První certifikační autorita, a.s.

Certifikační politika

vydávání kvalifikovaných certifikátů pro autentizaci internetových stránek právnickým osobám

(algoritmus RSA)

verze 1.082

OBSAH

tab. 1 – Vývoj dokumentu

Verze	Datum vydání	Schválil	Poznámka
1.00	16.11.2017	Ředitel společnosti První certifikační autorita, a.s.	První vydání.
1.01	31.01.2018	Ředitel společnosti První certifikační autorita, a.s.	Upřesnění textu v kapitolách 3.2.2.3 a 3.2.3, upřesnění názvu kapitoly 3.2.2.6, oprava formálních chyb.
1.02	30.04.2019	Ředitel společnosti První certifikační autorita, a.s.	Úprava textů dle požadavků EVCG (kapitoly 3.2.2.4, 4.9.1, 4.9.5.2).
1.03	07.03.2020	Generální ředitel společnosti První certifikační autorita, a.s.	Podpora Certificate Transparency.
1.04	01.04.2020	Generální ředitel společnosti První certifikační autorita, a.s.	Upřesnění vydávání certifikátů pro gTLD domény (v souladu s BRG).
1.05	28.11.2020	Generální ředitel společnosti První certifikační autorita, a.s.	Vyznačení klasifikace dokumentu, revize a upřesnění textu.
1.06	01.07.2021	Generální ředitel společnosti První certifikační autorita, a.s.	Upřesnění textu v 3.2.2.1, úprava userNotice v profilu certifikátu.
1.07	27.11.2021	Generální ředitel společnosti První certifikační autorita, a.s.	Aktualizace textů v souladu se zněním EVCG v.1.7.8 a BRG v.1.8.0.
1.08	11.06.2022	Generální ředitel společnosti První certifikační autorita, a.s.	Aktualizace hodnocení kryptografických modulů. Úpravy požadavků pro soulad s BRG do verze 1.8.4 - kapitoly 4.1.1, 4.2.1, 5.4.1 a 5.5.1. Revize textu.
1.081	25.04.2023	Generální ředitel společnosti První certifikační autorita, a.s.	Zpřesnění textu požadavků ve vazbě na EVCG. Doplnění způsobů používání důvodů zneplatnění v souladu s BRG 1.8.7 - kapitoly 4.9.1.1, 4.9.3, 7.2.2. Revize textu.
1.082	27.02.2024	Generální ředitel společnosti První certifikační autorita, a.s.	Z profilu certifikátu odstraněny PSD2 atributy. Zpřesnění textu požadavků ve vazbě na BRG. Revize textu.

1 ÚVOD

Tento dokument stanoví zásady, které První certifikační autorita, a.s., (dále též I.CA), kvalifikovaný poskytovatel služeb vytvářejících důvěru, uplatňuje při poskytování služby vytvářející důvěru vydávání kvalifikovaných certifikátů pro autentizaci internetových stránek právnickým osobám (dále též Služba, Certifikát) koncovým klientům, kterými mohou být výhradně právnické osoby, nebo organizační složky státu (dále jen Organizace).

Vydávané Certifikáty jsou určeny pro autentizaci internetových stránek a zabezpečení přenášených dat prostřednictvím šifrovacího protokolu SSL/TSL fungujícího na principu asymetrické kryptografie. Certifikáty jsou, v souladu s požadavky standardu ETSI EN 319 411-2 (viz kapitola 6.5.2), typu „Extended Validation", tj. jedná se o politiku EVCP dle standardu ETSI EN 319 411-1 (rovněž viz kapitola 6.5.2). Pro Službu poskytovanou podle této certifikační politiky (dále též CP) je využíván algoritmus RSA.

Právní požadavky na Službu jsou definovány:

- nařízením Evropského parlamentu a Rady č. 910/2014 o elektronické identifikaci a službách vytvářejících důvěru pro elektronické transakce na vnitřním trhu a o zrušení směrnice 1999/93/ES (eIDAS),
- zákonem České republiky č. 297/2016 Sb., o službách vytvářejících důvěru pro elektronické transakce,
- právní úpravou týkající se ochrany osobních údajů v souladu s nařízením Evropského parlamentu a Rady (EU) 2016/679 o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a o volném pohybu těchto údajů a o zrušení směrnice 95/46/ES.

Pozn.: Pokud jsou v dalším textu uváděny odkazy na technické standardy, normy nebo právní předpisy, jedná se vždy buď o uvedený technický standard, normu nebo právní předpis, resp. o technický standard, normu či právní předpis, který je nahrazuje. Pokud by byl tento dokument v rozporu s technickými standardy, normami nebo právními předpisy, které nahradí dosud platné, bude vydána jeho nová verze.

1.1 Přehled

Dokument **Certifikační politika vydávání kvalifikovaných certifikátů pro autentizaci internetových stránek právnickým osobám (algoritmus RSA)**, vypracovaný společností První certifikační autorita, a. s., se zabývá skutečnostmi, vztahujícími se k procesům životního cyklu vydávaných Certifikátů a vychází ze struktury, jejíž předlohou je osnova platného standardu RFC 3647 - Internet X.509 Public Key Infrastructure Certificate Policy and Certification Practices Framework, s přihlédnutím k platným standardům EU a k právu České republiky v dané oblasti (jednotlivé kapitoly jsou proto v tomto dokumentu zachovány i v případě, že jsou ve vztahu k ní irelevantní). Dokument je rozdělen do devíti základních kapitol, jejichž stručný popis je uveden v následujícím seznamu:

- Kapitola 1 identifikuje tento dokument přiřazeným jedinečným identifikátorem, obecně popisuje subjekty, které participují na poskytování této certifikační služby a definuje přípustné využívání vydávaných Certifikátů.
- Kapitola 2 popisuje problematiku odpovědností za zveřejňování informací, resp. dokumentace.

- Kapitola 3 popisuje procesy identifikace a autentizace žadatele o vydání Certifikátu, resp. zneplatnění Certifikátu, včetně definování typů a obsahů používaných jmen ve vydávaných Certifikátech.
- Kapitola 4 definuje procesy životního cyklu vydávaných Certifikátů, tzn. žádost o vydání a vlastní vydání Certifikátu, žádost o zneplatnění a vlastní zneplatnění Certifikátu, služby související s ověřováním stavu Certifikátu, ukončení poskytování Služby atd.
- Kapitola 5 zahrnuje problematiku fyzické, procesní a personální bezpečnosti, včetně definování množiny zaznamenávaných událostí a jejich uchovávání, problematiku po haváriích nebo kompromitaci.
- Kapitola 6 je zaměřena na technickou bezpečnost typu generování veřejných a soukromých klíčů, ochrany soukromých klíčů, včetně počítačové a síťové ochrany.
- Kapitola 7 definuje profil vydávaných Certifikátů a seznamů zneplatněných certifikátů.
- Kapitola 8 je zaměřena na problematiku hodnocení poskytované Služby.
- Kapitola 9 zahrnuje problematiku obchodní a právní.

Bližší podrobnosti o naplnění polí a rozšíření Certifikátů vydávaných podle této CP a o jejich správě mohou být uvedeny v odpovídající Certifikační prováděcí směrnici (dále CPS).

1.2 Název a identifikace dokumentu

Název a identifikace dokumentu:	Certifikační politika vydávání kvalifikovaných certifikátů pro autentizaci internetových stránek právnickým osobám (algoritmus RSA), verze 1.082
OID politiky:	1.3.6.1.4.1.23624.10.1.35.1.0

1.3 Participující subjekty

1.3.1 Certifikační autority (dále „CA")

Kořenová certifikační autorita společnosti První certifikační autorita, a.s., vydala ve dvoustupňové struktuře certifikačních autorit, v souladu s platnou právní úpravou a s požadavky technických standardů a norem, certifikát podřízené certifikační autoritě (dále též Autorita), provozované I.CA. Tato Autorita vydává Certifikáty dle této CP a certifikáty pro vlastní OCSP respondér.

1.3.2 Registrační autority (dále „RA")

Přijímání žádostí o Certifikáty není delegováno na žádnou třetí stranu, fyzické přijímání žádostí a ověřování žadatele je možné pouze na určených RA provozovaných I.CA. Taková RA:

- přijímá žádosti o služby uvedené v této CP, zejména přijímá žádosti o Certifikáty, zprostředkovává předání Certifikátů a seznamů zneplatněných certifikátů, poskytuje potřebné informace, přijímá reklamace atd.,
- při ověřování žádosti o Certifikát komunikuje s příslušnými subjekty,
- je zmocněna jménem CA uzavírat smlouvy o poskytování Služby,

- je oprávněna z naléhavých provozních nebo technických důvodů pozastavit zcela nebo zčásti výkon své činnosti,
- zajišťuje zpoplatňování služeb I.CA poskytovaných touto RA, pokud není stanoveno smlouvou jinak.

1.3.3 Držitelé certifikátů

Držitelem vydávaného Certifikátu může být výhradně Organizace, která na základě smlouvy se společností První certifikační autorita, a.s., požádala o vydání Certifikátu.

1.3.4 Spoléhající se strany

Spoléhající se stranou jsou subjekty spoléhající se při své činnosti na Certifikáty vydávané podle této CP.

1.3.5 Jiné participující subjekty

Jinými participujícími subjekty mohou být orgány činné v trestním řízení a další, kterým to dle platné právní úpravy přísluší.

1.4 Použití certifikátu

1.4.1 Přípustné použití certifikátu

Certifikáty vydávané podle této CP smějí být používány k autentizaci internetových stránek a k a zabezpečení přenášených dat. Certifikát smí být použit pouze pro autentizaci internetových stránek, jejichž jména jsou uvedena v Certifikátu (rozšíření subjectAlternativeName).

1.4.2 Zakázané použití certifikátu

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

1.5 Správa politiky

1.5.1 Organizace spravující dokument

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

1.5.2 Kontaktní osoba

Kontaktní osoba společnosti První certifikační autorita, a.s., v souvislosti s touto CP, resp. s odpovídající CPS, je výkonný ředitel I.CA. Platí kontaktní údaje uvedené v kapitole 2.2.

Mailová adresa certproblem@ica.cz je sledována nepřetržitě v režimu 24x7 a slouží pro hlášení problémů s Certifikátem, tedy např. podezření na kompromitaci klíče nebo na zneužití certifikátu.

1.5.3 Osoba rozhodující o souladu CPS s certifikační politikou

Jedinou osobou, která je odpovědná za rozhodování o souladu postupů společnosti První certifikační autorita, a.s., uvedených v CPS s touto CP, je generální 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 generální ředitel společnosti První certifikační autorita, a.s., osobu, která je oprávněna tyto změny provést. Nabytí platnosti nové verze CPS předchází její schválení generálním ředitelem společnosti První certifikační autorita, a.s.

1.6 Pojmy a zkratky

tab. 2 – Pojmy

Pojem	Vysvětlení
bezpečné kryptografické zařízení	zařízení, na kterém je uložen soukromý klíč
CA/Browser Forum	organizace, dobrovolné sdružení certifikačních autorit
certifikát se zástupným doménovým jménem	Wildcard Certificate, certifikát obsahující nejméně jedno zástupné doménové jméno v rozšíření subjectAlternativeName
doménové jméno	Domain Name, seřazený seznam jednoho nebo více doménových návěští přiřazených uzlu v DNS systému
doménové návěští	Domain Label, seřazený seznam žádného nebo více oktetů, který tvoří část doménového jména (v DNS systému, viz též RFC 8499); při použití teorie grafů návěští identifikuje jeden uzel v části grafu všech možných doménových jmen
doménový jmenný prostor	množina všech možných doménových jmen, která jsou podřízena jednomu uzlu v doménovém jmenném systému
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	zaručená elektronická pečeť, nebo uznávaná elektronická pečeť, nebo kvalifikovaná elektronická pečeť dle právní úpravy pro služby vytvářející důvěru
elektronický podpis	zaručený elektronický podpis, nebo uznávaný elektronický podpis, nebo kvalifikovaný elektronický podpis dle právní úpravy pro služby vytvářející důvěru
GET metoda	metoda komunikace klienta s http serverem způsobem požadavku na získání/stažení dat ze serveru, standardně

	preferovaná metoda zasílání http požadavků na OCSP odpovědi OCSP respondéru pomocí protokolu http
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 nebo pro elektronickou pečeť nebo pro autentizaci webových stránek	certifikát definovaný právní úpravou pro služby vytvářející důvěru
kvalifikovaný prostředek pro vytváření elektronických podpisů, resp. pečetí	prostředek pro vytváření elektronických podpisů, resp. pečetí, který splňuje požadavky stanovené v příloze II eIDAS
LDH návěští	LDH Label, typ doménového návěští v DNS – znakový řetězec složený z ASCII znaků, číslic a pomlčky s omezením, že pomlčka nesmí být na začátku a konci řetězce a celková délka nesmí přesáhnout 63 znaků (viz též RFC 5890) pozn.: zkratka LDH = Letters, Digits, Hyphen = písmena, číslice, pomlčka
objektový identifikátor	viz OID
OCSP respondér	server poskytující protokolem OCSP údaje o stavu certifikátu veřejného klíče
OCSP stapling	způsob minimalizace dotazů na OCSP respondér, RFC 4366 - TLS Extensions; umožní TLS serveru vracet jednou získanou OCSP odpověď na stav svého certifikátu (po dobu její platnosti) všem koncovým uživatelům přistupujícím k TLS serveru
orgán dohledu	subjekt dohlížející na kvalifikované poskytovatele služeb vytvářejících důvěru
ověřované doménové jméno	Authorization Domain Name, FQDN použité ke schválení pro uvedení v Certifikátu - CA může pro účely ověřování kontroly nad doménovým jménem použít FQDN získané z DNS CNAME dotazu
párová data	soukromý a jemu odpovídající veřejný klíč
phishing	podvodná technika používaná v elektronické komunikaci na Internetu k získávání citlivých údajů (hesla, čísla kreditních karet apod.)
písemná smlouva	text smlouvy v elektronické, nebo listinné podobě
P-návěští	P-Label, XN-návěští, které obsahuje od páté pozice dále platný výstup algoritmu Punycode (RFC 3492, kapitola 6.3)
podřízená CA	CA vydávající certifikáty koncovým uživatelům
POST metoda	metoda komunikace klienta s http serverem způsobem odesílání dat z klienta na server (např. odeslání dotazu na OCSP respondér prostřednictvím http protokolu)

právní úprava pro služby vytvářející důvěru	platné právní předpisy vztahující se ke službám vytvářejícím důvěru
právnická osoba	entita s právním postavením v rámci právního systému dané země
registrant doménového jména	někdy uváděn jako vlastník doménového jména, ale správněji osoby či entity registrované registrátorem doménového jména jako mající právo dohlížet na používání doménového jména, fyzická nebo právnická osoba vypisovaná jako „Registrant" příkazem WHOIS, nebo registrátorem doménového jména
registrátor doménového jména/ registrátor	osoba nebo entita, která registruje doménová jména z pověření nebo se souhlasem: ▪ internetové korporace pro přiřazování jmen a čísel (ICANN) - správce kořene DNS prostoru, ▪ správce TLD (např. .com) nebo ccTLD (např. .CZ, národního správce)
registrátor PSP	autorita odpovědná za registraci a přidělování čísel PSP v konkrétním státě, obvykle národní banka, v ETSI TS 119 495 označení NCA (National Competent Authority)
služba vytvářející důvěru / kvalifikovaná služba vytvářející důvěru	služba vytvářející důvěru / kvalifikovaná služba vytvářející důvěru definovaná eIDAS
smluvní partner	subjekt zajišťující na základě písemné smlouvy pro I.CA služby vytvářející důvěru nebo jejich části – nejčastěji se jedná o smluvní RA
softcard	programová emulace čipové karty pro přístup k soukromému klíči uloženému v HSM
soukromý klíč	jedinečná data pro vytváření elektronického podpisu/pečetě
spoléhající se strana	subjekt spoléhající se při své činnosti na certifikát
SSL certifikát	certifikát použitý pro identifikaci a šifrování v rámci komunikace prostřednictvím SSL/TLS protokolu
TWINS	obchodní produkt I.CA, obsahující dvojici certifikátů: ▪ kvalifikovaný certifikát pro elektronický podpis, ▪ komerční certifikát – vydaný výhradně na základě smluvního vztahu mezi I.CA a koncovým uživatelem
veřejný klíč	jedinečná data pro ověřování elektronického podpisu/pečetě
XN-návěští	XN-Label, třída návěští LDH začínající znaky "xn--" (viz RFC 5890)
základ doménového jména	Base Domain Name, část FQDN, která je prvním uzlem doménového jména nalevo od: ▪ registrem kontrolovaného (jména), nebo ▪ veřejné přípony plus registrem kontrolovaného jména, nebo

	▪ veřejné přípony
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
zástupné doménové jméno	Wildcard Domain Name, znakový řetězec začínající "*." bezprostředně následovaný FQDN

tab. 3 – Zkratky

Zkratka	Vysvětlení
ASCII	American Standard Code for Information Interchange, kódová tabulka definující znaky anglické abecedy a jiné znaky používané v informatice
BIH	Bureau International de l'Heure, (anglicky The International Time Bureau), Mezinárodní časová služba
bit	z anglického *binary digit* – číslice dvojkové soustavy – základní a současně nejmenší jednotka informace v číslicové technice
BRG	dokument „Baseline Requirements for the Issuance and Management of Publicly-Trusted Certificates" organizace CA/Browser Forum
CA	certifikační autorita
CAA	DNS Resource záznam – viz RFC 6844
ccTLD	country code TLD, národní doména nejvyšší úrovně, internetová doména na nejvyšší úrovni stromu internetových domén obvykle používána, nebo rezervována pro země, svrchované státy, nebo závislá území, všechny v ASCII definované národní domény nejvyššího řádu jsou tvořeny dvěma znaky
CEN	European Committee for Standardization, asociace sdružující národní standardizační orgány
CP	certifikační politika
CPS	certifikační prováděcí směrnice
CRL	Certificate Revocation List, seznam zneplatněných certifikátů obsahující certifikáty, které již nelze pokládat za platné
CT	Certificate Transparency, systém pro omezení chybného vydání certifikátu založený na zápisu certifikátů (resp. precertifikátů) do veřejných logů umožňujících detekci chybného vydání (zejména podvodného získání certifikátu jiným než oprávněným žadatelem)
ČR	Česká republika
ČSN	označení českých technických norem
DER, PEM	způsoby zakódování (formáty) certifikátu
DV	Domain Validation, typ SSL certifikátu

DNS	Domain Name System, hierarchický systém doménových jmen, který je realizovaný DNS servery a DNS protokolem, kterým si vyměňují informace, hlavním úkolem jsou vzájemné převody doménových jmen na IP adresy uzlů sítě a obráceně
EBA	European Banking Association, evropská bankovní asociace
EC	Elliptic Curve, eliptická křivka
ECC	Elliptic Curve Cryptography, kryptografie eliptických křivek
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
EV	Extended Validation, typ SSL certifikátu, resp. certifikát pro autentizaci internetových stránek
EVCG	dokument "Guidelines For The Issuance And Management Of Extended Validation Certificates" organizace CA/Browser Forum
EVCP	Extended Validation Certificate Policy, typ politiky vydávání certifikátů
EZS	elektronická zabezpečovací signalizace
FIPS	Federal Information Processing Standard, označení standardů v oblasti informačních technologií pro nevojenské státní organizace ve Spojených státech
FQDN	Fully Qualified Domain Name, plně kvalifikované doménové jméno, doménové jméno uvádějící označení všech nadřazených uzlů v internetovém doménovém jmenném systému
GDPR	General Data Protection Regulation, nařízení Evropského parlamentu a rady (EU) č. 2016/679 o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a o volném pohybu těchto údajů a o zrušení směrnice 95/46/ES (obecné nařízení o ochraně osobních údajů)
gTLD	generic TLD, obecná doména nejvyššího řádu (např. .org pro neziskové organizace)
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.
ICANN	Internet Corporation for Assigned Names and Numbers, organizace mj. přidělující a spravující doménová jména a IP adresy
IEC	International Electrotechnical Commission, světová organizace publikující standardy pro elektrotechniku, elektroniku, sdělovací techniku a příbuzné obory
IP	Internet Protocol, komunikační protokol pro přenos paketů a jejich směrování využívaný v Internetu
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
IT	Information Technology, informační technologie
ITU	International Telecommunication Union
ITU-T	Telecommunication Standardization Sector of ITU
MPSV	Ministerstvo práce a sociálních věcí
NCA	National Competent Authority, autorita odpovědná za registraci a přidělování čísel PSP v konkrétním státě, obvykle národní banka
NCP	Normalized Certificate Policy, typ certifikační politiky nekvalifikovaných certifikátů, kvalitativně shodný s politikou vydávání kvalifikovaných certifikátů
NCP+	Extended Normalized Certificate Policy, certifikační politika NCP, soukromý klíč je umístěn na bezpečném uživatelském zařízení
OCSP	Online Certificate Status Protocol, protokol pro zjišťování stavu certifikátu veřejného klíče
OID	Object Identifier, objektový identifikátor, číselná identifikace objektu
OSVČ	osoba samostatně výdělečně činná
OV	Organization Validation, typ SSL certifikátu
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
PSD	Payment Services Directive, směrnice Evropské unie o platebních službách č. 2007/64/EC

PSD2	revidovaná směrnice Evropské unie o platebních službách č. 2015/2366 účinná od 13. ledna 2018
PSP	Payment Service Provider, poskytovatel platebních služeb
PSS	Probabilistic Signature Scheme, schéma elektronického podpisu vyvinuté M. Bellarem a P. Rogawayem a standardizované jako část PKCS#1 v2.1
PTC	Publicly-Trusted Certificate, certifikát, jehož certifikát kořenový je distribuován jako důvěryhodná kotva v běžně dostupném aplikačním programovém vybavení
PUB	Publication, označení standardu FIPS
QSCD	Qualified Electronic Signature/Seal Creation Device, zařízení pro tvorbu kvalifikovaného elektronického podpisu nebo pečetě (dle eIDAS)
QWAC	Qualified Website Authentication Certificate, certifikát pro autentizaci internetových stránek
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)
RTS	Nařízení Komise v přenesené pravomoci (EU) 2018/389 ze dne 27. listopadu 2017, kterým se doplňuje směrnice Evropského parlamentu a Rady (EU) 2015/2366, pokud jde o regulační technické normy týkající se silného ověření klienta a společných a bezpečných otevřených standardů komunikace
SCT	Signed Certificate Timestamp, podepsané potvrzení („razítko") z příslušného CT logu o zařazení precertifikátu
sha, SHA	typ hashovací funkce
SSCD	Secure Signature Creation Device, bezpečné zařízení pro tvorbu elektronického podpisu (dle směrnice 1999/93/ES)
SSL	Secure Sockets Layer, komunikační protokol, resp. vrstva vložená mezi vrstvu transportní a aplikační, která poskytuje zabezpečení komunikace šifrováním a autentizaci komunikujících stran
TLD	Top Level Domain, doména na nejvyšší úrovni stromu internetových domén (pod jeho kořenem), v doménovém jméně je doména nejvyšší úrovně uvedena na konci
TLS	Transport Layer Security, komunikační protokol, následovník SSL
TS	Technical Specification, typ ETSI standardu
TSA	Time-Stamping Authority, autorita časových razítek
TSS	Time-Stamp Server, server časových razítek
TSU	Time-Stamp Unit, jednotka vydávající časová razítka
UPN	User Principal Name, uživatelské jméno ve tvaru dle RFC 822

UPS	Uninterruptible Power Supply/Source, zdroj nepřerušovaného napájení
URI	Uniform Resource Identifier, textový řetězec s definovanou strukturou sloužící k přesné specifikaci zdroje informací
UTC	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)
WHOIS	databáze, která slouží k evidenci údajů o majitelích internetových domén a IP adres
ZOOÚ	aktuální právní úprava 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.

2.2 Zveřejňování certifikačních informací

Základní adresy (dále též informační adresy), na nichž lze získat 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.

Elektronické adresy, které slouží pro kontakt veřejnosti s I.CA, jsou ssl@ica.cz, resp. info@ica.cz, ID datové schránky I.CA je a69fvfb.

Na výše uvedené internetové adrese lze získat informace o:

- certifikátech certifikačních autorit a časových autorit.
- 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, prováděcích směrnicích 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 certifikačních autorit 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.

Certifikační autorita vydávající Certifikáty vyhovuje požadavkům současné verze dokumentu „CA/Browser Forum – Guidelines for Issuance and Management of Extended Validation Certificates" (dále též EVCG), který je vystaven na adrese http://www.cabforum.org. V případě jakéhokoliv nesouladu mezi touto CP a zmíněným dokumentem má zmíněný dokument přednost.

I.CA provozuje testovací stránky umožňující nezávislým dodavatelům aplikačního programového vybavení testovat jejich software s různými stavy Certifikátů na adrese https://ica.cz/testovani-sluzeb.

2.3 Čas nebo četnost zveřejňování

I.CA zveřejňuje informace s následující periodicitou:

- certifikační politika – po schválení a vydání nové verze, aktualizace v závislosti na změnách normativních požadavků na vydávané Certifikáty, revize je prováděna nejméně jednou ročně,
- certifikační prováděcí směrnice – neprodleně (je-li určena ke zveřejnění),
- seznam vydaných certifikátů – aktualizace při každém vydání nového certifikátu určeného ke zveřejnění,
- seznam zneplatněných certifikátů (CRL) - viz kapitola 4.9.7,
- informace o zneplatnění certifikátu certifikační autority, s uvedením důvodu zneplatnění – bezodkladně,
- ostatní veřejné informace – není předem určeno, obecně však platí, že tyto informace musí reflektovat aktuální stav poskytovaných certifikačních služeb.

2.4 Řízení přístupu k jednotlivým typům úložišť

Veškeré veřejné informace zpřístupňuje I.CA bezplatně bez omezení.

Neveřejné informace jsou dostupné pouze pověřeným zaměstnancům I.CA, nebo subjektům definovaným platnou právní úpravou. Přístup k těmto informacím je řízen pravidly uvedenými v interní dokumentaci.

3 IDENTIFIKACE A AUTENTIZACE

3.1 Pojmenování

3.1.1 Typy jmen

Veškerá jména jsou konstruována v souladu 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 kapitole 7.

3.1.3 Anonymita nebo používání pseudonymu držitele certifikátu

Certifikáty vydávané podle této CP nepodporují anonymitu ani používání pseudonymu.

3.1.4 Pravidla pro interpretaci různých forem jmen

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

3.1.5 Jedinečnost jmen

Autorita zaručuje jedinečnost pole subject v Certifikátu příslušného držitele tohoto Certifikátu.

3.1.6 Uznávání, ověřování a poslání obchodních značek

Certifikáty vydané podle této CP mohou obsahovat v položce subject.organizationName také obchodní jména (obchodní značky v textovém tvaru). Údaj musí být ověřen, a to jedním z následujících způsobů:

- v registru vedeném státní agenturou, v případě České republiky Úřadem průmyslového vlastnictví, osobní kontaktem, písemnou poštou, e-mailem, telefonem, nebo z webové stránky příslušné agentury,
- z nezávislého kompetentního zdroje informací vytvořeného za účelem poskytování informací o obchodních značkách za předpokladu, že tento zdroj ověřil obchodní značku u příslušné státní agentury.

Ověřuje se, zda:

- má žadatel zaregistrováno používání této obchodní značky u příslušné vládní agentury v jurisdikci zapsaného a ověřeného sídla organizace,
- tato registrace je platná (bez vyznačení ukončení platnosti).

Autorita se může spolehnout na notářské osvědčení, které potvrzuje obchodní jméno, agenturu, která jméno registrovala a dále že zápis v registru je stále platný (bez vyznačení ukončení platnosti).

3.2 Počáteční ověření identity

Subjekty oprávněné podat žádost o vydání Certifikátu jsou vyjmenovány v kapitole 4.1.1. V následujících kapitolách jsou uvedena pravidla pro počáteční ověření jejich identity, konkrétně jsou postupy rozepsány v interní dokumentaci. Postup ověřování odpovídá požadavkům standardu CA/Browser Forum – Guidelines for The Issuance and Management of Extended Validation Certificates, mj.:

- ověřování je prováděno jedním a následně křížově kontrolováno druhým ověřovacím specialistou,
- všechny shromážděné informace a důkazy získané při ověřování žádosti jsou zakládány a je vyznačována jejich platnosti do konkrétního data.

Pokud dojde k nejasnostem ve výkladu ustanovení zmíněného standardu a z nich vyplývajících pravidel v interní dokumentaci bude pro konkrétní příklady vyžádáno právní stanovisko.

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 opatřena elektronickou pečetí a držitel soukromého klíče tak prokazuje, že v době tvorby elektronické pečetě soukromý klíč vlastnil.

3.2.2 Ověřování identity organizace

Postup je popsán v následujících kapitolách.

3.2.2.1 Právní identita a existence organizace

Požadavky na ověření vycházejí z toho, do jaké kategorie Organizace spadá. Možnosti jsou čtyři:

- soukromá organizace (Private Organization), tj. firma zapsané v obchodním rejstříku ČR (dále OR), zapsané nebo registrované podle zákona, nebo ustavené vládní agenturou,
- státní entita (Government Entity),
- subjekt registrovaný jinde než v OR, tj. registrovaný registrační agenturou (přidělující a ověřující právo podnikání), jehož registrace může být ověřena (Business Entity),
- mezinárodní organizace založená na základě smluv podepsaných vládami více států (Non-Commercial Entity).

Postup ověřování pro uvedené typy Organizace je popsán v interní dokumentaci. Zdroje použité při ověřování právní existence organizace v Certifikátech jsou uvedeny na webových stránkách www.ica.cz (v části "Rychlé odkazy" na úvodní stránce a dále "Zprávy pro uživatele el. podpisu").

3.2.2.2 Ověření fyzické existence

Autorita ověřuje, zda fyzická adresa poskytnutá žadatelem (atributy žádosti subject.streetAddress, localityName, stateOrProvinceName, postalCode, countryName) je adresou, kde žadatel nebo jeho mateřská či dceřiná společnost fyzicky existují a provádí obchodní činnost, tedy nejedná se pouze o P.O. box, nebo adresu zástupce společnosti.

3.2.2.3 Ověření provozní existence žadatele

Autorita ověřuje, že žadatel má schopnost provádět obchodní činnost ověřením provozní existence. Pro státní entity se pouze ověřuje právní identita a existence, pro ostatní subjekty se ověřuje, zda je splněna alespoň jedna z podmínek:

- subjekt podle záznamů v obchodním rejstříku nebo záznamů registrační agentury existuje již nejméně tři roky,
- subjekt má aktivní účet (běžný, vkladový) u finanční instituce spadající pod dozor národní banky, ověření se provádí:
  - získáním ověřeného doložení o existenci účtu přímo od finanční instituce,
  - nebo za použití notářského osvědčení potvrzujícího, že subjekt má aktivní běžný účet u finanční instituce spadající pod dozor národní banky,
- subjekt je uveden v aktuálním seznamu daňových subjektů finanční správy (Qualified Government Tax Information Source – QTIS) nebo ve všeobecně uznávaném nezávislém rejstříku (Qualified Independent Information Source – QIIS).

3.2.2.4 Ověření požadovaných DNS jmen

Pro ověřování oprávnění registranta doménového jména jsou používány následující metody ověřování v souladu s BRG (aktuální verzí):

- BRG, kapitola 3.2.2.4.2 „Email, Fax, SMS, or Postal Mail to Domain Contact“,
- BRG, kapitola 3.2.2.4.4 „Constructed Email to Domain Contact“,
- BRG, kapitola 3.2.2.4.7 „DNS Change“.

Omezení přípustných doménových jmen jsou uvedena v profilu certifikátu v kapitole 7.1.2 (položka dNSName).

Konkrétní postupy ověřování jsou popsány v interní dokumentaci a vycházejí z požadavků standardu BRG odkazovaného z EVCG.

3.2.2.5 Kontrola CAA záznamů

I.CA v DNS ověřuje, zda pro domény uvedené v žádosti existují Certification Authority Authorization Resource Records podle RFC 6844 (zkráceně CAA záznamy), které specifikují certifikační autority, které výhradně mohou pro danou doménu vydávat SSL certifikáty.

Vzhledem k tomu, že I.CA nevydává Certifikáty, které mohou obsahovat v DNS jménech zástupné znaky, řídí se pouze CAA záznamy obsahujícími značku „**issue**"; CAA záznamy se značkou „**issuewild**" se ignorují.

V souladu s RFC 6844 opraveném o Errata 5065 je pro každou doménu v žádosti procházen DNS strom od ověřované domény směrem vzhůru, dokud není nalezena první množina CAA záznamů pro:

- doménu nebo některý cíl jejího CNAME nebo DNAME alias řetězce,

- dále pro některou z nadřazených domén nebo její alias,

dokud není dosaženo TLD (pak množina CAA záznamů zůstane prázdná).

Alias řetězce jsou kontrolovány do hloubky maximálně osmi záznamů.

Podrobnosti viz RFC 6844, kapitola 4 opraveném o Errata 5065 v souladu s BRG.

I.CA provede první kontrolu a:

- pokud byla nalezena množina CAA záznamů, pak vyčká po dobu větší z hodnot (doba TTL CAA záznamu, 8 hodin),
- pokud neexistuje CAA záznam, potom vyčká 8 hodin,

a poté provede opakovanou kontrolu.

Další kroky ověření žádosti a vydání Certifikátu budou realizovány pouze pokud je při opakované kontrole zjištěno, že:

- buď žádný CAA záznam neexistuje,
- nebo je nalezena množina CAA záznamů a současně platí:
  - žádný z množiny CAA záznamů neobsahuje neznámou značku a současně není označen jako kritický,
  - a množina CAA záznamů se značkou **„issue"** je prázdná nebo obsahem některého záznamu z množiny CAA záznamů se značkou **„issue**" je „ica.cz“.

V opačném případě je žádost odmítnuta.

3.2.2.6 Další požadavky na ověření

Kromě výše uvedeného je kontrolováno:

- zda DNS jméno nebylo dříve odmítnuto z důvodu podezření na phishing nebo podvod, resp. zda nebylo v Certifikátech zneplatněných Autoritou z těchto důvodů,
- zda DNS jméno není na seznamu phishingových stránek,
- zda osoba žádající o Certifikát, osoba schvalující údaje Certifikátu, země zápisu, země registrace nebo místo podnikání nejsou na libovolném vládním seznamu zákazů, nežádoucích osob nebo na seznamu, který zakazuje s takovou zemí nebo Organizací obchodovat.

Podrobně jsou postupy uvedeny v interní dokumentaci.

3.2.3 Ověřování identity fyzické osoby

Pro ověření identity fyzické osoby při osobním kontaktu pro kategorie subjektů „Private Organization" (Organizace zapsané v obchodním rejstříku), „Government Entity" (státní a veřejnoprávní Organizace) je nutné předložit dva doklady, primární a sekundární, obsahující údaje uvedené dále.

- Primárním osobním dokladem pro občany ČR musí být platný občanský průkaz nebo cestovní pas. Primárním osobním dokladem pro cizince je platný cestovní pas, nebo jím v případě občanů členských států EU může být platný osobní doklad, sloužící k prokazování totožnosti na území příslušného státu. Z tohoto dokladu jsou ověřovány následující údaje:
  - celé občanské jméno,

- □ datum a místo narození, nebo rodné číslo, je-li v primárním dokladu uvedeno,
- □ číslo předloženého primárního osobního dokladu,
- □ adresa trvalého bydliště (je-li v primárním dokladu uvedena).

■ Sekundární osobní doklad musí být jednoznačným způsobem (rodné číslo, číslo občanského průkazu atd.) svázán s primárním osobním dokladem a musí obsahovat alespoň jeden z následujících údajů:

- □ datum narození (nebo rodné číslo, je-li uvedeno),
- □ adresu trvalého bydliště,
- □ fotografii obličeje.

Údaje v sekundárním osobním dokladu sloužící k jednoznačné identifikaci osoby zastupující Organizaci musí být shodné s těmito údaji v primárním osobním dokladu.

Pro ověření identity fyzické osoby při osobním kontaktu pro kategorie subjektu „Business Entity" (Organizace registrované jinde než v obchodním rejstříku registrační agenturou, která přiděluje právo podnikání, certifikát, licenci) je nutné předložit následující doklady:

■ Osobní prohlášení obsahující:

- □ celé jméno,
- □ adresu trvalého (nebo přechodného) pobytu,
- □ datum narození,
- □ prohlášení, že všechny informace uvedené v žádosti o Certifikát jsou pravdivé a správné.

■ Platný identifikační doklad vydaný orgánem státu, který obsahuje fotografii osoby a její podpis, jako např.:

- □ občanský průkaz,
- □ cestovní pas.

■ Nejméně dva sekundární dokladované důkazy o identitě osoby, které obsahují jméno osoby, přitom jeden z nich musí být od finanční instituce:

- □ řidičský průkaz,
- □ akceptovatelné dokumenty od finanční instituce jsou:
  - platná kreditní karta od finanční instituce spadající pod dozor národní banky,
  - platná debetní karta od finanční instituce spadající pod dozor národní banky,
  - výpis z hypotečního účtu, který není starší šesti měsíců,
  - bankovní výpis od finanční instituce spadající pod dozor národní banky, který není starší šesti měsíců,
- □ akceptovatelné dokumenty od jiné instituce jsou:
  - originál posledního účtu od dodavatele energií (nikoliv účet za mobilní telefon) potvrzující dodávky na adresu pobytu osoby,
  - kopie účtu za nájem, která není starší šesti měsíců,
  - ověřená kopie rodného listu,

- daňový výměr finančního úřadu za aktuální rok,
- ověřená kopie soudního rozhodnutí (např. rozvodový rozsudek, rozhodnutí o adopci atd.,
- platný identifikační doklad vydaný státní správou, který obsahuje jméno osoby a je jiný než primární doklad.

Fyzická osoba musí být ověření osobně přítomna, nebo je vyžadováno notářsky ověřené potvrzení, že výše popsané ověření proběhlo. Podrobně je postup ověření, včetně postupu ověření notáře, který vystavil případné potvrzení, popsán v interní dokumentaci.

3.2.4 Neověřované informace vztahující se k držiteli certifikátu

Není relevantní pro tento dokument – všechny informace musí být řádným způsobem ověřeny.

3.2.5 Ověřování kompetencí

V rámci postupů souvisejících s uzavřením smlouvy, podáním žádosti o Certifikát a s vydáním certifikátu je ověřováno:

- spolehlivý způsob komunikace se žadatelem, tj. jsou ověřovány kontaktní adresa, telefonní číslo, e-mailová adresa,
- oprávnění osoby podepisující smlouvu o vydání Certifikátu i osoby schvalující údaje v Certifikátu,
- ověření podpisu na smlouvě s držitelem Certifikátu,
- ověření schválení žádosti o Certifikát.

Konkrétní postupy jsou popsány v interní dokumentaci.

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 se jedná o vydání nového Certifikátu s novým veřejným klíčem, před vydáním každého nového Certifikátu musí I.CA provést kompletní postup ověření.

I.CA může použít pro vydání Certifikátu (pro stejného žadatele a doménu) informace získané při předchozím ověřování podle kapitoly 3.2 za podmínek uvedených v kapitole 4.2.1.

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

Službu výměny klíče po zneplatnění Certifikátu I.CA nepodporuje. Je nutné vydat nový Certifikát s novým veřejným klíčem. Platí stejné požadavky jako v případě počátečního ověření identity.

3.4 Identifikace a autentizace při požadavku na zneplatnění certifikátu

Subjekty oprávněné podat požadavek na zneplatnění Certifikátu jsou vyjmenovány v kapitole 4.9.2. Možné způsoby identifikace a autentizace jsou popsány dále v této kapitole.

V případě **osobního předání požadavku na zneplatnění Certifikátu na RA** musí být požadavek na zneplatnění Certifikátu písemný a podepsaný definovanou osobou pověřenou za Organizaci vystupovat ve smluvním vztahu s I.CA, identita této osoby musí být řádně ověřena primárním osobním dokladem (viz kapitola 3.2.3).

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

- prostřednictvím formuláře na webových stránkách společnosti (s využitím hesla pro zneplatnění Certifikátu),
- prostřednictvím nepodepsané elektronické zprávy obsahující heslo pro zneplatnění Certifikátu odeslané na adresu revoke@ica.cz z kontaktní mailové adresy zadané při registraci,
- prostřednictvím podepsané elektronické zprávy zaslané na adresu revoke@ica.cz z kontaktní mailové adresy zadané při registraci, elektronický podpis musí být realizován soukromým klíčem příslušným k certifikátu definované osoby pověřené za Organizaci vystupovat ve smluvním vztahu s I.CA,
- prostřednictvím datové schránky I.CA (s využitím hesla pro zneplatnění Certifikátu).

V případě použití **listovní zásilky pro předání požadavku na zneplatnění Certifikátu** s využitím hesla pro zneplatnění Certifikátu musí být tento zaslán doporučeně na adresu sídla společnosti I.CA.

Údaje, které musí požadavek na zneplatnění Certifikátu obsahovat, jsou uvedeny v kapitole 4.9.3.

I.CA si vyhrazuje právo akceptování i jiných forem postupů pro identifikaci a autentizaci požadavku na zneplatnění Certifikátu, které však nesmí být v rozporu s právní úpravou pro služby vytvářející důvěru nebo s požadavky technických standardů pro tento typ Certifikátu,

4 POŽADAVKY NA ŽIVOTNÍ CYKLUS CERTIFIKÁTU

4.1 Žádost o vydání certifikátu

4.1.1 Kdo může požádat o vydání certifikátu

Certifikáty jsou vydávány pouze organizacím na základě smlouvy se společností První certifikační autorita, a.s. - viz kapitola 1.3.3.

4.1.2 Registrační proces a odpovědnosti

Před zasláním žádosti o Certifikát musí mít žadatel se společností První certifikační autorita, a.s., uzavřenu smlouvu, jejíž součástí je definování podmínek užití Certifikátu.

Až poté zástupce žadatele může zaslat na e-mailovou adresu ssl@ica.cz žádost o Certifikát, jejímž obsahem bude žádost o Certifikát ve formátu PKCS#10 a prohlášení, že všechny informace uvedené v žádosti jsou pravdivé.

Držitel soukromého klíče, resp. držitel Certifikátu je povinen zejména:

- seznámit se s touto CP a smluvně se zavázat jednat podle ní,
- poskytovat pravdivé a úplné informace pro vydání Certifikátu,
- překontrolovat, zda údaje uvedené v žádosti o Certifikát a ve vydaném Certifikátu jsou správné a odpovídají požadovaným údajům,
- zvolit vhodné heslo pro zneplatnění Certifikátu (minimální/maximální délka hesla 4/32 znaků, povolené znaky 0..9, A..Z, a..z).

Poskytovatel Služby je povinen zejména:

- před uzavřením smlouvy o vydání Certifikátu informovat držitele Certifikátu, popř. Organizaci o smluvních podmínkách,
- uzavírat s držitelem Certifikátu, popř. s Organizací smlouvu o vydání Certifikátu, obsahující náležitosti požadované právní úpravou pro služby vytvářející důvěru, technickými standardy a normami,
- v procesu vydávání Certifikátu na RA ověřit všechny ověřitelné údaje uvedené v žádosti podle předložených dokladů,
- v případě, že soukromý klíč byl generován na QSCD, vyžadovat prokázání této skutečnosti,
- vydat Certifikát obsahující věcně správné údaje na základě informací, které jsou poskytovateli Služby k dispozici v době vydávání tohoto Certifikátu,
- zveřejňovat veřejné informace v souladu s ustanoveními kapitoly 2.2,
- zveřejnit certifikáty Autority a kořenové CA,
- činnosti spojené se Službou poskytovat v souladu s právní úpravou pro služby vytvářející důvěru, touto CP, příslušnou CPS, Systémovou bezpečnostní politikou – důvěryhodné systémy a provozní dokumentací.

4.2 Zpracování žádosti o certifikát

4.2.1 Provádění identifikace a autentizace

Při zpracování žádosti je prováděno:

- ověření pravosti původu žádosti,
- ověření vlastnictví soukromého klíče,
- ověření identity organizace,
- ověření, zda obsahuje identifikátor (Internetovou adresu) zařízení,
- ověření oprávnění užívat uvedené jméno domény druhého řádu.

Před schválením žádosti o Certifikát RA prověřuje:

- požadované doménové jméno proti seznamu phishingových stránek,
- další interní kritéria pro odhalení podvodných žádostí,
- pro domény uvedené v žádosti o Certifikát kontrola DNS na existenci a obsah CAA záznamu – viz kapitola 3.2.2.5.

V procesu ověřování ostatních údajů (pro stejného žadatele a doménu) může použít informace získané při předchozím ověřování za předpokladu, že nejsou starší než 398 dnů, v opačném případě je postupováno podle kapitoly 3.2.2.

4.2.2 Schválení nebo zamítnutí žádosti o certifikát

I.CA nevydává certifikáty pro gTLD doménu .onion. Pokud některá z ověření viz kapitola 4.2.1 skončí negativně, proces vydání Certifikátu je ukončen. V opačném případě pracovník RA vydání Certifikátu schválí.

4.2.3 Doba zpracování žádosti o certifikát

Pokud se podaří ověřit všechny položky žádosti, bude Certifikát vydán do pěti pracovních dnů.

4.3 Vydání certifikátu

4.3.1 Úkony CA v průběhu vydávání certifikátu

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

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

Ověřování vlastnictví soukromého klíče, podporovaných hashovacích funkcí v žádosti o Certifikát (minimálně SHA-256), kontrola kompetencí a kontroly formální správnosti údajů jsou prováděny jak programovým vybavením umístěným na pracovních stanicích operátorů CA, tak programovým vybavením jádra systému CA. Pokud některá z uvedených kontrol skončí negativně, proces vydání Certifikátu je ukončen.

Vydání Certifikátu je provedeno na základě vědomého a zaručeným elektronickým podpisem na bázi nekvalifikovaného certifikátu opatřeného příkazu oprávněného operátora CA k provedení operace vydání Certifikátu.

4.3.2 Oznámení o vydání certifikátu držiteli certifikátu certifikační autoritou

Vydaný Certifikát je automaticky zaslán na kontaktní e-mailovou adresu žadatele.

4.4 Převzetí vydaného certifikátu

4.4.1 Úkony spojené s převzetím certifikátu

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

I.CA může s Organizací sjednat postup odlišný od tohoto ustanovení CP. Tímto postupem však nesmí být dotčena příslušná ustanovení právní úpravy pro služby vytvářející důvěru.

4.4.2 Zveřejňování certifikátů certifikační autoritou

I.CA je povinna zajistit neprodlené zveřejnění jí vydaných Certifikátů, vyjma Certifikátů:

- obsahujících údaje, jejichž zveřejnění by bylo v rozporu s příslušnou právní úpravou (např. právní úprava týkající se ochrany osobních údajů),
- u kterých si žadatel o Certifikát vymínil, že nebudou zveřejněny.

4.4.3 Oznámení o vydání certifikátu certifikační autoritou jiným subjektům

Oznámení o vydání Certifikátu získá pouze žadatel o Certifikát.

4.5 Použití párových dat a certifikátu

4.5.1 Použití soukromého klíče a certifikátu držitelem certifikátu

Povinností držitelů Certifikátů je zejména:

- dodržovat veškerá relevantní ustanovení smlouvy o poskytování této Služby,
- užívat soukromý klíč a odpovídající Certifikát vydaný podle této CP pouze pro účely stanovené v této CP a právní úpravou pro služby vytvářející důvěru,
- nakládat se soukromým klíčem, který odpovídá veřejnému klíči obsaženému v Certifikátu vydaném podle této CP, takovým způsobem, aby nemohlo dojít k jeho neoprávněnému použití,
- neprodleně uvědomit poskytovatele Služby o skutečnostech, které vedou ke zneplatnění Certifikátu, zejména o:
  - podezření, že soukromý klíč byl zneužit, nebo

- neplatnosti či nepřesnosti údajů v Certifikátu,

v takových případech 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 (např. www.ica.cz, pracoviště RA, příslušný důvěryhodný seznam) certifikáty certifikačních autorit související s Certifikátem vydaným podle této CP, ověřit hodnoty jejich otisků a jejich platnost,
- provádět veškeré úkony potřebné k tomu, aby si ověřily, že Certifikát je platný,
- dodržovat veškerá ustanovení této CP a právní úpravy pro služby vytvářející důvěru, vztahující se k povinnostem spoléhající se strany.

4.6 Obnovení certifikátu

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

Služba obnovení Certifikátu není poskytována.

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

Službou výměny veřejného klíče je v kontextu této CP míněno vydání Certifikátu s novým veřejným klíčem, aniž by byly změněny jiné informace v Certifikátu.

Pro vydání takového Certifikátu platí požadavky kapitol 3.3.1 a 4.1 až 4.4.

4.7.1 Podmínky pro výměnu veřejného klíče v certifikátu

Viz kapitola 4.7.

4.7.2 Kdo může žádat 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

Službou změny údajů v Certifikátu je podle této CP míněno vydání nového Certifikátu, aniž by byl změněn veřejný klíč, s minimálně jednou změnou v obsahu položek uvedených v poli subject nebo rozšíření subjectAlternativeName vztahujících se k držiteli Certifikátu, nebo s odebraným, nebo přidaným dalším polem, jehož obsah musí být ověřen.

Služba změny údajů v Certifikátu není poskytována.

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

Viz kapitola 4.8.

4.8.6 Zveřejňování certifikátů se změněnými údaji certifikační autoritou

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

Žádosti o zneplatnění Certifikátu přijímá I.CA nepřetržitě prostřednictvím formuláře na webových stránkách společnosti.

Nepřetržitě je možné podat žádost o zneplatnění Certifikátu také prostřednictvím emailu, datové schránky a listovní zásilky. Takto podaná žádost je přijata nejpozději v první pracovní den následující po jejím doručení.

Osobní předání a přijetí žádosti o zneplatnění Certifikátu na RA je možné pouze v pracovní době příslušné RA, žádost je potom zpracována neprodleně.

Službu pozastavení platnosti Certifikátu I.CA neposkytuje, stejně jako neposkytuje možnost požádat o zneplatnění k určitému datu v budoucnosti.

4.9.1 Podmínky pro zneplatnění

4.9.1.1 Důvody zneplatnění Certifikátu

I.CA zneplatní Certifikát během 24 hodin a uvede odpovídající kód CRLReason (viz kapitola 7.2.2), pokud nastane jeden nebo více z následujících důvodů:

1. držitel Certifikátu podal písemnou žádost o zneplatnění Certifikátu (nespecifikováno – unspecified(0); tento kód se v CRL u položky neuvádí),
2. držitel Certifikátu oznámil certifikační autoritě, že původní žádost o Certifikát byla neoprávněná a že zpětně neudělí autorizaci (CRLReason #9, privilegeWithdrawn),
3. I.CA získá důkaz, že soukromý klíč držitele Certifikátu odpovídající klíči veřejnému v Certifikátu byl kompromitován (CRLReason #1, keyCompromise),
4. I.CA je vyrozuměna o předvedené nebo prokázané metodě, kterou je možné snadno vypočítat soukromý klíč držitele ze znalosti veřejného klíče uvedeného v Certifikátu (např. slabina Debian Weak Key) (CRLReason #1, keyCompromise),
5. I.CA získá důkaz, že na metodu pro ověření vlastnictví domény (viz kapitola 3.2.2.4) použitou pro ověření FQDN uvedeného ve vydaném Certifikátu nelze spoléhat (CRLReason #4, superseded).

I.CA zneplatní Certifikát do pěti dnů, pokud nastane jeden nebo více z následujících důvodů:

6. Certifikát nevyhovuje požadavkům na kryptografické algoritmy a jejich požadovaným parametrům (kvalitě, viz kapitoly 6.1.5 a 6.1.6) (CRLReason #4, superseded),
7. I.CA získá důkaz, že Certifikát byl zneužit (CRLReason #9, privilegeWithdrawn),
8. I.CA je vyrozuměna, že držitel Certifikátu porušil jednu nebo více ze svých důležitých povinností plynoucích ze smlouvy o vydání Certifikátu nebo smlouvy o podmínkách používání Certifikátu (CRLReason #9, privilegeWithdrawn),
9. I.CA je vyrozuměna o okolnostech indikujících, že plně kvalifikované jméno domény (FQDN) uvedené v Certifikátu není dále právně přípustně (tj. soud nebo arbitráž odňaly registrantovi právo používat doménové jméno, zrušily relevantní smlouvu, smlouva o licenci nebo službě mezi registrantem doménového jména a žadatelem o certifikát byla zrušena, nebo se registrantovi doménového jména nepodařilo doménové jméno obnovit) (CRLReason #5, cessationOfOperation),
10. Wild card certifikát - není relevantní pro SSL certifikáty vydávané společností I.CA (CRLReason #9, privilegeWithdrawn),
11. I.CA je vyrozuměna, že došlo ke podstatným změnám informací obsažených v Certifikátu (CRLReason #9, privilegeWithdrawn),
12. I.CA je vyrozuměna, že Certifikát nebyl vydán v souladu s CP nebo CPS (CRLReason #4, superseded),
13. I.CA zjistí, že některá informace v Certifikátu je nepřesná nebo zavádějící (CRLReason #9, privilegeWithdrawn),
14. oprávnění I.CA vydávat Certifikáty podle této CP vypršelo, bylo zneplatněno, nebo ukončeno a I.CA nepřipravila způsob, jak udržovat CRL/OCSP úložiště (nespecifikováno – unspecified(0); tento kód se v CRL u položky neuvádí),
15. zneplatnění je vyžadováno CP nebo CPS (nespecifikováno – unspecified(0); tento kód se v CRL u položky neuvádí),
16. CRLReason #1, keyCompromise v případech, že:
    - je I.CA je vyrozuměna o předvedené nebo prokázané metodě pro kompromitaci soukromého klíče držitele Certifikátu,
    - nebo je jasný důkaz, že konkrétní metoda použitá pro generování soukromého klíče obsahovala chybu.

4.9.1.2 Důvody zneplatnění certifikátu Autority

I.CA zneplatní certifikát Autority během sedmi dnů, pokud nastane některý z uvedených případů:

1. Autorita požádá písemně o zneplatnění,
2. Autorita oznámila kořenové certifikační autoritě, že původní žádost o její certifikát byla neoprávněná a že zpětně neudělí autorizaci,
3. kořenová certifikační autorita je vyrozuměna, že soukromý klíč Autority byl kompromitován, nebo nadále nesplňuje požadavky na kryptografické algoritmy a požadované parametry (kvalitu, viz kapitola 6.1.5 a 6.1.6),
4. kořenová certifikační autorita je vyrozuměna, že certifikát Autority byl zneužit,
5. kořenová CA je vyrozuměna, že certifikát Autority nebyl vydán v souladu s příslušnou CP nebo CPS, nebo nesplňuje její požadavky,
6. I.CA zjistí, že některá informace v certifikátu Autority je nepřesná nebo zavádějící
7. kořenová CA nebo Autorita ukončily z nějakého důvodu činnost a nepřevedly podporu zneplatňování na jinou CA,
8. právo kořenové CA nebo Autority vydávat certifikáty podle podmínek CP vypršelo, nebo bylo odvoláno či ukončeno, pokud kořenová CA nezajistila pro Autoritu pokračující správu úložiště CRL/OCSP,
9. zneplatnění je vyžádáno CP a/nebo CPS kořenové CA.

4.9.2 Kdo může požádat o zneplatnění

Žádost o zneplatnění mohou podat:

- držitel Certifikátu,
- subjekt, který k tomu byl explicitně určen ve smlouvě o poskytování Služby podle této CP,
- poskytovatel této Služby (oprávněným žadatelem o zneplatnění certifikátu vydaného I.CA je v tomto případě generální ředitel I.CA, resp. zastupující osoba a subjekt je o zneplatnění informován podepsaným mailem na adresu zadanou při registraci):
  - 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,
  - pokud zjistí, že při vydání Certifikátu nebyly splněny požadavky právní úpravy pro služby vytvářející důvěru,
  - dozví-li se prokazatelně, že Certifikát byl použit v rozporu s omezením definovaným v kapitole 1.4.2,
  - pokud je veřejný klíč v žádosti o vydání Certifikátu duplicitní s veřejným klíčem v již vydaném certifikátu,
- orgán dohledu, případně další subjekty definované právní úpravou pro služby vytvářející důvěru.

Držitel je povinen v případě podání žádosti o zneplatnění Certifikátu okamžitě přestat používat tento Certifikát i odpovídající soukromý klíč.

Kromě toho třetí strany (např. orgán dohledu, orgány činné v trestním řízení držitelé, spoléhající se strany, dodavatelé aplikačního SW) jiné třetí strany mohou zasílat hlášení o problému s Certifikáte informující Autoritu o dostatečných důvodech pro zneplatnění Certifikátu – viz kapitola 4.9.3.2.

4.9.3 Postup při žádosti o zneplatnění

4.9.3.1 Požadavek na zneplatnění Certifikátu podaný jeho držitelem

Pro předání žádosti o zneplatnění Certifikátu jsou přípustné následující možnosti:

- Prostřednictvím formuláře na k tomuto účelu vyhrazené internetové informační adrese http://www.ica.cz. Datum a čas zneplatnění Certifikátu jsou dány zpracováním platné žádosti o zneplatnění Certifikátu informačním systémem CA. O kladném vyřízení je žadatel informován. Žadatel volí důvod zneplatnění (viz kapitola 4.9.1.1, s výjimkou CRLReason #9, privilegeWithdrawn).
- Prostřednictvím e-mailu:
  - Elektronicky podepsaná elektronická zpráva – tělo zprávy musí obsahovat text (v českém nebo slovenském jazyce, s diakritikou nebo bez diakritiky, případně v jazyce anglickém):

    Zadam o zneplatneni certifikatu cislo = xxxxxxx,

    kde „*xxxxxxx*“ je sériové číslo Certifikátu a musí být buď v dekadickém nebo hexadecimálním tvaru (uvozeno řetězcem „0x“).
  - Elektronicky nepodepsaná elektronická zpráva – tělo zprávy musí obsahovat text (v českém nebo slovenském jazyce, s diakritikou nebo bez diakritiky, případně v jazyce anglickém):

    Zadam o zneplatneni certifikatu cislo = xxxxxxx

    Heslo pro zneplatneni = yyyyyy,

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

    Pozn.: Pokud žádost splňuje požadavky jedné z výše uvedených možností, odpovědný pracovník Certifikát v systému CA neprodleně zneplatní – datum a čas zneplatnění Certifikátu jsou dány zpracováním tohoto požadavku informačním systémem CA. O kladném vyřízení je žadatel informován. Žadatel může v textu také specifikovat důvod zneplatnění (viz kapitola 4.9.1.1).
- Prostřednictvím doporučené listovní zásilky nebo datové schránky – v zásilce musí být uvedena žádost v následujícím tvaru (v českém nebo slovenském jazyce, s diakritikou nebo bez diakritiky, případně v jazyce anglickém):

  Zadam o zneplatneni certifikatu cislo = xxxxxxx

  Heslo pro zneplatneni = yyyyyy,

  kde „*xxxxxxx*“ je sériové číslo Certifikátu a „*yyyyyy*“ je heslo pro zneplatnění. Sériové číslo je buď v dekadickém nebo hexadecimálním tvaru (uvozeno řetězcem „0x“). Žadatel může v textu také specifikovat důvod zneplatnění (viz kapitola 4.9.1.1). V případě, že žádost uvedené požadavky splňuje, odpovědný pracovník I.CA Certifikát v informačním

systému CA zneplatní – datum a čas zneplatnění Certifikátu jsou dány zpracováním tohoto požadavku v informačním systémem CA. V případě, že žádost nelze akceptovat (nesprávné heslo pro zneplatnění) bude žádost o zneplatnění Certifikátu zamítnuta. O vyřízení žádosti je žadatel informován stejným způsobem, jakým byla doručena žádost, buď prostřednictvím doporučeného dopisu zaslaného na poštovní adresu uvedenou jako adresa odesilatele, nebo prostřednictvím datové schránky.

4.9.3.2 Podezření na kompromitaci klíče a zneužití Certifikátu

Oznámení o podezření na kompromitaci soukromého klíče vztahujícího se k veřejnému klíči v Certifikátu, zneužití Certifikátu nebo jiné typy podvodu, kompromitace, zneužití, nevhodného chování spojené s vydaným Certifikátem je možné zaslat na mailovou adresu uvedenou v kapitole 1.5.2, případně doporučenou listovní zásilkou na adresu sídla společnosti, nebo podat prostřednictvím datové schránky – viz kapitola 2.2.

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

4.9.5.1 Požadavek na zneplatnění Certifikátu

Požadavek na zneplatnění Certifikátu je realizován bezodkladně po přijetí oprávněné žádosti o zneplatnění. CRL obsahující sériové číslo zneplatněného Certifikátu je vydán neprodleně po zneplatnění tohoto Certifikátu.

4.9.5.2 Hlášení problémů s Certifikáty

I.CA během 24 hodin po přijetí hlášeného problému s Certifikátem prozkoumá fakta a okolnosti hlášeného problému a poskytne předběžnou zprávu jak držiteli Certifikátu, tak tomu, kdo ohlásil problém.

I.CA ve spolupráci s držitelem Certifikátu a ohlašovatelem problému rozhodne, zda je nutné zneplatnění Certifikátu, o rozhodnutí informuje jak držitele Certifikátu, tak toho, kdo ohlásil problém.

Pokud je nutné zneplatnění Certifikátu, potom určí datum zneplatnění Certifikátu na základě následujících kritérií:

- povaha údajného problému,
- důsledky zneplatnění (pro držitele i spoléhající strany),
- počet obdržených hlášení o problému s Certifikátem vztahujících se k jednotlivému Certifikátu, nebo k držiteli Certifikátu,
- kdo si stěžuje (např. hlášení orgánu činného v trestním řízení, že stránka provozuje ilegální aktivity, má větší závažnost než stížnost od zákazníka uvádějícího, že nedostal objednané zboží),
- relevantní právní úprava.

Doba do zveřejnění zneplatnění Certifikátu nesmí přesáhnout interval uvedený v kapitole 4.9.1.

4.9.6 Povinnosti spoléhajících se 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

4.9.7.1 Stav Certifikátů

EVCG vyžadují, aby doba platnost CRL (rozdíl mezi nextUpdate a thisUpdate) byla maximálně 10 dnů. Ve společnosti I.CA je CRL vždy vydáván neprodleně po kladném zpracování žádosti o zneplatnění Certifikátu. Nedojde-li ke zneplatnění Certifikátu, je nový CRL vydáván zpravidla v intervalu 8 hodin, nejvýše však 24 hodin od vydání předchozího CRL.

4.9.7.2 Stav certifikátu CA vydávající Certifikáty

EVCG vyžadují, aby doba platnost CRL kořenové CA (rozdíl mezi nextUpdate a thisUpdate) byla maximálně 12 měsíců. Ve společnosti I.CA je CRL vždy vydáván neprodleně po kladném zpracování žádosti o zneplatnění certifikátu podřízené CA. Nedojde-li ke zneplatnění certifikátu, je nový CRL vydáván zpravidla v intervalu 6 měsíců, nejvýše však 12 měsíců od vydání předchozího CRL.

4.9.8 Maximální zpoždění při vydávání seznamu zneplatněných certifikátů

CRL je zveřejněn neprodleně po vydání, vždy jsou dodrženy podmínky popsané v kapitolách 4.9.5 a 4.9.7.

4.9.9 Dostupnost ověřování stavu certifikátu on-line

Služba uvěřováni stavu certifikátu s využitím protokolu OCSP je veřejně dostupná. Každý certifikát, vydaný podle této CP, obsahuje odkaz na příslušný (autorizovaný) OCSP respondér.

OCSP odpovědi vyhovují normám RFC 6960 a RFC 5019. Certifikát OCSP respondéru obsahuje rozšíření typu id-pkix-ocsp-nocheck, jak je definováno v RFC 6960.

4.9.10 Požadavky při ověřování stavu certifikátu on-line

OCSP umožňuje dotazy využívající metodu GET i POST. OCSP odpovědi na stav nevydaných certifikátů nevracejí stav good.

4.9.10.1 Stav Certifikátů

EVCG vyžadují, aby platnost OCSP odpovědi byla v rozsahu 8 hodni až 10 dnů, k datu vydání této verze CP je nastavena na 24 hodin.

Při zneplatnění certifikátu se OCSP odpověď aktualizuje okamžitě (pozastavení ani obnovení platnosti Certifikátu není poskytováno).

OSCP odpovědi jsou automaticky aktualizovány (tj. platnost položky v interní cache OCSP respondéru končí) nejdéle v okamžiku, kdy je splněna dřívější z následujících podmínek:

- v polovině platnosti OCSP odpovědi (pro odpovědi s platností kratší než 16 hodin),
- 8 hodin před koncem platnosti odpovědi (pro odpovědi s platností 16 hodin nebo delší).

4.9.10.2 Stav certifikátu CA vydávající Certifikáty

I.CA aktualizuje informaci poskytovanou prostřednictvím OCSP:

- do 24 hodin po zneplatnění certifikátu CA vydávající Certifikáty,
- a nejméně každých dvanáct měsíců.

4.9.11 Jiné možné způsoby oznamování zneplatnění

I.CA smluvně zavazuje držitele Certifikátu webových serverů, aby provedli konfiguraci serverů k provádění OCSP stapling dle RFC 4366 pro distribuci OCSP odpovědí.

4.9.12 Zvláštní postupy při kompromitaci klíče

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

4.9.13 Podmínky pro pozastavení platnosti certifikátu

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

4.9.14 Kdo může požádat o pozastavení platnosti

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

4.9.15 Postup při žádosti o pozastavení platnosti

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

4.9.16 Omezení doby pozastavení platnosti

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

4.10 Služby ověřování stavu certifikátu

4.10.1 Funkční charakteristiky

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

Skutečnost, že Autorita poskytuje informace o stavu Certifikátu formou OCSP, je uvedena v jí vydaných Certifikátech.

Záznamy o zneplatnění na CRL nebo v OCSP odpovědi jsou udržovány nejméně do doby konce platnosti odvolaného Certifikátu.

4.10.2 Dostupnost služeb

Autorita garantuje zajištění nepřetržité dostupnosti (sedm dní v týdnu, 24 hodin denně) a integrity seznamu jí vydaných Certifikátů a seznamu zneplatněných Certifikátů (CRL), a dále dostupnost služby OCSP.

Doba odpovědi na žádost o stav Certifikátu s využitím CRL nebo OCSP je za normálních provozních podmínek kratší než 10 vteřin.

I.CA udržuje prostřednictvím e-mailové adresy uvedené v kapitole 1.5.2 nepřetržitou 24x7 dostupnost tak, aby interně zareagovala na hlášení závažného problému s Certifikátem a, pokud je to nutné, přeposlala takové hlášení příslušnému orgánu a případně zneplatnila Certifikát, který je předmětem hlášení.

4.10.3 Další charakteristiky služeb stavu certifikátu

Není relevantní pro tento dokument – další charakteristiky služeb stavu certifikátu nejsou poskytovány.

4.11 Konec smlouvy o vydávání certifikátů

Platnost smlouvy o vydání certifikátu končí s ukončením platnosti posledního podle ní vydaného certifikátu.

4.12 Úschova a obnova klíčů

Není relevantní pro tento dokument, služba úschovy a obnovy klíčů 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 vytvářejících důvěru,
- veškeré procesy podporující poskytování výše uvedených služeb.

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

5.1 Fyzická bezpečnost

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 vytvářejících důvěru 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. 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 vytvářejících důvěru, 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 vytvářejících důvěru 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 vytvářejících důvěru, 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, na kterém záznamy vznikly.

Papírová média, která je nutno uchovávat, jsou skladována v jiné geografické lokalitě, než je umístěno provozní pracoviště, na kterém záznamy vznikly.

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 výkonným ředitelem I.CA a popsaném v interní dokumentaci.

5.2 Procedurální postupy

5.2.1 Důvěryhodné role

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

Všichni zaměstnanci I.CA v důvěryhodných rolích nesmí být ve střetu zájmů, který by mohl 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 jim příslušných OCSP respondérů,
- ničení soukromých klíčů veškerých certifikačních autorit a jim příslušných OCSP respondérů, včetně jejich záloh,

- zálohování a obnovu soukromých klíčů veškerých certifikačních autorit a jim příslušných OCSP respondérů,
- aktivaci a deaktivaci soukromých klíčů veškerých certifikačních autorit a jim příslušných OCSP respondérů.

Procesy ověřování údajů v žádosti o vydání o Certifikát a schválení vydání Certifikátu jsou prováděny dvěma důvěryhodnými osobami v rolích ověřovací specialista a specialista pro křížovou kontrolu. Jejich činnosti jsou popsány v interní dokumentaci.

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

5.2.3 Identifikace a autentizace pro každou roli

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

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 definované v interní dokumentaci.

5.3 Personální postupy

5.3.1 Požadavky na kvalifikaci, praxi a bezúhonnost

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

- 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 vytvářejících důvěru 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 vytvářejících důvěru, znalost

bezpečnostních postupů s odpovědností za bezpečnost a zkušenosti s bezpečností informací a hodnocením rizik.

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, které 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.

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.

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 uvedeným v interní dokumentaci a řídícím se zákoníkem práce (tento proces nebrání případnému trestnímu stíhání, pokud tomu odpovídá závažnost zjištěné neautorizované činnosti).

5.3.7 Požadavky na nezávislé dodavatele

I.CA může nebo musí některé činnosti zajišťovat smluvně, za činnost nezávislých dodavatelů plně odpovídá. Tyto obchodně právní vztahy jsou ošetřeny bilaterálními obchodními smlouvami. Jedná se o např. o smluvní registrační autority, zhotovitele programového aplikačního vybavení, dodavatele hardware, systémového programového vybavení, externí auditory atd. Tyto subjekty jsou povinny se řídit odpovídajícími veřejnými certifikačními politikami, relevantními částmi interní dokumentace, které jim budou poskytnuty,

a předepsanými normativními dokumenty. V případě porušení povinností stanovených v uvedených dokumentech jsou uplatňovány smluvní pokuty, případně je s dodavatelem okamžitě ukončena smlouva.

5.3.8 Dokumentace poskytovaná zaměstnancům

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

5.4 Postupy zpracování auditních záznamů

5.4.1 Typy zaznamenávaných událostí

I.CA zaznamenává veškeré události požadované právní úpravou pro služby vytvářející důvěru a příslušnými technickými standardy a normami, mj. o životním cyklu Certifikátů, a to i od delegovaných třetích stran zapojených v životním cyklu certifikátů.

Generování CRL a OCSP odpovědí je zaznamenáváno.

Speciálním případem zaznamenávání událostí je událost generování párových dat certifikačních autorit. Celý proces generování párových dat certifikačních autorit probíhá v souladu s právní úpravou pro služby vytvářející důvěru a s relevantními technickými standardy a normami. Generování je vždy prováděno podle připraveného scénáře ve fyzicky zabezpečeném prostředí a pod kontrolou více osob v důvěryhodných rolích.

O generování párových dat certifikačních autorit je vytvořen protokol s údaji požadovanými v technických standardech, který je podepsán přítomnými osobami v důvěryhodných rolích. V případě generování klíče certifikační autority vydávající certifikáty typu SSL koncovým klientům je navíc proveden videozáznam postupu generování.

Pro generování párových dat kořenové certifikační autority dále platí, že je mu osobně přítomen auditor kvalifikovaný v souladu s platnými technickými standardy, který rovněž podepíše vytvořený protokol a potvrdí tím, že autorita při generování párových dat postupovala v souladu s připraveným scénářem a zajistila při tom integritu a důvěrnost.

Záznam bezpečnostních událostí v systémech, na síťových prvcích a vstupů na provozní pracoviště je prováděn v souladu s požadavky standardů v kapitolách 6.5 a 6.6 tohoto dokumentu a splňuje požadavky EVCG.

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

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

5.4.2 Periodicita zpracování záznamů

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

5.4.3 Doba uchování auditních záznamů

Nestanoví-li relevantní právní úprava jinak, jsou auditní záznamy uchovávány po dobu nejméně deseti 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, odcizením a zničením (ať již úmyslným, nebo neúmyslným).

Elektronické auditní záznamy jsou ukládány ve dvou kopiích. Minimálně jedenkrát měsíčně se provádí uložení těchto auditních záznamů na médium, které je umístěno mimo provozní prostory I.CA.

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

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

5.4.5 Postupy pro zálohování auditních záznamů

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

5.4.6 Systém shromažďování auditních záznamů (interní nebo externí)

Systém shromažďování auditních záznamů je z pohledu informačních systémů CA 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 vytvářejícími důvěru je popsáno v interní dokumentaci.

5.5 Uchovávání záznamů

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

5.5.1 Typy uchovávaných záznamů

I.CA uchovává níže uvedené záznamy (v elektronické nebo listinné podobě), které souvisejí s poskytovanými službami vytvářejícími důvěru, a to i od delegovaných třetích stran zapojených v životním cyklu certifikátů, zejména:

- zprávy/protokoly o průběhu generování párových dat certifikačních autorit,

- videozáznam průběhu generování párových dat podřízené certifikační autority vydávající certifikáty typu SSL,
- záznamy související s životním cyklem Certifikátů (zejména dokumentace z ověření žádostí o vydání a zneplatnění certifikátů),
- auditní záznamy podle kapitoly 5.4.1,
- záznam o manipulaci s informacemi (např. převzetí, předání, uložení, kontrola, konverze do elektronické podoby atd.),
- provozní a bezpečnostní dokumentaci.

5.5.2 Doba uchování záznamů

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

Postupy při uchovávání záznamů jsou upraveny interní dokumentací.

5.5.3 Ochrana úložiště záznamů

Prostory, ve kterých se uchovávané záznamy nacházejí, jsou zabezpečeny formou opatření, vycházejících z požadavků provedené analýzy rizik a ze zákona o ochraně utajovaných informací.

Postupy při ochraně úložiště uchovávaných záznamů jsou upraveny interní dokumentací.

5.5.4 Postupy při zálohování záznamů

Postupy při zálohování záznamů jsou upraveny interní dokumentací.

5.5.5 Požadavky na používání časových razítek při uchovávání záznamů

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

5.5.6 Systém shromažďování uchovávaných záznamů (interní nebo externí)

Záznamy jsou ukládány na místo určené výkonným ředitelem I.CA.

Samotná problematika přípravy a způsobu ukládání záznamů v elektronické i písemné podobě je upravena interní dokumentací. Shromažďování uchovávaných 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 dohledovým a kontrolním subjektům a orgánům činných v trestním řízení, pokud je to právními normami vyžadováno.

O každém takto povoleném přístupu je pořizován písemný záznam.

5.6 Výměna klíče

Výměna párových dat certifikačních autorit v případě standardních situací (uplynutí platnosti certifikátů certifikačních autorit) je prováděna s dostatečným časovým předstihem (minimálně jeden rok před uplynutím doby platnosti tohoto certifikátu) 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 uvedených událostí postupuje I.CA v souladu s interním plánem pro zvládání krizových situací a plán obnovy a případně s další relevantní interní dokumentací.

5.7.2 Poškození výpočetních prostředků, programového vybavení nebo dat

Viz kapitola 5.7.1.

5.7.3 Postup při kompromitaci soukromého klíče

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 příslušnou certifikační autoritou,
- bezodkladně o této skutečnosti, včetně důvodu, informuje v souladu s kapitolou 2.2, pro zpřístupnění této informace je využit i příslušný seznam zneplatněných 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 vytvářejících důvěru.

5.7.4 Schopnost obnovit činnost po havárii

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

5.8 Ukončení činnosti CA nebo RA

Pro ukončování činnosti Autority platí následující pravidla:

- ukončení činnosti Autority musí být písemně oznámeno orgánu dohledu, všem držitelům platných Certifikátů a subjektům, které mají s I.CA uzavřenou smlouvu přímo se vztahující k poskytování služeb vytvářejících důvěru,
- ukončení činnosti Autority musí být zveřejněno na internetové adrese podle kapitoly 2.2,
- pokud je součástí ukončení činnosti Autority ukončení platnosti jejího certifikátu, musí být součástí oznámení i tato informace včetně uvedení důvodu ukončení platnosti,
- ukončování činnosti je řízený proces probíhající podle předem připraveného plánu, jehož součástí je popis postupu uchovávání a zpřístupňování informací pro poskytování důkazů v soudním a správním řízení a pro účely zajištění kontinuity služeb,
- po dobu platnosti i jen jediného Certifikátu vydaného Autoritou musí Autorita či její nástupce v případě zániku zajistit alespoň služby zneplatňování Certifikátů a vydávání CRL,
- následně Autorita prokazatelně zničí svůj soukromý klíč a o tomto zničení provede záznam, který bude uchováván podle pravidel této CP.

V případě odnětí statutu kvalifikovaného poskytovatele Služby:

- informace musí být písemně nebo elektronicky oznámena všem držitelům platných Certifikátů a subjektům, které mají s I.CA 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 certifikáty certifikačních autorit nelze nadále používat v souladu s účelem jejich vydání,
- o dalším postupu rozhodne generální 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.

6 ŘÍZENÍ TECHNICKÉ BEZPEČNOSTI

6.1 Generování a instalace párových dat

6.1.1 Generování párových dat

Generování párových dat certifikačních autorit a jejich OCSP respondérů, které probíhá v zabezpečených vyhrazených prostorách provozních pracovišť v souladu s požadavky kapitol 5.2 a 5.4.1, je prováděno v kryptografických modulech, které splňují požadavky právní úpravy pro služby vytvářející důvěru, tedy standardů ETSI a CEN.

Generování párových dat pracovníků podílejících se na vydávání Certifikátů je prováděno 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.

Veškeré požadavky na proces generování výše uvedených párových dat jsou popsány interní a externí dokumentací.

Generování párových dat vztahujících se k Certifikátům je prováděno na zařízeních, která jsou pod výhradní kontrolou příslušných držitelů soukromých klíčů. Úložištěm těchto párových dat může být jak hardware, tak software.

6.1.2 Předávání soukromého klíče jeho držiteli

Pro soukromé klíče certifikačních autorit a jejich OCSP respondérů není relevantní – soukromé klíče jsou uloženy v kryptografických modulech, které jsou pod výhradní kontrolou I.CA.

Služba generování párových dat držitelům Certifikátů a pracovníkům podílejícím se na vydávání Certifikátů není poskytována.

6.1.3 Předávání veřejného klíče vydavateli certifikátu

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

6.1.4 Poskytování veřejného klíče CA spoléhajícím se stranám

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

- obdržením na RA,
- prostřednictvím internetových informačních adres I.CA, příslušného orgánu dohledu, resp. prostřednictvím věstníku tohoto orgánu dohledu,
- každý žadatel o certifikát obdrží příslušné certifikáty certifikačních autorit při získání svého prvotního certifikátu.

6.1.5 Délky klíčů

Mohutnost klíče kořenové certifikační autority I.CA využívající algoritmus RSA je 4096 bitů, mohutnost klíčů v jí vydávaných certifikátech podřízených certifikačních autorit je minimálně

2048 bitů, mohutnost klíčů OCSP respondérů certifikačních autorit je minimálně 2048 bitů. Mohutnost klíčů v Certifikátech vydávaných podle této CP je minimálně 2048 bitů.

6.1.6 Parametry veřejného klíče a kontrola jeho kvality

Parametry algoritmů použitých při generování veřejných klíčů certifikačních autorit a jejich OCSP respondérů splňují požadavky uvedené v právní úpravě pro služby vytvářející důvěru, resp. v ní odkazovaných technických standardech nebo normách. Tyto klíče jsou generovány a kontrolovány příslušným technickým a programovým vybavením.

Parametry algoritmů použitých při generování veřejných klíčů ostatních držitelů certifikátů musí tyto požadavky rovněž splňovat a jsou stejným způsobem kontrolovány.

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

6.2.1 Řízení a standardy kryptografických modulů

Generování párových dat certifikačních autorit a jejich OCSP respondérů a uložení odpovídajících soukromých klíčů je prováděno v kryptografických modulech, které splňují požadavky právní úpravy pro služby vytvářející důvěru, tedy standardů ETSI a CEN, a jsou používány v souladu s jejich certifikací.

Pracovníci podílející se na vydávání certifikátů využívají čipové karty splňující požadavky na QSCD.

Používání kryptografických modulů koncovými uživateli je plně v jejich kompetenci.

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

Pokud je pro činnosti spojené s kryptografickým modulem nezbytná přítomnost více osob, potom každá z nich zná pouze část kódu k provedení těchto činností.

6.2.3 Úschova soukromého klíče

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

6.2.4 Zálohování soukromého klíče

Soukromé klíče certifikačních autorit a jejich OCSP respondérů chráněné kryptografickými moduly jsou zálohovány v zašifrované podobě, která zajišťuje stejnou úroveň ochrany jako kryptografické zařízení.

Pro soukromé klíče pracovníků podílejících se na vydávání Certifikátů není relevantní, jsou vygenerovány na čipových kartách v neexportovatelném tvaru.

Zálohování soukromých klíčů vztahujících se k Certifikátům koncových uživatelů je plně v kompetenci těchto koncových uživatelů.

6.2.5 Uchovávání soukromého klíče

Soukromé klíče certifikačních autorit a jejich OCSP respondérů nejsou nikde uchovávány, po uplynutí doby platnosti jsou včetně jejich záloh zničeny.

Doba uchování soukromých klíčů pracovníků podílejících se na vydávání Certifikátů je dána kapacitou paměti čipové karty.

Uchovávání soukromých klíčů vztahujících se k Certifikátům koncových uživatelů je plně v kompetenci těchto koncových uživatelů.

6.2.6 Transfer soukromého klíče do nebo z kryptografického modulu

Soukromé klíče certifikačních autorit a jejich OCSP respondérů jsou generovány v kryptografických modulech (jako neexportovatelné) a nelze je z kryptografického modulu (provozovaného v certifikovaném režimu) exportovat v žádném tvaru[1]. Import soukromého klíče CA do kryptografického modulu není prováděn.

Pro transfer soukromých klíčů pracovníků podílejících se na vydávání Certifikátů není relevantní, jsou vygenerovány v neexportovatelném tvaru.

Transfer soukromých klíčů vztahujících se k Certifikátům koncových uživatelů je plně v kompetenci těchto koncových uživatelů.

6.2.7 Uložení soukromého klíče v kryptografickém modulu

Soukromé klíče certifikačních autorit a jejich OCSP respondérů jsou uloženy v kryptografických modulech splňujících požadavky právní úpravy pro služby vytvářející důvěru, tedy standardů ETSI a CEN.

Soukromé klíče pracovníků podílejících se na vydávání Certifikátů jsou uloženy na čipových kartách splňujících požadavky na QSCD.

Případné uložení soukromých klíčů vztahujících se k Certifikátům koncových uživatelů v kryptografických modulech je plně v kompetenci těchto koncových uživatelů.

6.2.8 Postup aktivace soukromého klíče

Aktivace soukromých klíčů (umožnění jejich použití) certifikačních autorit a jejich OCSP respondérů v kryptografických modulech je prováděna:

- v případě aktivace čipovou kartou – vložením čipové karty a zadáním hesla,
- v případě aktivace pomocí softcard – předložením softcard a hesla.

Soukromé klíče pracovníků podílejících se na vydávání Certifikátů jsou aktivovány vložením čipové karty do snímače a zadáním PIN.

Aktivace soukromých klíčů vztahujících se k Certifikátům koncových uživatelů je plně v kompetenci těchto koncových uživatelů a závisí na způsobu uložení těchto soukromých klíčů.

[1] Výjimkou je zašifrovaná záloha, kterou lze použít pouze v kryptografickém modulu (resp. v HA/LB modulech), kde byl klíč vygenerován.

6.2.9 Postup deaktivace soukromého klíče

Deaktivace soukromých klíčů certifikačních autorit a jejich OCSP respondérů v kryptografických modulech je provedena vyjmutím čipové karty nebo ukončením příslušné aplikace.

Soukromé klíče pracovníků podílejících se na vydávání Certifikátů jsou deaktivovány vyjmutím čipové karty ze snímače.

Deaktivace soukromých klíčů vztahujících se k Certifikátům koncových uživatelů je plně v kompetenci těchto koncových uživatelů a závisí na způsobu uložení těchto soukromých klíčů.

6.2.10 Postup ničení soukromého klíče

Po uplynutí doby platnosti soukromého klíče příslušné certifikační autority a na základě následného potvrzení generálním ředitelem I.CA je tento soukromý klíč včetně jeho záloh zničen určeným postupem. O provedeném zničení je pořízen písemný záznam.

V případě soukromých klíčů OCSP respondérů je jejich ničení prováděno na příkaz osoby zastupující I.CA při vydání certifikátu OCSP respondéru. O provedeném zničení je pořízen písemný záznam.

Ničení soukromých klíčů pracovníků podílejících se na vydávání Certifikátů je plně v kompetenci těchto pracovníků, není předepsáno. Nutné je pouze v případě zaplnění paměti čipové karty.

Ničení soukromých klíčů vztahujících se k Certifikátům koncových uživatelů je plně v kompetenci těchto koncových uživatelů.

6.2.11 Hodnocení kryptografických modulů

Kryptografické moduly použité pro generování párových dat a uložení příslušných soukromých klíčů certifikačních autorit a jejich OCSP respondérů splňují požadavky právní úpravy pro služby vytvářející důvěru, tedy standardů ETSI a CEN, a jsou používány v souladu s příslušnou certifikací.

Čipové karty použité pro generování párových dat a uložení příslušných soukromých klíčů pracovníků podílejících se na vydávání Certifikátů splňují požadavky na QSCD.

Případné použití kryptografických modulů koncovými uživateli včetně jejich hodnocení je plně v kompetenci těchto koncových uživatelů.

6.3 Další aspekty správy párových dat

6.3.1 Uchovávání veřejných klíčů

Veškeré veřejné klíče jsou uchovávány ve formě certifikátů 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 a je stejná jako doba použitelnosti příslušných párových dat. V souladu s EVCG je doba platnosti Certifikátu nejvýše 398 dnů.

6.4 Aktivační data

6.4.1 Generování a instalace aktivačních dat

Aktivační data soukromých klíčů certifikačních autorit a jejich OCSP respondérů (čipová karta nebo softcard) jsou vytvářena před generováním nebo v průběhu generování příslušných párových dat.

Aktivačními daty soukromých klíčů pracovníků podílejících se na vydávání Certifikátů je PIN, který je plně po kontrolou těchto pracovníků.

Případné použití aktivační dat koncových uživatelů je plně v kompetenci těchto koncových uživatelů.

6.4.2 Ochrana aktivačních dat

Aktivační data soukromých klíčů certifikačních autorit a jejich OCSP respondérů (čipová karta nebo softcard) jsou chráněna nastaveným heslem.

Ochrana aktivačních dat soukromých klíčů pracovníků podílejících se na vydávání Certifikátů je plně po kontrolou těchto pracovníků.

Případná ochrana aktivačních dat koncových uživatelů je plně v kompetenci těchto koncových uživatelů.

6.4.3 Ostatní aspekty aktivačních dat

Není relevantní pro tento dokument.

6.5 Řízení počítačové bezpečnosti

6.5.1 Specifické technické požadavky na počítačovou bezpečnost

Úroveň bezpečnosti použitých komponent pro poskytování služeb vytvářejících důvěru je, včetně rozsahu potřebných kontrol, tj. i kontrol konfigurace důvěryhodných systémů a jejich periodicity, definována právní úpravou pro služby vytvářející důvěru, resp. v ní odkazovanými technickými standardy a normami.

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.
- 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 3: Certificate profile for certificates issued to legal persons.
- ČSN ETSI EN 319 412-4 Elektronické podpisy a infrastruktury (ESI) - Profily certifikátu – Část 4: Profil certifikátu pro certifikáty webových stránek.
- ETSI EN 319 412-4 Electronic Signatures and Infrastructures (ESI); Certificate Profiles; Part 4: Certificate profile for web site certificates.
- 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.
- ČSN EN 419 221-5 Profily ochrany pro TSP kryptografické moduly – Část 5: Kryptografický modul pro důvěryhodné služby.
- EN 419 221-5 Protection profiles for TSP Cryptographic modules - Part 5 Cryptographic Module for Trust Services.
- ISO/IEC 15408-1:2009 Information technology — Security techniques — Evaluation criteria for IT security — Part 1: Introduction and general model.
- ČSN EN ISO/IEC 15408-2 Informační technologie - Bezpečnostní techniky - Kritéria pro hodnocení bezpečnosti IT - Část 2: Bezpečnostní funkční komponenty.
- ISO/IEC 15408-2:2008 Information technology — Security techniques — Evaluation criteria for IT security — Part 2: Security functional components.
- ČSN EN ISO/IEC 15408-3 Informační technologie - Bezpečnostní techniky - Kritéria pro hodnocení bezpečnosti IT - Část 3: Komponenty bezpečnostních záruk.
- ISO/IEC 15408-3:2008 Information technology — Security techniques — Evaluation criteria for IT security — Part 3: Security assurance components.
- FIPS PUB 140-2 Requirements for Cryptographic Modules.
- ETSI TS 119 312 Electronic Signatures and Infrastructures (ESI); Cryptographic Suites.
- CA/Browser Forum - Baseline Requirements for the Issuance and Management of Publicly-Trusted Certificates (Baseline Requirements).
- CA/Browser Forum - Guidelines For The Issuance And Management Of Extended Validation Certificates.
- ČSN ISO/IEC 27006 Informační technologie – Bezpečnostní techniky – Požadavky na orgány provádějící audit a certifikaci systémů řízení bezpečnosti informací.
- ISO/IEC 17021 Conformity assessment -- Requirements for bodies providing audit and certification of management systems.
- ISO/IEC 17065 Conformity assessment -- Requirements for bodies certifying products, processes and services.
- 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 6960 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.
- EN 301 549 Accessibility requirements for ICT products and services.

6.6 Technické řízení životního cyklu

6.6.1 Řízení vývoje systému

Při vývoji systému je postupováno v souladu s interní dokumentací.

6.6.2 Řízení správy bezpečnosti

Kontrola řízení bezpečnosti informací, včetně kontroly souladu 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.

6.6.3 Řízení životního cyklu bezpečnosti

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

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

6.7 Řízení bezpečnosti sítě

Síťová infrastruktura provozního pracoviště je chráněna komerčním produktem typu firewall s integrovaným systémem IPS (Intrusion Prevention System). Detailní řešení řízení síťové bezpečnosti je popsáno v interní dokumentaci. Veškerá komunikace mezi RA a provozními pracovišti je vedena šifrovaně.

6.8 Označování časovými razítky

Řešení je uvedeno v kapitole 5.5.5.

7 PROFILY CERTIFIKÁTU, SEZNAMU ZNEPLATNĚNÝCH CERTIFIKÁTŮ A OCSP

7.1 Profil certifikátu

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

tab. 4 - Základní pole Certifikátu

Pole	Obsah
version	v3 (0x2)
serialNumber	jedinečné sériové číslo Certifikátu, větší než nula, s náhodnou částí nejméně 64 bitů z náhodného generátoru používaného pro kryptosystémy
signatureAlgorithm	minimálně sha256WithRSAEncryption
issuer	vydavatel Certifikátu
validity	
notBefore*	počátek platnosti Certifikátu (UTC)
notAfter*	počátek platnosti Certifikátu (UTC) + maximálně 398 dnů
subject	viz tab. 5 - atributem pole subject nesmí být **samotný** znak ".", "-" nebo " " (mezera) a atributy ani nesmí obsahovat jinou indikaci, že hodnota není uvedena, je neúplná, nebo neaplikovatelná
subjectPublicKeyInfo	musí splňovat požadavky kapitol 6.1.5 a 6.1.6
algorithm	rsaEncryption
subjectPublicKey	minimálně 2048 bitů
extensions	rozšíření vydávaného Certifikátu – viz tab. 6
signature	zaručená elektronická pečeť vydavatele Certifikátu

* Dobu platnosti určuje Autorita a je v souladu s EVCG (obvykle dvanáct měsíců).

tab. 5 - Položky pole subject

Všechny položky[2] pole subject jsou převzaty ze žádosti o Certifikát s výjimkou položek vytvářených Autoritou. Povinné položky musí být v žádosti obsaženy.

Položka pole subject	Obsah	Poznámka
Adresa umístění fyzického sídla subjektu		
countryName	dvoupísmenný kód země	povinná

[2] I.CA si vyhrazuje právo upravit množinu a obsah položek pole subject, vyžadovanou aktualizacemi standardů ETSI, nebo třetími stranami (např. společnost Microsoft).

	(ISO 3166-1)	
stateOrProvinceName	státu federace nebo kraj/provincie	povinná
localityName	město/obec	povinná
postalCode	poštovní směrovací číslo	volitelná
streetAddress	adresa ulice subjektu a popisné číslo	volitelná
Identifikace subjektu – vlastníka* SSL/TLS serveru		
organizationName	MUSÍ obsahovat úplné zapsané právní jméno subjektu; navíc může obsahovat na začátku pole obchodní jméno, za předpokladu že následuje úplné právní jméno subjektu uvedené v závorkách (kulatých).	povinná CA může zkrátit/ akceptovat zkrácení názvu za účelem, aby se text vešel do 64 znaků, a to za předpokladu, že třetí strana nemůže být uvedena v omyl, že komunikuje s jinou organizací
businessCategory (2.5.4.15)	MUSÍ obsahovat jeden z řetězců podle toho, do které kategorie subjekt spadá (EVCG, kapitola 8.5): ▪ „**Private Organization**" - firma zapsaná nebo registrovaná podle zákona nebo ustavené vládní agenturou; v ČR je to OR (obchodní rejstřík), ▪ „**Government Entity**" - vládní úřad (entita), ▪ „**Business Entity**" - subjekty registrované registrační agenturou, která přiděluje/ověřuje právo podnikání, certifikát, licenci (např. registrované jinde než v OR), jejichž registrace může být ověřena, ▪ „**Non-Commercial Entity**" - mezinárodní organizace založená na základě smluv podepsaných vládami více států	povinná
Úroveň, na jaké pracuje registrační agentura, která registrovala subjekt a registrační číslo		
jurisdictionCountryName (1.3.6.1.4.1.311.60.2.1.3)	ISO 3166-1 kód státu	▪ povinná, pokud byla registrace subjektu provedena (je řízena) na státní úrovni,

		▪ pro subjekty registrované v ČR pouze tento atribut, ▪ pokud je přítomno, potom NESMÍ být uvedeno jurisdictionLocalityName ani jurisdictionStateOrProvinceName
jurisdictionStateOrProvinceName (1.3.6.1.4.1.311.60.2.1.2)	UTF8String o maximální délce 128 znaků (textově úplný název kraje/provincie)	▪ povinná, pokud byla registrace subjektu provedena (je řízena) na úrovni „provincie"/kraje, ▪ současně MUSÍ být přítomno i jurisdictionCountryName, a NESMÍ být přítomno jurisdictionLocalityName, ▪ pro CZ nerelevantní, pro subjekty registrované v jiných státech může být potřebné uvádět
jurisdictionLocalityName (1.3.6.1.4.1.311.60.2.1.1)	UTF8String o maximální délce 128 znaků (textově úplný název lokality/města)	▪ povinná, pokud byla registrace subjektu provedena (je řízena) na úrovni lokality = města, ▪ potom současně MUSÍ být přítomno i jurisdictionCountryName a MUSÍ být přítomno i jurisdictionStateOrProvinceName, ▪ pro CZ nerelevantní, pro subjekty registrované v jiných státech může být potřebné uvádět

serialNumber	▪ **Private Organization**: registrační číslo, nebo, pokud není přidělováno, datum registrace, ▪ **Government Entity**: datum založení/zápisu/vzniku nebo číslo zákona nebo text vyjadřující, že subjekt je vládní entita, ▪ **Business Entity**: unikátní registrační číslo nebo pokud není přidělováno tak datum registrace, ▪ **Non-Commercial**: datum založení nebo číslo zákona nebo text vyjadřující, že subjekt je mezinárodní organizace	povinná
commonName	pokud uvedeno, MUSÍ se jednat o jediné dNSName serveru současně uvedené v první položce subjectAlternativeName (viz tab. 6)	volitelná, s ohledem na kompatibilitu doporučujeme uvádět musí se jednat o veřejné DNS jméno zástupné znaky nejsou povoleny

* Přesněji subjektu ovládajícího server (provozovat SSL server a/nebo vlastnit fyzický server může někdo jiný – hostingová firma apod.).

7.1.1 Číslo verze

Vydávané Certifikáty jsou v souladu s X.509 ve verzi 3.

7.1.2 Rozšíření certifikátu

tab. 6 - Rozšíření[3] Certifikátu

Rozšíření	Obsah	Poznámka
subjectAlternativeName		nekritické
dNSName (1 .. 10 výskytů)	DNS jméno hostitele (SSL/TLS serveru) / DNS domény na základě obsahu žádosti o certifikát s následujícími omezeními: ▪ MUSÍ se jednat o veřejné DNS jméno ▪ povinná nejméně 1 položka, přípustné maximálně 10 položek dNSName,	obsah první položky dNSName musí být totožný s obsahem položky subject.commonName, pokud je commonName uvedeno

[3] I.CA si vyhrazuje právo upravit množinu a obsah rozšíření Certifikátu, vyžadovanou aktualizacemi standardů ETSI, nebo třetími stranami (např. společnost Microsoft).

	▪ Certifikáty pro domény se zástupnými znaky (např. *.firma.cz) NESMĚJÍ být vydávány ▪ Certifikáty pro gTLD doménu .onion NEJSOU vydávány, ▪ Certifikáty pro doménová jména obsahující znak podtržení ("_") NEJSOU vydávány, ▪ FQDN musí být složeno pouze z LDH návěští (viz definice) spojených tečkou, na konci FQDN nesmí být tečka (chybně např. example.com.), ▪ Certifikáty pro doménová jména se smíšenou znakovou sadou (Internationalized Domain Names IDN, LDH návěští uvozená sekvencí "xn--") NEJSOU vydávány, ▪ všechny položky dNSName musí obsahovat stejná dvě doménová návěští uvedená nejvíce vpravo (nejvýznamnější návěští, tj. stejnou doménu druhé úrovně)	
certificatePolicies		nekritické
.policyInformation(1)		
policyIdentifier	EV (2.23.140.1.1)	OID uvedené v EVCG identifikátor politiky dle požadavků Microsoft
.policyInformation(2)		
policyIdentifier	viz kapitola 1.2	povinné
policyQualifiers		
cPSuri	http://www.ica.cz	
userNotice*	Tento kvalif. certifikat pro autentizaci internetovych stranek byl vydan v souladu s nariz. EU c. 910/2014. This is a EU qualified certificate for website auth. according to Reg. (EU) No 910/2014.	volitelné
.policyInformation(3)		doporučeno EN 319 411-2 pro QCP-w certifikáty

policyIdentifier	QCP-w (0.4.0.194112.1.4)	
QCStatements		nekritické
	id-etsi-qcs-QcCompliance (0.4.0.1862.1.1)	
	id-etsi-qcs-QcSSCD (0.4.0.1862.1.4)	může být uvedeno v případě, kdy soukromý klíč je generován a uložen na QSCD
	id-etsi-qcs-QcPDS (0.4.0.1862.1.5)	odkaz (URI, https) na zprávu pro uživatele (PDS)
	id-etsi-qcs-QcType (0.4.0.1862.1.6) = 0.4.0.1862.1.6.3	povinné id-etsi-qcs-QcType = id-etsi-qct-web
CRLDistributionPoints**	http://qcrldp1.ica.cz/qcw*RR*_rsa.crl http://qcrldp2.ica.cz/qcw*RR*_rsa.crl http://qcrldp3.ica.cz/qcw*RR*_rsa.crl	nekritické
authorityInformationAccess		nekritické
id-ad-ocsp**	http://ocsp.ica.cz/qcw*RR*_rsa	
id-ad-caIssuers**	http://q.ica.cz/qcw*RR*_rsa.cer	
basicConstraints		kritické
cA	False	
keyUsage	digitalSignature, keyEncipherment	kritické
extendedKeyUsage***	na základě obsahu žádosti; ▪ musí být obsažena alespoň id-kp-serverAuth, ▪ nebo id-kp-serverAuth a id-kp-clientAuth	nekritické, povinné; v případě absence tohoto rozšíření v žádosti bude doplněno: id-kp-serverAuth, id-kp-clientAuth
subjectKeyIdentifier	hash veřejného klíče (subjectPublicKey) ve vydávaném certifikátu	nekritické
authorityKeyIdentifier	hash veřejného klíče vydavatele certifikátu (Autority)	nekritické
keyIdentifier	hash veřejného klíče vydavatele certifikátu (Autority)	

Signed Certificate Timestamp	„razítka" nejméně ze dvou Certificate Transparency (CT) logů	„razítko" = podepsané potvrzení z příslušného CT logu o zařazení precertifikátu

* Vydavatel může text položky změnit.

** *RR* – poslední dvě číslice roku vydání certifikátu Autority.

*** Jedná se o podporovanou množinu, konkrétní EKU je přebíráno ze žádosti o Certifikát.

7.1.2.1 Všechny certifikáty

Ostatní pole a rozšíření jsou nastavena v souladu s RFC 5280. Autorita nevydá certifikát obsahující příznak keyUsage, hodnotu extendedKeyUsage, rozšíření certifikátu nebo další data nespecifikovaná v této kapitole 7.1.2, pokud nemá pro vložení takových dat do certifikátu důvod.

Autorita rovněž nevydá certifikáty:

- s rozšířeními, která jsou nerelevantní v kontextu veřejného Internetu,
- se sémantikou, která, pokud by byla zahrnuta, uvede v omyl spoléhající se stranu.

7.1.2.2 Aplikace RFC 5280

„Precertifikát", jak je popsán v RFC 6962 – Certificate Transparency, není považován za certifikát splňující požadavky RFC 5280.

7.1.3 Objektové identifikátory algoritmů

V procesu poskytování služeb vytvářejících důvěru jsou využívány algoritmy v souladu s příslušnými technickými standardy a normami a ve shodě s EVCG.

7.1.4 Tvary jmen

Autorita vydává Certifikáty s tvary jmen, vyhovujícími standardu RFC 5280.

Omezení jmen a atributů Certifikátu viz profil výše. Dále platí ustanovení kapitoly 3.1.

Ověřování oprávnění registranta doménového jména je uvedeno v kapitole 3.2.2.4.

7.1.5 Omezení jmen

Jména a názvy uvedené v Certifikátu musí, je-li to možné, přesně odpovídat údajům v dokumentech, kterými se žadatel o certifikát nebo držitel certifikátu prokazoval v procesu registrace.

7.1.6 Objektový identifikátor certifikační politiky

OID certifikační politiky, resp. politik jsou uvedena v položce certificatePolicies (viz tab. 6).

7.1.7 Použití rozšíření Policy Constraints

Není relevantní pro Certifikáty vydávané koncovým uživatelům.

7.1.8 Syntaxe a sémantika kvalifikátorů politiky

Viz rozšíření Certifikátu v kapitole 7.1.2 výše.

7.1.9 Zpracování sémantiky kritického rozšíření Certificate Policies

Není relevantní pro tento dokument – není označeno jako kritické.

7.2 Profil seznamu zneplatněných certifikátů

tab. 7 - Profil CRL[4]

Pole	Obsah
version	v2(0x1)
signatureAlgorithm	minimálně sha256WithRSAEncryption
issuer	vydavatel CRL
thisUpdate	datum a čas vydání CRL (UTC)
nextUpdate*	datum a předpokládaný čas vydání následujícího CRL (UTC)
revokedCertificates	seznam zneplatněných certifikátů
userCertificate	sériové číslo zneplatněného certifikátu
revocationDate	datum a čas zneplatnění certifikátu
crlEntryExtensions	rozšíření položky seznamu – viz tab. 8
crlExtensions	rozšíření CRL – viz tab. 8
signature	zaručené elektronická pečeť vydavatele CRL

* V případě certifikátu kořenové CA thisUpdate + maximálně 365 dní, v případě certifikátu podřízené CA thisUpdate + maximálně 24 hodin.

7.2.1 Číslo verze

Seznamy zneplatněných certifikátů jsou vydávány dle X.509 verze 2.

[4] I.CA si vyhrazuje právo upravit množinu a obsah polí CRL, vyžadovanou aktualizacemi standardů ETSI, nebo třetími stranami (např. společnost Microsoft).

7.2.2 Rozšíření CRL a záznamů v CRL

tab. 8 - Rozšíření CRL[3]

Rozšíření	Obsah	Poznámka
crlEntryExtensions		
CRLReason*	důvod zneplatnění certifikátu důvod certificateHold je nepřípustný, nepoužívá se při zneplatnění certifikátu podřízené CA je uveden jiný důvod, než unspecified (0)	nekritické, volitelné
crlExtensions		
authorityKeyIdentifier		
keyIdentifier	hash veřejného klíče vydavatele CRL (Autority)	nekritické
CRLNumber	jedinečné číslo vydávaného CRL	nekritické

* Pro Certifikáty koncových uživatelů jsou používány (podle jednotlivých důvodů zneplatnění – viz kapitola 4.9.1.1) pouze následující kódy CRLReason:

- keyCompromise (RFC 5280 CRLReason #1),
- affiliationChanged (RFC 5280 CRLReason #3),
- superseded (RFC 5280 CRLReason #4),
- cessationOfOperation (RFC 5280 CRLReason #5),
- privilegeWithdrawn (RFC 5280 CRLReason #9) - tento kód nemůže přímo použít držitel Certifikátu, je určován CA (nejdéle od 15.7.2023).

Aktualizace kódu a data zneplatnění u již zneplatněné CRL položky při pozdějším získání ověřitelného důkazu o kompromitace klíče není implementována.

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. Pro certifikáty nevydané příslušnou CA je vrácena odpověď unAuthorized.

Jako přenosový protokol je používáno pouze http.

Bližší podrobnosti jsou uvedeny v odpovídající certifikační prováděcí směrnici.

7.3.1 Číslo verze

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

7.3.2 Rozšíření OCSP

Konkrétní rozšíření uváděná v žádosti a odpovědi na stav certifikátu s využitím protokolu OCSP jsou uvedena v odpovídající certifikační prováděcí směrnici.

8 HODNOCENÍ SHODY A JINÁ HODNOCENÍ

8.1 Periodicita nebo okolnosti hodnocení

Periodicita hodnocení, včetně okolností pro provádění hodnocení, je dána právní úpravou pro služby vytvářející důvěru a jí odkazovanými technickými standardy a normami, dle kterých je hodnocení prováděno.

Periodicita hodnocení pro program Microsoft Trusted Root Program, včetně okolností pro provádění hodnocení, je striktně dána požadavky společnosti Microsoft. Doba činnosti Autority je rozdělena do nepřerušené posloupnosti auditních period, přičemž auditní perioda nepřekračuje jeden rok.

Periodicita jiných hodnocení je dána technickými standardy a normami, dle kterých je hodnocení prováděno.

8.2 Identita a kvalifikace hodnotitele

Identita (akreditovaný subjekt posuzování shody) a kvalifikace hodnotitele provádějícího hodnocení podle právní úpravy pro služby vytvářející důvěru, je dána touto právní úpravou a jí odkazovanými technickými standardy a normami.

Identita (akreditovaný subjekt posuzování shody) a kvalifikace hodnotitele provádějícího hodnocení, definované programem Microsoft Trusted Root Program jsou popsány v normě ETSI EN 319 403.

Kvalifikace hodnotitele provádějícího jiná hodnocení je dána příslušnými technickými standardy a normami.

8.3 Vztah hodnotitele k hodnocenému subjektu

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

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

8.4 Hodnocené oblasti

V případě provádění hodnocení požadovaného právní úpravou pro služby vytvářející důvěru jsou hodnocené oblasti konkretizovány touto právní úpravou.

Hodnocené oblasti pro program Microsoft Trusted Root Program jsou striktně dány požadavky společnosti Microsoft.

Hodnocené oblasti u jiných hodnocení jsou konkretizovány technickými standardy a normami, podle kterých je hodnocení prováděno.

8.5 Postup v případě zjištění nedostatků

Se zjištěními všech typů prováděných hodnocení je seznámen bezpečnostní manažer I.CA, který je povinen zajistit odstranění případných nedostatků. Pokud by byly zjištěny nedostatky, které by zásadním způsobem znemožňovaly poskytovat Službu, přeruší I.CA tuto Službu do doby, než budou tyto nedostatky odstraněny.

8.6 Sdělování výsledků hodnocení

Sdělování výsledků hodnocení podléhá požadavkům právní úpravy pro služby vytvářející důvěru a příslušných technických standardů a norem, v případě hodnocení požadované programem Microsoft Trusted Root Program potom požadavkům společnosti Microsoft.

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

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

8.7 Pravidelné samoaudity hodnocení kvality

Zaměstnanec I.CA provádí alespoň čtvrtletně, na náhodně vybraném vzorku o velikosti alespoň jednoho Certifikátu, nejméně však tří procent Certifikátů vydaných v době bezprostředně následující poté, kdy byl vybrán vzorek pro minulý samoaudit, kontrolu souladu s CP a CPS.

9 OSTATNÍ OBCHODNÍ A PRÁVNÍ ZÁLEŽITOSTI

9.1 Poplatky

9.1.1 Poplatky za vydání nebo obnovení certifikátu

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

9.1.2 Poplatky za přístup k certifikátu

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

9.1.3 Zneplatnění nebo přístup k informaci certifikátu

Přístup elektronickou cestou k informacím o zneplatněných certifikátech (CRL) a o stavech certifikátů vydaných Autoritou 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 platně 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 jiné finanční zajištění na poskytování služeb vytvářejících důvěru 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., zveřejněné v obchodním rejstříku.

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 vytvářejících důvěru,
- 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 generálního 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 právních předpisů, tedy zejména ZOOÚ a GDPR.

9.4.2 Informace považované za osobní údaje

Osobními údaji jsou veškeré osobní údaje podléhající ochraně ve smyslu příslušných právních předpisů.

Zaměstnanci I.CA, případně subjekty definované platnou právní úpravou 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 právních předpisů.

9.4.4 Odpovědnost za ochranu osobních údajů

Za ochranu osobních údajů je odpovědný generální ředitel I.CA.

9.4.5 Oznámení o používání osobních údajů a souhlas s jejich používáním

Problematika oznamování o používání osobních údajů a souhlasu s jejich zpracováním je v I.CA řešena v souladu s požadavky příslušných právních předpisů.

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 právních předpisů.

9.4.7 Jiné okolnosti zpřístupňování osobních údajů

V případě zpřístupňování osobních údajů postupuje I.CA striktně podle požadavků příslušných právních předpisů.

9.5 Práva duševního vlastnictví

Tato CP, veškeré související dokumenty, obsah webových stránek a procedury, zajišťující provoz důvěryhodných systémů podporujících 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 jimi vydaných zneplatněných certifikátů a k vydávání certifikátů jejich OCSP respondérů,
- použije soukromé klíče OCSP respondérů certifikačních autorit pouze v procesech poskytování odpovědí na stav certifikátu,
- certifikáty splňují náležitosti požadované právní úpravou pro služby vytvářející důvěru a příslušnými technickými standardy a normami,
- zneplatní vydané Certifikáty, pokud byla žádost o ukončení jejich platnosti podána způsobem definovaným v této CP.

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

- držitel Certifikátu neporušil povinnosti plynoucí mu ze smlouvy o poskytování Služby a této CP,
- spoléhající se strana neporušila povinnosti této CP.

Držitel Certifikátu vydaného dle této CP uplatňuje záruku vždy u RA, která zpracovala jeho žádost o vydání tohoto Certifikátu.

I.CA vyjadřuje a poskytuje příjemcům Certifikátů, tj. držitelům, dodavatelům aplikačního programového vybavení, se kterými má uzavřenou smlouvu o zahrnutí kořenového certifikátu do jejich produktů a veškerým spoléhajícím se stranám záruky, že při vydávání Certifikátů a v průběhu doby jejich platnosti bude při jejich správě vyhovovat své CP a CPS.

Záruky zahrnují:

- kontrolu práva užívat doménové jméno uváděné v Certifikátu,
- kontrolu práva žádat o Certifikát jménem Organizace,
- 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 certifikátů,
- že Certifikát může být zneplatněn z důvodů uvedených v této CP.

9.6.2 Zastupování a záruky RA

Určená RA:

- přejímá závazek za správnost jí poskytovaných služeb,
- nevyřídí kladně žádost, pokud se nepodařilo ověřit některou z položek žádosti, 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 Autority,
- odpovídá za vyřizování připomínek a stížností.

9.6.3 Zastupování a záruky držitele certifikátu

Záruky držitele Certifikátu jsou uvedeny ve smlouvě mezi I.CA a držitelem Certifikátu.

9.6.4 Zastupování a záruky spoléhajících se stran

Spoléhající se strany postupují podle této CP.

9.6.5 Zastupování a záruky ostatních zúčastněných subjektů

Není relevantní pro tento dokument.

9.7 Zřeknutí se záruk

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

9.8 Omezení odpovědnosti

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

V ostatních případech je maximální výše náhrady za škodu způsobenou jednomu držiteli Certifikátu nebo jedné spoléhající se straně za jeden Certifikát omezena na částku ekvivalentní hodnotě dvou tisíc dolarů v českých korunách dle směnného kurzu aktuálního v okamžiku vzniku škody.

9.9 Záruky a odškodnění

Pro poskytování služeb vytvářejících důvěru platí relevantní ustanovení platné právní úpravy týkající se vztahů mezi poskytovatelem a spotřebitelem a dále takové záruky, které byly sjednány mezi společností První certifikační autorita, a.s., a žadatelem o Službu. Smlouva nesmí být v rozporu s právní úpravou pro služby vytvářející důvěru a musí být vždy v elektronické nebo listinné formě.

Společnost První certifikační autorita, a.s.:

- se zavazuje, že splní veškeré povinnosti definované uzavřenou smlouvou i příslušnými politikami,
- poskytuje výše uvedené záruky po celou dobu platnosti smlouvy o poskytování Služby,
- 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.

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

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

Reklamaci je možné podat těmito způsoby:

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

- osobně v sídle společnosti.

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

- co nejvýstižnější popis závad a jejich projevů,
- sériové číslo reklamovaného produktu,
- požadovaný způsob vyřízení reklamace.

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

Reklamace, včetně vady, bude vyřízena bez zbytečných odkladů, a to nejpozději do 30 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 Autorita při příjmu žádosti o vydání Certifikátu zjistí, že existuje jiný Certifikát s duplicitním veřejným klíčem.

Další možné náhrady škody vycházejí z ustanovení příslušné právní úpravy a o jejich výši může rozhodnout soud.

9.10 Doba platnosti, ukončení platnosti

9.10.1 Doba platnosti

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

9.10.2 Ukončení platnosti

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

9.10.3 Důsledky ukončení a přetrvání závazků

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

9.11 Individuální upozorňování a komunikace se zúčastněnými subjekty

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

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

9.12 Novelizace

9.12.1 Postup při novelizaci

Postup je realizován řízeným procesem popsaným v interní dokumentaci.

9.12.2 Postup a periodicita oznamování

Vydání nové verze CP je vždy oznámeno formou zveřejňování informací.

9.12.3 Okolnosti, při kterých musí být změněn OID

OID politiky musí být změněn v případě, že se zásadně sníží záruky za důvěryhodnost Certifikátu s významným účinkem na akceptovatelnost tohoto Certifikátu v souladu s právní úpravou pro služby vytvářející důvěru.

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

9.13 Ustanovení o řešení sporů

V případě, že držitel Certifikátu nebo spoléhající se strana nesouhlasí s předloženým výkladem, mohou použít následující stupně odvolání:

- odpovědný pracovník RA,
- odpovědný pracovník I.CA (nutné elektronické nebo listinné podání),
- generální 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 Služby je provozován ve shodě s právními předpisy EU a České republiky a dále s relevantními mezinárodními standardy.

9.16 Různá ustanovení

9.16.1 Rámcová dohoda

Není relevantní pro tento dokument.

9.16.2 Postoupení práv

Není relevantní pro tento dokument.

9.16.3 Oddělitelnost ustanovení

Pokud soud, nebo veřejnoprávní orgán, v jehož jurisdikci jsou aktivity pokryté touto CP, stanoví, že provádění některého povinného požadavku je protiprávní, potom je rozsah tohoto požadavku omezen tak, aby požadavek byl platný a v souladu s platnou právní úpravou. I.CA o této skutečnosti informuje CA/Browser Forum.

9.16.4 Vymáhání (poplatky za právní zastoupení a zřeknutí se práv)

Není relevantní pro tento dokument.

9.16.5 Vyšší moc

Společnost První certifikační autorita, a.s., neodpovídá za porušení svých povinností vyplývajících ze smluvních vztahů s klientem vzniklých na základě zásahu vyšší moci, např. přírodních nebo lidskou činností způsobených katastrof velkého rozsahu, stávek či občanských nepokojů vždy spojených s vyhlášením nouzového stavu, nebo vyhlášení stavu ohrožení státu nebo válečného stavu, popř. výpadku komunikačního spojení.

9.17 Další ustanovení

Není relevantní pro tento dokument.

10 ZÁVĚREČNÁ USTANOVENÍ

Tato certifikační politika vydaná společností První certifikační autorita, a.s., nabývá platnosti a účinnosti dnem uvedeným v tab. 1.