První certifikační autorita, a.s.

Certifikační prováděcí směrnice

(algoritmus RSA)

Verze 1.61

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.
1.4	15.03.2017	Ředitel společnosti První certifikační autorita, a.s.	Aktualizace OID politik. Úprava dle požadavků legislativy pro služby vytvářející důvěru, technických standardů a norem. Úprava dle požadavků programu Microsoft Trusted Root Certificate Program.
1.5	03.04.2017	Ředitel společnosti První certifikační autorita, a.s.	Aktualizace OID politik.
1.6	20.11.2017	Ředitel společnosti První certifikační autorita, a.s.	Doplnění nových politik. Změna zápisu OID politik.
1.61	30.04.2018	Ředitel společnosti První certifikační autorita, a.s.	Změna systému číslování verzí dokumentu. Doplnění postupu kontroly seznamu QSCD. Doplnění postupu kontroly CAA záznamů.

1 ÚVOD

Tento dokument rozpracovává a upřesňuje zásady z konkrétních certifikačních politik (dále CP), které První certifikační autorita, a.s., (dále též I.CA), kvalifikovaný poskytovatel služeb vytvářejících důvěru, uplatňuje při poskytování kvalifikovaných služeb vytvářejících důvěru, nekvalifikovaných služeb vytvářejících důvěru a při vydávání dalších typů certifikátů (dále též Služby). Pro Služby poskytované podle této certifikační prováděcí směrnice (dále též CPS), resp. příslušných certifikačních politik je využíván algoritmus RSA.

Služby, pokud je to relevantní, jsou poskytovány všem koncovým uživatelům na základě uzavřeného smluvního vztahu. I.CA nijak neomezuje potenciální koncové uživatele, poskytování služby je nediskriminační, včetně jejího zpřístupnění pro osoby se zdravotním postižením.

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 certifikační prováděcí směrnice, resp. příslušné certifikační politiky v rozporu se standardy nebo zákony, které nahradí dosud platné, bude vydána její nová verze.

1.1 Přehled

Dokument **Certifikační prováděcí směrnice (algoritmus RSA)**, vypracovaný společností První certifikační autorita, a. s., se zabývá skutečnostmi, vztahujícími se k procesům životního cyklu vydávaných certifikátů a dodržuje strukturu, jejíž předlohou je osnova platného standardu RFC 3647, s přihlédnutím k platným standardům Evropské unie a k právu České republiky v dané oblasti (jednotlivé kapitoly jsou proto v tomto dokumentu zachovány i v případě, že jsou ve vztahu k ní irelevantní). Týká se certifikačních politik uvedených v kapitole 1.2.

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

- Kapitola 1 identifikuje tento dokument, obecně popisuje subjekty participující na poskytování Služeb 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 certifikátů, tzn. žádost o vydání a vlastní vydání certifikátů, žádost o zneplatnění a vlastní zneplatnění certifikátů, služby související s ověřováním stavu certifikátů, ukončení poskytování 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 odkazuje na profily certifikátů a seznamů zneplatněných certifikátů v konkrétních CP a uvádí typy a délky položek pole Subject a rozšíření SubjectAlternativeName.
- Kapitola 8 je zaměřena na problematiku hodnocení poskytovaných 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.*x.y*	Certifikační politika kořenové kvalifikované certifikační autority (algoritmus RSA)
1.3.6.1.4.1.23624.10.1.30.*x.y*	Certifikační politika vydávání kvalifikovaných certifikátů pro elektronické podpisy (algoritmus RSA)
1.3.6.1.4.1.23624.10.1.31.*x.y*	Certifikační politika vydávání kvalifikovaných certifikátů pro elektronické pečetě (algoritmus RSA)
1.3.6.1.4.1.23624.10.1.32.*x.y*	Certifikační politika vydávání certifikátů pro systém TSA (algoritmus RSA)
1.3.6.1.4.1.23624.10.1.32.*x.y*	Certifikační politika vydávání kvalifikovaných certifikátů pro elektronickou pečeť systému TSA2 (algoritmus RSA)
1.3.6.1.4.1.23624.10.1.33.*x.y*	Certifikační politika vydávání systémových certifikátů (algoritmus RSA)
1.3.6.1.4.1.23624.10.1.34.*x.y*	Certifikační politika vydávání kvalifikovaných certifikátů pro elektronické pečetě PSD2 (algoritmus RSA)
1.3.6.1.4.1.23624.10.1.35.*x.y*	Certifikační politika vydávání kvalifikovaných certifikátů pro autentizaci internetových stránek právnickým osobám, (algoritmus RSA)
1.3.6.1.4.1.23624.10.1.70.*x.y*	Certifikační politika vydávání komerčních certifikátů (algoritmus RSA)
1.3.6.1.4.1.23624.10.1.71.*x.y*	Certifikační politika vydávání komerčních technologických certifikátů (algoritmus RSA)
1.3.1.6.4.1.23624.10.1.72.*x.y*	Certifikační politika vydávání SSL certifikátů (algoritmus RSA)
1.3.6.1.4.1.23624.10.1.80.*x.y*	Certifikační politika vydávání certifikátů OCSP respondérů (algoritmus RSA)

1.3.6.1.4.1.23624.10.1.90.*x.y*	Certifikační politika vydávání kvalifikovaných certifikátů SK pro elektronické podpisy (algoritmus RSA)
1.3.6.1.4.1.23624.10.1.91.*x.y*	Certifikační politika vydávání kvalifikovaných certifikátů pro elektronické pečetě SK (algoritmus RSA)

* Vždy se jedná o aktuální verzi politiky ve tvaru *x.yz*, která je vystavena na webu společnosti http://www.ica.cz, přičemž *x* a *y* jsou součástí OID politiky.

Služba vydávání kvalifikovaných certifikátů je v souladu s nařízením eIDAS zařazena na důvěryhodném seznamu udržovaném orgánem dohledu.

1.3 Participující subjekty

1.3.1 Certifikační autority (dále "CA")

1.3.1.1 Kořenová certifikační autorita

Kořenová certifikační autorita společnosti První certifikační autorita, a.s. vydala v dvoustupňové struktuře certifikačních autorit, v souladu s platnou legislativou a s požadavky technických standardů a norem, certifikáty podřízeným certifikačním autoritám provozovaným I.CA a svému OCSP respondéru. Tyto autority vydávají certifikáty koncovým uživatelům a pro vlastní OCSP respondéry.

Kořenová 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 Služby koncovým uživatelům a systému TSA.

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 certifikátů

1.3.3.1 Certifikáty poskytovatele (I.CA)

Certifikáty jsou vydávány výhradně pro certifikační autority, jejich OCSP respondéry a pro časové servery autorit časových razítek, 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 certifikáty vydávané v rámci poskytování Služeb.

1.3.5 Jiné participující subjekty

Jinými participujícími subjekty jsou orgány činné v trestním řízení, případně orgány dohledu a další, kterým to podle 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 časových serverů autorit časových razítek smějí být používány výhradně pro ověřování časových razítek vydaných těmito časovými servery.

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 Zakázané 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 dokument

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

1.5.2 Kontaktní osoba

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

1.5.3 Osoba rozhodující o souladu CPS s certifikační politikou

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

1.5.4 Postupy při schvalování CPS

Pokud je potřebné provést změny v příslušné CPS a vytvořit její novou verzi, určuje ředitel společnosti První certifikační autorita, a.s., osobu, která je oprávněna tyto změny provést. Nabytí platnosti nové verze CPS předchází její schválení ředitelem společnosti První certifikační autorita, a.s.

1.6 Přehled použitých pojmů a zkratek

tab. 2 - Pojmy

Pojem	Vysvětlení
bezpečné kryptografické zařízení	zařízení, na kterém je uložen soukromý klíč
bit	z anglického *binary digit* - číslice dvojkové soustavy - základní a současně nejmenší jednotka informace v číslicové technice
časové razítko	elektronické časové razítko, nebo kvalifikované elektronické časové razítko dle platné legislativy pro služby vytvářející důvěru
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	elektronická pečeť, nebo zaručená elektronická pečeť, nebo uznávaná elektronická pečeť, nebo kvalifikovaná elektronická pečeť dle platné legislativy pro služby vytvářející důvěru
elektronická značka	elektronická značka dle platné legislativy pro služby vytvářející důvěru
elektronický podpis	elektronický podpis, nebo zaručený elektronický podpis, nebo kvalifikovaný elektronický podpis, nebo uznávaný elektronický podpis dle platné legislativy pro služby vytvářející důvěru
hashovací funkce	transformace, která jako vstup přijímá řetězec znaků o libovolné délce a výsledkem je řetězec znaků s pevnou délkou (hash)
kořenová CA	certifikační autorita vydávající certifikáty podřízeným certifikačním autoritám
kvalifikovaný certifikát pro elektronický podpis	certifikát definovaný platnou legislativou pro služby vytvářející důvěru
kvalifikovaný prostředek pro vytváření elektronických podpisů	prostředek pro vytváření elektronických podpisů, který splňuje požadavky stanovené v příloze II eIDAS

legislativa pro služby vytvářející důvěru	legislativa České republiky a Slovenské republiky vztahující se ke službám vytvářejícím důvěru pro elektronické transakce a nařízení eIDAS
OCSP respondér	server poskytující protokolem OCSP údaje o stavu certifikátu veřejného klíče
orgán dohledu	orgán dohledu nad dodržováním legislativy pro služby vytvářející důvěru
párová data	soukromý a jemu odpovídající veřejný klíč
písemná smlouva	text smlouvy v elektronické nebo listinné podobě
prostředek pro vytváření elektronických podpisů	konfigurované programové vybavení nebo technické zařízení, které se používá k vytváření elektronických podpisů
služba vytvářející důvěru / kvalifikovaná služba vytvářející důvěru	elektronická služba / kvalifikovaná služba vytvářející důvěru, definovaná eIDAS
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/značky/pečetě
spoléhající se strana	subjekt spoléhající se při své činnosti na certifikát
TWINS	obchodní produkt I.CA, obsahující dvojici certifikátů: ▪ kvalifikovaný certifikát pro elektronický podpis – vydaný v souladu s odpovídající CP, ▪ komerční certifikát – vydaný výhradně na základě smluvního vztahu mezi I.CA a koncovým uživatelem
veřejný klíč	jedinečná data pro ověřování elektronické podpisu/značky/pečetě
vydávající, podřízená CA	pro účely tohoto dokumentu CA vydávající certifikáty koncovým uživatelům
zákon o ochraně utajovaných informací	zákon České republiky č. 412/2005 Sb., o ochraně utajovaných informací a o bezpečnostní způsobilosti, ve znění pozdějších předpisů
zákoník práce	zákon České republiky č. 262/2006 Sb., zákoník práce, ve znění pozdějších předpisů

tab. 3 - Zkratky

Zkratka	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
CRL	Certificate Revocation List, seznam zneplatněných certifikátů obsahující certifikáty, které již nelze pokládat za platné
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.
IEC	International Electrotechnical Commission, světová organizace publikující standardy pro elektrotechniku, elektroniku, sdělovací techniku a příbuzné obory
IPS	Intrusion Prevention System, systém prevence průniku
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
QSCD	Qualified Electronic Signature/Seal Creation Device, zařízení pro tvorbu kvalifikovaného elektronického podpisu/pečetě
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
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	Coordinated Universal 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)
ZOOÚ	aktuální legislativa týkající se ochrany osobních údajů

2 ODPOVĚDNOST ZA ZVEŘEJŇOVÁNÍ A ZA ÚLOŽIŠTĚ

2.1 Úložiště

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

2.2 Zveřejňování certifikačních informací

Základní adresy (dále též informační adresy), na nichž lze nalézt informace o společnosti První certifikační autorita, a.s., jsou:

- adresa sídla společnosti:

  První certifikační autorita, a.s.

  Podvinný mlýn 2178/6

  190 00 Praha 9

  Česká republika
- internetová adresa http://www.ica.cz,
- sídla registračních autorit.

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

Na výše uvedené internetové adrese lze získat informace o:

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

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

V případě zneplatnění certifikátů sloužících v procesech vydávání certifikátů koncovým uživatelům, vydávání seznamů zneplatněných certifikátů a poskytování informací o stavu certifikátů (dále též infrastrukturní certifikáty) z důvodu podezření na kompromitaci, případně samotné kompromitace příslušného soukromého klíče oznámí I.CA tuto skutečnost na své

internetové informační adrese a prostřednictvím celostátně distribuovaného deníku Hospodářské noviny nebo Mladá fronta Dnes, resp. Hospodárske noviny nebo Sme.

2.3 Čas nebo četnost zveřejňování

Viz kapitola 2.3 konkrétní CP.

2.4 Řízení přístupu k jednotlivým typům úložišť

Veškeré veřejné informace 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 s platnými technickými standardy a normami.

3.1.2 Požadavek na významovost jmen

V procesu vydávání certifikátu je vždy vyžadována významovost všech ověřitelných jmen uvedených v položkách pole Subject, resp. rozšíření SubjectAlternativeName. Podporované položky tohoto pole a rozšíření jsou uvedeny v konkrétní CP.

3.1.3 Anonymita nebo používání pseudonymu držitele certifikátu

Viz kapitola 3.1.3 konkrétní CP.

3.1.4 Pravidla pro interpretaci různých forem jmen

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

3.1.5 Jedinečnost jmen

Uvedeno v kapitole 3.1.5 konkrétní certifikační politiky.

3.1.6 Uznávání, ověřování a poslání obchodních značek

Certifikáty, vydávané podle této CPS, resp. příslušných CP mohou obsahovat pouze obchodní značky, jejichž vlastnictví nebo pronájem byly doloženy. Veškeré důsledky plynoucí z neoprávněného užívání ochranné známky nesou držitelé certifikátů.

3.2 Počáteční ověření identity

Postup ověřování identity je uveden v kapitole 3.2 konkrétní CP a dále upřesněn v interním dokumentu:

- „Směrnice pro pracovníky RA I.CA“.

3.2.1 Ověřování vlastnictví soukromého klíče

Vlastnictví soukromého klíče odpovídajícího veřejnému klíči v žádosti o Certifikát se prokazuje předložením žádosti ve formátu PKCS#10. Ta je zmíněným soukromým klíčem elektronicky podepsána, resp. opatřena elektronickou značkou nebo pečetí a držitel

soukromého klíče tak prokazuje, že v době tvorby elektronického podpisu, resp. elektronické značky nebo pečetě soukromý klíč vlastnil.

3.2.2 Ověřování identity organizace

Postup popsán v kapitole 3.2.2 konkrétní CP a dále v interním dokumentu:

- „Směrnice pro pracovníky RA I.CA“.

3.2.3 Ověřování identity fyzické osoby

Postup je popsán v kapitole 3.2.3 konkrétní CP a dále v interním dokumentu:

- „Směrnice pro pracovníky RA I.CA“.

3.2.4 Neověřované informace vztahující se k držiteli certifikátu

Neověřované informace jsou vždy uvedeny v kapitole 3.2.4 konkrétní CP.

3.2.5 Ověřování kompetencí

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

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

Postup ověřování dalších specifických práv je popsán v kapitole 3.2.5 konkrétní CP.

3.2.6 Kritéria pro interoperabilitu

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

3.3 Identifikace a autentizace při požadavku na výměnu klíče

3.3.1 Identifikace a autentizace při běžném požadavku na výměnu klíče

Vždy je nutné vydat nový certifikát s novým veřejným klíčem. Požadavky jsou uvedeny v kapitole 3.3.1 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, resp. certifikátů pro autentizaci internetových stránek 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, resp. opatřena elektronickou značkou nebo 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 elektronickým podpisem /značkou/ pečetí potvrzuje, že údaje o subjektu nebyly změněny.

3.3.2 Identifikace a autentizace při požadavku na výměnu klíče 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 požadavku na zneplatnění certifikátu

Konkrétní způsoby identifikace a autentizace při zpracování požadavků na zneplatnění certifikátu jsou uvedeny v kapitole 3.4 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,
- časového serveru autority časových razítek,

je ředitel I.CA.

Žadatelem o zneplatnění certifikátu kořenové certifikační autority, popř. certifikátu, souvisejícího s kvalifikovanými certifikačními službami, může být taktéž představitel úřadu, který společnosti První certifikační autorita, a.s., udělil statut kvalifikovaného poskytovatele služeb vytvářejících důvěru. 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 Kdo může požádat o vydání certifikátu

Žádost o vydání certifikátu může podat fyzická osoba nebo Organizace. Subjekty oprávněné podat žádost o vydání certifikátu jsou uvedeny v kapitole 4.1.1 konkrétní CP.

4.1.2 Registrační proces a odpovědnosti

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

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.

Poskytovatel Služeb je zejména povinen Služby poskytovat v souladu s platnou legislativou, konkrétní CP a touto CPS, Systémovou bezpečnostní politikou 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“.

Kontrola CAA záznamů, tam kde je to relevantní, je prováděna podle interního dokumentu:

- „Postupy ověřování při žádosti o QC-web/EV SSL certifikát“.

4.2.1 Provádění identifikace a autentizace

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

4.2.2 Schválení nebo zamítnutí žádosti o certifikát

V případě vydávání certifikátů poskytovatele Služeb 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 kapitole 4.2.2 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.

Pro certifikáty koncových uživatelů platí, že po kladném rozhodnutí o vydání certifikátu je I.CA povinna neprodleně Certifikát vydat. Přibližné časové údaje pro vydání certifikátu v pracovní dny a hodiny, není-li smluvně uvedeno jinak, jsou uvedeny v následujícím seznamu:

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

Výjimku tvoří SSL certifikáty, resp. certifikáty pro autentizaci internetových stránek 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 kapitole 4.3.1 konkrétní CP a upřesněny v interní dokumentaci:

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

4.3.2 Oznámení o vydání certifikátu držiteli certifikátu certifikační autoritou

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 kapitole 4.4.1 konkrétní CP.

Detailně je proces je popsán v interní dokumentaci:

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

4.4.2 Zveřejňování certifikátů certifikační autoritou

Certifikáty poskytovatele jsou zveřejňovány na webových stránkách I.CA, certifikáty související s kvalifikovanými službami vytvářejícími důvěru jsou navíc předány orgánu dohledu.

Pro certifikáty koncových uživatelů I.CA zajistí zveřejnění jí vydaných, vyjma Certifikátů:

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

4.4.3 Oznámení o vydání certifikátu certifikační autoritou jiným subjektům

Platí ustanovení kapitoly 4.4.2 a případně požadavky platné legislativy pro služby vytvářející důvěru.

4.5 Použití párových dat a certifikátu

4.5.1 Použití soukromého klíče a certifikátu držitelem certifikátu

Povinností držitele certifikátu mj. je:

- dodržovat veškerá relevantní ustanovení smlouvy o poskytování Služeb,
- užívat soukromý klíč a odpovídající certifikát vydaný podle konkrétní CP pouze pro účely stanovené v této CP a případně platnou legislativou pro služby vytvářející důvěru,
- nakládat se soukromým klíčem, který odpovídá veřejnému klíči obsaženému v certifikátu vydaném podle konkrétní CP, takovým způsobem, aby nemohlo dojít k jeho neoprávněnému použití,
- neprodleně uvědomit poskytovatele Služeb o skutečnostech, které vedou ke zneplatnění certifikátu, zejména o podezření, že soukromý klíč byl zneužit, požádat o zneplatnění certifikátu a ukončit používání příslušného soukromého klíče.

4.5.2 Použití veřejného klíče a certifikátu spoléhající se stranou

Spoléhající se strany jsou zejména povinny:

- získat z bezpečného zdroje certifikáty certifikačních autorit související s certifikátem koncového uživatele vydaným podle konkrétní CP, ověřit hodnoty jejich otisků a jejich platnost,
- provádět veškeré úkony potřebné k tomu, aby si ověřily, že certifikát je platný, tj.:
  - ověřit platnost certifikátu podle RFC5280, kapitola 6 (včetně celé certifikační cesty a odvolání platnosti certifikát),

- ověřit kvalifikovanost vydavatele kvalifikovaného certifikátu (jeho uvedení na seznamu důvěryhodných služeb s příslušnými atributy),

- dodržovat veškerá ustanovení odpovídající CP a případně platné legislativy pro služby vytvářející důvěru, vztahující se k povinnostem spoléhající se strany.

4.6 Obnovení certifikátu

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

Služba obnovení certifikátu není poskytována.

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

4.6.1 Podmínky pro obnovení certifikátu

Viz kapitola 4.6.

4.6.2 Kdo může žádat o obnovení

Viz kapitola 4.6.

4.6.3 Zpracování požadavku na obnovení certifikátu

Viz kapitola 4.6.

4.6.4 Oznámení o vydání nového certifikátu držiteli certifikátu

Viz kapitola 4.6.

4.6.5 Úkony spojené s převzetím obnoveného certifikátu

Viz kapitola 4.6.

4.6.6 Zveřejňování obnovených certifikátů certifikační autoritou

Viz kapitola 4.6.

4.6.7 Oznámení o vydání certifikátu certifikační autoritou jiným subjektům

Viz kapitola 4.6.

4.7 Výměna veřejného klíče v certifikátu

Popsáno v kapitole 4.7 konkrétní certifikační politiky.

4.7.1 Podmínky pro výměnu veřejného klíče v certifikátu

Viz kapitola 4.7.

4.7.2 Kdo může požádat o výměnu veřejného klíče v certifikátu

Viz kapitola 4.7.

4.7.3 Zpracování požadavku na výměnu veřejného klíče v certifikátu

Viz kapitola 4.7.

4.7.4 Oznámení o vydání nového certifikátu držiteli certifikátu

Viz kapitola 4.7.

4.7.5 Úkony spojené s převzetím certifikátu s vyměněným veřejným klíčem

Viz kapitola 4.7.

4.7.6 Zveřejňování certifikátů s vyměněným veřejným klíčem certifikační autoritou

Viz kapitola 4.7.

4.7.7 Oznámení o vydání certifikátu certifikační autoritou jiným subjektům

Viz kapitola 4.7.

4.8 Změna údajů v certifikátu

Popsáno v kapitole 4.8 konkrétní certifikační politiky.

4.8.1 Podmínky pro změnu údajů v certifikátu

Viz kapitola 4.8.

4.8.2 Kdo může požádat o změnu údajů v certifikátu

Viz kapitola 4.8.

4.8.3 Zpracování požadavku na změnu údajů v certifikátu

Viz kapitola 4.8.

4.8.4 Oznámení o vydání certifikátu se změněnými údaji držiteli certifikátu

Viz kapitola 4.8.

4.8.5 Úkony spojené s převzetím certifikátu se změněnými údaji certifikační autoritou

Viz kapitola 4.8.

4.8.6 Zveřejňování certifikátů se změněnými údaji

Viz kapitola 4.8.

4.8.7 Oznámení o vydání certifikátu certifikační autoritou jiným subjektům

Viz kapitola 4.8.

4.9 Zneplatnění a pozastavení platnosti certifikátu

4.9.1 Podmínky pro zneplatnění

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 musí být zneplatněn na základě následujících okolností:

- dojde ke kompromitaci, resp. existuje důvodné podezření, že došlo ke kompromitaci, soukromého klíče odpovídajícího veřejnému klíči tohoto certifikátu,
- žádost ředitele I.CA,
- nastanou-li skutečnosti uvedené v platné legislativě týkající se služeb vytvářejících důvěru, resp. v technických standardech a normách.

4.9.1.2 Certifikáty koncových uživatelů

Certifikát musí být zneplatněn na základě následujících okolností:

- dojde ke kompromitaci, resp. existuje důvodné podezření, že došlo ke kompromitaci, soukromého klíče odpovídajícího veřejnému klíči tohoto certifikátu,
- je porušeno ustanovení smlouvy o poskytování Služby podle konkrétní CP ze strany držitele certifikátu,
- v případech, kdy nastanou skutečnosti uvedené v platné legislativě pro služby vytvářející důvěru nebo příslušných technických standardech a normám (např. neplatnost údajů v certifikátu),
- pokud je veřejný klíč v žádosti o vydání Certifikátu duplicitní s veřejným klíčem v již vydaném Certifikátu.

I.CA si vyhrazuje právo akceptování i jiných podmínek na zneplatnění certifikátu koncového uživatele, které však nesmí být v rozporu s platnou legislativou pro služby vytvářející důvěru.

4.9.2 Kdo může požádat o zneplatnění

4.9.2.1 Certifikáty poskytovatele (I.CA)

Žádost o zneplatnění mohou podat:

- ředitel I.CA,
- případně další subjekty definované platnou legislativou pro služby vytvářející důvěru.

4.9.2.2 Certifikáty koncových uživatelů

Žádost o zneplatnění mohou podat:

- držitel certifikátu,
- subjekt, který k tomu byl explicitně určen ve smlouvě o poskytování příslušné Služby,
- osoba oprávněná z pozůstalostního řízení držitele certifikátu,
- poskytovatel Služby (oprávněným žadatelem o zneplatnění Certifikátu vydaného I.CA je v tomto případě ředitel I.CA):
  - v případě, že certifikát byl vydán na základě nepravdivých údajů,
  - pokud prokazatelně zjistí, že soukromý klíč, patřící k veřejnému klíči uvedenému v certifikátu, byl kompromitován,
  - dozví-li se prokazatelně, že certifikát byl použit v rozporu s omezením definovaným v kapitole 1.4.2,
  - dozví-li se prokazatelně, že držitel Certifikátu zemřel, nebo soud držiteli Certifikátu omezil svéprávnost, nebo pokud údaje, na jejichž základě byl Certifikát vydán, pozbyly pravdivosti,
  - pokud je veřejný klíč v žádosti o vydání certifikátu duplicitní s veřejným klíčem v již vydaném certifikátu,
  - pokud zjistí, že při vydání certifikátu nebyly splněny požadavky platné legislativy pro služby vytvářející důvěru,
- případně orgán dohledu, resp. subjekty definované platnou legislativou pro služby vytvářející důvěru.

4.9.3 Postup při žádosti o zneplatnění

Způsob podání žádosti o zneplatnění certifikátu koncového uživatele je vždy popsán v kapitole 4.9.3 konkrétní CP.

Požadavky na identifikaci a autentizaci jsou uvedeny v kapitole 3.4.

4.9.4 Prodleva při požadavku na zneplatnění certifikátu

Požadavek na zneplatnění certifikátu musí být podán bezodkladně.

4.9.5 Doba zpracování žádosti o zneplatnění

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 třetích stran při kontrole zneplatnění

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

4.9.7 Periodicita vydávání seznamu zneplatněných certifikátů

Periodicita vydávání seznamu zneplatněných certifikátů je uvedena v kapitole 4.9.7 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 Dostupnost ověřování stavu certifikátu on-line

Služba ověřováni 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 stavu certifikátu on-line

Viz kapitola 4.9.9.

4.9.11 Jiné způsoby oznamování zneplatnění certifikátu

Není relevantní pro tento dokument.

4.9.12 Zvláštní postupy při kompromitaci klíče

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

4.9.13 Podmínky pro pozastavení platnosti certifikátu

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

4.9.14 Kdo může požádat o pozastavení platnosti

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

4.9.15 Postup při žádosti o pozastavení platnosti

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

4.9.16 Omezení doby pozastavení platnosti

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

4.10 Služby ověření stavu certifikátu

4.10.1 Funkční charakteristiky

Seznamy veřejných certifikátů jsou poskytovány formou zveřejňování informací, seznamy zneplatněných certifikátů jsou poskytovány jak formou zveřejňování informací, tak uvedením distribučních míst CRL v jí vydaných certifikátech.

Skutečnost, že certifikační autority poskytují informace o stavu certifikátu formou OCSP (služba OCSP), je uvedena v jimi vydaných certifikátech.

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.

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 stavu certifikátu

I.CA na seznamu zneplatněných certifikátů udržuje i expirované certifikáty, a to po dobu tří dnů po jejich expiraci. Důvodem omezení doby, po kterou jsou expirované certifikáty na CRL uváděny, je snaha udržet rozsah CRL v rozumných mezích.

V případě rozhodnutí I.CA o ukončení služby poskytování stavu certifikátů (CRL), I.CA vydá a zveřejní poslední CRL s hodnotou položky "nextupdate" rovnou "99991231235959Z".

I.CA ve službě stavu certifikátu (OCSP) poskytuje v odpovědi i informaci o stavu expirovaných certifikátů, pokud od jejich expirace neuplynula doba delší než tři dny (v souladu s CRL a s ohledem na konzistentnost informací v CRL a OCSP).

V případě, že se pro certifikát vydávající CA blíží doba jeho expirace, uvede I.CA v poslední OCSP odpovědi pro každý vydaný certifikát hodnotu položky "nextupdate" rovnou "99991231235959Z".

4.11 Konec smlouvy o vydávání certifikátů

Po ukončení platnosti smlouvy o vydávání certifikátů přetrvávají z ní vyplývající závazky I.CA, a to po dobu platnosti posledního podle ní vydaného certifikátu.

4.12 Úschova a obnova klíčů

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

4.12.1 Politika a postupy při úschově a obnově klíčů

Viz kapitola 4.12.

4.12.2 Politika a postupy při zapouzdřování a obnovování šifrovacího klíče relace

Viz kapitola 4.12.

5 POSTUPY SPRÁVY, ŘÍZENÍ A PROVOZU

Postupy správy, řízení a provozu jsou zaměřeny především na:

- důvěryhodné systémy určené k podpoře Služeb,
- veškeré procesy podporující poskytování výše uvedených Služeb.

Postupy správy, řízení a provozu jsou řešeny jak v základních dokumentech Celková bezpečnostní politika, Systémová bezpečnostní politika, Certifikační prováděcí směrnice, Plán pro zvládání krizových situací a plán obnovy, tak v upřesňujících interních dokumentech. Uvedené dokumenty reflektují výsledky periodicky prováděné analýzy rizik.

5.1 Fyzická bezpečnost

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

Důvěryhodné systémy určené k podpoře Služeb jsou umístěny ve vyhrazených prostorách provozních pracovišť. Tyto prostory jsou zabezpečené obdobně, jako zabezpečené oblasti kategorie „Důvěrné“ podle zákona o ochraně utajovaných informací.

5.1.2 Fyzický přístup

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

5.1.3 Elektřina a klimatizace

V prostorách, kde jsou umístěny důvěryhodné systémy určené k podpoře 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

Důvěryhodné systémy určené k podpoře Služeb jsou umístěny takovým způsobem, aby nemohly být zaplaveny ani stoletou vodou. Provozní pracoviště jsou podle potřeby vybavena čidly průniku vody pro případ zaplavení vodou z topení, nebo vodou ze střechy při prudkém dešti.

5.1.5 Protipožární opatření a ochrana

V objektech provozních pracovišť a pracovišť pro uchovávání informací je instalována elektronická požární signalizace (EPS). Vstupní dveře vyhrazených prostor, ve kterých jsou umístěny důvěryhodné systémy určené k podpoře 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 dle platné legislativy pro služby vytvářející důvěru uchovávat, jsou skladována v jiné geografické lokalitě, než je umístěno provozní pracoviště.

5.1.7 Nakládání s odpady

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

5.1.8 Zálohy mimo budovu

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

5.2 Procedurální postupy

5.2.1 Důvěryhodné role

Pro vybrané činnosti jsou ve společnosti I.CA definovány důvěryhodné role. Postup jmenování zaměstnanců do důvěryhodných rolí, specifikace těchto rolí včetně odpovídajících činností a odpovědností jsou uvedeny v interní dokumentaci, zejména v dokumentech:

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

Všichni zaměstnanci I.CA v důvěryhodných rolích nesmí být ve střetu zájmů, které by mohly ohrozit nestrannost operací I.CA.

5.2.2 Počet osob požadovaných pro zajištění jednotlivých činností

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

- inicializaci kryptografického modulu,
- generování párových dat veškerých certifikačních autorit a OCSP respondéru kořenové certifikační autority,
- ničení soukromých klíčů veškerých certifikačních autorit a OCSP respondéru kořenové certifikační autority,
- zálohování soukromých klíčů certifikačních autorit, vydávajících kvalifikované certifikáty koncovým uživatelům, včetně kořenové certifikační autority,
- obnovu soukromých klíčů veškerých certifikačních autorit a jejich OCSP respondérů,
- aktivaci a deaktivaci soukromých klíčů veškerých certifikačních autorit a OCSP respondéru kořenové certifikační autority.

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

Podrobné informace jsou vždy uvedeny v kapitole 5.2.2 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“.

Pro vybrané činnosti využívají pracovníci v důvěryhodných rolích dvoufaktorovou autentizaci.

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 postupy

5.3.1 Požadavky na kvalifikaci, praxi a bezúhonnost

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

- občanská bezúhonnost - prokazováno výpisem z rejstříku trestů, nebo čestným prohlášením,
- 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 služeb vytvářejících důvěru,
- znalost v oblasti infrastruktury veřejných klíčů a informační bezpečnosti.

Ostatní zaměstnanci I.CA podílející se na zajištění 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.

Pro vykonávání řídící funkce musí mít vedoucí zaměstnanci zkušenosti získané praxí nebo odbornými školeními s ohledem na důvěryhodnost Služeb, znalost bezpečnostních postupů s odpovědností za bezpečnost a zkušenosti s bezpečností informací a hodnocením rizik.

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 školení

Zaměstnanci I.CA jsou odborně zaškoleni pro používání určeného programového vybavení a speciálních zařízení. Zaškolení se provádí kombinací metody samostudia a metodickým vedením již zaškoleným pracovníkem. Školení zahrnuje oblasti informační bezpečnosti, ochrany osobních údajů a další relevantní témata.

Problematika je detailně popsána v interním dokumentu:

- „Kontrolní činnost, bezúhonnost a odbornost“.

5.3.4 Požadavky a periodicita doškolování

Dvakrát za 12 měsíců jsou zaměstnancům I.CA poskytovány aktuální informace o vývoji v předmětných oblastech.

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

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 dodavatele

I.CA může nebo musí některé činnosti zajišťovat smluvně, za činnost nezávislých dodavatelů plně odpovídá. Tyto obchodně právní vztahy jsou upraveny 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 certifikačními politikami, relevantními částmi interní dokumentace I.CA, které jim budou poskytnuty a předepsanými normativními dokumenty. V případě porušení povinností stanovených v uvedených dokumentech jsou vyžadovány smluvní pokuty, případně je s dodavatelem okamžitě ukončena smlouva.

5.3.8 Dokumentace poskytovaná zaměstnancům

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

5.4 Postupy zpracování auditních záznamů

Zaznamenávány jsou veškeré události požadované v případě kvalifikovaných certifikátů platnou legislativou pro služby vytvářející důvěru a jí odkazovanými technickými standardy a normami, v ostatních případech relevantními technickými standardy a normami, 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 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

Speciálními případy zaznamenávání událostí jsou události generování párových dat kořenové certifikační autority a generování párových dat podřízené certifikační autority. V případě autority kořenové celý proces probíhá v souladu s platnou legislativou pro služby vytvářející důvěru a relevantními technickými standardy a normami, 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.

Pro generování párových dat certifikační autority minimálně platí, že:

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

S ohledem na požadavky relevantních technických standardů a norem a platné legislativy pro služby vytvářející důvěru 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 interním dokumentu:

- „Příručka administrátora“,

v případě bezpečnostního incidentu okamžitě.

5.4.3 Doba uchování auditních záznamů

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

5.4.4 Ochrana auditních záznamů

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

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

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

Ochrana výše uvedených typů auditních záznamů je popsána v interní dokumentaci - viz kapitola 5.4.

5.4.5 Postupy pro zálohování auditních záznamů

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

5.4.6 Systém shromažďování auditních záznamů (interní nebo externí)

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

5.4.7 Postup při oznamování události subjektu, který ji způsobil

Subjekt není o zapsání události do auditního záznamu informován.

5.4.8 Hodnocení zranitelnosti

Hodnocení zranitelnosti je ve společnosti První certifikační autorita, a.s., prováděno v periodických intervalech jako součást analýzy rizik. Sledování zranitelnosti zařízení a programového vybavení souvisejících se Službami je popsáno v interním dokumentu:

- „Příručka administrátora“.

5.5 Uchovávání záznamů

Uchovávání záznamů, tj. informací a dokumentace, je ve společnosti První certifikační autorita, a.s., upraveno interní dokumentací.

- „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 uchovávaných záznamů

I.CA uchovává níže uvedené záznamy (v elektronické nebo listinné podobě), které souvisejí s poskytovanými Službami, 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,
- záznamy související s životním cyklem vydaných certifikátů, včetně těchto certifikátů a certifikátů s nimi souvisejících,
- případný videozáznam průběhu generování párových dat certifikační autority,
- další záznamy potřebné pro vydávání certifikátů,
- záznam o manipulaci s informacemi (např. převzetí, předání, uložení, kontrola, konverze do elektronické podoby atd.),
- aplikační programové vybavení, provozní a bezpečnostní dokumentace.

5.5.2 Doba uchování záznamů

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

Ostatní záznamy jsou uchovávány v souladu s ustanoveními kapitoly 5.4.3.

Postupy při uchovávání záznamů jsou upraveny interní dokumentací I.CA - viz kapitola 5.5..

5.5.3 Ochrana úložiště záznamů

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

Postupy při ochraně úložiště záznamů jsou upraveny interní dokumentací - viz kapitola 5.5.

5.5.4 Postupy při zálohování záznamů

Postupy při zálohování záznamů jsou upraveny interní dokumentací - viz kapitola 5.5..

5.5.5 Požadavky na používání časových razítek při uchovávání záznamů

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

5.5.6 Systém shromažďování uchovávaných záznamů (interní nebo externí)

Záznamy jsou ukládány na místo určené ředitelem I.CA.

Samotná problematika přípravy a způsobu ukládání záznamů v elektronické i písemné podobě je upravena interní dokumentací - viz kapitola 5.5. Shromažďování záznamů je evidováno.

5.5.7 Postupy pro získání a ověření uchovávaných informací

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

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

O každém takto povoleném přístupu je pořizován písemný záznam.

5.6 Výměna klíče

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

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

5.7 Obnova po havárii nebo kompromitaci

5.7.1 Postup ošetření incidentu nebo kompromitace

V případě výskytu těchto událostí postupuje I.CA v souladu s 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, programového vybavení nebo dat

Viz kapitola 5.7.1.

5.7.3 Postup při kompromitaci soukromého klíče

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

- ukončí jeho používání,
- okamžitě a trvale zneplatní příslušný certifikát a zničí jemu odpovídající soukromý klíč,
- zneplatní všechny platné certifikáty vydané touto autoritou,

- bezodkladně o této skutečnosti, včetně důvodu, informuje na své internetové informační adrese, pro zpřístupnění této informace je využit i seznam zneplatněných certifikátů,
- v případě kvalifikovaných certifikátů oznámí orgánu dohledu 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 Služeb.

5.7.4 Schopnost obnovit činnost po havárii

V případě havárie postupuje I.CA v souladu s 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 certifikátů orgánu dohledu,
- ukončení činnosti CA musí být zveřejněno na internetové adrese podle kapitoly 2.2,
- pokud je součástí ukončení činnosti CA ukončení platnosti jejího certifikátu, musí být součástí oznámení i tato informace včetně uvedení důvodu ukončení platnosti,
- ukončování činnosti je řízený proces probíhající podle předem připraveného plánu, jehož součástí je popis postupu uchovávání a zpřístupňování informací pro poskytování důkazů v soudním a správním řízení a pro účely zajištění kontinuity Služeb,
- po dobu platnosti 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 CPS, resp. konkrétní CP.

V případě odnětí statutu kvalifikovaného poskytovatele služeb vytvářejících důvěru:

- informace musí být písemně nebo elektronicky oznámena všem držitelům platných certifikátů a subjektům, které mají uzavřenou smlouvu přímo se vztahující k poskytování služeb vytvářejících důvěru,
- informace musí být zveřejněna v souladu s kapitolou 2.2 a na všech pracovištích registračních autorit; součástí informace bude i sdělení, že kvalifikované systémové certifikáty nelze nadále používat v souladu s účelem jejich vydání,
- o dalším postupu rozhodne ředitel I.CA na základě rozhodnutí orgánu dohledu.

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

Problematika plánovaného ukončení činnosti I.CA jako kvalifikovaného poskytovatele služeb vytvářejících důvěru je detailně uvedena v interním dokumentu:

- „Ukončení činnosti služeb I.CA“.

6 ŘÍZENÍ TECHNICKÉ BEZPEČNOSTI

6.1 Generování a instalace párových dat

6.1.1 Generování párových dat

Generování párových dat certifikačních autorit a jim odpovídajících OCSP respondérů, které probíhá v zabezpečených vyhrazených prostorách provozních pracovišť, podle předem připraveného scénáře, v souladu s požadavky kapitol 5.2 a 5.4.1 a o jehož průběhu je vyhotoven písemný protokol, je prováděno v kryptografickém modulu, který byl hodnocen podle FIPS PUB 140-2 úroveň 3.

Veškeré požadavky na proces generování párových dat CA 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 QSCD. Soukromé klíče těchto párových dat jsou na čipové kartě uloženy v neexportovatelném tvaru a k jejich použití je nutné zadat PIN.

- Generování párových dat vztahujících se k certifikátům vydávaným koncovým uživatelům je prováděno na zařízeních, která jsou pod výhradní kontrolou příslušných držitelů soukromých klíčů. Úložištěm těchto párových dat může být jak hardware, tak software. V případě kvalifikovaných certifikátů, jejichž soukromý klíč odpovídající veřejnému klíči v Certifikátu je uložen na zařízení typu QSCD, je průběžně prováděna kontrola přítomnosti zařízení na důvěryhodném seznamu EU.

6.1.2 Předávání soukromého klíče jeho držiteli

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

Služba generování párových dat koncovým uživatelům není poskytována.

6.1.3 Předávání veřejného klíče vydavateli certifikátu

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

6.1.4 Poskytování veřejného klíče CA spoléhajícím se stranám

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

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

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

6.1.5 Délky klíčů

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 Parametry veřejného klíče a kontrola jeho 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 příslušný certifikát neprodleně zneplatněn, držitel takového certifikátu o tomto neprodleně a vhodným způsobem informován a vyzván ke generování nových párových dat.

6.1.7 Účely použití klíče (dle rozšíření key usage X.509 v3)

Možnosti použití klíče jsou uvedeny v rozšíření certifikátu.

6.2 Ochrana soukromého klíče a technologie kryptografických modulů

Konkrétní postupy ochrany soukromého klíče certifikačních autorit 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 Řízení a standardy kryptografických modulů

Generování párových dat a uložení soukromých klíčů certifikačních autorit a jejich OCSP respondérů probíhá v kryptografických modulech, které splňují požadavky legislativy pro služby vytvářející důvěru, tedy standardu FIPS PUB 140-2 úroveň 3.

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

Pokud je pro činnosti spojené s kryptografickým modulem nezbytná přítomnost dvou členů vedení I.CA, pak každý z nich zná část pouze kódu k provedení těchto činností.

6.2.3 Úschova soukromého klíče

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

6.2.4 Zálohování soukromého klíče

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

6.2.5 Uchovávání soukromého klíče

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

6.2.6 Transfer soukromého klíče do nebo z kryptografického modulu

Transfer soukromých klíčů podřízených certifikačních autorit vydávajících certifikáty koncovým uživatelům v souladu s legislativou pro služby vytvářející důvěru z a do kryptografického modulu probíhá za přímé osobní účasti nejméně dvou členů vedení I.CA.

Transfer soukromých klíčů ostatních podřízených certifikačních autorit a všech OCSP respondérů z kryptografického modulu probíhá za přímé osobní účasti nejméně jednoho člena vedení I.CA.

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

O provedeném transferu je vždy pořízen písemný záznam.

6.2.7 Uložení soukromého klíče v kryptografickém modulu

Soukromé klíče certifikačních autorit a jejich OCSP respondérů jsou uloženy v kryptografickém modulu, splňujícím požadavky platné legislativy pro služby vytvářející důvěru, tedy standardu FIPS PUB 140-2 úroveň 3.

6.2.8 Postup aktivace soukromého klíče

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

Aktivace soukromých klíčů OCSP respondérů ostatních certifikačních autorit uložených v kryptografickém modulu je prováděna za přímé osobní účasti jednoho člena vedení I.CA s využitím aktivační čipové karty podle přesně určeného postupu, který je upraven interním dokumentu:

- „HSM/Private Server“.

Aktivace soukromého klíče časového serveru autority časových razítek je prováděna postupem popsaným v interním dokumentu:

- „Správa TSS“.

O provedené aktivaci je pořízen písemný záznam.

6.2.9 Postup deaktivace soukromého klíče

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

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

Postup je upraven interním dokumentem:

- „HSM/Private Server“.

O provedené deaktivaci je pořízen písemný záznam.

Aktivace soukromého klíče časového serveru autority časových razítek je prováděna postupem popsaným v interním dokumentu:

- „Správa TSS“.

O provedené deaktivaci je pořízen písemný záznam.

6.2.10 Postup ničení soukromého klíče

Ničení soukromých klíčů certifikačních autorit a jejich OCSP respondérů uložených v kryptografickém modulu je realizováno nativními prostředky tohoto kryptografického modulu a za přímé osobní účasti nejméně dvou členů vedení I.CA podle přesně určeného postupu, který je upraven interním dokumentem:

- „HSM/Private Server“,

Ničení soukromého klíče časového serveru autority časových razítek je prováděna postupem popsaným v interním dokumentu:

- „Správa TSS“.

O provedeném ničení je pořízen písemný záznam.

Externí média, na kterých jsou uloženy zálohy výše uvedených soukromých klíčů, jsou rovněž zničena. Ničení, spočívající ve fyzické destrukci těchto nosičů, probíhá za přímé osobní účasti nejméně dvou členů vedení I.CA podle přesně určeného postupu, který je upraven interní dokumentací. O provedeném ničení je pořízen písemný záznam.

6.2.11 Hodnocení kryptografických modulů

Kryptografické moduly, sloužící ke generování párových dat a uložení soukromých klíčů certifikačních autorit a jejich OCSP respondérů splňují požadavky legislativy pro služby vytvářející důvěru, tedy standardu FIPS PUB 140-2 úroveň 3. Bezpečnost modulů je sledována po celou dobu jejich využívání.

6.3 Další aspekty správy párových dat

6.3.1 Uchovávání veřejných klíčů

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

6.3.2 Doba funkčnosti certifikátu a doba použitelnosti párových dat

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

6.4 Aktivační data

6.4.1 Generování a instalace aktivačních dat

Aktivační data certifikačních autorit, jejich OCSP respondérů a časových serverů jsou vytvářena v průběhu generování odpovídajících párových dat. Konkrétní postup je popsán v interní dokumentaci:

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

6.4.2 Ochrana aktivačních dat

Aktivační data certifikačních autorit, jejich OCSP respondérů a časových serverů jsou chráněna způsobem popsaným v interní dokumentaci:

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

6.4.3 Ostatní aspekty aktivačních dat

Aktivační data soukromých klíčů certifikačních autorit, jejich OCSP respondérů a časových serverů nesmí být použita k jiným účelům, ani přenášena nebo uchovávána v otevřené podobě. Veškeré aspekty jsou popsány v interní dokumentaci:

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

6.5 Řízení počítačové bezpečnosti

6.5.1 Specifické technické požadavky na počítačovou bezpečnost

Úroveň bezpečnosti použitých komponent pro poskytování Služeb je definována v případě kvalifikovaných certifikátů služeb platnou legislativou pro služby vytvářející důvěru a jí odkazovanými technickými standardy a normami, v ostatních případech relevantními technickými standardy a normami. 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 počítačové bezpečnosti I.CA je založeno na požadavcích uvedených v technických standardech a normách, zejména:

- CEN/TS 419261 Security requirements for trustworthy systems managing certificates and time-stamps.
- ČSN ETSI EN 319 401 Elektronické podpisy a infrastruktury (ESI) - Obecné požadavky politiky pro poskytovatele důvěryhodných služeb.
- ETSI EN 319 401 Electronic Signatures and Infrastructures (ESI); General Policy Requirements for Trust Service Providers.
- ČSN ETSI EN 319 403 Elektronické podpisy a infrastruktury (ESI) - Posuzování shody poskytovatelů důvěryhodných služeb - Požadavky na orgány posuzování shody posuzující poskytovatele důvěryhodných služeb.
- ETSI EN 319 403 Electronic Signatures and Infrastructures (ESI); Trust Service Provider Conformity Assessment - Requirements for conformity assessment bodies assessing Trust Service Providers.
- ČSN ETSI EN 319 411-1 Elektronické podpisy a infrastruktury (ESI) - Požadavky politiky a bezpečnosti na poskytovatele důvěryhodných služeb vydávající certifikáty - Část 1: Obecné požadavky.

- 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 na poskytovatele důvěryhodných služeb vydávající kvalifikované certifikáty EU.
- 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.
- 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 certifikačních autorit se dále řídí požadavky technických standardů a norem:

- FIPS PUB 140-2 Requirements for Cryptographic Modules.
- ISO 3166-1 Codes for the representation of names of countries and their subdivisions - Part 1: Country codes.
- ITU-T - X.501 Information technology – Open Systems Interconnection – The Directory: Models.
- ITU-T - X.509 Information technology – Open Systems Interconnection – The Directory: Public-key and attribute certificate frameworks.
- ITU-T - X.520 Information technology – Open Systems Interconnection – The Directory: Selected attribute types.
- RSA Laboratories - PKCS#10: Certification Request Syntax Standard.
- RFC 2560 X.509 Internet Public Key Infrastructure Online Certificate Status Protocol - OCSP.
- RFC 3647 Internet X.509 Public Key Infrastructure Certificate Policy and Certification Practices Framework.
- RFC 5019 The Lightweight Online Certificate Status Protocol (OCSP) Profile for High-Volume Environments.
- RFC 5280 Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile.
- RFC 6844 DNS Certification Authority Authorization (CAA) Resource Record.
- RFC 6962 Certificate Transparency.
- draft dokumentu EBA: Regulatory Technical Standards on Strong Customer Authentication and common and secure communication under Article 98 of Directive 2015/2366 (PSD2).

- ČSN ETSI EN 319 412-1 Elektronické podpisy a infrastruktury (ESI) - Profily certifikátu - Část 1: Přehled a společné datové struktury.
- ETSI EN 319 412-1 Electronic Signatures and Infrastructures (ESI); Certificate Profiles; Part 1: Overview and common data structures.
- ČSN ETSI EN 319 412-2 Elektronické podpisy a infrastruktury (ESI) - Profily certifikátu - Část 2: Profil certifikátu pro certifikáty vydávané fyzickým osobám.
- ETSI EN 319 412-2 Electronic Signatures and Infrastructures (ESI); Certificate Profiles; Part 2: Certificate profile for certificates issued to natural persons.
- ČSN ETSI EN 319 412-3 Elektronické podpisy a infrastruktury (ESI) - Profily certifikátu - Část 3: Profil certifikátu pro certifikáty vydávané právnickým osobám.
- ETSI EN 319 412-3 Electronic Signatures and Infrastructures (ESI); Certificate Profiles; Part 2: Certificate profile for certificates issued to legal persons.
- ČSN ETSI EN 319 412-5 Elektronické podpisy a infrastruktury (ESI) - Profily certifikátu - Část 5: Prohlášení „QC Statements“.
- ETSI EN 319 412-5 Electronic Signatures and Infrastructures (ESI); Certificate Profiles; Part 5: QCStatements.

6.6 Technické řízení životního cyklu

6.6.1 Řízení vývoje systému

Při vývoji systému je postupováno v souladu s interní dokumentací:

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

6.6.2 Řízení správy bezpečnosti

Kontrola řízení bezpečnosti informací, včetně kontroly souladu s technickými standardy a normami, je prováděna v rámci periodických kontrol služeb vytvářejících důvěru a dále formou auditů systému řízení bezpečnosti informací (ISMS).

Bezpečnost informací se v I.CA řídí těmito normami:

- ČSN ISO/IEC 27000 Informační technologie - Bezpečnostní techniky - Systémy řízení bezpečnosti informací - Přehled a slovník.
- ČSN ISO/IEC 27001 Informační technologie - Bezpečnostní techniky - Systémy řízení bezpečnosti informací - Požadavky.
- ČSN ISO/IEC 27002 Informační technologie - Bezpečnostní techniky - Soubor postupů pro opatření bezpečnosti informací.
- ČSN ISO/IEC 27006 Informační technologie - Bezpečnostní techniky - Požadavky na orgány provádějící audit a certifikaci systémů řízení bezpečnosti informací.

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 prováděno procesním přístupem typu „Plánování-Zavedení-Kontrola-Využití“ (Plan-Do-Check-Act, PDCA), který se skládá z navazujících procesů:

- vybudování - stanovení rozsahu a hranic, kterých se řízení bezpečnosti informací týká, určení bezpečnostní politiky, plánů a výběr bezpečnostních opatření v závislosti na vyhodnocených rizicích, to vše v souladu s celkovou bezpečnostní politikou, což je popsáno v interní dokumentaci:
  - 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 - účelné a systematické prosazení vybraných bezpečnostních opatření, 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 - zajištění zpětné vazby, pravidelné sledování a hodnocení úspěšných i nedostatečných stránek řízení bezpečnosti informací, předávání poznatků vedení společnosti k posouzení,, což je popsáno v dokumentech:
  - zprávy z interních kontrol,
  - zprávy z externích kontrol a auditů,
- údržba a zlepšování - provádění opatření k nápravě a zlepšování, na základě rozhodnutí vedení organizace.

6.7 Řízení bezpečnosti sítě

Informační systém kořenové certifikační autority je ve stavu off-line a není tedy propojen s žádnou externí síti. Ostatní důvěryhodné systémy určené k podpoře Služeb umístěné na provozních pracovištích I.CA nejsou přímo dostupné z veřejné sítě Internet. Tyto systémy jsou chráněny komerčním produktem typu firewall s integrovaným systémem IPS (Intrusion Prevention System). Veškerá komunikace mezi RA a provozními pracovišti je vedena šifrovaně. Detailní řešení řízení síťové bezpečnosti je popsáno v interní dokumentaci:

- „Systémová bezpečnostní politika CA a TSA - Důvěryhodné systémy pro vydávání certifikátů a časových razítek“,
- „Příručka administrátora“,
- „Firewall – provozní pracoviště“,
- „Plán pro zvládání krizových situací a plán obnovy“,
- „Obnova komponenty provozního pracoviště“,
- „Přemístění provozního pracoviště“.

6.8 Označování časovými razítky

Řešení je uvedeno v kapitole 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, pokud jsou tyto v certifikátu obsaženy:

- v kvalifikovaných certifikátech pro elektronický podpis, pečeť a pro autentizaci internetových stránek, systémových certifikátech, nekvalifikovaných (komerčních) SSL certifikátech (OVCP a DVCP) 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 pole Subject a rozšíření SubjectAlternativeName

Pole/položka	**Kvalifikované certifikáty pro elektronický podpis, pečeť a autentizaci internetových stránek, systémové certifikáty, nekvalifikované SSL certifikáty (OVCP, DVCP)**	**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)
businessCategory	UnboundDirectoryString (1..64)	
jurisdictionCountryName	PrintableString (2)	
jurisdictionStateOrProvinceName	UTF8String (1..128)	
jurisdictionLocalityName	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)	nepovoleno	UTF8String (1..255)
rfc822Name	IA5String (1..320) kontrola: správný formát email	IA5String (1..320) kontrola: správný formát email

	adresy	adresy
dNSName	IA5String (1..255) kontrola: správný formát DNS jména	nepovoleno
Description	UnboundDirectoryString (1..1024)	
DN Qualifier	PrintableString (1..64)	
DMDName	UnboundDirectoryString (1..64)	

7.1 Profil certifikátu

Viz kapitola 7.

7.1.1 Číslo verze

Viz kapitola 7.

7.1.2 Rozšíření certifikátu

Viz kapitola 7.

7.1.3 Objektové identifikátory algoritmů

Viz kapitola 7.

7.1.4 Tvary jmen

Viz kapitola 7.

7.1.5 Omezení jmen

Viz kapitola 7.

7.1.6 Objektový identifikátor certifikační politiky

Viz kapitola 7.

7.1.7 Použití rozšíření Policy Constrainsts

Viz kapitola 7.

7.1.8 Syntaxe a sémantika kvalifikátorů politiky

Viz kapitola 7.

7.1.9 Zpracování sémantiky kritického rozšíření Certificate Policies

Viz kapitola 7.

7.2 Profil seznamu zneplatněných certifikátů

Viz kapitola 7.

7.2.1 Číslo verze

Viz kapitola 7.

7.2.2 Rozšíření CRL a záznamů v CRL

Pro kvalifikované certifikáty obsahuje CRL rozšíření (ExpiredCertsOnCRL) udávající, že v něm jsou po definovanou dobu (viz 4.10.3) obsaženy i expirované certifikáty.

7.3 Profil OCSP

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

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

tab. 5 - Profil OCSP žádosti

Položky žádosti	Poznámky
OCSPRequest ::= SEQUENCE {	
tbsRequest TBSRequest	
TBSRequest ::= SEQUENCE {	
version [0] EXPLICIT Version DEFAULT v1,	
requestorName [1] EXPLICIT GeneralName OPTIONAL	
requestList SEQUENCE OF Request,	OCSP respondér odpoví pouze na první požadavek ze seznamu v OCSP žádosti, ostatní ignoruje (RFC5019)
Request ::= SEQUENCE {	
reqCert CertID,	povinná položka, (pokud není obsažena, odpovědí bude malformedRequest)
CertID ::= SEQUENCE {	
hashAlgorithm AlgorithmIdentifier,	OID hashovacího algoritmu pro následující dvě položky - identifikace vydavatele dotazovaného certifikátu specifikuje klient, OCSP respondér neomezuje (zpracuje žádosti se všemi hashAlgoritmy, které umí openssl).

issuerNameHash OCTET STRING,	hash pole vydavatele (Issuer) certifikátu, který je předmětem žádosti
issuerKeyHash OCTET STRING,	hash veřejného klíče vydavatele certifikátu, který je předmětem žádosti
serialNumber CertificateSerialNumber }	sériové číslo certifikátu, který je předmětem žádosti
singleRequestExtensions [0]EXPLICIT Extensions OPTIONAL	podle RFC5019 nesmí být použito, pokud je přítomno v žádosti, je ignorováno
Extensions ::= SEQUENCE SIZE (1..MAX) OF Extension	
Extension ::= SEQUENCE { extnID OBJECT IDENTIFIER, critical BOOLEAN DEFAULT FALSE, extnValue OCTET STRING }	(podle RFC6960 se zde se může vyskytovat: -*ServiceLocator*)
}	
requestExtensions [2] EXPLICIT Extensions OPTIONAL	ignorováno
Extensions ::= SEQUENCE SIZE (1..MAX) OF Extension	ignorována všechna Extensions
Extension ::= SEQUENCE {	
extnID OBJECT IDENTIFIER, critical BOOLEAN DEFAULT FALSE, extnValue OCTET STRING }	(podle RFC6960 se může vyskytovat: - *Nonce* - je ignorováno podle RFC5019, - *AcceptableResponses*, - *PreferredSignatureAlgorithm*s)
}	
optionalSignature [0] EXPLICIT Signature OPTIONAL	ignorováno (RFC5019)
Signature ::= SEQUENCE {	
signatureAlgorithm AlgorithmIdentifier,	
signature BIT STRING	
certs [0] EXPLICIT SEQUENCE OF Certificate OPTIONAL }	
}	

tab. 6 - Profil OCSP odpovědi

Položky odpovědi	**Poznámky**
OCSPResponse ::= SEQUENCE {	
responseStatus OCSPResponseStatus	
OCSPResponseStatus ::= ENUMERATED	*(0) successful* - úspěšná odpověď na OCSPrequest *(1) malformedRequest* - vraceno v případě chyby syntaxe OCSPrequest; *(2) internalError* - interní chyba OCSP respondéru *(3) tryLater* - nepoužíváno *(5) sigRequired* - nikdy nevraceno, podpis žádosti není požadován *(6) unauthorized* - v případě, že OCSP respondér nepozná vydavatele = cizí certifikát (klient není oprávněn k provedení dotazu na tento server - RFC2560, nebo server není

	schopen odpovědět autoritativně, např. nemá k dispozici autoritativní informaci o odvolání certifikátu - RFC5019)
responseBytes [0] EXPLICIT ResponseBytes OPTIONAL }	pouze v případě OCSPResponseStatus=*successful*
ResponseBytes ::= SEQUENCE {	
responseType OBJECT IDENTIFIER	vždy *Basic OCSP Response*
response OCTET STRING	
BasicOCSPResponse ::= SEQUENCE {	
tbsResponseData ResponseData,	
ResponseData ::= SEQUENCE {	
version [0] EXPLICIT Version DEFAULT v1,	v1
responderID ResponderID,	
ResponderID ::= CHOICE { byName [1] Name, byKey [2] KeyHash }	vraceno byName=DN vydavatele
producedAt GeneralizedTime,	čas, kdy respondér podepsal odpověď
responses SEQUENCE OF SingleResponse,	vracena pouze jediná odpověď na první certifikát v seznamu v žádosti
SingleResponse ::= SEQUENCE {	
certID CertID,	

CertID ::= SEQUENCE {
hashAlgorithm AlgorithmIdentifier,
issuerNameHash OCTET STRING,
issuerKeyHash OCTET STRING,
serialNumber CertificateSerialNumber
}
	totožný obsah s atributem *CertID* uvedeným v žádosti

certStatus CertStatus,	stav odvolání platnosti certifikátu, jedna z vyjmenovaných možností níže
CertStatus ::= CHOICE {	
good [0] IMPLICIT NULL,	certifikát nebyl odvolán (v intervalu platnosti) nebo čas vytvoření OCSP odpovědi byl mimo interval platnosti certifikátu
revoked [1] IMPLICIT RevokedInfo,	certifikát byl odvolán (v intervalu platnosti)
RevokedInfo ::= SEQUENCE {	
revocationTime GeneralizedTime	čas zneplatnění certifikátu
revocationReason [0] EXPLICIT CRLReason OPTIONAL }	v odpovědi uváděn důvod
CRLReason ::= ENUMERATED	může obsahovat: *unspecified* (0), *keyCompromise* (1), *cACompromise* (2), *affiliationChanged* (3), *superseded* (4), *cessationOfOperation* (5), *removeFromCRL* (8), *privilegeWithdrawn* (9),

	aACompromise (10) I.CA nepřipouští důvod odvolání *certificateHold* (6) = dočasné pozastavení, hodnota (7) není použita
unknown [2] IMPLICIT UnknownInfo UnknownInfo ::= NULL	I.CA toto nepoužívá (používáno OCSPResponseStatus= unauthorized podle RFC5019) (poskytovatel není schopen odpovědět, o stavu certifikátu „nic neví", obvykle proto, že se jedná o cizí certifikát)
}	
thisUpdate GeneralizedTime,	čas, ke kterému je znám stav certifikátu
nextUpdate [1] EXPLICIT GeneralizedTime OPTIONAL,	vždy uvedeno (povinné dle RFC5019); čas, kdy končí platnost této odpovědi a do kdy bude dostupná nová odpověď
singleExtensions [1] EXPLICIT Extensions	
Extensions::= SEQUENCE SIZE (1..MAX) OF Extension Extension::= SEQUENCE { extnID OBJECT IDENTIFIER, critical BOOLEAN DEFAULT FALSE, extnValue OCTET STRING }	odpověď může obsahovat rozšíření: - ***id-commonpki-at-certHash*** - vloženo nejméně u certifikátů SK (tzv. pozitivní prohlášení); pro hash z dotazovaného certifikátu se použije algoritmus podle podpisu certifikátu respondéru (sha256) - ***id-pkix-ocsp-archive-cutoff*** - pro kvalifikované certifikáty udává, po jakou dobu po expiraci certifikátu lze spoléhat na stav certifikátu uvedený v OCSP odpovědi
}	
responseExtensions [1] EXPLICIT Extensions OPTIONAL }	odpověď neobsahuje pole responseExtensions
Extensions::= SEQUENCE SIZE (1..MAX) OF Extension Extension::= SEQUENCE { extnID OBJECT IDENTIFIER, critical BOOLEAN DEFAULT FALSE, extnValue OCTET STRING }	(podle RFC6960 zde může být: - id-pkix-ocsp-nonce, - id-pkix-ocsp-extended-revoke)
}	
signatureAlgorithm AlgorithmIdentifier,	sha256WithRSAEncryption
signature BIT STRING,	
certs [0] EXPLICIT SEQUENCE OF Certificate OPTIONAL	uváděn: - certifikát vydávající CA - certifikát OCSP respondéru
}	
}	
}	
}	

7.3.1 Číslo verze

Viz kapitola 7.3.

7.3.2 Rozšíření OCSP

Viz tabulky v kapitola 7.3.

OCSP odpověď vracející stav certifikátu "good" může obsahovat pozitivní prohlášení ve formě položky CertHash rozšíření singleExtensions.

8 HODNOCENÍ SHODY A JINÁ HODNOCENÍ

Informace o hodnocení jsou uvedeny v konkrétních certifikačních politikách.

8.1 Periodicita nebo okolnosti hodnocení

Viz kapitola 8.

8.2 Identita a kvalifikace hodnotitele

Viz kapitola 8.

8.3 Vztah hodnotitele k hodnocenému subjektu

Viz kapitola 8.

8.4 Hodnocené oblasti

Viz kapitola 8.

8.5 Postup v případě zjištění nedostatků

Viz kapitola 8.

8.6 Sdělování výsledků hodnocení

Viz kapitola 8.

9 OSTATNÍ OBCHODNÍ A PRÁVNÍ ZÁLEŽITOSTI

9.1 Poplatky

9.1.1 Poplatky za vydání nebo obnovení certifikátu

Poplatky za vydání certifikátů pro koncové uživatele jsou uvedeny v aktuálním ceníku služeb, který je k dispozici na internetové informační adrese I.CA nebo v případě uzavřeného smluvního vztahu mezi Organizací a I.CA v této smlouvě. Poplatky za certifikáty, jejichž držitelem je I.CA, nejsou účtovány.

Služba obnovení certifikátu není poskytována.

9.1.2 Poplatky za přístup k certifikátu

Přístup elektronickou cestou k veřejným certifikátům vydaným podle konkrétních CP - viz kapitola - 1.2 - I.CA nezpoplatňuje.

9.1.3 Zneplatnění nebo přístup k informaci o stavu certifikátu

Přístup elektronickou cestou k informacím o zneplatněných certifikátech (CRL) a o stavech certifikátů (OCSP) vydaných podle certifikačních politik - viz kapitola 1.2 - I.CA nezpoplatňuje.

9.1.4 Poplatky za další služby

Není relevantní pro tento dokument.

9.1.5 Postup při refundování

Není relevantní pro tento dokument.

9.2 Finanční odpovědnost

9.2.1 Krytí pojištěním

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

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

9.2.2 Další aktiva

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

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

9.2.3 Pojištění nebo krytí zárukou pro koncové uživatele

Není relevantní pro tento dokument, služba není poskytována.

9.3 Důvěrnost obchodních informací

9.3.1 Rozsah důvěrných informací

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

- veškeré soukromé klíče, sloužící v procesu poskytování Služeb,
- obchodní informace I.CA,
- veškeré interní informace a dokumentace,
- veškeré osobní údaje.

9.3.2 Informace mimo rámec důvěrných informací

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

9.3.3 Odpovědnost za ochranu důvěrných informací

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

9.4 Ochrana osobních údajů

9.4.1 Politika ochrany osobních údajů

Ochrana osobních údajů a dalších neveřejných informací je v I.CA řešena v souladu s požadavky příslušných zákonných norem, tedy ZOOÚ.Tyto požadavky jsou rozpracovány v interní dokumentaci:

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

9.4.2 Informace považované za osobní údaje

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

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

9.4.3 Informace nepovažované za osobní údaje

Za osobní údaje nejsou považovány informace, které nespadají do působnosti příslušných zákonných norem, tedy ZOOÚ.

9.4.4 Odpovědnost za ochranu osobních údajů

Za ochranu osobních údajů je odpovědný ředitel I.CA.

9.4.5 Oznámení o používání osobních údajů a souhlas s jejich zpracováním

Problematika oznamování o používání osobních údajů a souhlasu s jejich zpracováním je v I.CA řešena v souladu s požadavky příslušných zákonných norem, tedy ZOOÚ.

9.4.6 Poskytování osobních údajů pro soudní či správní účely

Poskytování osobních údajů pro soudní, resp. správní účely je v I.CA řešeno v souladu s požadavky příslušných zákonných norem, tedy ZOOÚ.

9.4.7 Jiné okolnosti zpřístupňování osobních údajů

V případě zpřístupňování osobních údajů postupuje I.CA striktně podle požadavků příslušných zákonných norem, tedy ZOOÚ.

9.5 Práva duševního vlastnictví

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

9.6 Zastupování a záruky

9.6.1 Zastupování a záruky CA

I.CA zaručuje, že:

- použije soukromé klíče certifikačních autorit pouze pro vydávání certifikátů koncovým uživatelům (vyjma kořenové certifikační autority I.CA), vydávání seznamů zneplatněných certifikátů a k vydávání certifikátů OCSP respondérů,
- použije soukromé klíče OCSP respondérů certifikačních autorit pouze v procesech poskytování odpovědí na stav certifikátu,
- certifikáty vydávané koncovým uživatelům splňují v případě certifikátů kvalifikovaných náležitosti požadované platnou legislativou pro služby vytvářející důvěru a příslušnými technickými standardy a normami, v případě ostatních certifikátů náležitosti požadované příslušnými technickými standardy a normami,
- zneplatní vydané certifikáty, pokud byla žádost o ukončení jejich platnosti podána způsobem definovaným v této CPS, resp. v konkrétní CP.

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

- držitel certifikátu neporušil povinnosti plynoucí mu ze smlouvy o poskytování Služeb, této CPS, resp. konkrétní CP,
- spoléhající se strana neporušila povinnosti této CPS, resp. konkrétní CP.

Držitel certifikátu vydaného podle této CPS, resp. konkrétní CP uplatňuje záruku vždy u RA, která zpracovala jeho žádost o vydání tohoto certifikátu.

I.CA vyjadřuje a poskytuje držitelům certifikátů a veškerým spoléhajícím se stranám záruky, že při vydávání těchto certifikátů a v průběhu doby jejich platnosti bude při jejich správě vyhovovat této CPS, resp. konkrétní CP.

Záruky zahrnují:

- kontrolu práva žádat o certifikát,
- ověření informací uváděných v žádosti o vydání certifikátu, včetně kontroly naplnění položek, obsažených v žádosti o certifikát (formát PKCS#10) a identity,
- že smlouva o vydání certifikátu odpovídá platným právním normám,
- že v režimu 24x7 je udržováno úložiště informací o stavu certifikátu,
- že certifikát může být zneplatněn z důvodů uvedených v platné legislativě pro služby vytvářející důvěru a této CPS, resp. konkrétní CP.

9.6.2 Zastupování a záruky RA

Určená RA:

- přejímá závazek za správnost jí poskytovaných služeb,
- nevyřídí kladně žádost, pokud se nepodařilo ověřit některou z položek žádosti s výjimkou položek neověřovaných, nebo držitel certifikátu odmítá potřebné údaje sdělit, nebo není oprávněn k podání žádosti o certifikát,
- v případě osobního podání žádosti o zneplatnění certifikátu odpovídá za včasné předání této žádostí k vyřízení na pracoviště CA,
- odpovídá za vyřizování připomínek a stížností.

9.6.3 Zastupování a záruky držitele certifikátu

Ve smlouvě mezi I.CA a držitelem certifikátu je vždy uvedeno, že je povinen 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

Není relevantní pro tento dokument.

9.7 Zřeknutí se záruk

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

9.8 Omezení odpovědnosti

Společnost První certifikační autorita, a.s., neodpovídá v případě této Služby za škody způsobené spoléhajícím se stranám v případech, kdy nesplnily povinnosti, požadované platnou legislativou pro služby vytvářející důvěru a touto CPS, resp. konkrétní CP. Dále neodpovídá za škody vzniklé v důsledku porušení závazků I.CA z důvodu vyšší moci.

9.9 Záruky a odškodnění

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

Společnost První certifikační autorita, a.s.:

- se zavazuje, že splní veškeré povinnosti definované jak platnou legislativou, včetně legislativy pro služby vytvářející důvěru v případě certifikátů kvalifikovaných, tak příslušnými politikami,
- poskytuje výše uvedené záruky po celou dobu platnosti smlouvy o poskytování Služeb,
- souhlasí s tím, že dodavatelé aplikačního programového vybavení, se kterými má platnou smlouvu na distribuci kořenového certifikátu, nepřebírají žádné závazky nebo odpovědnosti, s výjimkou případů, kdy poškození či ztráta byly přímo způsobeny programovým vybavením tohoto dodavatele,
- další možné náhrady škody vycházejí z ustanovení příslušné legislativy a o jejich výši může rozhodnout soud.

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

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

Reklamaci je možné podat těmito způsoby:

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

Reklamující osoba (držitel certifikátu nebo spoléhající se strana) je povinna uvést:

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

O reklamaci rozhodne I.CA nejpozději do tří pracovních dnů od doručení reklamace. Vyrozumí o tom reklamujícího formou elektronické pošty, zprávy do datové schránky nebo doporučenou zásilkou, pokud se strany nedohodnou na jiném způsobu.

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

Nový certifikát bude příslušnému držiteli certifikátu 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 CA 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 kapitole 9.10.

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

9.10.2 Ukončení platnosti

Certifikační politiky - viz kapitola 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 kapitola 9.10.

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

9.11 Individuální upozorňování a komunikace se zúčastněnými subjekty

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

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

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

9.12 Novelizace

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

9.12.1 Postup při novelizaci

Certifikační politiky - viz kapitola 9.12.

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

9.12.2 Postup a periodicita oznamování

Certifikační politiky - viz kapitola 9.12.

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

9.12.3 Okolnosti, při kterých musí být změněn OID

Certifikační politiky - viz kapitola 9.12.

V případě této CPS - OID není přiřazován.

9.13 Ustanovení o řešení sporů

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

V ostatních případech platí, že pokud držitel certifikátu nebo spoléhající se strana nesouhlasí s návrhem na vyřešení sporu, mohou použít následující stupně odvolání:

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

- ředitel I.CA (nutné elektronické nebo listinné podání).

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

9.14 Rozhodné právo

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

9.15 Shoda s platnými právními předpisy

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

9.16 Různá ustanovení

Další ustanovení jsou vždy popsána v konkrétní certifikační politice.

9.16.1 Rámcová dohoda

Viz kapitola 9.16.

9.16.2 Postoupení práv

Viz kapitola 9.16.

9.16.3 Oddělitelnost ustanovení

Viz kapitola 9.16.

9.16.4 Zřeknutí se práv

Viz kapitola 9.16.

9.16.5 Vyšší moc

Viz kapitola 9.16.

9.17 Další ustanovení

Není relevantní pro tento dokument.

10 ZÁVĚREČNÁ USTANOVENÍ

Tato certifikační prováděcí směrnice vydaná společností První certifikační autorita, a.s., nabývá platnosti a účinnosti dnem 30.4.2018.