První certifikační autorita, a.s.

CERTIFIKAČNÍ PROVÁDĚCÍ SMĚRNICE

VYDÁVÁNÍ KVALIFIKOVANÝCH CERTIFIKÁTŮ A/NEBO KVALIFIKOVANÝCH SYSTÉMOVÝCH CERTIFIKÁTŮ

Verze 3.4

Tabulka 1 - Identifikace

Název	Certifikační prováděcí směrnice vydávání kvalifikovaných certifikátů a/nebo kvalifikovaných systémových certifikátů
Společnost	První certifikační autorita, a.s.
Schválil	Ředitel společnosti První certifikační autorita, a.s.

Tabulka 1a – Vývoj dokumentu

Verze	Datum vydání	Shrnutí změn
3.0	23. 10. 2009	Vydávání certifikátů s parametry splňujícími požadavky platné legislativy na problematiku hashovacích funkcí (využívání algoritmů rodiny SHA-2) a minimální přípustné délky kryptografického klíče pro algoritmus RSA (2048 bitů)
3.1.	01.04.2011	v případě prvotního certifikátu akceptace elektronické poštovní adresy pouze v položce SubjectAlternativeName.rfc822Name, podporované položky key usage, extended key usage, vstupní kontroly, úprava textu
3.2	17.12.2012	aktualizace názvů interních směrnic
3.3	12.01.2015	aktualizace odkazovaných norem a standardů
3.4	22.09.2015	Aktualizace a revize dokumentu

Obsah

1 Úvod

Tento dokument byl vypracován na základě požadavků platné legislativy vztahující k problematice využívání kryptografických algoritmů v procesu vytváření elektronického podpisu. Společnost První certifikační autorita, a.s., vydává v souladu s doporučeními technické specifikace ETSI[1] TS 102 176-1 kvalifikované certifikáty s využitím hashovacích funkcí SHA-256 a SHA-512 v kombinaci s algoritmem RSA a délkou klíče 2048 bitů.

1.1 Přehled

Společnost **První certifikační autorita, a.s.,** (dále též I.CA) je od:

- 18. 03. 2002 prvním akreditovaným poskytovatelem certifikačních služeb v České republice pro oblast vydávání kvalifikovaných certifikátů podle zákona č. 227/2000 Sb., o elektronickém podpisu a o změně některých dalších zákonů (zákon o elektronickém podpisu),
- 01. 02. 2006 akreditovaným poskytovatelem certifikačních služeb v České republice pro oblast vydávání kvalifikovaných systémových certifikátů podle zákona č. 227/2000 Sb., o elektronickém podpisu a o změně některých dalších zákonů (zákon o elektronickém podpisu),
- 01. 02. 2006 prvním akreditovaným poskytovatelem certifikačních služeb v České republice pro oblast vydávání kvalifikovaných časových razítek podle zákona č. 227/2000 Sb., o elektronickém podpisu a o změně některých dalších zákonů (zákon o elektronickém podpisu)
- 21. 09. 2006 prvním zahraničním kvalifikovaným poskytovatelem certifikačních služeb ve Slovenské republice, kterému byla udělena akreditace v oblasti poskytování kvalifikovaných certifikátů a časových razítek podle aktuálního znění zákona č. 215/2002 Z.z., o elektronickom podpise a o zmene a doplnení niektorých zákonov v platnom znení a s ním spojených vykonávacích vyhlášok.

Dokument ***Certifikační prováděcí směrnice vydávání kvalifikovaných certifikátů a/nebo kvalifikovaných systémových certifikátů*** (**dále též CPS**), vypracovaný společností První certifikační autorita, a. s., se zabývá skutečnostmi, vztahujícími se k procesům životního cyklu kvalifikovaných certifikátů, a je v souladu:

- s dokumentem Směrnice 1999/93/ES Evropského parlamentu a Rady ze dne 13. prosince 1999 o zásadách Společenství pro elektronické podpisy,
- s aktuálním zněním zákona č. 227/2000 Sb., o elektronickém podpisu, a s ním souvisejících předpisů a vyhlášek,
- s aktuálním zněním zákona č. 215/2002 Z.z., o elektronickom podpise a s ním spojených vykonávacích vyhlášok

a striktně dodržuje strukturu, definovanou vyhláškou č. 378/2006 Sb., jejíž předlohou je osnova standardu RFC 3647 - Internet X.509 Public Key Infrastructure Certificate Policy and Certification Practices Framework, s přihlédnutím k doporučením orgánů EU a k právu České republiky a Slovenské republiky v dané oblasti (jednotlivé kapitoly jsou proto v tomto dokumentu zachovány i v případě, že jsou ve vztahu k ní irelevantní).

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

V procesu poskytování certifikačních služeb v oblasti vydávání kvalifikovaných certifikátů a kvalifikovaných systémových certifikátů provozuje společnost První certifikační autorita, a.s., jednoúrovňovou certifikační autoritu (kořenová certifikační autorita), která vydala tzv. „self-signed“ kořenový certifikát I.CA, jehož správa je ve společnosti První certifikační autorita, a.s., řízena speciálními dokumenty.

[1] European Telecommunications Standards Institute

1.2 Název a identifikace dokumentu

Název tohoto dokumentu: Certifikační prováděcí směrnice vydávání kvalifikovaných certifikátů a/nebo kvalifikovaných systémových certifikátů, verze 3.4
OID dokumentu: není přiřazeno

Tato CPS se vztahuje k následujícím CP:

OID	CP
1.3.6.1.4.1.23624.1.1.30.3.1	Certifikační politika vydávání kvalifikovaných certifikátů
1.3.6.1.4.1.23624.1.1.40.3.1	Certifikační politika vydávání kvalifikovaných systémových certifikátů
1.3.6.1.4.1.23624.1.1.202.1.2	Certifikační politika vydávání kvalifikovaných mandátních certifikátů
1.3.6.1.4.1.23624.1.1.203.1.0	Certifikační politika vydávání kvalifikovaných systémových certifikátů SK

1.3 Participující subjekty

1.3.1 Certifikační autority (dále „CA“)

Společnost První certifikační autorita, a.s., nezřizuje ani nepodporuje podřízené certifikační autority poskytující kvalifikované certifikační služby.

1.3.2 Registrační autority (dále „RA“)

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

- přijímají žádosti o služby uvedené v této CPS, zejména přijímají žádosti o certifikáty, zprostředkovávají předání certifikátů a seznamů zneplatněných certifikátů, poskytují potřebné informace, vyřizují reklamace atd.,
- jsou oprávněny z naléhavých provozních nebo technických důvodů pozastavit zcela nebo zčásti výkon své činnosti - toto opatření jsou povinny neprodleně hlásit řediteli I.CA, který je potvrdí, zruší nebo změní,
- jsou zmocněny jménem I.CA uzavírat smlouvy o poskytování kvalifikované certifikační služby,
- zajišťují zpoplatňování služeb I.CA, pokud není stanoveno smlouvou jinak,
- v případě smluvní RA plní jménem I.CA obdobné funkce jako vlastní RA na základě písemné smlouvy mezi I.CA a provozovatelem RA.

Výše uvedené typy registračních autorit mohou být stacionární nebo mobilní.

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

Držitelem certifikátu je fyzická osoba, právnická osoba nebo organizační složka státu, která požádala o vydání certifikátu pro sebe nebo pro podepisující/označující osobu a které byl certifikát vydán.

Podepisující osobou je fyzická osoba, která je držitelem prostředku pro vytváření elektronických podpisů a jedná jménem svým nebo jménem jiné fyzické či právnické osoby

Označující osobou je fyzická osoba, právnická osoba nebo organizační složka státu, která drží prostředek pro vytváření elektronických značek a označuje datovou zprávu elektronickou značkou. Elektronická značka může výt vytvářena zařízením, zastupujícím výše uvedené osoby (např. automatické odpovědi e-podatelny na došlé e-maily).

1.3.4 Spoléhající se strany

Spoléhající se stranou jsou subjekty, spoléhající se při své činnosti na kvalifikovaný certifikát nebo kvalifikovaný systémový certifikát vydaný společností První certifikační autorita, a.s.

1.3.5 Jiné participující subjekty

Jinými participujícími subjekty jsou orgány dozoru dle ZoEP, orgány činné v trestním řízení a další, kterým to ze zákona přísluší.

1.4 Použití certifikátu

1.4.1 Přípustné použití certifikátu

Kvalifikované certifikáty a kvalifikované systémové certifikáty, vydávané I.CA lze využívat pouze v procesech ověřování elektronického podpisu/značky v souladu s platnou legislativou (ZoEP, VoEP).

1.4.2 Omezení použití certifikátu

Kvalifikované certifikáty a kvalifikované systémové certifikáty nesmí být využívány v rozporu s vydávaným účelem, definovaným relevantní certifikační politikou (dále CP) a platnou legislativou (ZoEP, VoEP a dalšími právními předpisy).

1.5 Správa politiky

1.5.1 Organizace spravující certifikační politiku nebo certifikační prováděcí směrnici

Tuto CPS spravuje společnost První certifikační autorita, a.s.

1.5.2 Kontaktní osoba organizace spravující certifikační politiku nebo certifikační prováděcí směrnici

Ředitel společnosti První certifikační autorita, a.s. určuje osobu, jejíž kontaktní údaje jsou uvedeny na internetové adrese.

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

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

1.5.4 Postupy při schvalování souladu s bodem 1.5.3

V případě, že je potřebné provést změny a tedy i vytvořit novou verzi této CPS, určuje ředitel společnosti První certifikační autorita, a.s. osobu, která je oprávněna tyto změny provádět. Nabytí platnosti nové verze CPS předchází její schválení ředitelem společnosti První certifikační autorita, a.s. Proces změny je popsán v interní dokumentaci „***Změnové řízení***“.

1.6 Přehled použitých pojmů a zkratek

Dále uvedený přehled pojmů a zkratky je platný pro tento dokument. V případě pojmu může být na pravé straně v závorkách uveden zdroj, v němž se nachází původní pojem včetně definice. Použité zkratky mají alternativní charakter, tzn. v textu může být použita jak plný text, tak i jeho zkratka, přičemž obojí má totožnou obsahovou hodnotu.

Tabulka 3 – Pojmy a zkratky

Pojem	Vysvětlení
bit	z anglického *binary digit* - dvojková číslice je základní a současně nejmenší jednotkou informace, používanou především v číslicové a výpočetní technice
CRL (Certificate Revocation List)	seznam zneplatněných certifikátů obsahující certifikáty, které již nelze pokládat za platné
držitel certifikátu	fyzická osoba, právnická osoba nebo organizační složka státu, která požádala o vydání certifikátu pro sebe nebo pro podepisující osobu a které byl certifikát vydán
elektronický podpis, resp. elektronická značka	údaje, resp. informace, které splňují požadavky platné legislativy[2]
hash (otisk, fingerprint, …)	transformace, která jako vstup přijímá řetězec znaků o libovolné délce a výsledkem je řetězec znaků s pevnou délkou
I.CA	První certifikační autorita, a.s.
kvalifikovaný certifikát, kvalifikovaný systémový certifikát	certifikát, který má náležitosti podle platné legislativy
následný certifikát	• certifikát, který byl v souladu se smlouvou o poskytování kvalifikované certifikační služby, uzavřenou mezi žadatelem a I.CA, vydán žadateli na základě nové žádosti o kvalifikovaný certifikát (struktura PKCS#10) v období platnosti kvalifikovaného certifikátu, ke kterému je vydáván tento následný kvalifikovaný certifikát**, nebo** • certifikát, který byl v souladu se smlouvou o poskytování kvalifikované certifikační služby, uzavřenou mezi žadatelem a I.CA, vydán žadateli na základě nové žádosti o kvalifikovaný systémový certifikát (struktura PKCS#10) v období platnosti kvalifikovaného systémovému certifikátu, ke kterému je vydáván tento následný kvalifikovaný systémový certifikát
označující osoba	fyzická osoba, právnická osoba nebo organizační složka státu, která drží prostředek pro vytváření elektronických značek a označuje datovou zprávu elektronickou značkou
párová data (dvojice soukromý a veřejný klíč)	jedinečná data pro vytváření elektronického podpisu/značky spolu s odpovídajícími daty pro ověřování elektronického podpisu/značky
podepisující osoba	fyzická osoba, která je držitelem prostředku pro vytváření elektronických podpisů a jedná jménem svým nebo jménem jiné fyzické či právnické osoby
RA	registrační autorita Certifikační autority I.CA – souhrnný název pro vlastní stacionární registrační autoritu (VSRA), vlastní mobilní registrační autoritu (VMRA), smluvní registrační autoritu (SRA)
smluvní partner	poskytovatel certifikačních služeb, který zajišťuje na základě písemné smlouvy pro I.CA certifikační služby nebo jejich části - nejčastěji se jedná o smluvní RA
soukromý klíč	jedinečná data pro vytváření elektronického podpisu/ značky
spoléhající se strana	subjekt, spoléhající se při své činnosti na certifikát, vydaný I.CA
veřejný klíč	jedinečná data pro ověřování elektronického podpisu/ značky
TWINS	dvojice současně vydávaného kvalifikovaného a „nekvalifikovaného“

[2] Viz ZoEP

	certifikátu
VoEP	• vyhláška č. 378/2006 Sb., o postupech kvalifikovaných poskytovatelů certifikačních služeb, o požadavcích na nástroje elektronického podpisu a o požadavcích na ochranu dat pro vytváření elektronických značek (vyhláška o postupech kvalifikovaných poskytovatelů certifikačních služeb) • sada vyhlášek Slovenské republiky, vztahujících se k problematice aktuálního znění zákona Slovenské republiky č. 215/2002 Z.z., o elektronickom podpise a o zmene a doplnení niektorých zákonov
zablokování	• stav, ve kterém se certifikát nachází od doby, kdy jej I.CA zneplatnila, do doby, kdy I.CA zveřejnila CRL, ve kterém je tento certifikát poprvé zařazen
zaručený elektronický podpis	elektronický podpis splňující požadavky české, resp. slovenské legislativy
ZoEP	• aktuální znění zákona č. 227/2000 Sb., o elektronickém podpisu a o změně některých dalších zákonů (zákon o elektronickém podpisu) • aktuální znění zákona Slovenské republiky č. 215/2002 Z.z., o elektronickom podpise a o zmene a doplnení niektorých zákonov

2 Odpovědnosti za zveřejňování, úložiště informací a dokumentace

2.1 Úložiště informací a dokumentace

Společnost První certifikační autorita, a.s. s ohledem na požadavky ZoEP zřizuje a provozuje úložiště informací a dokumentace, za která taktéž, jako poskytovatel certifikačních služeb odpovídá.

2.2 Zveřejňování informací a dokumentace

Základní adresy (dále též informační adresy), na nichž lze nalézt veřejné informace o společnosti První certifikační autorita, a.s., (certifikační politiky, zprávy pro uživatele, další informace dle ZoEP a VoEP, ostatní veřejné a aktuální informace a dokumenty atd.), případně odkazy pro zjištění dalších informací, jsou:

a) adresa sídla společnosti:

První certifikační autorita, a.s.
Podvinný mlýn 2178/6
190 00 Praha 9
Česká republika

b) internetová adresa http://www.ica.cz

c) sídla registračních autorit

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

a) sídlo registrační autority, která smluvní vztah s I.CA zprostředkovala

b) elektronická poštovní adresa info@ica.cz

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

Na výše uvedené internetové adrese lze získat informace o:

- veřejných certifikátech - přímo se zveřejňují následující informace (ostatní informace lze získat z certifikátu):
  - číslo certifikátu,
  - obsah položky Obecné jméno (Common Name),
  - 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).

Povoleným protokolem pro přístup k veřejným informacím jsou HTTP, HTTPS, FTP. Jiné protokoly nejsou povoleny. I.CA může bez udání důvodu přístup prostřednictvím některých z uvedených protokolů zrušit nebo pozastavit, přitom je povinna dodržet příslušná ustanovení ZoEP a VoEP. Tyto změny je I.CA povinna zveřejnit prostřednictvím svých informačních adres. Podrobnější informace o možnostech a příslušných parametrech uvedených protokolů I.CA zveřejňuje tamtéž.

V případech odejmutí akreditace nebo vzniku důvodné obavy ze zneužití dat pro vytváření elektronických značek, resp. elektronických podpisů vydávaných certifikátů nebo seznamů zneplatněných certifikátů, oznámí I.CA tuto skutečnost na své internetové informační adrese a prostřednictvím celostátně distribuovaného deníku Hospodářské noviny nebo Mladá fronta Dnes.

2.3 Periodicita zveřejňování informací

I.CA zveřejňuje informace s následující periodicitou:

- certifikační politika - před prvním vydáním certifikátu podle dané politiky,
- seznam vydaných certifikátů – aktualizace při každém vydání nového certifikátu určeného ke zveřejnění,
- seznam zneplatněných certifikátů (CRL) - maximálně za 24 hodin od vydání předchozího CRL (zpravidla à 8 hodin),
- informace požadované ZoEP, VoEP (zejména získání nebo odejmutí akreditace, zneplatnění kořenového certifikátu I.CA s uvedením důvodu zneplatnění) – bezodkladně,
- ostatní veřejné informace – není předem určeno, obecně však platí, že tyto informace musí reflektovat aktuální stav poskytovaných kvalifikovaných 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 pracovníkům I.CA, smluvním partnerům nebo subjektům, definovaným platnou legislativou. Přístup k těmto informacím je řízen pravidly, uvedenými v interní dokumentaci, zejména:

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

3 Identifikace a autentizace

3.1 Pojmenovávání

3.1.1 Typy jmen

Veškerá jména jsou konstruována v souladu se standardem X.501, resp. s navazujícím standardem X.520.

3.1.2 Požadavek na významovost jmen

Platí, že u vydávaných certifikátů musí jména vyjadřovat účel, ke kterému je certifikát vydáván. Konkrétní obsah jmen je definován v konkrétní CP.

3.1.3 Anonymita a používání pseudonymu

Viz kapitola 3.1.3 konkrétní CP.

3.1.4 Pravidla pro interpretaci různých forem jmen

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

3.1.5 Jedinečnost jmen

Jednoznačnost jména subjektu je zaručena použitím položky Subject.SerialNumber. V případech, kdy hodnotu SerialNumber určuje I.CA, je jednoznačnost zaručena. V případech, kdy hodnotu SerialNumber určuje žadatel a dojde ke kolizi s již zavedeným jednoznačným jménem jiného kvalifikovaného certifikátu/ kvalifikovaného systémového certifikátu, I.CA upozorní žadatele a požádá ho, aby některý z požadovaných údajů změnil či doplnil. Pokud žadatel toto neučiní, kvalifikovaný certifikát/ kvalifikovaný systémový certifikátu se mu nevydá.

3.1.6 Obchodní značky

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

3.2 Počáteční ověření identity

Postup ověřování identity je uveden v interní dokumentaci ***„Směrnice pro pracovníky RA I.CA“.***

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

Vlastnictví dat pro vytváření elektronických podpisů/ značek, odpovídajících datům pro ověřování elektronických podpisů/značek, která daná žádost o certifikát (struktura PKCS#10) obsahuje a která budou obsažena ve vydaném certifikátu, se prokazuje předložením této žádosti ověřujícímu subjektu, kterým může být pracovník registrační nebo certifikační autority. S ohledem na skutečnost, že tato žádost je elektronicky podepsána/označena daty pro vytváření elektronických podpisů/značek (tzv. soukromý klíč), odpovídajících datům pro ověřování elektronických podpisů/značek (tzv. veřejný klíč) obsažených v žádosti, dokazuje tímto způsobem žadatel o certifikát, že v době tvorby elektronického podpisu/značky vlastnil soukromý klíč, odpovídající veřejnému klíči, který je v žádosti uveden.

3.2.2 Ověřování identity právnické osoby nebo organizační složky státu

I.CA vyžaduje originál nebo úředně ověřenou kopii výpisu z obchodního, nebo jiného zákonem určeného rejstříku/registru, živnostenského listu, zřizovací listiny, resp. jiného dokladu stejné právní váhy a který/která musí obsahovat úplné obchodní jméno, identifikační číslo (je-li přiřazeno), adresu sídla, jména osoby/osob, oprávněné/oprávněných k zastupování (statutárních zástupců) a způsob, jakým za právnickou osobu jednají a podepisují.

3.2.3 Ověřování identity fyzické osoby

V procesu ověřování identity jsou vyžadovány dva doklady, obsahující následující údaje.

Primárním osobním dokladem pro občany ČR musí být občanský průkaz. Primárním osobním dokladem pro cizince je platný cestovní pas, popř. obdobný doklad stejné právní váhy. Z tohoto dokladu jsou ověřovány následující údaje:

- celé občanské jméno,
- datum narození (nebo rodné číslo u občanů České republiky, resp. Slovenské republiky),
- číslo předloženého primárního osobního dokladu,
- adresa trvalého bydliště (je-li v primárním dokladu uvedena).

Sekundární osobní doklad musí být vydán orgánem veřejné moci nebo jinou organizací, jejíž existenci lze doložit, a musí obsahovat celé občanské jméno fyzické osoby vyřizující žádost a dále nejméně jeden z následujících údajů:

- datum narození žadatele (nebo rodné číslo u občanů ČR),
- adresu trvalého bydliště žadatele,
- fotografii obličeje žadatele.

Údaje požadované v sekundárním osobním dokladu musí být shodné s těmito údaji v primárním osobním dokladu.

Blíže je postup popsán v interním dokumentu:

- ***„Směrnice pro pracovníky RA I.CA“.***

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

Všechny informace musí být řádným způsobem ověřeny.

3.2.5 Ověřování specifických práv

Tyto skutečnosti jsou pro aplikaci vydání tohoto dokumentu irelevantní.

3.2.6 Kritéria pro interoperabilitu

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

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

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

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

3.3.1.1 Certifikáty poskytovatele (I.CA)

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

3.3.1.2 Certifikáty koncových uživatelů

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

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

3.3.2 Identifikace a autentizace při výměně párových dat po zneplatnění certifikátu

I.CA nepodporuje výměnu párových dat již zneplatněného certifikátu. Jediný způsob, jak získat nový certifikát, je získání prvotního certifikátu.

3.4 Identifikace a autentizace při zpracování požadavků na zneplatnění certifikátu

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

4 Požadavky na životní cyklus certifikátu

V souladu s legislativou, odkazující se na doporučení technické specifikace ETSI TS 119 312 Electronic Signatures and Infrastructures (ESI); Cryptographic Suites, je v procesu vydávání kvalifikovaných certifikátů a kvalifikovaných systémových certifikátů využíván algoritmus RSA s SHA-256 (sha256RSA) a délka kryptografického klíče pro algoritmus RSA 2048 bitů.

4.1 Žádost o vydání certifikátu

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

4.1.1.1 Odpovědnost žadatele

Žadatel je povinen zejména:

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

4.1.1.2 Odpovědnost poskytovatele

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

4.2 Zpracování žádosti o certifikát

Proces zpracování žádosti o certifikát je popsaný v interní dokumentaci:

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

4.2.1 Identifikace a autentizace

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

4.2.2 Přijetí nebo odmítnutí žádosti o certifikát

V případě, že je výsledek kontrol procesu žádání o **prvotní certifikát** pozitivní, pracovník RA okopíruje předložené osobní doklady (není-li smluvně stanoveno jinak). Dokument „Protokol o podání žádosti na vydání kvalifikovaného certifikátu I.CA“, jehož součástí je věta „**Žadatel souhlasí s tím, aby společnost První certifikační autorita, a.s. skladovala pořízené kopie jeho osobních dokladů v souladu s platnou legislativou.**“ nechá žadateli o certifikát, popř. zmocněnci, podepsat. Pokud žadatel o certifikát, popř. zmocněnec odmítne tento protokol podepsat, je pracovník RA povinen proces vydávání certifikátu ukončit a kopie osobních dokladů zničit – skartovat (není-li smluvně stanoveno jinak).

V případě vyřizování žádosti o **následný certifikát** elektronickou cestou je postupováno v souladu s ustanoveními kapitoly 4.7.3.

4.2.3 Doba zpracování žádosti o certifikát

I.CA nestanovuje pevný časový limit, ve kterém dojde ke zpracování žádosti o certifikát, neboť se jedná o časový sled následujících činností, z nichž některé záleží pouze na žadateli o certifikát. Časové údaje jsou uvedeny v následujícím seznamu:

- generování žádosti o vydání certifikátu – jednotky minut,

- vydání certifikátu (pracovní dny, není-li smluvně uvedeno jinak):
  - prvotní certifikát (žadatel se MUSÍ osobně dostavit na RA) - doba vydání certifikátu je do 15 minut a jen ve výjimečných případech může být tato doba delší,
  - následný certifikát (žadatel se NEMUSÍ osobně dostavit na RA) - jednotky minut (předpokladem je předchozí zaplacení příslušného poplatku).

4.3 Vydání certifikátu

4.3.1 Úkony CA v průběhu vydání certifikátu

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

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

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

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

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

Uvedené postupy jsou detailně popsány v interní dokumentaci:

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

4.4 Převzetí vydaného certifikátu

Proces převzetí vydaného certifikátu je detailně popsán v interní dokumentaci:

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

4.4.1 Úkony spojené s převzetím certifikátu

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

Proces je detailně popsán v interní dokumentaci:

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

4.4.2 Zveřejňování vydaných certifikátů poskytovatelem

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

Veřejné certifikáty koncových uživatelů jsou zveřejněny způsobem podle bodu 2.2.

4.4.3 Oznámení o vydání certifikátu jiným subjektům

V případech vydání prvotního certifikátu, popř. následného certifikátu při dostavení se žadatele/zmocnitele na RA, získá oznámení o vydaném certifikátu pracovník RA. Dále platí ustanovení kapitoly 4.4.2 a požadavky platné legislativy, na jejímž základě získala I.CA akreditaci.

4.5 Použití párových dat a certifikátu

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

Povinností podepisující nebo označující osoby mj. je:

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

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

Spoléhající se strany jsou zejména povinny:

- provádět veškeré úkony potřebné k tomu, aby si ověřily, že elektronický podpis/značka je platný a odpovídající certifikát nebyl zneplatněn,
- dodržovat veškerá ustanovení relevantní CP, v souladu s kterou byl využívaný certifikát vydán,
- při činnostech, souvisejících s používáním vydaného certifikátu, dodržovat veškerá relevantní ustanovení ZoEP, VoEP a relevantní CP.

4.6 Obnovení certifikátu

Službou obnovení certifikátu je v kontextu tohoto dokumentu myšleno obnovení již zneplatněného certifikátu a/nebo vydání následného certifikátu se stejnými daty pro ověřování elektronických podpisů/značek a novou dobou platnosti. Je nutné vydat nový certifikát s novým veřejným klíčem. Platí stejné požadavky jako v případě počátečního ověření identity.

4.6.1 Podmínky pro obnovení certifikátu

Služba obnovení již zneplatněného certifikátu není poskytována.

4.6.2 Subjekty oprávněné požadovat obnovení certifikátu

Služba obnovení již zneplatněného certifikátu není poskytována.

4.6.3 Zpracování požadavku na obnovení certifikátu

Služba obnovení již zneplatněného certifikátu není poskytována.

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

Služba obnovení již zneplatněného certifikátu není poskytována.

4.6.5 Úkony spojené s převzetím obnoveného certifikátu

Služba obnovení již zneplatněného certifikátu není poskytována.

4.6.6 Zveřejnění vydaných obnovených certifikátů poskytovatelem

Služba obnovení již zneplatněného certifikátu není poskytována.

4.6.7 Oznámení o vydání obnoveného certifikátu ostatním subjektům

Služba obnovení již zneplatněného certifikátu není poskytována.

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

V případě, že certifikát obsahuje elektronickou adresu, je před vypršením platnosti tohoto certifikátu informace o této skutečnosti spolu s návodem jak postupovat na uvedenou adresu zaslána.

Procesy výměny dat pro ověřování elektronických podpisů, resp. elektronických značek, uvedené v následujících podkapitolách, jsou popsány v interní dokumentaci:

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

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

Podmínky pro výměnu dat pro ověřování elektronických podpisů jsou uvedeny v kapitole 3.3.1. I.CA si vyhrazuje právo akceptování i jiných forem postupů.

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

Výměnu dat pro ověřování elektronických podpisů/značek jsou oprávněni požadovat držitelé certifikátu.

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

Pokud je ověření elektronických podpisů pozitivní a obsah položek žádosti o výměnu dat pro ověřování elektronických podpisů/značek v certifikátu splňuje požadavky uvedené v kapitole 3.3.1, je postupováno v souladu s kapitolou 4.3.1, v opačném případě je řízení k vydání certifikátu ukončeno.

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

Viz relevantní části kapitoly 4.3.2.

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

Viz relevantní části kapitoly 4.4.1.

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

Viz kapitola 4.4.2.

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

Viz kapitola 4.4.3.

4.8 Změna údajů v certifikátu

4.8.1 Podmínky pro změnu údajů v certifikátu

QC: viz kapitola 4.7.1.

QSC: služba není poskytována.

4.8.2 Subjekty oprávněné požadovat změnu údajů v certifikátu

QC: viz kapitola 4.7.2.

QSC: služba není poskytována.

4.8.3 Zpracování požadavku na změnu údajů v certifikátu

QC: viz kapitola 4.7.3.

QSC: služba není poskytována.

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

QC: viz kapitola 4.3.2.

QSC: služba není poskytována.

4.8.5 Úkony spojené s převzetím certifikátu se změněnými údaji

QC: viz kapitola 4.4.1.

QSC: služba není poskytována.

4.8.6 Zveřejnění vydaných certifikátů se změněnými údaji

QC: viz kapitola 4.4.2.

QSC: služba není poskytována.

4.8.7 Oznámení o vydání certifikátu se změněnými údaji jiným subjektům

QC: viz kapitola 4.4.3.

QSC: služba není poskytována.

4.9 Zneplatnění a pozastavení platnosti certifikátu

Žádosti o zneplatnění certifikátu přijímá I.CA nepřetržitě pouze prostřednictvím předání žádosti elektronickou cestou a listovní zásilkou. Osobní předání na RA je možné pouze v pracovní době příslušné RA. Postupy v této kapitole jsou rozpracovány v interní dokumentaci. Zneplatnění certifikátu provede I.CA taktéž na základě podnětu subjektů oprávněných ze zákona.

Službu pozastavení platnosti certifikátu I.CA neposkytuje.

4.9.1 Podmínky pro zneplatnění certifikátu

Certifikát může být zneplatněn na základě následujících okolností:

- dojde ke kompromitaci, resp. existuje důvodné podezření, že došlo ke kompromitaci dat pro vytváření elektronických podpisů/značky,
- porušení ustanovení smlouvy o poskytování kvalifikované certifikační služby ze strany držitele certifikátu, resp. podepisující/označující osoby.
- žádost držitele nebo podepisující/označující osoby.
- nastanou-li skutečnosti uvedené v ZoEP a VoEP (např. neplatnost údajů v certifikátů).

I.CA si vyhrazuje právo akceptování i jiných okolností podmínek na zneplatnění certifikátu, které však nesmí být v rozporu s ZoEP, VoEP.

4.9.2 Subjekty oprávněné žádat o zneplatnění certifikátu

Žádost o zneplatnění mohou podat:

- podepisující/označující osoba, držitel certifikátu nebo subjekt, který k tomu byl explicitně určen ve smlouvě o poskytování kvalifikované certifikační služby v oblasti vydávání certifikátů (např. při vydávání certifikátu pro zaměstnance),
- osoba oprávněná z pozůstalostního řízení,
- poskytovatel certifikačních služeb - oprávněným žadatelem o zneplatnění certifikátu vydaného I.CA je v tomto případě ředitel I.CA,
- další subjekty, definované ZoEP, VoEP .

4.9.3 Požadavek na zneplatnění certifikátu

V případě **osobního předání žádosti o zneplatnění certifikátu na RA** musí žádost obsahovat sériové číslo certifikátu buď v dekadickém tvaru nebo hexadecimální (uvozeno řetězcem „0x“), celé občanské jméno fyzické osoby, které byl certifikát vydán a heslo pro zneplatnění. Pokud si tato osoba heslo pro zneplatnění nepamatuje, musí tuto skutečnost do písemné žádosti explicitně uvést, včetně čísla primárního osobního dokladu předloženého při žádosti o vydání certifikátu. Tímto primárním osobním dokladem se musí pracovníkovi RA prokázat. Pracovník RA předá výše uvedenou žádost (dálkovým přístupem) na provozní pracoviště certifikační autority. Odpovědný pracovník CA rozhodne, zda je žádost oprávněná a rozhodnutí sdělí prostřednictvím pracovníka RA. V případě, že je žádost oprávněná, je okamžik přijetí této žádosti na provozní pracoviště certifikační autority zároveň datem a časem zneplatnění tohoto certifikátu. V případě, že žádost nelze akceptovat (špatné heslo pro zneplatnění, neprokazatelná identita fyzické osoby), pokusí se pracovník RA v součinnosti s touto fyzickou osobou tyto skutečnosti napravit a pokud to z libovolného důvodu nebude možné, žádost o zneplatnění certifikátu bude zamítnuta. Pro zmocněnce platí ustanovení podkapitol 3.2.3.

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

- Elektronicky podepsaná/označená elektronická zpráva - tělo zprávy musí být následujícího tvaru (v českém nebo slovenském jazyce, s diakritikou nebo bez diakritiky):

  Zadam o zneplatneni certifikatu cislo = xxxxxxx

  nebo

  Žádám o zneplatnění certifikátu číslo = xxxxxxx

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

- Elektronicky nepodepsaná/neoznačená elektronická zpráva - tělo zprávy musí být následujícího tvaru (v českém nebo slovenském jazyce, s diakritikou nebo bez diakritiky):

  Zadam o zneplatneni certifikatu cislo = xxxxxxx

  Heslo pro zneplatneni = yyyyyy

  nebo

  Žádám o zneplatnění certifikátu číslo = xxxxxxx

  Heslo pro zneplatnění = yyyyyy

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

  Pokud žádost splňuje výše uvedené požadavky, odpovědný pracovník provozního pracoviště certifikační autority neprodleně certifikát zneplatní. Datum a čas zneplatnění je určen okamžikem přijetí platné žádosti o zneplatnění certifikátu serverem I.CA. V případě, že žádost nesplňuje uvedené požadavky, je zamítnuta a žadatel je elektronickou cestou (v případě vyplnění elektronické poštovní adresy) o této skutečnosti informován. O kladném vyřízení není žadatel explicitně informován a tuto skutečnost zjistí v nejbližším vydaném seznamu zneplatněných certifikátů.

- Prostřednictvím formuláře na k tomuto účelu vyhrazené internetové informační adrese http://www.ica.cz/

Datum a čas zneplatnění certifikátu ve třech výše uvedených možnostech je určen okamžikem přijetí platné žádosti o zneplatnění certifikátu serverem I.CA. V případě, že žádost nesplňuje požadavky, je zamítnuta a žadatel je elektronickou cestou o této skutečnosti informován. O kladném vyřízení není žadatel explicitně informován a tuto skutečnost zjistí v nejbližším vydaném seznamu zneplatněných certifikátů

V případě **použití listovní zásilky o zneplatnění certifikátu** musí být v zásilce musí být uvedena žádost v následujícím tvaru (v českém nebo slovenském jazyce):

Žádám o zneplatnění certifikátu číslo = xxxxxxx

Heslo pro zneplatnění = yyyyyy

kde „xxxxxxx" je sériové číslo certifikátu a „yyyyyy" je heslo pro zneplatnění.

Sériové číslo je buď v dekadickém tvaru nebo hexadecimální (uvozeno řetězcem „0x"). Pokud si žadatel heslo pro zneplatnění nepamatuje, musí tuto skutečnost do písemné žádosti explicitně uvést, včetně čísla primárního osobního dokladu předloženého při žádosti o vydání certifikátu a žádost vlastnoručně podepsat. V případě, je že žádost o zneplatnění certifikátu oprávněná, je okamžik přijetí doporučené listovní zásilky na I.CA zároveň datem a časem zneplatnění tohoto certifikátu. O vyřízení žádosti je žadatel informován doporučeným dopisem na poštovní adresu uvedenou jako adresa odesilatele.

4.9.4 Doba odkladu požadavku na zneplatnění certifikátu

Služba není poskytována.

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

Reakcí I.CA na přijetí platné žádosti o zneplatnění certifikátu je jeho neprodlené zneplatnění. Do doby zveřejnění seznamu zneplatněných certifikátů je dotyčný certifikát zablokován[3]. Maximální prodlení mezi zneplatněním certifikátu a zveřejněním seznamu zneplatněných certifikátů, na kterém je tento certifikát poprvé uveden, je nejvýše 24 hodin. Postupy jsou uvedeny v interní dokumentaci ***„Operátor CA"***.

Odblokování certifikátu, který byl zablokován na základě platné žádosti o jeho zneplatnění, I.CA nepovoluje.

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

Spoléhající se strany jsou povinny provádět veškeré úkony potřebné k tomu, aby si ověřily, že elektronické podpisy/značky jsou platné a jim odpovídající certifikáty nebyly zneplatněny. Pro tyto účely jsou spoléhající se strany povinny používat CRL, vydaná a elektronicky označená, resp. podepsaná I.CA. Déle platí ustanovení kapitoly 4.5.2.

4.9.7 Periodicita vydávání seznamu zneplatněných certifikátů

Seznam zneplatněných certifikátů je společností První certifikační autorita, a.s. vydáván v pravidelných intervalech, minimálně jedenkrát za 24 hodin (zpravidla à 8 hodin), v případě nutnosti bezodkladně.

[3] Stav, ve kterém se certifikát nachází od doby, kdy jej I.CA zneplatnila, do doby, kdy I.CA zveřejnila CRL, ve kterém je tento certifikát poprvé zařazen.

Činnosti operátorů CA v procesu vytváření a vydávání CRL jsou popsané v interní dokumentaci ***„Operátor CA“***.

4.9.8 Maximální zpoždění při vydávání seznamu zneplatněných certifikátů

V procesu vydávání CRL je s ohledem na platnou legislativu vždy dodrženo ustanovení kapitoly 4.9.5.

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

Služba může být poskytována smluvním partnerům za specifických podmínek.

4.9.10 Požadavky při ověřování statutu certifikátu na on-line

Viz kapitola 4.9.9.

4.9.11 Jiné způsoby oznamování zneplatnění certifikátu

Služba není poskytována.

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

Služba není poskytována.

4.9.13 Podmínky pro pozastavení platnosti certifikátu

Služba není poskytována.

4.9.14 Subjekty oprávněné požadovat pozastavení platnosti certifikátu

Služba není poskytována.

4.9.15 Zpracování požadavku na pozastavení platnosti certifikátu

Služba není poskytována.

4.9.16 Omezení doby pozastavení platnosti certifikátu

Služba není poskytována.

4.10 Služby související s ověřováním statutu certifikátu

4.10.1 Funkční charakteristiky

Seznamy veřejných certifikátů jsou poskytovány formou zveřejňování informací, seznamy zneplatněných certifikátů jsou poskytovány jak formou zveřejňování informací, tak uvedením distribučních míst CRL ve vydaném certifikátu.

4.10.2 Dostupnost služeb

Služba poskytování veřejných certifikátů formou zveřejňování informací je dostupná 7 dní v týdnu 24 hodin denně.

I.CA garantuje zajištění nepřetržité dostupnosti (7dní v týdnu 24 hodin denně) a integrity seznamu zneplatněných certifikátů (platné CRL).

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

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

4.10.3 Další charakteristiky služeb statutu certifikátu

Další charakteristiky služeb statutu certifikátu nejsou poskytovány. I.CA může bez udání důvodu poskytování charakteristik služeb statutu certifikátu rozšířit, přitom je povinna dodržet příslušná ustanovení ZoEP a VoEP.

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

I.CA ukončí poskytování služeb držiteli certifikátu, resp. podepisující/označující osobě ve chvíli, kdy:

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

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

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

Služba není poskytována.

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

Služba není poskytována.

5 Management, provozní a fyzická bezpečnost

Management bezpečnosti poskytovaných kvalifikovaných certifikačních služeb v oblasti vydávání certifikátů je zaměřen především na:

- systémy, které vydávají a elektronicky označují, resp. podepisují certifikáty a seznamy zneplatněných certifikátů,
- veškeré procesy poskytování certifikačních služeb v oblasti vydávaní certifikátů dle ZoEP a VoEP.

Implementovaná bezpečnostní opatření v oblasti fyzické a provozní bezpečnosti jsou rozpracovány v interních bezpečnostních normách a směrnicích, které jsou v uvedeny následujících podkapitolách.

5.1 Fyzická bezpečnost

Problematika fyzické bezpečnosti je uvedena v interní dokumentaci, zejména:

- ***„Řízení fyzického přístupu do místností I.CA“,***
- ***„Požární bezpečnost“,***
- ***„Bezpečnostní incidenty“,***
- ***„Obnova komponenty provozního pracoviště“,***
- ***„Přemístění provozního pracoviště“,***
- ***„Kamerový systém – provozní pracoviště“.***

5.1.1 Umístění a konstrukce

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

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

5.1.2 Fyzický přístup

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

5.1.3 Elektřina a klimatizace

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

5.1.4 Vliv vody

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

5.1.5 Protipožární 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 umístěna zařízení, určená k výkonu hlavních certifikačních služeb, jsou opatřeny protipožární vložkou. V samotných prostorách se nachází hasicí přístroj.

5.1.6 Ukládání médií

Paměťová média, obsahující provozní zálohy a záznamy v elektronické podobě, jsou ukládána v kovových skříních, popř. trezorech. Kopie jsou ukládány v jiné geografické lokalitě, než kde je umístěno provozní pracoviště. Papírová média, která je nutno, mj. podle platné legislativy týkající se elektronického podpisu, archivovat, jsou skladována v jiné geografické lokalitě, než je umístěno provozní pracoviště.

5.1.7 Nakládání s odpady

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

5.1.8 Zálohy mimo budovu provozního pracoviště

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

5.2 Procesní bezpečnost

5.2.1 Důvěryhodné role

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

Problematikou se zabývají interní dokumenty, zejména:

- ***„Systémová bezpečnostní politika CA“,***
- ***„Příručka administrátora“.***

5.2.2 Počet osob požadovaných na zajištění jednotlivých činností

Ve společnosti První certifikační autorita, a.s., jsou pro procesy poskytování kvalifikovaných certifikačních služeb definovány činnosti, které se musí vykonávat jedině za účasti více než jediné osoby. Jedná se zejména o:

- generování párových dat pro vytváření/ověřování elektronické značky, resp. elektronického podpisu I.CA vydávaných certifikátů a seznamů zneplatněných certifikátů,
- ničení dat pro vytváření elektronické značky, resp. elektronického podpisu I.CA vydávaných certifikátů a seznamů zneplatněných certifikátů,
- zálohování/obnovu dat pro vytváření elektronické značky, resp. elektronického podpisu I.CA vydávaných certifikátů a seznamů zneplatněných certifikátů.

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 a autentizaci - upraveno interní dokumentací, zejména:

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

5.2.4 Role vyžadující rozdělení povinností

Role, vyžadující rozdělení povinností v procesu poskytování kvalifikovaných certifikačních služeb v oblasti certifikátů, jsou definované v interní bezpečností dokumentaci ***„Systémová bezpečnostní politika CA“***.

5.3 Personální bezpečnost

Oblast personální bezpečnosti je uvedena v interní dokumentaci ***„Kontrolní činnost, bezúhonnost a odbornost“.***

5.3.1 Požadavky na kvalifikaci, zkušenost a bezúhonnost

Pracovníci v důvěryhodných rolích jsou vybíráni a přijímáni na základě dále popsaných personálních kriterií:

- naprostá občanská bezúhonnost - prokazováno tím, že tyto osoby nemají žádný záznam v rejstříku trestů (výpis z registru trestů nebo čestné prohlášení),
- vysokoškolské vzdělání v rámci akreditovaného bakalářského nebo magisterského studijního programu a nejméně 3 roky praxe v oblasti informačních a komunikačních technologií, nebo středoškolské vzdělání a nejméně 5 let praxe v oblasti informačních a komunikačních technologií, přičemž z toho nejméně 1 rok v oblasti poskytování certifikačních služeb,
- znalost v oblasti infrastruktury veřejných klíčů a informační bezpečnosti,
- v jednotlivých případech lze zkrátit délku uvedené praxe až o jednu třetinu stanovené délky na základě přezkoušení, při němž pracovník prokáže dostatečné znalosti k výkonu důvěryhodné funkce.

Ostatní pracovníci jsou přijímáni na základě následujících kriterií:

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

5.3.2 Posouzení spolehlivosti osob

Zdrojem informací všech kmenových pracovníků I.CA jsou:

- sami tito pracovníci,
- osoby, které tyto pracovníky znají,
- veřejné zdroje informací.

Pracovníci poskytují prvotní informace osobním pohovorem při přijímání do pracovního poměru, které aktualizují při periodických pohovorech s nadřízeným pracovníkem v průběhu pracovního poměru.

5.3.3 Požadavky na přípravu pro výkon role, vstupní školení

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

5.3.4 Požadavky a periodicita školení

Pro kmenové pracovníky pořádá vedení I.CA minimálně jedenkrát ročně interní výukový seminář, zaměřený na problematiku bezpečnosti informací.

5.3.5 Periodicita a posloupnost rotace pracovníků mezi různými rolemi

Z důvodů možné zastupitelnosti v mimořádných případech jsou pracovníci I.CA motivováni na získávání znalostí potřebných na zastávání jiné role v I.CA. Změna role je možná pouze v mimořádných případech (epidemické onemocnění, atp.) jako dočasné opatření.

5.3.6 Postihy za neoprávněné činnosti zaměstnanců

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

5.3.7 Požadavky na nezávislé zhotovitele (dodavatele)

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

5.3.8 Dokumentace poskytovaná zaměstnancům

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

5.4 Auditní záznamy (logy)

Činnosti spojené s oblastí auditních záznamů/logů je uvedena v interní dokumentaci, zejména:

- *„**Příručka administrátora**“,*
- ***„Příprava uchovávaných informací“,***
- *„**Záloha dat provozních systémů**“ .*

5.4.1 Typy zaznamenávaných událostí

Dle požadavků CWA 14167-1 - Security Requirements for Trustworthy Systems Managing Certificates for Electronic Signatures - Part 1: System Security Requirements jsou minimálně logovány následující události:

- z hlediska systému významné události prostředí a klíčového hospodářství,
- spuštění a ukončení funkcí auditu,
- změny parametrů auditu,
- akce, prováděné při chybách úložiště auditních záznamů,
- všechny pokusy přístupu k systému

a dále:

- záznam o požadavku na vydání certifikátu,
- záznam o vydání a případném zveřejnění certifikátu,
- záznam o požadavku na zneplatnění certifikátu,
- záznam o zneplatnění certifikátu,
- záznam o zařazení zneplatněného certifikátu do CR,
- záznam o zveřejnění CRL,
- všechny události vztahující se k životnímu cyklu párových dat a certifikátů CA.

Záznamy v auditním souboru obsahují následující parametry:

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

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

Auditní systém je navržen a provozován způsobem, který zaručuje udržování auditní 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 bezpečnostní dokumentaci, v případě bezpečnostního incidentu okamžitě - uvedeno v interním dokumentu ***„Příručka administrátora“***.

5.4.3 Doba uchovávání auditních záznamů

Auditní záznamy jsou uchovávány v souladu s požadavky ZoEP.

5.4.4 Ochrana auditních záznamů

Auditní záznamy jsou uloženy způsobem, zajišťujícím jejich ochranu před jejich změnami, krádeží a zničení (ať již úmyslnému, tak neúmyslnému).

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

Procesy jsou uvedeny v interní dokumentaci, zejména:

- ***„Příručka administrátora“,***
- ***„Příprava uchovávaných informací“,***
- ***„Záloha dat provozních systémů“ ,***
- ***„Dokumenty agendy certifikačních služeb“.***

5.4.5 Postupy pro zálohování auditních záznamů

Zálohování elektronických auditních záznamů probíhá obdobným způsobem jako zálohovaní ostatních elektronických informací. Procesy jsou uvedeny v interní dokumentaci, zejména:

- ***„Příručka administrátora“,***
- ***„Záloha dat provozních systémů“ .***

5.4.6 Systém shromažďování auditních záznamů (interní nebo externí)

Systém shromažďování auditních záznamů je ve vztahu k I.CA interní, ve vztahu k smluvním partnerům externí.

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, v případě incidentu, majícího vliv na bezpečnost poskytovaných služeb okamžitě.

5.5 Uchovávání informací a dokumentace

Uchovávání informací a dokumentace je u I.CA prováděno dle požadavků ZoEP (ČR, SR) a dalších právních norem (aktuální znění zákona ČR č. 499/2004 Sb., o archivnictví a spisové službě a o změně některých zákonů, zákon Slovenskej národnej rady č. 149/1975 Zb. o archívnictve v znení neskorších predpisov).

Problematika spojená s uchováváním informací a dokumentace je detailně řešena v interní dokumentaci, zejména:

- ***„Řízení fyzického přístupu do místností I.CA“,***
- ***„Příprava uchovávaných informací“,***
- ***„Záloha dat provozních systémů“ ,***
- ***„Příručka administrátora“,***
- ***„Dokumenty agendy certifikačních služeb“.***

5.5.1 Typy informací a dokumentace, které se uchovávají

I.CA uchovává informace a dokumentaci v souladu se ZoEP a VoEP. Tyto informace a dokumenty jsou konkretizovány v interních dokumentech ***„Dílčí spisový a skartační řád pro agendy certifikačních služeb“*** a ***„Dokumenty agendy certifikačních služeb“***.

5.5.2 Doba uchovávání uchovávaných informací a dokumentace

Doba uchovávaných informací a dokumentace je uvedena v interním dokumentu ***„Dílčí spisový a skartační řád pro agendy certifikačních služeb“***.

5.5.3 Ochrana úložiště uchovávaných informací a dokumentace

Uchovávané informace a dokumentace obsahují i osobní data klientů a proto je vzhledem k zákonu ČR č. 101/2000 Sb. dbáno zvýšené ochrany těchto dat. Prostory, ve kterých se uchovávané informace a dokumentace nacházejí, jsou zabezpečeny formou opatření, vycházejících z požadavků objektové a fyzické bezpečnosti.

Uchovávané informace a dokumentace jsou přístupné oprávněným:

- pracovníkům I.CA,
- kontrolním subjektům, orgánům činných v trestním řízení a soudům, pokud je to právními normami vyžadováno.

O každém takto povoleném přístupu je pořizován písemný záznam.

5.5.4 Postupy při zálohování uchovávaných informací a dokumentace

Postupy při zálohování uchovávaných informací a dokumentace jsou upraveny interní dokumentací I.CA, uvedenou v záhlaví kapitoly 5.5.

5.5.5 Požadavky na používání časových razítek při uchovávání informací a dokumentace

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

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

Informace a dokumentace jsou ukládány na místo, určené ředitelem I.CA. Samotná problematika přípravy a způsobu ukládání informací a dokumentace v elektronické i písemné podobě je upravena interními normami a směrnicemi, uvedenými v záhlaví kapitoly 5.5 a dokumentem ***„Dílčí spisový a skartační řád pro agendy certifikačních služeb“***.

5.5.7 Postupy pro získání a ověření uchovávaných informací a dokumentace

Postupy jsou popsány v interní dokumentaci I.CA, uvedené v záhlaví kapitoly 5.5 a v dokumentu ***„Dokumenty agendy certifikačních služeb“***.

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

Výměna dat pro ověřování elektronických značek/podpisů v nadřízeném kvalifikovaném systémovém certifikátu I.CA je v případě standardních situací (uplynutí platnosti certifikátu) s dostatečným časovým předstihem (minimálně jeden rok před uplynutím doby platnosti tohoto certifikátu) prováděna formou vydání nového kořenového certifikátu I.CA. V případě nestandardních situací (např. dojde-li k takovému vývoji kryptoanalytických metod, že by mohla být ohrožena bezpečnost procesu tvorby

elektronických podpisů, resp. značek, tzn. změny kryptografických algoritmů, délky klíčů atd.) je tato činnost prováděna v adekvátním časovém období.

Jak v případě standardních situací, tak nestandardních situací je výměna dat pro ověřování elektronických značek/podpisů v nadřízeném kvalifikovaném systémovém certifikátu I.CA držitelům certifikátů a veřejnosti s předstihem (je-li to možné) vhodnou formou sdělena.

5.7 Obnova po havárii nebo kompromitaci

5.7.1 Postup v případě incidentu

Postupy jsou uvedeny v interních dokumentech, zejména:

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

5.7.2 Poškození výpočetních prostředků, software nebo dat

V případě poškození výpočetních prostředků, softwaru nebo dat postupuje I.CA v souladu s interními dokumenty, zejména:

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

5.7.3 Postup při kompromitaci dat pro vytváření elektronických značek poskytovatele

V případě vzniku důvodné obavy kompromitace dat pro vytváření elektronických značek, resp. elektronických podpisů pro označování, resp. podepisování vydávaných certifikátů a seznamů zneplatněných certifikátů I.CA:

- ukončí jejich používání,
- okamžitě a trvale zneplatní příslušný kořenový certifikát I.CA a jemu odpovídající data pro vytváření elektronických značek, resp. elektronických podpisů (soukromý klíč),
- zneplatní všechny platné certifikáty, které byly výše uvedenými daty elektronicky označeny, resp. elektronicky podepsány,
- bezodkladně o této skutečnosti, včetně důvodu informuje na své internetové informační adrese a v nejméně jednom celostátně distribuovaném deníku (viz kapitola 2.2), pro zpřístupnění této informace je využit i seznam zneplatněných certifikátů,
- oznámí příslušnému úřadu informaci o zneplatnění příslušného kořenového certifikátu I.CA s uvedením důvodu zneplatnění,
- pokud je to možné, informuje držitele platných certifikátů o zneplatnění těchto certifikátů, a to prostřednictvím zaslání zprávy elektronickou poštou na elektronickou adresu, kterou tyto osoby uvedly v žádosti o vydání certifikátu, součástí této informace je důvod ukončení platnosti příslušného kořenového certifikátu I.CA.

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 procesu vydávání certifikátů a seznamu zneplatněných certifikátů.

5.7.4 Schopnosti obnovit činnost po havárii

V případě havárie postupuje I.CA v souladu s interními dokumenty, zejména:

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

5.8 Ukončení činnosti CA nebo RA

V případě plánovaného ukončení činnosti I.CA jako kvalifikovaného poskytovatele certifikačních služeb v oblasti vydávání certifikátů, tzn. z jiných důvodů, než-li jsou mimořádné události jakými jsou stávky, občanské nepokoje, válečný stav, přírodní katastrofy celostátního rozsahu nebo jiné výsledky působení vyšší moci, zajistí I.CA provedení následujících činností:

- Certifikáty vydané v souladu s legislativou České republiky:
    - ohlásí příslušnému úřadu záměr ukončit činnost poskytování kvalifikovaných certifikačních služeb v oblasti vydávání certifikátů nejméně 3 měsíce před plánovaným ukončením činnosti,
    - vynaloží veškeré možné úsilí pro to, aby evidence, vedená dle platné legislativy, byla převzata jiným kvalifikovaným poskytovatelem certifikačních služeb v oblasti vydávání certifikátů, v případě, že se jí nepodařilo tuto evidenci předat jinému kvalifikovanému poskytovateli certifikačních služeb v oblasti vydávání certifikátů, ohlásí nejpozději 30 dnů před plánovaným datem ukončení činnosti tuto skutečnost příslušnému úřadu a zajistí předání této evidence příslušnému úřadu - tuto informaci zahrne do zprávy, odeslané všem svým klientům, kteří jsou držiteli platných smluv o poskytování kvalifikovaných certifikačních služeb v oblasti vydávání certifikátů, pokud toto bude známo nejméně 2 měsíce před plánovaným ukončením činnosti,
    - zpřístupnění informaci o ukončení činnosti I.CA v oblasti vydávání certifikátů na své internetové informační adrese nejméně 2 měsíce před plánovaným ukončením činnosti,
    - ukončí poskytování kvalifikované certifikačních služeb v oblasti vydávání certifikátů,
    - prokazatelné zničí svá data pro vytváření elektronických značek, sloužící k označování vydávaných certifikátů a seznamu zneplatněných certifikátů.

- Certifikáty vydané v souladu s legislativou Slovenské republiky:
    - ohlásí příslušnému úřadu záměr ukončit činnost poskytování kvalifikovaných certifikačních služeb v oblasti vydávání certifikátů nejméně 6 měsíců před plánovaným ukončením činnosti,
    - ohlásí každému držiteli platného kvalifikovaného certifikátu záměr ukončit činnost poskytování kvalifikovaných certifikačních služeb v oblasti vydávání certifikátů nejméně 6 měsíců před plánovaným ukončením činnosti,
    - může se dohodnout s jiným kvalifikovaným poskytovatelem certifikačních služeb v oblasti vydávání certifikátů o převzetí záznamů o vydaných a zrušených certifikátech a provozní dokumentaci – pokud žádný kvalifikovaný poskytovatel certifikačních služeb v oblasti vydávání certifikátů tyto záznamy nepřevezme:
        - zaniká platnost všech jím vydaných kvalifikovaných certifikátů ode dne zániku tohoto kvalifikovaného poskytovatele certifikačních služeb v oblasti vydávání certifikátů,
        - převezme tyto záznamy úřad.

Problematika plánovaného ukončení činnosti I.CA jako kvalifikovaného poskytovatele certifikačních služeb v oblasti vydávání certifikátů je detailně uvedena v interní dokumentaci ***„Ukončení činnosti služeb I.CA“.***

6 Technická bezpečnost

6.1 Generování a instalace párových dat

6.1.1 Generování párových dat

Generování párových dat I.CA, které probíhá v zabezpečené zóně v souladu s dokumentem Systémová bezpečnostní politika CA a o jehož průběhu je vyhotoven písemný protokol, je prováděno v kryptografickém modulu, který splňuje požadavky české, resp. slovenské legislativy, vztahující se k problematice elektronického podpisu. Použitý modul svými vlastnostmi odpovídá požadavkům vyžadovaným ZoEP a VoEP. I.CA používá pro párová data, sloužící k označování, resp. podepisování vydávaných certifikátů a seznamů zneplatněných certifikátů délku rovnou 2048 bitů.

V průběhu procesu generování párových dat I.CA, sloužících k označování, resp. podepisování vydávaných certifikátů a seznamů zneplatněných certifikátů, musí být minimálně fyzicky přítomni:

- ředitel I.CA,
- bezpečnostní manager,
- vedoucí provozního pracoviště.

Konkrétní technický postup generace párových dat I.CA, sloužících k označování, resp. podepisování vydávaných certifikátů a seznamů zneplatněných certifikátů a následné vyhotovení certifikátu CA, příslušného k těmto párovým datům, je popsán v interní dokumentaci I.CA:

- ***„Řízení fyzického přístupu do místností I.CA“*,**
- ***„HSM/Private Server“.***

O průběhu generování párových dat I.CA, sloužících k označování, resp. podepisování vydávaných certifikátů a seznamů zneplatněných certifikátů je vyhotoven písemný protokol obsahující:

- jmenný seznam přítomných pracovníků s uvedením: jména, příjmení, titulu,
- datum a čas zahájení a ukončení generace párových dat s přesností minimálně na minuty,
- místo, kde ke generaci párových dat došlo,
- popis zařízení, na kterém byla generace prováděna, umožňující jednoznačnou identifikaci tohoto zařízení,
- kompletní výpis certifikátu CA, obsahující data pro ověřování elektronických značek, resp. elektronických podpisů vydávaných certifikátů a seznamů zneplatněných certifikátů, obsažená v právě vygenerovaných párových datech,
- datum vyhotovení protokolu,
- vlastnoruční podpisy všech pracovníků, kteří se na generaci párových dat podíleli.

I.CA z principiálních bezpečnostních důvodů neposkytuje službu generování párových dat klienta na svých zařízeních. Klient je povinen používat taková zařízení, resp. aplikace, které splňují požadavky ZoEP a VoEP.

V případě generování párových dat používaných v procesech správy systémových komponent I.CA, komunikaci s RA na vlastních zařízeních, jsou pracovníci I.CA a RA povinni využívat certifikáty vydané I.CA.

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

S ohledem na skutečnost, že žadatel o certifikát generuje soukromý klíč zásadně na zařízení a v prostředí, která jsou v okamžiku generování pod jeho výhradní kontrolou, není tento proces uplatňován.

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

Data pro ověřování elektronických podpisů/značek je nutno I.CA doručit. I.CA podporuje následující způsoby doručení dat pro ověřování elektronického podpisu/značky:

- osobně na datovém nosiči,
- zasláním prostřednictvím elektronické pošty,
- I.CA si vyhrazuje i jiný způsob pro doručení dat pro ověřování elektronických podpisů/značek (uložení žádosti o certifikát na v systému I.CA).

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

Data pro ověřování elektronických značek, resp. elektronických podpisů I.CA vydaných certifikátů a seznamů zneplatněných certifikátů jsou obsažena v certifikátu CA, jehož získání je garantováno následujícími způsoby:

- obdržením na RA (osobní návštěva),
- prostřednictvím internetových informačních adres I.CA a příslušného úřadu, případně prostřednictvím věstníku příslušného úřadu,
- každý žadatel o certifikát obdrží kořenový certifikát I.CA při získání svého prvotního certifikátu na RA.

6.1.5 Délky párových dat

V procesu poskytování kvalifikovaných certifikačních služeb využívá I.CA výhradně nejprověřenější klasický asymetrický šifrový algoritmus RSA. Mohutnost klíčů (resp. parametrů daného algoritmu) použitých pro označování, resp. podepisování vydávaných certifikátů a seznamů zneplatněných certifikátů je 2048 bitů, mohutnost klíčů (resp. parametrů daného algoritmu) na straně klienta je 2048 bitů.

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

Algoritmy, použité pro generování celočíselných hodnot nutných pro fungování elektronického podpisu (např. testy prvočíselnosti atd.), musí mít parametry uvedené v platné legislativě (ZoEP, VoEP), resp. v ní odkazovaných technických standardech nebo normách.

I.CA kontroluje možný dvojí výskyt stejných dat pro ověření elektronických podpisů/značek ve vydávaných certifikátech. V případě duplicitního výskytu dat pro ověření elektronických podpisů/značek je žadatel o certifikát požádán o vygenerování nových párových dat. Již vydaný certifikát je neprodleně zneplatněn, držitel takového certifikátu je o tomto neprodleně a vhodným způsobem informován a vyzván ke generování nových párových dat.

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

Uvedeno v kapitole 1.4.

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

Konkrétní postupy jsou popsány v interní dokumentaci I.CA:

- ***„Řízení fyzického přístupu do místností I.CA“ ,***
- ***„HSM/Private Server“.***

6.2.1 Standardy a podmínky používání kryptografických modulů

Generování párových dat I.CA a uložení soukromého klíče I.CA, sloužícího pro vytváření elektronických značek, resp. elektronických podpisů vydávaných certifikátů a seznamů zneplatněných certifikátů, probíhá v kryptografickém modulu, který splňuje požadavky standardu FIPS PUB 140-2 úroveň 3 a VoEP.

6.2.2 Sdílení tajemství

Ochrana sdílením tajemství je realizována prostředky kryptografického modulu. Při provádění citlivých činností, které souvisejí se zásadními činnostmi I.CA (viz. kapitoly 6.1.1 a 6.2.10), je nezbytná přítomnost tří pověřených pracovníků I.CA, z nichž dva znají část kódu k provedení těchto činností.

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

Služba není poskytována.

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

Kryptografický modul, použitý pro správu párových dat I.CA, umožňuje zálohování soukromého klíče, sloužícího pro vytváření elektronických značek, resp. elektronických podpisů vydávaných certifikátů a seznamů zneplatněných certifikátů. Soukromý klíč je v zašifrované podobě zálohován prostřednictvím čipových karet kryptografického modulu.

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

Po uplynutí doby platnosti soukromého klíče dat určených k označování, resp. podepisování vydávaných certifikátů a seznamů zneplatněných certifikátů je tento (včetně záloh) zničen a jeho další zálohování se neprovádí. Uchovávání těchto soukromých klíčů představuje bezpečnostní riziko, a proto je u I.CA zakázáno.

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

Soukromý klíč, sloužící pro vytváření elektronických značek, resp. elektronických podpisů vydávaných certifikátů a seznamů zneplatněných certifikátů, je generován přímo v kryptografickém modulu.

Vkládání soukromého klíče do kryptografického modulu ze šifrované zálohy probíhá za přímé osobní účasti nejméně dvou určených pracovníků I.CA. V okamžiku jeho vkládání musí být vyhrazená

stanice a kryptografický modul odpojeny od počítačové sítě. O vložení soukromého klíče je pořízen písemný záznam.

6.2.7 Uložení dat pro vytváření elektronických značek v kryptografickém modulu

Soukromý klíč, sloužící k vytváření elektronických značek, resp. elektronických podpisů je uložen v kryptografickém modulu, splňujícím požadavky FIPS PUB 140-2 úroveň 3.

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

Aktivaci soukromého klíče, sloužícího pro vytváření elektronických značek, resp. elektronických podpisů vydávaných certifikátů a seznamů zneplatněných certifikátů provádějí určení pracovníci I.CA prostřednictvím aktivační čipové karty podle přesně určeného postupu, který je upraven interní dokumentací. Po aktivaci je systém připraven k označování, resp. podepisování vydávaných certifikátů, seznamů zneplatněných certifikátů a aktivační čipová karta se vyjme.

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

Deaktivaci soukromého klíče, sloužícího pro vytváření elektronických značek, resp. elektronických podpisů vydávaných certifikátů a seznamů zneplatněných certifikátů, provádí určení pracovníci I.CA prostřednictvím kryptografického modulu a čipové karty podle přesně určeného postupu, který je upraven interní dokumentací. O provedené deaktivace je pořízen písemný záznam, který podepíší určení pracovníci I.CA.

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

Data pro vytváření elektronických značek, resp. elektronických podpisů sloužící k označování, resp. podepisování vydávaných certifikátů a seznamů zneplatněných certifikátů jsou uložena v kryptografickém modulu. Ničení těchto dat je realizováno prostředky kryptografického modulu. Zálohy těchto dat uložené v zašifrované podobě na externích médiích jsou rovněž zničeny. Ničení spočívá ve fyzické destrukci těchto nosičů.

Při ničení dat pro vytváření elektronických značek, resp. elektronických podpisů, sloužících k označování, resp. podepisování vydávaných certifikátů a seznamů zneplatněných certifikátů musí být minimálně fyzicky přítomni:

- ředitel I.CA,
- bezpečnostní manager,
- vedoucí provozního pracoviště.

O průběhu ničení dat pro vytváření elektronických značek, resp. elektronických podpisů, sloužící k označování, resp. podepisování vydávaných certifikátů a seznamů zneplatněných certifikátů je sepsán protokol.

6.2.11 Hodnocení kryptografického modulu

Nástroj elektronického podpisu pro elektronické označování, resp. podepisování vydávaných certifikátů a seznamů zneplatněných certifikátů, byl certifikován na shodu s požadavky standardu FIPS PUB 140-2 úroveň 3.

6.3 Další aspekty správy párových dat

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

Problematika uchovávání dat pro ověřování elektronických značek, resp. podpisů je řešena v souladu s ZoEP a VoEP.

Se všemi certifikáty CA je nakládáno způsobem, uvedeným v kapitolách 5.4 a 5.5.

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

Maximální doba platnosti certifikátu, který je vydán podepisující/označující osobě, je uvedena v těle tohoto certifikátu (viz kapitola 7.1).

6.4 Aktivační data

6.4.1 Generování a instalace aktivačních dat

Aktivační data jsou vytvářena v průběhu procesu instalace, kdy jsou generována párová data I.CA, sloužící pro vytváření a ověřování elektronických značek, resp. podpisů vydávaných certifikátů a seznamů zneplatněných certifikátů.

Konkrétní postupy jsou popsány v interním dokumentu ***„HSM/Private Server“***.

6.4.2 Ochrana aktivačních dat

Výše uvedená aktivační data jsou pracovníky I.CA chráněna způsobem, uvedeným v interním bezpečnostní dokumentaci ***„HSM/Private Server“*** a ***„Příručka administrátora“***.

6.4.3 Ostatní aspekty aktivačních dat

Výše uvedená aktivační data jsou určena výhradně pro procesy poskytování kvalifikovaných certifikačních služeb a nesmí být použita k jiným účelům, ani přenášena nebo uchovávána v otevřené podobě.

6.5 Počítačová bezpečnost

6.5.1 Specifické technické požadavky na počítačovou bezpečnost

Bezpečnost použitých komponent informačních systémů pro poskytování kvalifikovaných certifikačních služeb v oblasti vydávání certifikátů je definována ve VoEP odkazovaném dokumentu CWA 14167-1 - Security Requirements for Trustworthy Systems Managing Certificates for Electronic Signatures - Part 1: System Security Requirements.

Konkrétní řešení specifických technických požadavků počítačové bezpečnosti je popsáno v interní dokumentaci, zejména:

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

6.5.2 Hodnocení počítačové bezpečnosti

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

- CWA 14167-1 - Security Requirements for Trustworthy Systems Managing Certificates for Electronic Signatures - Part 1: System Security Requirements/Bezpečnostní požadavky na důvěryhodné systémy spravující certifikáty pro elektronický podpis – část 1: Požadavky na bezpečnost systémů,
- ČSN ETSI TS 101 456 - Elektronické podpisy a infrastruktury; Požadavky na postupy certifikační autority vydávající kvalifikované certifikáty,
- ETSI TS 102 042 – Electronic Signatures and Infrastructures (ESI); Policy requirements for certification authorities issuing public key certificates,
- ČSN ISO/IEC 27001 Informační technologie - Bezpečnostní techniky - Systémy řízení bezpečnosti informací – Požadavky,
- ČSN ISO/IEC 27002 Informační technologie - Bezpečnostní techniky - Soubor postupů pro opatření bezpečnosti informací,
- ČSN ISO/IEC 27003 Informační technologie - Bezpečnostní techniky - Směrnice pro implementaci systému řízení bezpečnosti informací,
- ČSN ISO/IEC 27005 Informační technologie - Bezpečnostní techniky – Řízení rizik bezpečnosti informací,
- ČSN ISO/IEC 15408 Informační technologie – Kritéria pro hodnocení bezpečnosti IT,
- RFC 5280 Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile.

6.6 Bezpečnost životního cyklu

6.6.1 Řízení vývoje systému

Vývojové práce pro potřeby společnosti První certifikační autority, a.s. jsou realizovány na bázi smluvního vztahu s příslušným dodavatelem.

V případě vývoje systému v oblastech provozní činnosti, systémového programového vybavení, změn v bezpečnostní dokumentační základně atd. je postupováno dle interního dokumentu „***Změnové řízení***“.

6.6.2 Kontroly řízení bezpečnosti

Soulad se standardy (viz kapitola 6.5.2), ZoEP a VoEP je ověřován pravidelnými audity systému managementu bezpečnosti informací, prováděnými pracovníky nezávislých firem a kontrolami bezpečnostní shody, prováděnými interními pracovníky I.CA. Tato problematika je popsána v interním dokumentu ***„Kontrolní činnost, bezúhonnost a odbornost“***.

I.CA si vyhrazuje právo provádění i jiných typů kontrol, resp. auditů.

6.6.3 Řízení bezpečnosti životního cyklu

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

- vybudování – definování bezpečnostní politiky, plánů, cílů, procesů a postupů s ohledem na řízení rizik a bezpečnost informací tak, aby byly v souladu s celkovou bezpečnostní politikou,
- implementace a provoz - bezpečnostní politiky, plánů, cílů, procesů a postupů,
- monitorování a přehodnocování – posouzení procesu s ohledem na bezpečnostní politiku a předání poznatků vedení společnosti k posouzení,
- využití – na základě rozhodnutí vedení organizace provedení nápravných opatření.

6.7 Síťová bezpečnost

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

Detailní řešení řízení síťové bezpečnosti je popsáno v interní dokumentaci, zejména:

- ***„Systémová bezpečnostní politika CA“,***
- ***„Obnova komponenty provozního pracoviště“,***
- ***„Přemístění provozního pracoviště“,***
- ***„Příručka administrátora“,***
- ***„Firewall – provozní pracoviště“.***

6.8 Časová razítka

Řešení je uvedeno v kapitole 5.5.5.

7 Profily certifikátu, seznamu zneplatněných certifikátů a OCSP

Profily certifikátu a seznamu zneplatněných certifikátů jsou vždy uvedeny v konkrétní CP (viz kapitola 1.2). V následujících kapitolách jsou případně popsány pouze změny, jejichž provedení si I.CA v konkrétní certifikační politice vyhradila.

7.1 Profil certifikátu

Viz kap. 7.1.

7.1.1 Číslo verze

Viz kap. 7.1.

7.1.2 Rozšiřující položky v certifikátu

Viz kap. 7.1.

7.1.3 Objektové identifikátory (dále OID) algoritmů

Viz kap. 7.1.

7.1.4 Způsoby zápisu jmen a názvů

Viz kap. 7.1.

7.1.5 Omezení jmen a názvů

Viz kap. 7.1.

7.1.6 OID certifikační politiky

Viz kap. 7.1.

7.1.7 Rozšiřující položka „Policy Constrainst“

Viz kap. 7.1.

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

Viz kap. 7.1.

7.1.9 Způsob zápisu kritické rozšiřující položky „Certificate Policies“

Viz kap. 7.1.

7.2 Profil seznamu zneplatněných certifikátů

Viz kap. 7.1.

7.2.1 Číslo verze

Viz kap. 7.1.

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

Viz kap. 7.1.

7.3 Profil OCSP

Služba není poskytována.

7.3.1 Číslo verze

Služba není poskytována.

7.3.2 Rozšiřující položky OCSP

Služba není poskytována.

8 Hodnocení shody a jiná hodnocení

S ohledem na skutečnost, že společnost První certifikační autorita, a.s. je akreditovaným poskytovatel certifikačních služeb, jsou periodicita hodnocení, včetně okolností pro provádění hodnocení striktně dány požadavky ZoEP a VoEP, jedná se zejména o audit systému řízení bezpečnosti informací, který je prováděn každé dva roky a kontroly bezpečnostní shody v intervalu 4 let (celková), resp. každého roku (částečná).

Společnost První certifikační autorita, a.s. si vyhrazuje právo provádění i jiných forem kontrol.

Problematika hodnocení je upřesněna interním dokumentem ***„Kontrolní činnost, bezúhonnost a odbornost“***.

8.1 Periodicita hodnocení nebo okolnosti pro provedení hodnocení

Celková kontrola bezpečnostní shody je prováděna po 4 letech od předchozí celkové kontroly bezpečnostní shody. Během těchto 4 let jsou prováděny roční částečné kontroly bezpečnostní shody.

Audit systému bezpečnosti informací je prováděn po 2 letech od předchozího auditu systému bezpečnosti informací a je prováděn podle požadavků normy ČSN EN ISO 19011.

8.2 Identita a kvalifikace hodnotitele

Identita a kvalifikace hodnotitele je upravena interním dokumentem ***„Kontrolní činnost, bezúhonnost a odbornost“***.

8.3 Vztah hodnotitele k hodnocené entitě

V případě auditu systému managementu bezpečnosti informací je hodnotitelem externí, nezávislá organizace.

V případě celkové kontroly bezpečnostní shody nebo částečné kontroly bezpečnostní shody je hodnotitelem fyzická/právnická osoba, pověřená ředitelem společnosti První certifikační autorita, a.s.

8.4 Hodnocené oblasti

Cílem kontroly bezpečnostní shody je ověření, že společnost První certifikační autorita, a.s.:

- provozuje důvěryhodné systémy v souladu se ZoEP a VoEP,
- provádí změny v důvěryhodných systémech v souladu s bezpečnostní dokumentací, a to jejími částmi upravujícími řízení změn.

Předmětem kontroly bezpečnostní shody:

- jsou všechny důvěryhodné systémy I.CA (celková kontrola bezpečnostní shody), nebo
- jsou všechny změny, které I.CA provedla od provedení předchozí roční kontroly bezpečnostní shody (částečná kontrola bezpečnostní shody) a jejich vliv na důvěryhodné systémy I.CA, nebo
- je v případě, že v důvěryhodných systémech I.CA nenastaly od předchozí částečné kontroly bezpečnostní shody žádné změny, ověření této skutečnosti.

Cílem auditu systému managementu bezpečnosti informací je objektivní a na I.CA nezávislé ověření, že je v důvěryhodných systémech I.CA v oblasti vydávání certifikátů zaveden a uplatňován systém managementu bezpečnosti informací.

8.5 Postupy v případě zjištěných nedostatků

V případě nedostatků, zjištěných na základě výsledné zprávy konkrétního hodnocení je bezpečnostní manager povinen do 15 dnů po obdržení zprávy určit, jaká opatření k odstranění nedostatků musí I.CA přijmout.

Zjistí-li příslušný úřad, že I.CA porušuje povinnosti stanovené ZoEP, VoEP uloží jí, aby ve stanovené lhůtě zjednala nápravu a případně určí, jaká opatření k odstranění nedostatků je I.CA povinna přijmout.

8.6 Sdělování výsledků hodnocení

Sdělování výsledků hodnocení je prováděno formou písemné závěrečné zprávy, která je hodnotícím subjektem předána řediteli, resp. bezpečnostnímu managerovi společnosti.

V nejbližším možném termínu svolá bezpečnostní manager schůzi bezpečnostního výboru, na kterém bude vedení společnosti s výsledky hodnocení seznámeno.

Sdělování výsledků hodnocení taktéž podléhá požadavkům ZoEP a VoEP.

9 Ostatní obchodní a právní záležitosti

9.1 Poplatky

9.1.1 Poplatky za vydání nebo obnovení certifikátu

Poplatky za prvotní, popř. následný certifikát, jsou uvedeny v aktuálním ceníku služeb, který je k dispozici na internetové informační adrese I.CA. Služba obnovení certifikátu není poskytována.

9.1.2 Poplatky za přístup k certifikátu na seznamu vydaných certifikátů

Přístup k vydaným veřejným certifikátům elektronickou cestou I.CA nezpoplatňuje.

9.1.3 Poplatky za informace o statutu certifikátu a o zneplatnění certifikátu

Přístup k informacím o zneplatněných certifikátech (aktuální CRL) nebo statutech certifikátů elektronickou cestou I.CA nezpoplatňuje.

9.1.4 Poplatky za další služby

Poplatek za předání certifikátu (prvotní, následný) prostřednictvím záznamového média (např. disketa) je uveden v aktuálním ceníku služeb, který je k dispozici na internetové informační adrese I.CA.

Zneplatnění certifikátu a stažení elektronické verze certifikačních politik (ve všeobecně používaném formátu PDF) je poskytováno zdarma.

Poplatky za nadstandardní služby jsou stanovovány smluvně.

9.1.5 Jiná ustanovení týkající se poplatků (vč. refundací)

I.CA si vyhrazuje právo změny výše poplatku za vydání prvotního, popř. následného certifikátu. I.CA je rovněž oprávněna stanovit pro individuálně uzavřené smlouvy odlišnou výši těchto poplatků.

9.2 Finanční odpovědnost

9.2.1 Krytí pojištěním

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

9.2.2 Další aktiva a záruky

Společnost První certifikační autorita, a.s., prohlašuje, že má k dispozici dostatečné finanční zdroje a jiné finanční zajištění na provoz v souladu s požadavky uvedenými v ZoEP a s ohledem na riziko vzniku odpovědnosti za škodu.

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

9.2.3 Pojištění nebo krytí zárukou pro koncové uživatele

Služba není poskytována.

9.3 Citlivost obchodních informací

9.3.1 Výčet citlivých informací

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

- data pro vytváření elektronických značek, resp. elektronických podpisů (soukromý klíč) příslušná k datům pro ověřování elektronických značek, resp. elektronických podpisů, obsažených v kořenových certifikátech I.CA,
- data pro vytváření elektronických značek, resp. elektronických podpisů (soukromý klíč), příslušná k datům pro ověřování elektronických podpisů/značek obsažených v účelových certifikátech I.CA (např. klíče pro komunikaci s RA),
- ostatní kryptograficky podstatné informace sloužící k provozu I.CA a RA,
- vybrané obchodní informace I.CA,
- interní informace a dokumentace s ohledem na poskytování kvalifikovaných certifikačních služeb,
- osobní údaje.

9.3.2 Informace mimo rámec citlivých informací

Za veřejné se považují zejména typy informací, které nepatří do žádné z uvedených skupin v kapitole 9.3.1.

9.3.3 Odpovědnost za ochranu citlivých informací

Každý pracovník, který přijde do styku s informacemi uvedenými v kapitole 9.3.1, je nesmí bez souhlasu ředitele I.CA poskytnout třetí straně.

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

9.4 Ochrana osobních údajů

9.4.1 Politika ochrany osobních údajů

Ochrana osobních údajů a dalších neveřejných informací je v I.CA řešena v souladu s požadavky příslušných zákonných norem.

9.4.2 Osobní údaje

Osobními informacemi jsou veškeré osobní údaje klientů, uživatelů či pracovníků podléhající ochraně ve smyslu příslušných zákonných norem.

9.4.3 Údaje, které nejsou považovány za důvěrné

Informace, které nejsou považovány za důvěrné, jsou obecně údaje zveřejňované způsobem, uvedeným v kapitole 2.2.

9.4.4 Odpovědnost za ochranu osobních údajů

Za ochranu osobních údajů a dalších neveřejných informací je odpovědna I.CA.

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

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

9.4.6 Poskytování citlivých informací pro soudní či správní účely

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

9.4.7 Jiné okolnosti zpřístupňování osobních údajů

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

Osoby uvedené v kapitole 9.3.3 může zbavit mlčenlivosti ten, v jehož zájmu tuto povinnost mají, nebo soud.

9.5 Práva duševního vlastnictví

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

9.6 Zastupování a záruky

9.6.1 Zastupování a záruky CA

I.CA zaručuje, že:

- použije soukromé klíče příslušné certifikátům CA pouze k označování, resp. podepisování vydávaných certifikátů a seznamu zneplatněných certifikátů,
- vydávané certifikáty splňují náležitosti požadované ZoEP a VoEP,
- zneplatní certifikáty, pokud byla žádost o ukončení jejich platnosti podána způsobem definovaným v relevantní CP.

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

- klient neporušil povinnosti plynoucí mu ze smlouvy o poskytování kvalifikované certifikační služby a relevantní CP,

- spoléhající se strana neporušila povinnosti relevantní CP.

Klient uplatňuje záruku vždy u RA, která zpracovala jeho prvotní žádost. Pokud RA není schopna vyřídit záruční nároky ve své pravomoci, postoupí je k řízení I.CA a o této skutečnosti klienta vyrozumí. Na používání certifikátu, který I.CA nevydala, se záruky nevztahují.

9.6.2 Zastupování a záruky RA

RA přejímá závazek za správné poskytování služeb. RA nevyřídí kladně žádost, pokud žadatel hodnověrným způsobem neprokázal svoji identitu, nedoložil údaje uvedené v žádosti o službu, odmítá potřebné údaje sdělit nebo odmítne podepsat příslušné dokumenty (viz příslušné kapitoly relevantní CP). RA dále zodpovídá:

- za včasné předání žádostí o zneplatnění vydaných certifikátů k vyřízení na pracoviště CA.
- za vyřizování připomínek a stížností klientů.

9.6.3 Zastupování a záruky držitele certifikátu a podepisující nebo označující osoby

Držitel certifikátu nebo podepisující/označující osoba postupují v souladu s ZoEP a VoEP a ručí za správnost jimi uváděných informací v celém životním cyklu využívání poskytované certifikační služby.

9.6.4 Zastupování a záruky spoléhajících se stran

Spoléhající se strany postupují v souladu s ZoEP a VoEP.

9.6.5 Zastupování a záruky ostatních zúčastněných subjektů

Služba není poskytována.

9.7 Zřeknutí se záruk

Společnost První certifikační autorita, a.s., se především striktně řídí ZoEP a nemůže se zříci záruk v něm určených.

9.8 Omezení odpovědnosti

Společnost První certifikační autorita, a.s., neodpovídá za škody způsobené spoléhajícím se stranám v případech, kdy nesplnily povinnosti, požadované certifikační politikou, dle které byl certifikát vydán.

9.9 Odpovědnost za škodu, náhrada škody

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

Společnost První certifikační autorita, a.s.:

- se zavazuje, že splní veškeré povinnosti definované jak příslušnými právními předpisy, tak příslušnými certifikačními politikami,
- poskytuje výše uvedené záruky po celou dobu platnosti smlouvy o poskytování certifikačních služeb uzavřené se zákazníkem,
- jiné záruky, než výše uvedené, neposkytuje.

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

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

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

Oprávněnou reklamaci je možné podat těmito způsoby:

- e-mailem na adresu: reklamace@ica.cz,
- doporučenou poštovní zásilkou na adresu sídla společnosti,
- osobně v sídle společnosti.

Reklamující osoba (držitel certifikátu) je povinna uvést:

- číslo smlouvy,
- číslo příjmového dokladu,
- co nejvýstižnější popis závad a jejich projevů.

Povinnost I.CA:

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

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

Nový certifikát bude držiteli poskytnut zdarma v následujících případech:

- existuje-li důvodné podezření, že došlo ke kompromitaci dat pro vytváření elektronických značek, resp. podpisů, kterými I.CA elektronicky označuje, resp. podepisuje vydávané certifikáty a seznamy zneplatněných certifikátů, nabídne I.CA držitelům bezplatné vydání nového certifikátu - případné náklady na vydání nových certifikátů hradí I.CA, která po dobu zablokování certifikátů nese veškerou odpovědnost za případné škody vzniklé v souvislosti se zneužitím těchto certifikátů.
- v případě, že I.CA při příjmu žádosti o vydání certifikátu zjistí, že existuje jiný certifikát se stejným veřejným klíčem, je žadatel o certifikát vyzván k vygenerování nové žádosti, a tedy i nových párových dat - držitel již existujícího certifikátu, který vlastní veřejný klíč stejný jako žadatel o vydání certifikátu, je vyzván k vygenerování nových párových dat, jeho původní certifikát je okamžitě zneplatněn a držitel je o této skutečnosti informován.

9.10 Doba platnosti, ukončení platnosti

9.10.1 Doba platnosti

Tato CPS platí minimálně po dobu platnosti posledního podle ní vydaného certifikátu.

9.10.2 Ukončení platnosti

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

9.10.3 Důsledky ukončení a přetrvání závazků

V případě ukončení platnosti této CPS vzhledem k ukončení poskytování kvalifikované služby zůstávají v platnosti omezení a ustanovení, týkají se obchodních a právních záležitostí.

9.11 Komunikace mezi zúčastněnými subjekty

Pro individuální oznámení a komunikaci s držitelem certifikátu, resp. podepisující/označující osobou může I.CA využít jimi dodané e-mailové adresy, poštovní adresy, telefonická čísla nebo osobní jednání.

Komunikovat s I.CA lze taktéž způsoby uvedenými na adrese http://www.ica.cz/.

9.12 Změny

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

9.12.1 Postup při změnách

Certifikační politiky - viz kap. 9.12. V případě této CPS - postup je realizován řízeným procesem uvedeném v interním dokumentu ***„Změnové řízení“.***

9.12.2 Postup při oznamování změn

Certifikační politiky - viz kap. 9.12. V případě této CPS - vydání nové verze je vždy oznámeno formou zveřejňování informací.

9.12.3 Okolnosti, při kterých musí být změněno OID

Certifikační politiky - viz kap. 9.12. V případě této CPS - OID není přiřazován.

9.13 Řešení sporů

Tato CPS a jí odpovídající certifikační politika, jejich výklad a aplikace se řídí ZoEP a VoEP.

V případě, že držitel certifikátu, podepisující osoba, spoléhající se strana nebo smluvní partner nesouhlasí s předloženým výkladem, mohou použít následující stupně odvolání:

- odpovědný pracovník RA,
- odpovědný pracovník I.CA (nutné písemné podání),
- ředitel I.CA (nutné písemné podání a složení finanční jistiny, která je vrácena v případě kladného vyřízení stížnosti).

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

9.14 Rozhodné právo

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

9.15 Shoda s právními předpisy

Systém poskytování kvalifikovaných certifikačních služeb je provozován ve shodě s požadavky ZoEP a VoEP.

9.16 Další ustanovení

9.16.1 Rámcová shoda

Tyto skutečnosti jsou pro aplikaci vydání tohoto dokumentu irelevantní.

9.16.2 Postoupení práv

Tyto skutečnosti jsou pro aplikaci vydání tohoto dokumentu irelevantní.

9.16.3 Oddělitelnost ustanovení

Tyto skutečnosti jsou pro aplikaci vydání tohoto dokumentu irelevantní.

9.16.4 Zřeknutí se práv

Tyto skutečnosti jsou pro aplikaci vydání tohoto dokumentu irelevantní.

9.16.5 Vyšší moc

Společnost První certifikační autorita, a.s., neodpovídá za porušení svých povinností vyplývající ze zásahu vyšší moci, např. přírodních nebo lidskou činností způsobených katastrof velkého rozsahu, stávek či občanských nepokojů vždy spojených s vyhlášením nouzového stavu, nebo vyhlášení stavu ohrožení státu nebo válečného stavu.

9.17 Další opatření

Tyto skutečnosti jsou pro aplikaci vydání tohoto dokumentu irelevantní.

10 Závěrečná ustanovení

Tato CPS, vydaná společností První certifikační autorita, a.s., nabývá platnosti a účinnosti dnem 22.09.2015.