

6.4 Aktivační data

6.4.1 Generování a instalace aktivačních dat

Aktivační data certifikačních autorit, jejich OCSP respondérů a TSS serverů jsou vytvářena v průběhu generování příslušných párových dat. Konkrétní postup je popsán v interním dokumentu:

- „HSM/Private Server“,
- „Správa TSS“.

6.4.2 Ochrana aktivačních dat

Aktivační data jsou chráněna způsobem popsaným v interní dokumentaci:

- „HSM/Private Server“,
- „Správa TSS“.

6.4.3 Ostatní aspekty aktivačních dat

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

6.5 Počítačová bezpečnost

6.5.1 Specifické technické požadavky na počítačovou bezpečnost

Úroveň bezpečnosti použitých komponent pro poskytování certifikačních služeb je definována v případě kvalifikovaných certifikačních služeb platnou legislativou týkající se elektronického podpisu a jí odkazovanými technickými standardy, v ostatních případech relevantními technickými standardy. Detailně je řešení popsáno v interní dokumentaci, zejména :

- „Systémová bezpečnostní politika CA“,
- „Plán pro zvládání krizových situací a plán obnovy“,
- „Obnova komponenty provozního pracoviště“,
- „Přemístění provozního pracoviště“,
- „Záloha dat provozních systémů“,
- „Příprava uchovávaných informací“,
- „Příručka administrátora“,
- „Řízení fyzického přístupu do místností I.CA“,
- „HSM/Private Server“,
- „Správa TSS“.

6.5.2 Hodnocení počítačové bezpečnosti

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

- CWA 14167-1 - Security Requirements for Trustworthy Systems Managing Certificates for Electronic Signatures - Part 1: System Security Requirements /Bezpečnostní požadavky na důvěryhodné systémy spravující certifikáty pro elektronický podpis - část 1: Požadavky na bezpečnost systémů.
- ČSN ETSI TS 101 456 - Elektronické podpisy a infrastruktury - Požadavky na postupy certifikační autority vydávající kvalifikované certifikáty.
- ETSI TS 101 456 Electronic Signatures and Infrastructures (ESI); Policy requirements for certification authorities issuing qualified certificates.

- ETSI TS 102 042 Electronic Signatures and Infrastructures (ESI); Policy requirements for certification authorities issuing public key certificates.
- 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 319 411-2 Elektronické podpisy a infrastruktury (ESI) - Požadavky politiky a bezpečnosti na poskytovatele důvěryhodných služeb vydávající certifikáty - Část 2: Požadavky politiky na certifikační autority vydávající kvalifikované certifikáty.
- ETSI EN 319 411-2 Electronic Signatures and Infrastructures (ESI); Policy and security requirements for Trust Service Providers issuing certificates; Part 2: Requirements for trust service providers issuing EU qualified certificates.
- 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.

Detailně je problematika popsána v interním dokumentu:

- „Kontrolní činnost, bezúhonnost a odbornost".

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.
- 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 Bezpečnost životního cyklu

6.6.1 Řízení vývoje systému

Při vývoji systému je postupováno v souladu s interní dokumentací:

- „Změnové řízení“,
- „Metodika vývoje“.

6.6.2 Kontroly řízení bezpečnosti

Kontrola řízení bezpečnosti informací, včetně kontroly souladu se standardy, je prováděna v rámci periodických kontrol podle platné legislativy týkající se elektronického podpisu a dále 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 resp. STN ISO/IEC 27000 Informačné technológie. Bezpečnostné metódy. Systémy riadenia informačnej bezpečnosti. Prehľad a slovník.
- ČSN ISO/IEC 27001 Informační technologie - Bezpečnostní techniky - Systémy řízení bezpečnosti informací - Požadavky, resp. STN ISO/IEC 27001 Informačné technológie. Bezpečnostné metódy. Systémy riadenia informačnej bezpečnosti. Požiadavky.
- ČSN ISO/IEC 27002 Informační technologie - Bezpečnostní techniky - Soubor postupů pro opatření bezpečnosti informací, resp. STN ISO/IEC 27002 Informačné technológie. Bezpečnostné metódy. Pravidlá dobrej praxe riadenia informačnej bezpečnosti.
- ČSN ISO/IEC 27006 Informační technologie - Bezpečnostní techniky - Požadavky na orgány provádějící audit a certifikaci systémů řízení bezpečnosti informací.

Problematika je popsána v interním dokumentu:

- Kontrolní činnost, bezúhonnost a odbornost.

6.6.3 Řízení bezpečnosti životního cyklu

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

- vybudování - definování bezpečnostní politiky, plánů, cílů, procesů a postupů s ohledem na řízení rizik a bezpečnost informací tak, aby byly v souladu s celkovou bezpečnostní politikou, což je popsáno v interních dokumentech:
  - Celková bezpečnostní politika,
  - Politika bezpečnosti informací (ISMS),
  - Přístupy k posuzování a ošetřování rizik bezpečnosti informací
  - Rozsah ISMS (kvalifikované i komerční certifikační služby),
  - Analýza rizik, Závěrečná zpráva (kvalifikované i komerční certifikační služby),
  - Prohlášení o aplikovatelnosti (kvalifikované i komerční certifikační služby),
  - Plán ošetření /zvládání rizik (kvalifikované i komerční certifikační služby),
  - Zbytková rizika – manažerské shrnutí (kvalifikované i komerční certifikační služby),
- implementace a provoz - bezpečnostní politiky, plánů, cílů, procesů a postupů, což je popsáno v interních dokumentech:
  - „Řízení fyzického přístupu do místností I.CA“,
  - „Požární bezpečnost“,
  - „HSM/Private Server“,
  - „Řízení bezpečnosti informací“,
  - „Záloha dat provozních systémů“,
  - „Příručka administrátora“,
  - „Firewall – provozní pracoviště“,
  - „Kontrolní činnost, bezúhonnost a odbornost“,
  - „Změnové řízení“,
  - „Bezpečnostní incidenty“,
  - „Obnova komponenty provozního pracoviště“,
  - „Přemístění provozního pracoviště“,
  - „Firewall - provozní pracoviště“,
  - „Politika pro používání elektronické pošty“,
  - „Kamerový systém – provozní pracoviště“,
  - „Krizové scénáře“,
  - projekty fyzické bezpečnosti provozních pracovišť,
  - v další dokumentaci vedené na provozním pracovišti (viz „Příručka administrátora“),

- monitorování a přehodnocování - posouzení procesu s ohledem na bezpečnostní politiku a předání poznatků vedení společnosti k posouzení, což je popsáno v dokumentech:
  - zprávy z interních kontrol,
  - zprávy z externích kontrol a auditů,
- využití - na základě rozhodnutí vedení organizace provedení nápravných opatření.

6.7 Síťová bezpečnost

Informační systém kořenové certifikační autority je ve stavu off-line a není tedy propojen s žádnou externí síti. Zbývající komponenty, tedy OCSP respondér kořenové certifikační autority, jednotlivé certifikační autority a případně jejich OCSP respondéry, a TSS systému TSA, jsou chráněny komerčním produktem typu firewall. Detailní řešení řízení síťové bezpečnosti je popsáno v interní dokumentaci:

- „Systémová bezpečnostní politika CA“,
- „Příručka administrátora“,
- „Firewall – provozní pracoviště“,
- „Plán pro zvládání krizových situací a plán obnovy“,
- „Obnova komponenty provozního pracoviště“,
- „Přemístění provozního pracoviště“.

6.8 Časová razítka

Řešení je uvedeno v kap. 5.5.5.

7 PROFILY CERTIFIKÁTU, SEZNAMU ZNEPLATNĚNÝCH CERTIFIKÁTŮ A OCSP

Profily certifikátu, seznamu zneplatněných certifikátů a OCSP jsou vždy uvedeny v konkrétní CP. V následujících kapitolách jsou případně popsány pouze změny, jejichž provedení si I.CA v konkrétní certifikační politice vyhradila.

Přípustné typy a délka položek ve znacích pro pole Subject a SubjectAlternativeName:

- v kvalifikovaných certifikátech, kvalifikovaných systémových certifikátech, nekvalifikovaných (komerčních) SSL certifikátech (OVCP a DVCP) a nekvalifikovaných certifikátech pro elektronické pečetě, jsou uvedeny v tabulce ve druhém sloupci tab. 4,
- v ostatních typech nekvalifikovaných certifikátů, jsou uvedeny ve třetím sloupci tabulce tab. 4.

tab. 4 - Typy a délka položek polí Subject a SubjectAlternativeName

Pole/položka	**Kvalifikované certifikáty, kvalifikované systémové certifikáty, nekvalifikované SSL certifikáty (OVCP, DVCP), nekvalifikované certifikáty pro elektronické pečetě**	**Ostatní typy nekvalifikovaných certifikátů**
Subject		
countryName	PrintableString (2)	PrintableString (2)
givenName	UTF8String (1..64)	PrintableString, UTF8String (1..64)
surName	UTF8String (1..64)	PrintableString, UTF8String (1..64)
pseudonym	UTF8String (1..128)	PrintableString, UTF8String (1..128)
serialNumber	PrintableString (1..64)	PrintableString (1..64)
commonName	UTF8String (1..64)	PrintableString, UTF8String (1..64)
initials	UTF8String (1..64)	PrintableString, UTF8String (1..64)
emailAddress	IA5String (1..64)	IA5String (1..64)
name	UTF8String (1..128)	PrintableString, UTF8String (1..128)
generationQualifier	UTF8String (1..64)	PrintableString, UTF8String (1..64)

organizationName	UTF8String (1..64)	PrintableString, UTF8String (1..64)
organizationalUnitName	UTF8String (1..64)	PrintableString, UTF8String (1..64)
title	UTF8String (1..64)	PrintableString, UTF8String (1..64)
stateOrProvinceName	UTF8String (1..128)	PrintableString, UTF8String (1..128)
localityName	UTF8String (1..128)	PrintableString, UTF8String (1..128)
streetAddress	UTF8String (1..128)	PrintableString, UTF8String (1..128)
postalCode	UTF8String (1..40)	PrintableString, UTF8String (1..40)
organizationIdentifier	UTF8String (1..128)	PrintableString, UTF8String (1..128)
SubjectAlternativeName		
otherName.IKMPSV (1.3.6.1.4.1.11801.2.1)	UTF8String (1..10)	nepovoleno
otherName.ICA_SN (1.3.6.1.4.1.23624.4.6)	UTF8String (1..8) kontrola: pouze čísla/znaky "0" až "9"	UTF8String (1..7) kontrola: pouze čísla/znaky "0" až "9"
otherName.universalPrincipalName (1.3.6.1.4.1.311.20.2.3, Microsoft UPN)	UTF8String (1..max)	UTF8String (1..max)
rfc822Name	IA5String (1..320) kontrola: správný formát email adresy	IA5String (1..320) kontrola: správný formát email adresy
dNSName	IA5String (1..max) kontrola: správný formát DNS jména	nepovoleno

7.1 Profil certifikátu

Viz kap. 7.

7.1.1 Číslo verze

Viz kap. 7.

7.1.2 Rozšiřující položky v certifikátu

Viz kap. 7.

7.1.3 Objektové identifikátory (dále “OID”) algoritmů

Viz kap. 7.

7.1.4 Způsoby zápisu jmen a názvů

Viz kap. 7.

7.1.5 Omezení jmen a názvů

Viz kap. 7.

7.1.6 OID certifikační politiky

Viz kap. 7.

7.1.7 Rozšiřující položka „Policy Constrainsts“

Viz kap. 7.

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

Viz kap. 7.

7.1.9 Způsob zápisu kritické rozšiřující položky „Certificate Policies“

Viz kap. 7.

7.2 Profil seznamu zneplatněných certifikátů

Viz kap. 7.

7.2.1 Číslo verze

Viz kap. 7.

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

Viz kap. 7.

7.3 Profil OCSP

Seznam certifikačních autorit I.CA, které poskytují službu OCSP, je v kap. 4.9.9.

7.3.1 Číslo verze

Viz kap. 7.

7.3.2 Rozšiřující položky OCSP

Viz kap. 7.

8 HODNOCENÍ SHODY A JINÁ HODNOCENÍ

Informace o hodnocení jsou uvedeny v konkrétních certifikačních politikách.

8.1 Periodicita hodnocení nebo okolnosti pro provedení hodnocení

Viz kap. 8.

8.2 Identita a kvalifikace hodnotitele

Viz kap. 8.

8.3 Vztah hodnotitele k hodnocenému subjektu

Viz kap. 8.

8.4 Hodnocené oblasti

Viz kap. 8.

8.5 Postup v případě zjištění nedostatků

Viz kap. 8.

8.6 Sdělování výsledků hodnocení

Viz kap. 8.

9 OSTATNÍ OBCHODNÍ A PRÁVNÍ ZÁLEŽITOSTI

9.1 Poplatky

9.1.1 Poplatky za vydání nebo obnovení certifikátu

Poplatky za prvotní, popř. následný certifikát koncového uživatele, jsou uvedeny v aktuálním ceníku služeb, který je k dispozici na internetové informační adrese I.CA.

Poplatky za certifikáty, jejichž držitelem je I.CA, nejsou účtovány.

Služba obnovení certifikátu není poskytována.

9.1.2 Poplatky za přístup k certifikátu na seznamu vydaných certifikátů

Přístup elektronickou cestou k veřejným certifikátům vydaným podle certifikačních politik - viz kap. 1.2 - I.CA nezpoplatňuje.

9.1.3 Poplatky za informace o statutu certifikátu nebo o zneplatnění certifikátu

Přístup elektronickou cestou k informacím o zneplatněných certifikátech (CRL) nebo stavech certifikátů (OCSP) vydaných podle certifikačních politik - viz kap. 4.9.9 - I.CA nezpoplatňuje.

9.1.4 Poplatky za další služby

Poplatky za nadstandardní služby jsou stanovovány smluvně.

9.1.5 Jiná ustanovení týkající se poplatků (vč. refundací)

Není relevantní pro tento dokument.

9.2 Finanční odpovědnost

9.2.1 Krytí pojištěním

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

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

9.2.2 Další aktiva a záruky

Společnost První certifikační autorita, a.s., prohlašuje, že má k dispozici dostatečné finanční zdroje a jiné finanční zajištění na provoz v souladu s požadavky uvedenými v platné legislativě týkající se elektronického podpisu v případě kvalifikovaných certifikačních služeb

a s požadavky relevantních technických standardů v ostatních případech a s ohledem na riziko vzniku odpovědnosti za škodu.

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

9.2.3 Pojištění nebo krytí zárukou pro koncové uživatele

Není relevantní pro tento dokument, služba není poskytována.

9.3 Citlivost obchodních informací

9.3.1 Výčet citlivých informací

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

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

9.3.2 Informace mimo rámec citlivých informací

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

9.3.3 Odpovědnost za ochranu citlivých informací

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

9.4 Ochrana osobních údajů

Problematika ochrany osobních údajů je v I.CA řešena v souladu s požadavky příslušných zákonných norem. Tyto požadavky jsou rozpracovány v interních dokumentech:

- „Ochrana osobních údajů v I.CA“,
- „Řízení bezpečnosti informací“.

9.4.1 Politika ochrany osobních údajů

Viz kap. 9.4

9.4.2 Osobní údaje

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

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

9.4.3 Údaje, které nejsou považovány za citlivé

Za citlivé 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 důvěrných informací a souhlas s používáním citlivých informací

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

9.4.6 Poskytnutí citlivých informací pro soudní či správní účely

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

9.4.7 Jiné okolnosti zpřístupňování osobních údajů

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

9.5 Práva duševního vlastnictví

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

9.6 Zastupování a záruky

9.6.1 Zastupování a záruky CA

I.CA zaručuje, že:

- použije soukromé klíče příslušné certifikátům CA pouze v procesech vydávání certifikátů koncovým uživatelům a seznamů zneplatněných certifikátů,

- použije soukromé klíče příslušné OCSP respondérům příslušných CA, pokud tato autorita službu OCSP poskytuje - viz kap. 4.9.9 - pouze v procesech poskytování odpovědí na stav certifikátu vydaného touto CA,
- certifikáty vydávané koncovým uživatelům splňují náležitosti požadované platnou legislativou týkající se elektronického podpisu a relevantními technickými standardy,
- zneplatní vydané certifikáty, pokud byla žádost o ukončení jejich platnosti podána způsobem definovaným v příslušné CP.

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

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

Držitel certifikátu uplatňuje záruku vždy u RA, která zpracovala jeho žádost o vydání certifikátu.

9.6.2 Zastupování a záruky RA

Pro každou registrační autoritu platí, že tato:

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

9.6.3 Zastupování a záruky držitele certifikátu, podepisující nebo označující osoby

Ve smlouvě mezi I.CA a držitelem certifikátu nebo držitelem soukromého klíče je vždy uvedeno, že jsou povinni řídit se ustanoveními CP. podle které byl certifikát vydán.

9.6.4 Zastupování a záruky spoléhajících se stran

Spoléhající se strany postupují podle CP, podle které byl certifikát vydán.

9.6.5 Zastupování a záruky ostatních zúčastněných subjektů

Služba není poskytována.

9.7 Zřeknutí se záruk

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

9.8 Omezení odpovědnosti

Společnost První certifikační autorita, a.s., neodpovídá za škody způsobené spoléhajícím se stranám v případech, kdy nesplnily povinnosti, požadované certifikační politikou, dle které byl certifikát vydán. Dále neodpovídá za škody vzniklé v důsledku porušení závazků I.CA z důvodu vyšší moci.

9.9 Odpovědnost za škodu, náhrada škody

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

Společnost První certifikační autorita, a.s.:

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

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

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

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

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 (držitel certifikátu) je povinna uvést:

- co nejvýstižnější popis závad a jejich projevů,
- 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

Doba platnosti a podmínky ukončení platnosti certifikačních politik jsou vždy uvedeny v konkrétní CP.

9.10.1 Doba platnosti

Certifikační politiky - viz kap. 9.10.

Tato CPS nabývá platnosti dnem uvedeným v kap. 10 a platí do doby jejího nahrazení novou verzí, nebo minimálně po dobu platnosti posledního certifikátu vydané podle některé z certifikačních politik - viz kap. 1.2.

9.10.2 Ukončení platnosti

Certifikační politiky - viz kap. 9.10.

Jedinou osobou, která je oprávněna schvalovat ukončení platnosti této CPS, a to v případě jejího nahrazení novou verzí, nebo ukončení činnosti poskytovatele certifikačních služeb, je ředitel společnosti První certifikační autorita, a.s.

9.10.3 Důsledky ukončení a přetrvání závazků

Certifikační politiky - viz kap. 9.10.

Tato CPS platí minimálně po dobu platnosti posledního certifikátu vydané podle některé z certifikačních politik - viz kap. 1.2.

9.11 Komunikace mezi zúčastněnými subjekty

Pokud jsou zúčastněné subjekty organizačnímu částmi I.CA, řídí se komunikace mezi nimi interními pravidly I.CA.

V ostatních případech I.CA využívá pro individuální oznámení a komunikaci se zúčastněnými subjekty jimi dodané e-mailové adresy, poštovní adresy, telefonní čísla, osobní jednání atd. Komunikovat s I.CA lze způsoby uvedenými na adrese http://www.ica.cz/.

9.12 Změny

Postup v případě certifikačních politik je vždy popsán v konkrétní certifikační politice.

9.12.1 Postup při změnách

Certifikační politiky - viz kap. 9.12.

V případě této CPS - postup je realizován řízeným procesem uvedeném v interním dokumentu.

9.12.2 Postup při oznamování změn

Certifikační politiky - viz kap. 9.12.

V případě této CPS - postup je realizován řízeným procesem uvedeném v interním dokumentu.

9.12.3 Okolnosti, při kterých musí být změněn OID

Certifikační politiky - viz kap. 9.12.

V případě této CPS - OID není přiřazován.

9.13 Řešení sporů

Pokud jsou všechny strany sporu organizačnímu částmi I.CA, řídí se řešení sporů interními pravidly I.CA.

V jiných případech, pokud držitel certifikátu, spoléhající se strana nebo smluvní partner nesouhlasí s návrhem na vyřešení sporu, mohou použít následující stupně odvolání:

- odpovědný pracovník RA,
- odpovědný pracovník I.CA (nutné písemné podání),
- ředitel I.CA (nutné písemné 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 právními předpisy

Systém poskytování certifikačních služeb je v případě kvalifikovaných certifikačních služeb provozován ve shodě s platnou legislativou týkající se elektronického podpisu a z ní odkazovanými technickými standardy, v případě komerčních služeb ve shodě s relevantními technickými standardy.

9.16 Další ustanovení

Další ustanovení jsou vždy popsána v konkrétní certifikační politice.

9.16.1 Rámcová dohoda

Viz kap. 9.16.

9.16.2 Postoupení práv

Viz kap. 9.16.

9.16.3 Oddělitelnost ustanovení

Viz kap. 9.16.

9.16.4 Zřeknutí se práv

Viz kap. 9.16.

9.16.5 Vyšší moc

Viz kap. 9.16.

9.17 Další opatření

Není relevantní pro tento dokument.

10 ZÁVĚREČNÁ USTANOVENÍ

Tato certifikační politika vydaná společností První certifikační autorita, a.s., nabývá platnosti a účinnosti dnem 06.04.2016.