První certifikační autorita, a.s.
(akreditovaný poskytovatel certifikačních služeb)

CERTIFIKAČNÍ POLITIKA

VYDÁVÁNÍ KVALIFIKOVANÝCH SYSTÉMOVÝCH CERTIFIKÁTŮ

Stupeň důvěrnosti: veřejný dokument

Verze 3.1

Tabulka 1 – Vývoj dokumentu

Verze	Datum vydání	Schválil	Pozn
3.0	23.10.2009	Ředitel společnosti První certifikační autorita, a.s.	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	Ředitel společnosti První certifikační autorita, a.s.	v případě prvotního certifikátu akceptace elektronické poštovní adresy pouze v položce SubjectAlternativeName.rfc822Name, podporované položky key usage, extended key usage, vstupní kontroly, úprava textu

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 s 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 politika vydávání kvalifikovaných systémových certifikátů** (dále též CP), vypracovaný společností První certifikační autorita, a. s. se zabývá skutečnostmi, vztahujícími se k procesům životního cyklu kvalifikovaných systémových certifikátů, 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

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

- Kapitola 1 identifikuje tento dokument přiřazeným jedinečným identifikátorem (jedná se o OID této certifikační politiky), obecně popisuje subjekty, které participují na poskytování této certifikační služby, a definuje přípustné využívání vydávaných kvalifikovaných systémových certifikátů.
- Kapitola 2 obsahuje problematiku odpovědností za zveřejňování a úložiště informací, resp. dokumentace.
- Kapitola 3 popisuje procesy identifikace a autentizace žadatele o vydání kvalifikovaného systémového certifikátu, resp. zneplatnění kvalifikovaného systémového certifikátu, včetně definování typů a obsahů používaných jmen v žádostech, resp. vydávaných kvalifikovaných systémových certifikátech.
- Kapitola 4 definuje procesy životního cyklu kvalifikovaného systémového certifikátu, tzn. žádost o vydání kvalifikovaného systémového certifikátu, zneplatnění kvalifikovaného systémového

[1] European Telecommunications Standards Institute

certifikátu, služby související s ověřováním statutu kvalifikovaného systémového certifikátu, ukončení poskytování certifikačních služeb atd.

- Kapitola 5 zahrnuje problematiku fyzické, procesní a personální bezpečnosti, včetně definování množiny zaznamenávaných událostí a jejich uchovávání, problematiku po haváriích nebo kompromitaci.
- Kapitola 6 je zaměřena na technickou bezpečnost typu generování veřejných a soukromých klíčů, ochrany soukromých klíčů, včetně počítačové a síťové ochrany.
- Kapitola 7 definuje profil vydávaných kvalifikovaných systémových certifikátů a seznamů zneplatněných kvalifikovaných systémových certifikátů.
- Kapitola 8 je zaměřena na problematiku hodnocení poskytovaných certifikačních služeb
- Kapitola 9 zahrnuje problematiku obchodní a právní.

S ohledem na skutečnost, že společnost První certifikační autorita, a.s. vydává více druhů certifikátů dle různých politik, měl se by potenciální uživatel certifikátu vydávaného dle této certifikační politiky s tímto dokumentem a ujistit se o tom, že odpovídá jeho požadavkům na využívání kvalifikovaného systémového certifikátu.

Tento dokument může být mimo jiné využit nezávislými institucemi (např. auditorskými společnostmi) jako základ pro potvrzení toho, že certifikační služby v oblasti vydávaní kvalifikovaných systémových 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.

1.2 Název a identifikace dokumentu

Název tohoto dokumentu	:	Certifikační politika vydávání kvalifikovaných systémových certifikátů
OID	:	1.3.6.1.4.1. 23624.1.1.40.3.1

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 CP, 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 a podepisující nebo označující osoby, kteří požádali o vydání certifikátu nebo kvalifikovaného systémového certifikátu (dále certifikátu) 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 osobu a které byl certifikát vydán.

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 certifikát vydaný společností První certifikační autorita, a.s., na elektronickou značku, ověřovanou tímto certifikátem.

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 systémové certifikáty vydávané dle této certifikační politiky společností První certifikační autorita, a.s. lze využívat pouze v procesech ověřování elektronického značky v souladu s platnou legislativou (ZoEP, VoEP).

1.4.2 Omezení použití certifikátu

Kvalifikované systémové certifikáty vydávané dle této certifikační politiky společností První certifikační autorita, a.s. nesmí být využívány v rozporu s vydávaným účelem (definovaným touto certifikační politikou) 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 certifikační politiku, resp. jí odpovídající certifikační prováděcí směrnici 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 (viz kapitola 2.2).

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

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

1.5.4 Postupy při schvalování souladu s bodem 1.5.3

V případě, že je potřebné provést změny v této politice a vytvořit její novou verzi, určuje ředitel společnosti První certifikační autorita, a.s. osobu, která je oprávněna tyto změny provádět. Nabytí platnosti nové verze CP (uvedeno v kapitole 10) předchází její schválení ředitelem společnosti První certifikační autorita, a.s.

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 použit jak plný text, tak i jeho zkratka, přičemž obojí má totožnou obsahovou hodnotu.

Tabulka 2 – Pojmy a zkratky

Pojem	Vysvětlení
bit	z anglického *binary digit* - číslice dvojkové soustavy je základní a současně nejmenší jednotkou informace používanou především v číslicové a výpočetní technice
CRL (Certification Revocation List)	seznam zneplatněných certifikátů
držitel certifikátu	fyzická osoba, právnická osoba nebo organizační složka státu, která požádala o vydání certifikátu pro sebe nebo pro označující osobu a které byl certifikát vydán
elektronický podpis, resp. elektronická značka	elektronickým podpisem údaje v elektronické podobě, které jsou připojené k datové zprávě nebo jsou s ní logicky spojené a které slouží jako metoda k jednoznačnému ověře-ní identity podepsané osoby ve vztahu k datové zprávě elektronickou značkou údaje v elektronické podobě, které jsou připojené k datové zprávě nebo jsou s ní logicky spojené a které splňují následující požadavky : 1. jsou jednoznačně spojené s označující osobou a umožňují její identifikaci prostřed-nictvím kvalifikovaného systémového certifikátu, 2. byly vytvořeny a připojeny k datové zprávě pomocí prostředků pro vytváření elek-tronických značek, které označující osoba může udržet pod svou výhradní kontrolou, 3. jsou k datové zprávě, ke které se vztahují, připojeny takovým způsobem, že je možné zjistit jakoukoli následnou změnu dat,
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 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	jedinečná data pro vytváření elektronického podpisu, resp. elektronické značky spolu s odpovídajícími daty pro ověřování elektronického podpisu, resp. elektronické značky
RA	registrační autorita
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, resp. elektronické značky
spoléhající se strana	subjekt, spoléhající se při své činnosti na certifikát, vydaný I.CA
veřejný klíč	jedinečná data pro ověřování elektronického podpisu, resp. elektronické značky
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)
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
ZoEP	Aktuální znění zákona č. 227/2000 Sb., o elektronickém podpisu a o změně některých dalších zákonů (zákon o elektronickém podpisu)

2 Odpovědnosti za zveřejňování a 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 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 (viz kapitoly 2.2 a 2.3) 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.

3 Identifikace a autentizace

3.1 Pojmenovávání

3.1.1 Typy jmen

Níže uvedené podkapitoly definují požadavky na obsah položek žádosti o certifikát, které budou následně po nezbytných kontrolách ve vydaném certifikátu (viz kapitola 7.1) obsaženy.

3.1.1.1 countryName (stát)

Povinná položka (např. CZ) může obsahovat pouze kód státu, v němž má žadatel o kvalifikovaný systémový certifikát:

- fyzická osoba nepodnikající – adresu trvalého pobytu podle primárního[2] osobního dokladu
- fyzická osoba podnikající, právnická osoba, organizační složka státu, zaměstnanec, atd. – adresu sídla/pracoviště dle výpisu z obchodního rejstříku, živnostenského listu, zřizovací listiny, atd.

V procesu kontroly žádosti o prvotní certifikát pracovník RA ověřuje správnost podle výše uvedených dokladů (pokud není kód státu explicitně uveden, uvede se kód státu, který předkládaný doklad vydal) a v případě neshody žádost odmítne. Kód státu musí odpovídat normě ISO 3166. V procesu kontroly žádosti o následný certifikát je postupováno v souladu s kapitolou 4, resp. s jejími relevantními podkapitolami.

Tato položka se v žádosti o certifikát a v jí odpovídajícím vydaném certifikátu musí vyskytnout právě jednou.

3.1.1.2 commonName (Obecné jméno)

Povinná položka může obsahovat :

- název zařízení (např. Příjem elektronické pošty), doménové jméno serveru (např. www.firma.cz) – v případě doménového jména serveru vyžaduje se hodnověrně doložený souhlas vlastníka nebo čestné prohlášení žadatele o certifikát, potvrzující vlastnictví doménového jména
- název fyzické osoby podnikající, právnické osoby, organizační složky státu, atd. (např. Společnost, a.s.) - dle výpisu z obchodního rejstříku, živnostenského listu, zřizovací listiny, atd.
- celé jméno žadatele o certifikát včetně titulů tak, jak je uvedeno v jeho primárním osobním dokladu (např. Ing. Petr Jan Holoubek Ph.D.), popř. v dalších předložených dokumentech; pokud žádost obsahuje titul, který není v předloženém osobním dokladu uveden, popř. nekoresponduje s titulem uvedeným v předloženém primárním osobním dokladu, je žadatel o certifikát povinen doložit oprávněnost použití uvedeného titulu nezpochybnitelným způsobem[3].

V procesu kontroly žádosti o prvotní certifikát pracovník RA ověřuje správnost dle výše uvedených dokumentů a pokud zjistí neshodu, žádost odmítne. V procesu kontroly žádosti o následný certifikát je postupováno v souladu s kapitolou 4, resp. s jejími relevantními podkapitolami. Položka, která může obsahovat znaky s diakritikou, se v žádosti o prvotní/následný certifikát a v jí odpovídajícím vydaném certifikátu musí vyskytnout právě jednou.

[2] Akceptovatelné primární, resp. sekundární doklady jsou uvedeny v relevantních podkapitolách kapitoly 3.2.
[3] Např. diplomem, ve kterém je uvedeno, že žadatel má právo daný titul používat.

3.1.1.3 stateOrProvinceName (kraj)

Nepovinná položka může obsahovat pouze označení nižšího územně správního celku, do něhož spadá:

- fyzická osoba nepodnikající – místo trvalého bydliště podle primárního osobního dokladu žadatele o kvalifikovaný systémový certifikát, tedy město, obec nebo jinou správní jednotku, která je v primárním osobním dokladu uvedena (např. Praha)
- fyzická osoba podnikající, právnická osoba, organizační složka státu, zaměstnanec atd. – místo sídla dle výpisu z obchodního rejstříku, živnostenského listu, zřizovací listiny, atd., tedy město, obec nebo jiná správní jednotka, která je v dokladu uvedena.

I.CA si vyhrazuje právo na základě písemné smlouvy s žadatelem o certifikát i jiný způsob naplnění a používání této položky.

V procesu kontroly žádosti o prvotní certifikát pracovník RA ověřuje správnost tohoto údaje v případě, že byl uveden, a pokud zjistí neshodu, danou žádost odmítne. V procesu kontroly žádosti o následný certifikát je postupováno v souladu s kapitolou 4, resp. s jejími relevantními podkapitolami.

Tato položka, která může obsahovat znaky s diakritikou, se v žádosti o certifikát a v jí odpovídajícím vydaném certifikátu může vyskytnout maximálně jednou.

3.1.1.4 localityName (místo)

Nepovinná položka může obsahovat:

- fyzická osoba nepodnikající – místo trvalého bydliště podle primárního osobního dokladu (např. Praha 7, Ovenecká 1047/17 17000) žadatele o certifikát, které je v primárním osobním dokladu uvedeno
- fyzická osoba podnikající, právnická osoba, organizační složka státu, zaměstnanec, atd. – místo sídla dle výpisu z obchodního rejstříku, živnostenského listu, zřizovací listiny, atd.

I.CA si vyhrazuje právo na základě písemné smlouvy s žadatelem o certifikát i jiný způsob naplnění a používání této položky.

V procesu kontroly žádosti o prvotní certifikát pracovník RA ověřuje správnost tohoto údaje v případě, že byl uveden, a pokud zjistí neshodu, danou žádost odmítne. V procesu kontroly žádosti o následný certifikát je postupováno v souladu s kapitolou 4, resp. s jejími relevantními podkapitolami.

Tato položka, která může obsahovat znaky s diakritikou, se v žádosti o certifikát a v jí odpovídajícím vydaném certifikátu může vyskytnout maximálně jednou.

3.1.1.5 organizationName (organizace)

Položka (povinnost/nepovinnost naplnění závisí na typu certifikátu) může obsahovat pouze obchodní název (např. Společnost, a.s.) podle výpisu z obchodního rejstříku nebo jiného zákonem určeného rejstříku/registru, živnostenského listu, zřizovací listiny atd. - žadatel o certifikát je povinen doložit oprávněnost použití obsahu položky nezpochybnitelným způsobem[4] .

I.CA si vyhrazuje právo na základě písemné smlouvy se žadatelem o certifikát i jiný způsob naplnění této položky (např. pro zajištění shody s požadavky technických standardů).

V procesu kontroly žádosti o prvotní certifikát pracovník RA ověřuje správnost tohoto údaje v případě, že byl uveden, a pokud zjistí neshodu, danou žádost odmítne. V procesu kontroly žádosti o následný certifikát je postupováno v souladu s kapitolou 4, resp. s jejími relevantními podkapitolami.

[4] Např. v případě obchodního jména živnostníka patřičným živnostenským listem, v případě, že podepisující osoba je majitelem firmy, společníkem nebo zaměstnancem pak výpisem z obchodního rejstříku.

Tato položka, která může obsahovat znaky s diakritikou, se v žádosti o certifikát a v jí odpovídajícím vydaném certifikátu může vyskytnout maximálně jednou.

3.1.1.6 organizationUnitName (organizační jednotka)

Nepovinná položka může obsahovat název nebo identifikátor.

V procesu kontroly žádosti o prvotní certifikát pracovník RA ověřuje správnost tohoto údaje v případě, že byl uveden a doložen, potvrzením o zaměstnání a pokud zjistí neshodu, danou žádost odmítne. V procesu kontroly žádosti o následný certifikát je postupováno v souladu s kapitolou 4, resp. s jejími relevantními podkapitolami.

I.CA si vyhrazuje právo na základě písemné smlouvy s žadatelem o certifikát i jiný způsob naplnění a používání této položky.

Tato položka, která může obsahovat znaky s diakritikou, se v žádosti o certifikát a v jí odpovídajícím vydaném certifikátu může vyskytnout vícekrát.

3.1.1.7 emailAddress (elektronická poštovní adresa)

V žádosti o prvotní certifikát se tato položka nesmí vyskytnout, v procesu kontroly žádosti o následný certifikát a v jí odpovídajícím vydaném certifikátu je postupováno v souladu s kapitolami 3.1.1.13 a 4, resp. s jejími relevantními podkapitolami.

3.1.1.8 initials (iniciály)

Nepovinná položka může obsahovat pouze iniciály úplného jména žadatele o certifikát (např. PJH).

V procesu kontroly žádosti o prvotní certifikát pracovník RA ověřuje správnost tohoto údaje v případě, že byl uveden, a pokud zjistí neshodu oproti primárnímu dokladu, danou žádost odmítne. V procesu kontroly žádosti o následný certifikát je postupováno v souladu s kapitolou 4, resp. s jejími relevantními podkapitolami.

Tato položka, která může obsahovat znaky s diakritikou, se v žádosti o certifikát a v jí odpovídajícím vydaném certifikátu může vyskytnout maximálně jednou.

3.1.1.9 name (jméno)

Nepovinná položka (např. Ing. Petr Jan Holoubek PhD) může obsahovat celé jméno žadatele o certifikát včetně titulů tak, jak je uvedeno v jeho primárním osobním dokladu, popř. v dalších dokumentech. V procesu kontroly žádosti o prvotní certifikát pracovník RA ověřuje správnost dle výše uvedených dokumentů a pokud zjistí neshodu, žádost odmítne. Pokud žádost obsahuje titul, který není uveden, popř. nekoresponduje s titulem uvedeným v předloženém primárním osobním dokladu, je žadatel o certifikát povinen doložit oprávněnost použití uvedeného titulu nezpochybnitelným způsobem. V procesu kontroly žádosti o následný certifikát je postupováno v souladu s kapitolou 4, resp. s jejími relevantními podkapitolami. Položka, která může obsahovat znaky s diakritikou, se v žádosti o prvotní/následný certifikát a v jí odpovídajícím vydaném certifikátu musí vyskytnout maximálně jednou.

3.1.1.10 title (titul)

Obsahem nepovinné položky může být např. postavení žadatele o certifikát v určité (zpravidla firemní) hierarchii, identifikátor nebo v případě komunikace orgánů veřejné moci označení příslušných právních předpisů. I.CA si vyhrazuje právo na základě písemné smlouvy se žadatelem o certifikát i jiný způsob naplnění a používání této položky.

V procesu kontroly žádosti o prvotní certifikát je obsah této položky pracovníkem RA ověřován v závislosti na skutečnostech, které jsou v něm obsaženy[5]. V procesu kontroly žádosti o následný certifikát je postupováno v souladu s kapitolou 4, resp. s jejími relevantními podkapitolami.

Tato položka, která může obsahovat znaky s diakritikou, se v žádosti o certifikát a v jí odpovídajícím vydaném certifikátu může vyskytnout vícekrát.

3.1.1.11 serialNumber (sériové číslo subjektu)

Jedinečné číslo předmětu, sloužící k rozlišení klientů I.CA, obecně vyplňuje I.CA a je naplněno řetězcem „ICA - “ a za něj připojeno na řetězec převedené identifikační číslo žadatele o certifikát. V případě certifikátu vydaného v souladu s touto CP se v žádosti o prvotní certifikát vyskytnout nesmí, v žádosti o následný certifikát a v jí odpovídajícím vydaném certifikátu se musí vyskytnout právě jednou.

3.1.1.12 generationQualifier (generační rozlišení)

Nepovinná položka se používá pro označení umístění v rodinném stromu (např. Ml., St.).

V procesu kontroly žádosti o prvotní certifikát pracovník RA správnost tohoto údaje v případě, že byl uveden, neověřuje, nejsou však povoleny výrazy vulgární, propagující fašismus, rasovou a třídní nenávist. V procesu kontroly žádosti o následný certifikát je postupováno v souladu s kapitolou 4, resp. s jejími relevantními podkapitolami.

I.CA si vyhrazuje právo na základě písemné smlouvy se žadatelem o certifikát i jiný způsob naplnění této položky.

Tato položka, která může obsahovat znaky s diakritikou, se v žádosti o certifikát a v jí odpovídajícím vydaném certifikátu může vyskytnout maximálně jednou.

3.1.1.13 Subject Alternative Name (alternativní jméno předmětu)

Pokud žadatel o certifikát použil alternativní jméno předmětu, je nutno ověřit skutečnosti v něm uváděné (pokud se jedná o skutečnosti vyžadující ověření). Jako součást alternativního jména se připouští :

- ***otherName*** *(ostatní) :* Microsoft Universal Principal Name (UPN) – v případě žádosti o prvotní certifikát se tato položka nesmí vyskytnout. V případě žádosti o následný certifikát a v jí odpovídajícím vydaném certifikátu je postupováno v souladu s kapitolou 4, resp. s jejími relevantními podkapitolami.
- ***rfc822Name*** *(elektronická adresa, např. holy@quick.cz),* nepovinná položka :
  - prvotní certifikát: může obsahovat pouze elektronickou poštovní adresu ve formátu RFC 822 žadatele o certifikát
  - následné certifikáty:
    - pokud není tato položka vyplněna, pak pokud je naplněna položka emailAddress (viz kapitola 3.1.1.7, provede I.CA naplnění položky rfc882Name obsahem položky emailAddress
    - pokud je tato položka vyplněna a současně je naplněna i položka emailAddress, pak pokud je jejich obsah rozdílný, doplní I.CA do druhé instance položky rfc882Name obsah položky emailAddress
- ***dNSName*** *(jméno doménového serveru, např. www.server.cz)*: nepovinná položka
- ***uniformResourceIdentifier*** *(URI, např. http://www.moje.cz)*: nepovinná položka
- ***iPAddress*** *(IP adresa, např. 81.91.85.214)*: nepovinná položka

V procesu kontroly žádosti o prvotní certifikát je vyžadováno buď hodnověrně doložené vlastnictví elektronické poštovní adresy, doménového jména serveru, URI nebo IP adresy, nebo čestné prohlášení[6]

[5] Pokud žadatel požaduje obsah „Praktický lékař“, je možné žádost přijmout, pokud prokáže, že je praktickým lékařem; pokud bude požadovat obsah typu „Linuxový guru“, toto nelze zkontrolovat a žádost se zamítne.

žadatele o certifikát, v němž toto vlastnictví potvrzuje - v případě nesplnění této podmínky má pracovník RA právo danou žádost odmítnout. V procesu kontroly žádosti o následný certifikát je postupováno v souladu s kapitolou 4, resp. s jejími relevantními podkapitolami.

Jednotlivé uvedené položky se v rámci alternativního jména mohou vyskytnout jednou nebo vícekrát, případně se nemusí vyskytnout vůbec. I.CA může bez udání důvodu množinu uvedených položek omezit, případně rozšířit.

3.1.2 Požadavek na významovost jmen

Význam a obsah naplnění jednotlivých položek je upřesněn v podkapitolách kapitoly 3.1.1.

3.1.3 Anonymita a používání pseudonymu

Tyto skutečnosti jsou pro aplikaci vydání tohoto dokumentu irelevantní.

3.1.4 Pravidla pro interpretaci různých forem jmen

Pokud se jedná o jména nebo jiné skutečnosti, které jsou uvedeny v osobním dokladu fyzické osoby nebo v jiných dokumentech, které jsou přípustné pro prokazování identity, případně vztahu fyzické osoby k právnické osobě, přenášejí se tato jména v té podobě, v jaké jsou v dokumentu uvedena. Vlastní transkripce se zásadně pro účely vydávání certifikátů neprovádí. V případě žádosti o prvotní certifikát je pro kódování základních položek striktně vyžadován typ UTF8String s výjimkou položek countryName, serialNumber (typ PrintableString) a položek rfc822Name, dNSName , uniformResourceIdentifier (typ IA5String) a iPAddress (OctetString). Délka obsahu jednotlivých položek se řídí platnými technickými standardy. V případě žádosti o následný certifikát akceptuje I.CA výskyt a kódování položky použité v předchozím (obnovovaném) certifikátu, případně může změnit kódování na typ uvedený ve výše uvedeném odstavci.

3.1.5 Jedinečnost jmen

Jednoznačnost jména subjektu je zaručena použitím výše definovaného postupu pro tvorbu položky SerialNumber (viz kapitola 3.1.1.11). 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 systémového certifikátu, I.CA upozorní žadatele a požádá ho, aby některý z požadovaných údajů změnil či doplnil. Pokud žadatel toto neučiní, kvalifikovaný systémový certifikát se mu nevydá.

3.1.6 Obchodní značky

I.CA uznává pouze ty ochranné známky, jejichž vlastnictví nebo pronájem žadatel doložil. Autentizaci ochranných známek jinými způsoby I.CA neprovádí. Veškeré důsledky plynoucí z neoprávněného užívání ochranné známky nese žadatel o certifikát.

---

[6] Čestné prohlášení pro účely této položky je realizováno formou stvrzení pravdivosti údajů ve smlouvě o vydání kvalifikovaného certifikátu.

3.2 Počáteční ověření identity

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 značek, odpovídajících datům pro ověřování elektronických značek, která daná žádost o certifikát (struktura PKCS#10) obsahuje a která budou obsažena ve vydaném certifikátu, se prokazuje předložením žádosti o certifikát ověřujícímu subjektu, kterým může být pracovník registrační nebo certifikační autority. S ohledem na skutečnost, že tato žádost je elektronicky označena daty pro vytváření elektronických značek (tzv. soukromý klíč), odpovídajících datům pro ověřování elektronických značek (tzv. veřejný klíč) obsažených v žádosti, dokazuje tímto způsobem žadatel o certifikát, že v době tvorby elektronické 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

I.CA vyžaduje od žadatele o certifikát předložení jeho následujících údajů :

- 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).

Pokud dojde během trvání smluvního vztahu k I.CA ke změnám ve výše uvedených údajích nebo v údajích, uvedených v certifikátu, je držitel certifikátu, resp. podepisující osoba povinna tyto změny ohlásit I.CA. Požadavky při registraci žadatele o prvotní certifikát jsou uvedeny v kapitolách 3.2.3.1 až 3.2.3.3.

3.2.3.1 Fyzická osoba nepodnikající

3.2.3.1.1 Předkládané doklady na RA

V případě, že se **žadatel dostaví osobně na RA**, předkládá žadatel o certifikát následující typy dokladů:

- Originál platného primárního osobního dokladu žadatele a originál dalšího osobního dokladu (sekundárního). Primární osobní doklad pro občany České republiky musí být občanský průkaz, platný cestovní pas, popř. obdobný doklad stejné právní váhy. Primární osobní doklad pro cizince je platný cestovní pas, popř. obdobný doklad stejné právní váhy. Občané Slovenské republiky mohou jako primární osobní doklad použít občanský průkaz. Sekundární osobní doklad musí být vydán orgánem veřejné moci nebo jinou organizací, jejíž existenci lze doložit. Sekundární osobní doklad musí obsahovat celé občanské jméno fyzické osoby žadatele o certifikát a dále nejméně jeden z následujících údajů:
    - datum narození žadatele (nebo rodné číslo u občanů České republiky nebo Slovenské republiky)
    - adresa trvalého bydliště žadatele

- fotografii obličeje žadatele

Údaje požadované v sekundárním osobním dokladu musí být shodné s těmito údaji v primárním osobním dokladu. O shodnosti rozhoduje pracovník RA. Pokud žadatel nepředloží dva osobní doklady výše popsané kvality, nebude žádost přijata. Příkladem akceptovatelného sekundárního osobního dokladu jsou např. cestovní pas, řidičský průkaz, služební průkazy státních úřadů, průkaz poslance, služební průkaz policie, zbrojní průkaz, vojenská knížka, průkaz zdravotního pojištění, průkazka hromadné dopravy, firemní průkazky, studentský průkaz atd.

V případě, že je **žadatel na RA zastupován zmocněncem**, předkládá zmocněnec následující typy dokladů:

- Originály platného primárního osobního dokladu a dalšího osobního dokladu (sekundárního) zmocněnce (kvalita primárního a sekundárního dokladu je uvedena výše)
- Originály, případně úředně ověřené kopie primárního a sekundárního osobního dokladu žadatele o certifikát (kvalita primárního a sekundárního dokladu je uvedena výše)
- Plná moc (nerozhodne-li ředitel I.CA jinak) s úředně ověřeným podpisem zmocnitele - pokud je plná moc v cizím jazyce (kromě slovenštiny), musí být přeložena do češtiny úředním překladatelem (v zahraničí[7] provedené úřední ověření podpisů musí být tzv. „superlegalizováno“, tj. potvrzeno zastupitelským úřadem České republiky v zemi původu plné moci; v případě dokladů, ověřených v zemích uvedených na http://www.hcch.net/, nemusí být superlegalizace provedena[8]
- Pokud je žadatel zákonným zástupcem[9] klienta, požaduje se o tom úřední doklad:
  - Rodiče nebo osvojitelé zastupují své nezletilé děti - protože nezletilec má omezenou svéprávnost, smlouvy s I.CA za něj musí uzavírat jeho zákonný zástupce. Dokladem je rodný list dítěte. Osvojení se dokládá buď výpisem z matriky nebo rozhodnutím soudu. Ve všech uvedených případech postačí záznam o dítěti v občanském průkazu.
  - Poručník nebo opatrovník je osobám bez plné způsobilosti k právním úkonům, včetně dospělých, ustanoven soudem. Dokladem je soudní rozhodnutí.
    - Opatrovníkem nebo poručníkem dítěte může být ustanoven také orgán sociálně-právní ochrany dítěte (zpravidla obec nebo obcí zřízený veřejný opatrovník). V tom případě jde o právnickou osobou a vedle usnesení soudu dokládá ještě skutečnosti, vztahující se k právnickým osobám.
    - Opatrovník může být ustanoven také osobám s tělesným postižením, které nemají omezenou svéprávnost, ale potřebují při právních úkonech asistenci (např. nevidomým).

3.2.3.1.2 Kontrolované a ověřované doklady na RA

V případě, že se žadatel **dostaví osobně na RA**, je pracovníkem RA kontrolováno a ověřováno:

- Zda osoba, která je uvedena v žádosti o certifikát, je totožná s osobou žadatele (dle platného primárního dokladu) a že údaje uvedené v žádosti odpovídají údajům v předložených dokladech. Shoda je nutná u těchto údajů:
  - příjmení, jméno
  - bydliště (město)

[7] Podle slovenského zákona smí ověřování dokladů pro použití v cizině provádět pouze notář - § 2 zákona NÁRODNEJ RADY SLOVENSKEJ REPUBLIKY ze dne 22.12.1992.

[8] Vv tomto případě je třeba postupovat individuálně, ve spolupráci s žadatelem o certifikát , resp. spoluprací pracovníka RA s I.CA.

[9] Zákonným zástupcem dítěte není pro účely ZoEP pěstoun.

- oblast (ulice, pokud je uvedena)

- Plnoletost žadatele
- Platnost předkládaných dokladů
- Pokud se žadatel prokazuje cestovním pasem, kontrola na shodu bydliště se neprovádí
- Příslušník cizího státu musí splňovat podmínky pro právní subjektivitu a svéprávnost alespoň podle práva CZ - pokud je nesplňuje, je třeba ověřit, zda splňuje podmínky podle práva státu jehož je příslušníkem. V takovém případě je třeba postupovat individuálně, ve spolupráci s žadatelem a I.CA.

V případě, že je žadatel na RA zastupován zmocněncem, jsou dále kontrolovány:

- shoda údajů o žadateli, uvedených v žádosti o službu a na plné moci (není-li smluvně zajištěno jinak), resp. dokladu o zákonném zastupování
- platnost a správnost předložených dokladů zástupce s údaji na plné moci (není-li smluvně zajištěno jinak), resp. dokladu o zákonném zastupování a oprávněnost k podání žádané služby

3.2.3.2 Fyzická osoba podnikající (OSVČ) nebo zaměstnanec

3.2.3.2.1 Předkládané doklady na RA

- Doklady ve stejném rozsahu jako v kapitole 3.2.3.1.1
- Doklad uvedený v kapitole 0. Pokud je tento doklad v cizím jazyce, platí pro ověření pravidla, uvedená v kapitole 3.2.3.1.
- V případě zaměstnance - potvrzení o zaměstnaneckém poměru k danému zaměstnavateli, pokud není uzavřena s I.CA rámcová smlouva. Potvrzení musí být opatřeno podpisem osoby s právem jednání za příslušného zaměstnavatele. Pokud tato osoba není osobou oprávněnou k zastupování zaměstnavatele, tj. není statutárním zástupcem (není uveden na výpisu z obchodního rejstříku nebo jiného zákonem určeného rejstříku nebo registru, živnostenský list, zřizovací listina, atd. jako osoba oprávněná jednat), požaduje se navíc úředně ověřený doklad (plná moc, pověření, doklad o zákonném zastupování) podepsaný statutárním zástupcem zaměstnavatele, potvrzující oprávněnost této osoby jednat za zaměstnavatele.

3.2.3.2.2 Kontrolované a ověřované doklady na RA

Pracovníkem RA je kontrolováno a ověřováno:

- zda údaje, uvedené v žádosti o certifikát, se shodují s údaji v dokladech předložených žadatelem, resp. zmocněncem - při kontrole postupuje pracovník RA stejně jako u fyzické osoby nepodnikající
- potvrzení o zaměstnaneckém poměru k danému zaměstnavateli
- zda je osoba, podepisující potvrzení o zaměstnaneckém poměru, uvedená v úředně ověřeném dokladu (plná moc, pověření, doklad o zákonném zastupování), oprávněna zastupovat zaměstnavatele - pracovník RA musí zkontrolovat, zda tato osoba má právo takovéto pověření provést, popřípadě zda uděluje plnou moc oprávněné osobě v souladu s výpisem výše uvedených dokumentů[10] (v případě fyzické/právnické osoby se jedná o výpis z obchodního nebo jiného zákonem předepsaného rejstříku, živnostenského listu, zřizovací listiny, zákona atd., v případě organizační složky státu/orgánu veřejné moci se jedná o zvláštní právní předpisy)

[10] Pokud je na výpisu z obchodního rejstříku uvedeno např. že"podpisové právo za společnost má předseda představenstva spolu s dalším členem představenstva" znamená to, že plnou moc může udělit pouze předseda představenstva spolu s dalším členem představenstva (tudíž musí být na plné moci ověřené podpisy těchto dvou osob).

3.2.3.3 Organizační složku státu (např. elektronická podatelna - orgán veřejné moci) a ostatní právnické osoby

V případě, že zástupcem organizační složky státu, resp. právnické osoby, jakožto žadatele o kvalifikovaný systémový certifikát, je její zaměstnanec, je postupováno v souladu s kapitolou 3.2.3.1.2.

V případě, že organizační složka státu, resp. právnická osob pověří zastupováním třetí stranu na základě smluvního vztahu, platí relevantní požadavky předchozích kapitol.

3.2.4 Neověřené informace vztahující se k držiteli certifikátu nebo označující osobě

V případě informací, které se nedají ověřit, je postupováno v souladu s relevantními podkapitolami kapitoly 3.1.2.

3.2.5 Ověřování specifických práv

Viz kapitola 3.1.1.2 odstavec *název zařízení*.

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“)

Identifikace a autentizace žadatele o vydání následného certifikátu (struktura PKCS#10) je prováděna ověřením elektronického značky žádosti o vydání následného kvalifikovaného systémového certifikátu – v procesu ověřování elektronické značky žádosti o tento certifikát musí být použit platný kvalifikovaný systémový certifikát vydaný dle dokumentu Certifikační politika vydávání kvalifikovaných systémových certifikátů - verze 3.0 a vyšší, ke kterému je vydáván tento následný certifikát nebo musí být použit platný kvalifikovaný certifikát pro obnovu (tzv. „podpisový certifikát“, volitelně vydávaný např. v procesu žádosti o kvalifikovaný systémový certifikát) a vydaný dle dokumentu Certifikační politika vydávání kvalifikovaných certifikátů - verze 3.0 a vyšší.

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

V případě **osobního předání žádosti o zneplatnění certifikátu na RA,** musí žadatel o zneplatnění certifikátu prokázat, že je držitelem tohoto certifikátu. V případě, že je zastupován zmocněncem, platí ustanovení kapitoly 3.2.3.1. Žádost o zneplatnění certifikátu musí být písemná a podepsaná žadatelem.

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

- elektronicky označená, resp. podepsaná elektronická zpráva - (revoke@ica.cz), elektronická značka musí být realizována daty pro vytváření elektronické značky příslušnými k předmětnému certifikátu, jenž má být zneplatněn, resp. elektronický podpis musí být realizován daty pro vytváření elektronického podpisu příslušnými k datům pro ověřování elektronického podpisu, obsažených ve vydaném kvalifikovaném certifikátu pro obnovu k tomuto kvalifikovanému systémovému certifikátu, jenž má být zneplatněn
- elektronicky nepodepsaná elektronická zpráva, obsahující heslo pro zneplatnění certifikátu - (revoke@ica.cz)
- prostřednictvím formuláře na internetové informační adrese (http://www.ica.cz)
- prostřednictvím datové schránky.

V případě použití **listovní zásilky o zneplatnění certifikátu** musí být tato zaslána doporučeně na adresu sídla společnosti (viz kapitola 2.2).

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

4 Požadavky na životní cyklus certifikátu

4.1 Žádost o vydání certifikátu

4.1.1 Subjekty oprávněné podat žádost o vydání certifikátu

Vydávání certifikátů I.CA je komerčně nabízenou službou každému subjektu, který se smluvně zaváže jednat podle této CP.

I.CA požaduje minimální věk 18 let pro osobu, která žádá o certifikát. Žadatelé o certifikát ve věku od 15 do 18 let musí žádat prostřednictvím svého zákonného zástupce.

Pokud je žadatel zastupován zmocněncem, musí mít zmocněnec oprávnění žadatele zastupovat.

4.1.2 Registrační proces a odpovědnosti poskytovatele a žadatele

Registrační proces, včetně odpovědností jak poskytovatele kvalifikované certifikační služby, tak žadatele o tuto službu, jsou uvedeny v následujících kapitolách.

4.2 Zpracování žádosti o certifikát

4.2.1 Identifikace a autentizace

Podporované hashovací funkce, využívané při tvorbě elektronické značky žádosti o certifikát a hashovací funkce použité v procesu vydávání tohoto certifikátu : žádost SHA-256 -> vydaný certifikát SHA-256, žádost SHA-512 -> vydaný certifikát SHA-512.

V případě, že žádost o certifikát bude využívat jinou než výše uvedenou hashovací funkci, nebude certifikát vydán.

Žadatel o **prvotní certifikát** vytvoří žádost o vydání certifikátu (struktura PKCS#10) a po jejím uložení na záznamové médium se žadatel, popř. zmocněnec s touto žádostí a potřebnými doklady dostaví na RA. Následující proces identifikace a autentizace pracovníkem RA zahrnuje následující fáze:

1. Ověření vlastnictví dat pro vytváření elektronických značek (viz kapitola 3.2.1) – pracovník RA tuto skutečnost kontroluje prostřednictvím speciálního aplikačního programového vybavení takovým způsobem, že pomocí dat pro ověřování elektronických značek, uvedených v žádosti o certifikát, ověří platnost elektronické značky na této žádosti. Pokud je ověření platnosti elektronické značky negativní, RA žádost nepřijme a řízení k vydání certifikátu ukončí.
2. Kontrola předložených originálů osobních dokladů žadatele o certifikát, popř. zmocněnce (viz kapitola 3.2.3.1). V případě pochybností o pravosti předloženého primárního osobního dokladu žadatele o certifikát, popř. zmocněnce je proces vydávání certifikátu ukončen. V případě pochybností o pravosti předloženého sekundárního osobního dokladu nebo v případě neshody vyžadovaných údajů s primárním osobním dokladem, je žadatel o certifikát, popř. zmocněnec požádán o předložení jiného sekundárního osobního dokladu. Pokud žadatel o certifikát, popř. zmocněnec nepředloží sekundární osobní doklad požadovaných vlastností, pracovník RA žadatele o certifikát, popř. zmocněnce odmítne a proces vydávání certifikátu ukončí.
3. S ohledem na typ vydávaného certifikátu následuje kontrola dalších dokladů – viz relevantní podkapitoly 3.2.
4. Kontrola údajů obsažených v žádosti o certifikát s údaji obsaženými v předkládaných dokladech žadatele o certifikát. V případě neshody pracovník RA žadatele o certifikát, popř. zmocněnce odmítne a proces vydávání certifikátu ukončí.
5. Kontrola existence hesla pro zneplatnění (lze zadat jak v průběhu tvorby žádosti o certifikát, tak prostřednictvím pracovníka RA v průběhu formálních kontrol žádosti o certifikát) a jeho kvality

(požadované parametry - minimální/maximální délka hesla 4/32 znaků, povolené znaky 0..9, A..Z, a..z). Toto heslo bude držitelem certifikátu použito při případném zneplatnění certifikátu.

Žadatel o **následný certifikát** vytvoří žádost o vydání certifikátu (struktura PKCS#10), splňující následující požadavky :

1. položky atributu Subject (viz kapitola 7.1.1) musí být totožné jako v certifikátu, ke kterému je tento následný certifikát požadován
2. data pro ověřování elektronických značek (veřejný klíč) musí být jiná než v původním certifikátu
3. ostatní položky žádosti podléhají aktuálním pravidlům pro vydávání certifikátů dle této CP
4. Pro kvalitu hesla na zneplatnění certifikátu akceptuje I.CA jednu z následujících možností - povolené znaky 0..9, A..Z, a..z, minimální/maximální délka 4znaky/32 znaků, nebo heslo pro zneplatnění následného certifikátu může být totožné jako heslo pro zneplatnění následného certifikátu
5. vlastnictví dat pro vytváření elektronických značek je (soukromý klíč) prokazováno způsobem uvedeným v kapitole 3.2.1

a zvolí jeden z níže uvedených postupů:

1. osobní dostavení se žadatele o certifikát, resp. jeho zmocněnce na RA – postup je totožný jako při vydávání prvotního certifikátu
2. bez nutnosti osobního dostavení se žadatele o certifikát na RA – v rámci kontrol v procesu vydání následného certifikátu elektronickou cestou jsou využívána také párová data, která jsou předmětem výměny, resp. „podpisový certifikát“ (viz kapitola 3.3.1)

4.2.2 Přijetí nebo odmítnutí žádosti o certifikát

V případě, že je výsledek kontrol (viz relevantní části kapitoly 4.2.1) procesu žádání o **prvotní certifikát** pozitivní, pracovník RA okopíruje předložené osobní doklady, resp. úředně ověřené kopie (není-li smluvně stanoveno jinak). Dokument „Protokol o podání žádosti na vydání kvalifikovaného systémového 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 kvalifikovaný 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 provozního pracoviště certifikační autority nezbytné kontroly (zejména formální správnost údajů obsažených v žádosti, řádné naplnění položek žádosti) a další činnosti (komunikace s pracovníky RA atd.).

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

V procesu vydávání **prvotního certifikátu** je žadatel o certifikát, popř. zmocněnec informován prostřednictvím pracovníka RA a v případě, že byla v žádosti uvedena elektronická adresa, je vydaný certifikátna tuto adresu taktéž zaslán.

V případě, že žadatel o tento typ **následného certifikátu** zaslal žádost elektronickou cestou a je známa jeho elektronická poštovní adresa, je mu následný certifikát na tuto adresu elektronicky zaslán.

4.4 Převzetí vydaného certifikátu

4.4.1 Úkony spojené s převzetím certifikátu

Pokud byly splněny podmínky pro vydání **prvotního certifikátu**, tzn.:

- splněny podmínky registrace
- zaplacení určeného poplatku (není-li smluvně stanoveno jinak)
- prokázání vlastnictví dat pro vytváření elektronických značek odpovídající datům pro ověřování elektronických značek, která bude vydaný certifikát obsahovat
- podepsání příslušné smlouvy

je povinností žadatele o certifikát tento certifikát přijmout. Jediným způsobem, jakým může žadatel postupovat v případě, že tento certifikát nemá zájem převzít, je zažádat v souladu s touto CP o jeho zneplatnění. Pracovník RA předá žadateli záznamové médium obsahující požadovaný certifikát a odpovídající certifikát CA (v předepsaných formátech). V případě, že byla v žádosti uvedena elektronická adresa, jsou vydaný certifikát a kořenový certifikát I.CA (v předepsaných formátech) na tuto adresu taktéž zaslány.

V případě podání žádosti o vydání **následného certifikátu** elektronickou cestou, zašle I.CA na žadatelovu elektronickou adresu vydaný certifikát a odpovídající kořenový certifikát I.CA, v případě vyřizování žádosti na RA, získá žadatel vydaný certifikát, popř. odpovídající kořenový certifikát I.CA od pracovníka RA.

Tuto CP získá žadatel na RA, popř. ji může stáhnout z informační adresy.

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

4.4.2 Zveřejňování vydaných certifikátů poskytovatelem

I.CA je povinna zajistit neprodlené zveřejnění vydaných certifikátů, vyjma takových, u kterých si klient vymínil, že nebudou zveřejňovány.

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, podepisující nebo označující osobou

Držitelé certifikátů a podepisující osoby jsou zejména povinni:

- bez zbytečného odkladu podávat přesné, pravdivé a úplné informace I.CA ve vztahu k vydanému certifikátu
- dodržovat veškerá relevantní ustanovení smlouvy o poskytování kvalifikované certifikační služby
- seznámit se s relevantními ustanoveními příslušné smlouvy o poskytování kvalifikované certifikační služby o vydání a používání certifikátu případné podepisující osoby a dbát na jejich dodržování ze strany těchto osob
- zacházet s prostředky jakož i s daty pro vytváření zaručeného elektronického podpisu, resp. elektronické značky s náležitou péčí tak, aby nemohlo dojít k jejich neoprávněnému použití
- uvědomit neprodleně poskytovatele certifikačních služeb, který vydal tento certifikát (tzn. I.CA), o tom, že hrozí nebezpečí zneužití jejich dat pro vytváření elektronického podpisu, resp. elektronické značky
- využívat data pro vytváření elektronických podpisů, resp. elektronických značek související s vydaným certifikátem v souladu s ustanoveními příslušných certifikačních politik
- při činnostech, souvisejících s daty pro vytváření zaručeného elektronického podpisu, resp. elektronické značky dodržovat veškerá relevantní ustanovení ZoEP, VoEP a příslušných certifikačních politik.

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 elektronická značka je platná a odpovídající certifikát nebyl zneplatněn
- dodržovat veškerá ustanovení této CP, v souladu se kterou byl využívaný certifikát vydán
- při činnostech souvisejících s používáním vydaného certifikátu dodržovat veškerá relevantní ustanovení ZoEP, VoEP a této 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 značek a novou dobou platnosti.

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, 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 uplynutím platnosti tohoto certifikátu informace o této skutečnosti spolu s návodem, jak postupovat v případě žádosti o tento typ následného certifikátu, zaslána na uvedenou adresu.

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 značek 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 značek jsou oprávněni požadovat držitelé certifikátu.

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

Pokud je ověření elektronických značek pozitivní (viz relevantní části kapitol 3.3.1, 4.2.1) a obsah položek žádosti o výměnu dat pro ověřování elektronických značek v certifikátu splňuje požadavky uvedené v kapitole 3.3.1, je postupováno v souladu s kapitolou 4.3, 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

Služba není poskytována.

4.8.1 Podmínky pro změnu údajů v certifikátu

Služba není poskytována.

4.8.2 Subjekty oprávněné požadovat změnu údajů v certifikátu

Služba není poskytována.

4.8.3 Zpracování požadavku na změnu údajů v certifikátu

Služba není poskytována.

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

Služba není poskytována.

4.8.5 Úkony spojené s převzetím certifikátu se změněnými údaji

Služba není poskytována.

4.8.6 Zveřejnění vydaných certifikátů se změněnými údaji

Služba není poskytována.

4.8.7 Oznámení o vydání certifikátu se změněnými údaji jiným subjektům

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 detailně 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 značek
- porušení ustanovení smlouvy o poskytování kvalifikované certifikační služby ze strany držitele certifikátu, resp. označující/podepisující osoby
- žádost držitele nebo označující/podepisující osoby
- nastanou-li skutečnosti uvedené v ZoEP a VoEP (např. neplatnost údajů v certifikátů).

I.CA si vyhrazuje právo akceptování i jiných 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 nebo hexadecimální tvaru (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 (nesprávné 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 označená/podepsaná 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 nebo hexadecimálním tvaru (uvozeno řetězcem „0x“)

- elektronicky neoznačená/nepodepsaná 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 nebo hexadecimálním tvaru (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 žádosti o zneplatnění certifikátu** musí být v zásilce uvedena žádost v následujícím tvaru (v českém 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 nebo hexadecimálním tvaru (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, že je 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[11]. Maximální prodlení mezi zneplatněním certifikátu a zveřejněním seznamu zneplatněných certifikátů, na kterém je tento certifikát poprvé uveden, je nejvýše 24hodin.

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 značky jsou platné a jim odpovídající certifikáty nebyly zneplatněny. Pro tyto účely jsou spoléhající se strany povinny používat CRL, vydaná a elektronicky označená 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, nejvýše 24 hodin od vydání předchozího CRL (zpravidla à 8 hodin).

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.

[11] 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.

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).

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 osobu

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

- skončila platnost certifikátu, aniž by bylo v souladu s touto 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 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 certifikáty a seznamy zneplatněných certifikátů
- veškeré procesy poskytování certifikačních služeb v oblasti vydávaní certifikátů dle ZoEP a VoEP

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

5.1 Fyzická bezpečnost

5.1.1 Umístění a konstrukce

Objekt provozního pracoviště je umístěn v geograficky odlišné lokalitě než ředitelství společnosti, obchodní a vývojová pracoviště, pracovišť registračních autorit a obchodních míst.

Zařízení, určená k výkonu hlavních kvalifikovaných certifikačních služeb v oblasti vydávání kvalifikovaných certifikátů nebo kvalifikovaných systémových certifikátů, jsou umístěna ve vyhrazených prostorách provozního pracoviště. Tyto prostory jsou zabezpečené obdobně jako zabezpečené oblasti kategorie „Důvěrné“.

5.1.2 Fyzický přístup

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

5.1.3 Elektřina a klimatizace

V prostorách, určených k výkonu hlavních kvalifikovaných certifikačních služeb v oblasti vydávání kvalifikovaných certifikátů nebo kvalifikovaných systémových certifikátů, 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), resp. diesel agregátu.

5.1.4 Vliv vody

Všechny kritické systémy provozního pracoviště jsou umístěny takovým způsobem, aby nebyly zaplaveny ani stoletou vodou.

5.1.5 Protipožární opatření a ochrana

V objektu provozního pracoviště je instalována elektronická požární signalizace (EPS). Vstupní dveře vyhrazených prostor, ve kterých jsou umístěna zařízení, určená k výkonu hlavních kvalifikovaných certifikačních služeb v oblasti vydávání kvalifikovaných certifikátů nebo kvalifikovaných systémových certifikátů, 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.

Papírová média, která je nutno dle ZoEP a VoEP 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 pracovišť CA znehodnocen skartováním.

5.1.8 Zálohy mimo budovu provozního pracoviště

Kopie provozních a pracovních záloh jsou uloženy na místě určeném ředitelem I.CA.

5.2 Procesní bezpečnost

5.2.1 Důvěryhodné role

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

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 I.CA vydávaných certifikátů a seznamů zneplatněných certifikátů
- ničení dat pro vytváření elektronické značky I.CA vydávaných certifikátů a seznamů zneplatněných certifikátů
- zálohování/obnovu dat pro vytváření elektronické značky I.CA vydávaných certifikátů a seznamů zneplatněných certifikátů
- aktivace kryptografického modulu, obsahujícího data pro vytváření elektronické značky 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 (jméno, certifikát) a autentizaci (heslo, soukromý klíč) k těm komponentám, které jsou pro jejich činnost nezbytné.

5.2.4 Role vyžadující rozdělení povinností

Role, vyžadující rozdělení povinností v procesu poskytování kvalifikovaných certifikačních služeb v oblasti certifikátů, jsou definované v interní bezpečnostní dokumentaci.

5.3 Personální bezpečnost

5.3.1 Požadavky na kvalifikaci, zkušenost a bezúhonnost

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

- naprostá občanská bezúhonnost - prokazováno tím, že tyto osoby nemají žádný záznam v rejstříku trestů (výpis z rejstříku trestů nebo čestné prohlášení)
- vysokoškolské vzdělání v rámci akreditovaného bakalářského nebo magisterského studijního programu a nejméně 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 své funkce.

Ostatní pracovníci I.CA jsou přijímáni na základě následujících kritérií:

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

5.3.2 Posouzení spolehlivosti osob

Zdrojem informací 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 jsou aktualizovány 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.

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 povinností stanovených v uvedených dokumentech jsou vyžadovány smluvní pokuty, případně je s dodavatelem 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)

5.4.1 Typy zaznamenávaných událostí

S ohledem na skutečnost, že I.CA je akreditovaným poskytovatelem certifikačních služeb, jsou v procesu poskytování těchto služeb zaznamenávány veškeré události požadované ZoEP a VoEP.

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

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

5.4.2 Periodicita zpracování záznamů

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

5.4.3 Doba uchovávání auditních záznamů

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

5.4.4 Ochrana auditních záznamů

Auditní záznamy v elektronické a papírové podobě jsou uloženy způsobem, zajišťujícím ochranu před jejich změnami, krádeží a zničením (ať již úmyslnému, tak neúmyslnému).

Elektronické auditní záznamy 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.

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

Ochrana výše uvedených typů auditních záznamů je definována v interní bezpečnostní dokumentaci.

5.4.5 Postupy pro zálohování auditních záznamů

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

5.4.6 Systém shromažďování auditních záznamů (interní nebo externí)

Systém shromažďování auditních záznamů je 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 a VoEP.

5.5.1 Typy informací a dokumentace, které se uchovávají

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

- smlouvy o poskytování kvalifikované certifikační služby, včetně žádosti o poskytování služby
- kopie předložených dokladů, předkládaných při uzavření smlouvy o poskytování kvalifikované certifikační služby
- potvrzení o převzetí certifikátu držitelem, popř. zmocněncem, případně souhlas držitele se zveřejněním certifikátu v seznamu vydaných certifikátů
- prohlášení držitele certifikátu o tom, že mu byly před uzavřením smlouvy o poskytování kvalifikované certifikační služby poskytnuty písemné informace o přesných podmínkách pro využívání této služby, o podmínkách reklamací a řešení vzniklých sporů, a o tom, zda je či není poskytovatel kvalifikovaných certifikačních služeb akreditován
- dokumenty a záznamy související s životním cyklem vydaného certifikátu včetně tohoto certifikátu

- další záznamy požadované ZoEP a VoEP
- aplikační programové vybavení a veškerá dokumentace společnosti, která je nutná pro provádění kontrol
- identifikace místa, kde jsou uloženy informace a dokumentace, jejichž uchování je vyžadováno ZoEP a VoEP
- veškeré seznamy zneplatněných certifikátů
- identifikační údaje osoby, která provedla ověření totožnosti žadatele o certifikát, popř. zmocnitele včetně obchodního názvu případného smluvního partnera, který tuto činnost pro I.CA zajišťuje
- záznam o manipulaci (např. převzetí, předání, uložení, kontrola, konverze do elektronické podoby atp.) s informacemi
- provozní a bezpečnostní dokumentace.

5.5.2 Doba uchovávání uchovávaných informací a dokumentace

I.CA zajišťuje uchovávání informací a dokumentace dle kapitoly 5.5.1 po dobu nejméně 10 od jejich vzniku (nestanoví-li relevantní legislativní norma jinak).

Po celou dobu existence I.CA jsou uchovávány informace, vztahující se ke kořenovým certifikátům I.CA, s výjimkou příslušných dat pro vytváření elektronické značky.

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

5.5.3 Ochrana úložiště uchovávaných informací a dokumentace

Uchovávané informace a dokumentace obsahují i osobní data klientů, a proto je vzhledem k platné legislativě 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.

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

5.5.4 Postupy při zálohování uchovávaných informací a dokumentace

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

5.5.5 Požadavky na používání časových razítek při uchovávání informací a dokumentace

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

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

Informace a dokumentace jsou ukládány na místo určené ředitelem I.CA. Registrační autority jsou povinny provést předarchivaci v určených termínech a vzniklá data předat pověřeným pracovníkům I.CA.

Samotná problematika přípravy a způsobu ukládání informací a dokumentace v elektronické i písemné podobě je upravena interními normami a směrnicemi. Shromažďování uchovávaných informací je evidováno.

5.5.7 Postupy pro získání a ověření uchovávaných informací a dokumentace

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

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

O každém takto povoleném přístupu je pořizován písemný záznam.

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

Výměna dat pro ověřování elektronických značek v nadřízeném kvalifikovaném systémovém certifikátu I.CA (kořenový certifikát I.CA) je v případě standardních situací (uplynutíplatnosti 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 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 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 a kompromitace

V případě výskytu uvedených událostí postupuje I.CA v souladu s interním dokumentem Plán pro zvládání krizových situací a plán obnovy a s dokumentací, na kterou tento plán odkazuje.

5.7.2 Poškození výpočetních prostředků, software nebo dat

V případě poškození výpočetních prostředků, softwaru nebo dat postupuje I.CA v souladu s interním dokumentem Plán pro zvládání krizových situací a plán obnovy a s dokumentací, na kterou tento plán odkazuje.

5.7.3 Postup při kompromitaci dat pro vytváření elektronických značek poskytovatele

V případě vzniku důvodné obavy kompromitace dat pro vytváření elektronických značek pro označování 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 (soukromý klíč)
- zneplatní všechny platné certifikáty, které byly výše uvedenými daty elektronicky označeny
- bezodkladně o této skutečnosti, včetně důvodu informuje na své internetové informační adrese a v nejméně jednom celostátně distribuovaném deníku; 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 interním dokumentem Plán pro zvládání krizových situací a plán obnovy a sdokumentací, na kterou tento plán odkazuje.

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 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:

- 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 kvalifikovaných certifikačních služeb v oblasti vydávání certifikátů
- prokazatelné zničí svá data pro vytváření elektronických značek, sloužící k označování vydávaných certifikátů a seznamu zneplatěných certifikátů.

V případě ukončení činnosti konkrétního pracoviště RA je tato skutečnost oznámena na internetové adrese http://www.ica.cz, případně formou vývěsky (je-li to možné) na pracovišti této RA.

V případě odnětí akreditace I.CA bez prodlení informuje o této skutečnosti nejen subjekty, kterým poskytuje své kvalifikované certifikační služby, ale i další dotčené osoby způsobem uvedeným v kapitolách 2.2 a 2.3.

6 Technická bezpečnost

6.1 Generování a instalace párových dat

6.1.1 Generování párových dat

Generování párových dat I.CA (soukromý klíč, kterým I.CA elektronicky označuje vydávané certifikáty a seznamy zneplatněných certifikátů, a veřejný klíč sloužící pro ověřování těchto značek), 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 ZoEP a VoEP. Veškeré požadavky na proces generování párových dat I.CA, sloužících k označování vydávaných certifikátů a seznamů zneplatněných certifikátů, jsou definovány v interní bezpečnostní dokumentaci.

I.CA z principiálních bezpečnostních důvodů neposkytuje službu generování párových dat žadatele o certifikát na svých zařízeních. Samotné klíče musí podporovat algoritmus RSA.

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

Veřejný klíč je nutno I.CA doručit. I.CA podporuje následující způsoby doručení dat pro ověřování elektronické značky - osobně na datovém nosiči a/nebo elektronickou cestou.

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 I.CA vydaných certifikátů a seznamů zneplatněných certifikátů jsou obsažena v kořenovém certifikátu I.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.

Způsoby získání dat pro ověřování elektronických značek označujících osob jsou uvedeny v kapitole 2.

6.1.5 Délky párových dat

V procesu poskytování kvalifikovaných certifikačních služeb využívá I.CA výhradně nejprověřenější klasický asymetrický 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 vytváření elektronických značek a kontrola jejich kvality

Algoritmy použité pro generování celočíselných hodnot nutných pro fungování elektronické značky (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 značek ve vydávaných certifikátech. V případě duplicitního výskytu dat pro ověření elektronických 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 vytváření 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

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 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 vydávaných certifikátů a seznamů zneplatněných certifikátů. Soukromý klíč je v zašifrované podobě zálohován prostřednictvím čipových karet.

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

Po uplynutí doby platnosti soukromého klíče určeného k elektronickému označování 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 vydávaných certifikátů a seznamů zneplatněných certifikátů, je generován přímo v kryptografickém modulu.

Vkládání soukromého klíče do kryptografického modulu v případě, že se jedná o jeho obnovení 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 je uložen bezpečným způsobem v kryptografickém modulu, splňujícím požadavky platné legislativy.

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 vydávaných certifikátů a seznamů zneplatněných certifikátů, vygenerovaný v kryptografickém modulu, provádí určení pracovníci I.CA prostřednictvím vlastní aktivace kryptografického modulu a 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. Po aktivaci je zařízení přístupné pouze určeným odpovědným pracovníkům I.CA.

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 vydávaných certifikátů a seznamů zneplatněných certifikátů, provádí určení pracovníci I.CA prostřednictvím kryptografického modulu a aktivační čipové karty podle přesně určeného postupu, který je upraven interní dokumentací. O provedené deaktivaci 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

Soukromý klíč, sloužící k označování vydávaných certifikátů a seznamů zneplatněných certifikátů, je uložen v kryptografickém modulu. Ničení soukromého klíče je realizováno prostředky kryptografického modulu. Zálohy soukromých klíčů uložených v zašifrované podobě na externích médiích, jsou rovněž zničeny. Ničení spočívá ve fyzické destrukci těchto nosičů. Veškeré požadavky na proces ničení soukromého klíče, sloužícího k označování vydávaných certifikátů a seznamů zneplatněných certifikátů jsou definovány v interní bezpečnostní dokumentaci.

6.2.11 Hodnocení kryptografického modulu

Kryptografický modul, sloužící pro elektronické označování 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 je řešena v souladu s ZoEP a VoEP.

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

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

6.4 Aktivační data

6.4.1 Generování a instalace aktivačních dat

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

6.4.2 Ochrana aktivačních dat

Výše uvedená aktivační data jsou pracovníky I.CA chráněna způsobem uvedeným v interní bezpečnostní dokumentaci.

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

Úroveň bezpečnosti použitých komponent pro poskytování kvalifikovaných certifikačních služeb v oblasti vydávání certifikátů je definována ZoEP a VoEP.

Detailní řešení specifických technických požadavků počítačové bezpečnosti je popsáno v interní dokumentaci.

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.
- ČSN ISO/IEC 17799 - Informační technologie – Soubor postupů pro management bezpečnosti informací.
- ČSN ISO/IEC 27001 Informační technologie - Bezpečnostní techniky - Systémy managementu bezpečnosti informací – Požadavky.
- ČSN ISO/IEC TR 13335 - Informační technologie – Směrnice pro řízení bezpečnosti IT 1-3.
- ČSN EN ISO 19011 - Směrnice pro auditování systému managementu jakosti a/nebo systému environmentálního managementu.

6.6 Bezpečnost životního cyklu

6.6.1 Řízení vývoje systému

Při vývoji systému je postupováno v souladu s interní dokumentací.

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 auditorských firem, a kontrolami bezpečnostní shody, prováděnými pracovníky I.CA. Tato problematika je popsána v interní dokumentaci. 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 mimo jiné chráněn komerčním produktem typu firewall. Veškerá komunikace mezi RA a provozním pracovištěm certifikační autority je vedena šifrovaně. Detailní řešení řízení síťové bezpečnosti je popsáno v interní dokumentaci.

6.8 Časová razítka

Řešení je uvedeno v kapitole 5.5.5.

7 Profily certifikátu, seznamu zneplatněných certifikátů a OCSP

7.1 Profil certifikátu

7.1.1 Základní položky certifikátu

Tabulka 3 – Údaje vydávaného kvalifikovaného systémového certifikátu

Položka	Obsah	Pozn.
Version	v3 (0x2)	povinná, generuje I.CA
serialNumer	jedinečné sériové číslo vydávaného certifikátu (přiděluje I.CA)	povinná, generuje I.CA
Signature	identifikátor algoritmu, použitého I.CA pro elektronickou značku vydávaného certifikátu (tzn. tohoto certifikátu)	povinná, generuje I.CA
Issuer	Informace o vydavateli certifikátu - viz Tabulka 4	povinná, generuje I.CA
Validity		povinná, generuje I.CA
• notBefore	počátek platnosti vydávaného certifikátu (UTC[12])	
• notAfter	konec platnosti vydávaného certifikátu (UTC)	
Subject	informace o označující osobě/držiteli certifikátu : • countryName (C) • commonName (CN) • ctateOrProvinceName (S) • cocalityName (L) • organizationName (O) • organizationalUnitName (OU) • emailAddress (E) • initials (I) • name (N) • title (T) • serialNumber • generationQualifier	viz kapitola 3.1
subjectPublicKeyInfo		povinná, generuje I.CA
• algorithm	identifikátor algoritmu využívaný veřejným klíčem uvedeným ve vydávaném certifikátu	
• subjectPublicKey	veřejný klíč podepisující osoby (2048 bitů)	
Extensions	rozšíření vydávaného certifikátu	viz Tabulka 5

Tabulka 4 – Issuer

Položka	Obsah
Organization (O)	První certifikační autorita, a.s.
OrganizationUnitName(OU)	I.CA – Accredited Provider of Certification Services

[12] **U**niversal **C**o-ordinated **T**ime, Standard přijatý 1.1.1972 pro světový koordinovaný čas (Coordinated Universal Time – UTC) - funkci "oficiálního časoměřiče" atomového času pro celý svět vykonává Bureau International de l'Heure (BIPM)

CommonName (CN)	I.CA – Qualified Certification Authority, MM/RRRR
Country (C)	CZ

Pozn
MM/RRRR je měsíc a rok počátku platnosti certifikátu vydavatele

7.1.2 Čísla verzí

Všechny vydávané certifikáty jsou v souladu s X.509 ve verzi 3.

7.1.3 Rozšiřující položky v certifikátu

Tabulka 5 – Rozšiřující položky kvalifikovaného certifikátu

Položka	Obsah	Upřesnění
SubjectAlternativeName	otherName, rfc822Name, dNSName, URI, iPAddress	nekritická a nepovinná položka viz kapitola 3.1.1.13
AutorityKeyIdentifier		nekritická a povinná položka, generuje I.CA
• KeyIdentifier	Hash veřejného klíče vydavatele certifikátu	
Subject Key Identifier	Hash veřejného klíče vydaného certifikátu	nekritická a povinná položka, generuje I.CA
Certificate Policies		nekritická a povinná položka, generuje I.CA
• Policy	viz kapitola 7.1.7	
• Explicit Text	viz kapitola 7.1.9	
CRL Distribution Points	seznam distribučních míst CRL, dosažitelných protokolem http	nekritická a povinná položka, v případě písemné smlouvy s klientem je možno doplnit další jím požadovaná distribuční míst, generuje I.CA
Key Usage :		kritická a povinná položka; obecně jsou akceptovány pouze bity digitalSignature, nonRepudiation, keyEncipherment, dataEncipherment, keyAgreement; pokud bude žádost o vydání certifikátu obsahovat jiný bit, bude zamítnuta a certifikát nebude vydán.
	v případě neuvedení položky v žádosti : digitalSignature,	(generuje I.CA)

	nonRepudiation. **v případě uvedení položky v žádosti :** není-li nastaven bit nonRepudiation, je žádost zamítnuta a certifikát není vydán, v opačném případě je nastavení bitů přebíráno ze žádosti - s ohledem na kompatibilitu s produkty třetích stran I.CA doporučuje nastavení bitu digitalSignature – implementováno v generátorech žádostí vytvořených I.CA	Pozn. Uplatnění, resp. neuplatnění bitů digitalSignature, keyEncipherment, dataEncipherment, keyAgreement lze modifikovat - za škodu způsobenou touto modifikací je odpovědný žadatel o certifikát, resp. podepisující osoba.
Extended Key Usage	anyExtendedKeyUsage, id-kp-serverAuth, id-kp-clientAuth, id-kp-emailProtection	nepovinná položka, přebíraná ze žádosti o certifikát, v případě anyExtendedKeyUsage nastaví I.CA tuto položku jako nekritickou, v ostatních případech přebíráno ze žádosti
nsComment	číslo čipové karty	nekritická položka a povinná položka pouze v případě vydání certifikátu na čipovou kartu, generuje I.CA

I.CA si vyhrazuje právo výše uvedenou množinu rozšiřujících položek rozšířit nebo omezit.

7.1.4 Objektové identifikátory (dále OID) algoritmů

V procesu poskytování kvalifikovaných certifikačních služeb je využívány algoritmy, uvedené v platné legislativě, resp. v příslušných technických standardech, na které je touto legislativou odkazováno.

7.1.5 Způsoby zápisu jmen a názvů

Uvedeno v kapitole 3.1.

7.1.6 Omezení jmen a názvů

Pro jméno předmětu není žádné omezení s výjimkou omezení vyplývajících z kapitoly 3.1.2. O přípustnosti konkrétního obsahu jednotlivých položek předmětu rozhoduje s konečnou platností pracovník registrační autority, který provádí vyřizování požadavku na vydání certifikátu. V případě nesouhlasu může žadatel postupovat podle kapitoly 9.13.

7.1.7 OID certifikační politiky

Tato CP je určena pro vydávání a správu kvalifikovaných systémových certifikátů a je jí přiděleno OID uvedené v kapitole 1.2.

7.1.8 Rozšiřující položka „Policy Constrainsts“

Není aplikováno.

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

Obsah textu oznámení (user notice) rozšiřující položky kvalifikátorů politiky „Policy Qualifiers“ je následující :

Tento kvalifikovany systemovy certifikat je vydan podle zakona c. 227/2000 Sb. v platnem zneni/This is qualified system certificate according to Czech Act No. 227/2000 Coll.

7.1.10 Způsob zápisu kritické rozšiřující položky „Certificate Policies“

Viz Tabulka 5.

7.2 Profil seznamu zneplatněných certifikátů

Tabulka 6 – Základní položky CRL

Položka	Obsah
Version	verze v2
SignatureAlgorithm	identifikátor a parametry algoritmu, použitého I.CA pro elektronickou značku vydávaného CRL
Issuer	označení vydavatele CRL (viz Tabulka 5)
thisUpdate	datum a čas vydání CRL (UTC)
nextUpdate	datum a předpokládaný čas vydání následujícího CRL (UTC)
revokedCertificates • userCertificate • revocationDate	seznam zneplatněných certifikátů jedinečné sériové číslo zneplatněného certifikátu datum a čas zneplatnění certifikátu
crlExtensions	Rozšíření CRL (viz Tabulka 7)

7.2.1 Číslo verze

Seznamy zneplatněných certifikátů jsou vydávány dle X509 verze 2.

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

Tabulka 7 – Rozšiřující položky CRL

Položka	Obsah	Kritická
AutorityKeyIdentifier • KeyIdentifier	hash veřejného klíče vydavatele certifikátu	NE

CRL Number	Číslo CRL	NE
IssuingDistributionPoint	http adresa/adresy, odkud lze CRL získat	ANO

7.3 Profil OCSP

Viz kapitola 4.9.9.

7.3.1 Číslo verze

Služba není poskytována.

7.3.2 Rozšířující položky OCSP

Služba není poskytována.

8 Hodnocení shody a jiná hodnocení

8.1 Periodicita hodnocení nebo okolnosti pro provedení hodnocení

S ohledem na skutečnost, že společnost První certifikační autorita, a.s. je akreditovaným poskytovatel certifikačních služeb, jsou periodicity hodnocení, včetně okolností pro provádění hodnocení striktně dány požadavky ZoEP a VoEP, jedná se zejména o audit systému řízení bezpečnosti informací, kontroly bezpečnostní shody a audit bezpečnosti poskytování certifikačních činností.

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

8.2 Identita a kvalifikace hodnotitele

Identita a kvalifikace hodnotitele provádějícího hodnocení požadované ZoEP a VoEP je dána touto legislativou, v ostatních případech je vyžadována certifikace pro uvedenou činnost.

8.3 Vztah hodnotitele k hodnocenému subjektu

V případě provádění hodnocení požadovaného ZoEP a VoEP je vztah hodnotitele k poskytovateli certifikačních služeb dán touto legislativou, v ostatních případech se jedná o externího hodnotitele.

8.4 Hodnocené oblasti

V případě provádění hodnocení požadovaného ZoEP a VoEP jsou hodnocené oblasti konkretizovány touto legislativou, v ostatních případech jsou hodnocené oblasti dány standardy, dle kterých je hodnocení prováděno.

8.5 Postup v případě zjištěných nedostatků

Se zjištěními všech typů prováděných hodnocení je seznámen bezpečnostní manager, který je povinnen zajistit odstranění případných nedostatků.

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 které budou mimo vedení společnosti přítomni vedoucí jednotlivých oddělení, na které přítomné s výsledky hodnocení seznámí.

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 CP (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, příslušná k datům pro ověřování elektronických značek, obsažených v kořenových certifikátech I.CA
- data pro vytváření elektronických podpisů/značek 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
- veškeré interní informace a dokumentace s ohledem na poskytování kvalifikovaných certifikačních služeb dle ZoEP
- veškeré 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 odpovědná 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 (viz relevantní části kapitol 3 a 4) 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 CP, 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 této 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 této CP
- spoléhající se strana neporušila povinnosti této 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, uvedených v kapitola 1.3.2. RA nevyřídí kladně žádost, pokud žadatel hodnověrným způsobem neprokázal svoji identitu, nedoložil údaje uvedené v o službu, odmítá potřebné údaje sdělit nebo odmítne podepsat příslušné dokumenty (viz příslušné kapitoly této 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 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

Hranice odpovědnosti společnosti První certifikační autorita, a.s. se v oblasti poskytování kvalifikovaných certifikačních služeb řídí platnou legislativou.

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, kterými I.CA elektronicky označuje 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

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

9.10.2 Ukončení platnosti

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

9.10.3 Důsledky ukončení a přetrvání závazků

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

9.11 Komunikace mezi zúčastněnými subjekty

Pro individuální oznámení a komunikaci s držitelem certifikátu, resp. podepisující 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

9.12.1 Postup při změnách

Postup je realizován řízeným procesem uvedeném v interním dokumentu.

9.12.2 Postup při oznamování změn

Postup je realizován řízeným procesem uvedeném v interním dokumentu.

9.12.3 Okolnosti, při kterých musí být změněno OID

V případě vydání nové verze tohoto dokumentu je pro tento dokument přiděleno nové OID.

9.13 Řešení sporů

Tato CP a jí odpovídající certifikační prováděcí směrnice (dále též CPS), 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

Smlouva o poskytování kvalifikovaných certifikačních služeb v oblasti vydávání certifikátů může obsahovat ustanovení o působení vyšší moci.

9.17 Další opatření

Tyto skutečnosti jsou pro aplikaci vydání tohoto dokumentu irelevantní.

10 Závěrečná ustanovení

Tato CP, vydaná společností První certifikační autorita, a.s., nabývá platnosti a účinnosti dnem 1. 4. 2011.