První certifikační autorita, a.s.

CERTIFIKAČNÍ PROVÁDĚCÍ SMĚRNICE

VYDÁVÁNÍ KOMERČNÍCH CERTIFIKÁTŮ

Verze 3.3

Tabulka 1 – Vývoj dokumentu

Verze	Datum vydání	Schválil	Pozn.
3.0	24.10.2009	Ředitel společnosti První certifikační autorita, a.s.	Vydávání certifikátů s parametry, splňujícími doporučení technické specifikace ETSI[1] TS 102 176-1 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
3.2	17. 12. 2012	Ředitel společnosti První certifikační autorita, a.s.	aktualizace názvů interních směrnic
3.3	22.09.2015	Ředitel společnosti První certifikační autorita, a.s	Aktualizace a revize dokumentu

1 European Telecommunications Standards Institute

Obsah

1 Úvod

S ohledem na doporučení technické specifikace ETSI TS 102 176-1 Electronic Signatures and Infrastructures (ESI); Algorithms and Parameters for Secure Electronic Signatures; Part 1: Hash functions and asymmetric algorithms, vztahující se k využívání kryptografických algoritmů v procesu vydávání a správy certifikátů vydává společnost První certifikační autorita, a.s. komerční certifikáty s využitím hashovacích funkcí SHA-256 a SHA-512 v kombinaci s algoritmem RSA s délkou klíče 2048 bitů.

1.1 Přehled

Dokument **Certifikační prováděcí směrnice vydávání komerčních certifikátů** (dále též CPS), vypracovaný společností První certifikační autorita, a. s., se zabývá skutečnostmi, vztahujícími se k procesům životního cyklu certifikátů a dodržuje strukturu dle 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. 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 certifikátů.
- Kapitola 2 obsahuje problematiku odpovědností za zveřejňování a úložiště informací, resp. dokumentace.
- Kapitola 3 popisuje procesy identifikace a autentizace žadatele o vydání prvotního/následného certifikátu, resp. zneplatnění certifikátu, včetně definování typů a obsahů používaných jmen v žádostech, resp. vydávaných certifikátech.
- Kapitola 4 definuje procesy životního cyklu certifikátu, tzn. žádost o vydání prvotního/následného certifikátu, zneplatnění certifikátu, služby související s ověřováním statutu 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 certifikátů a seznamů zneplatněných certifikátů.
- Kapitola 8 je zaměřena na problematiku hodnocení poskytovaných certifikačních služeb.
- Kapitola 9 zahrnuje problematiku obchodní a právní.

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

V procesu poskytování certifikačních služeb v oblasti vydávání komerčních 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 jednoznačné určení dokumentu

Název tohoto dokumentu: Certifikační prováděcí směrnice vydávání komerčních certifikátů verze 3.3
OID dokumentu: není přiřazeno

Tato CPS se vztahuje k následující CP:

OID	CP
1.3.6.1.4.1.23624.1.1.60.3.1	Certifikační politika vydávání komerčních certifikátů

1.3 Participující subjekty

1.3.1 Certifikační autority (dále "CA")

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

1.3.2 Registrační autority (dále "RA")

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

- přijímají žádosti o služby uvedené v této CPS, zejména přijímají žádosti o certifikáty, zprostředkovávají předání certifikátů a seznamů zneplatněných certifikátů, poskytují potřebné informace, vyřizují reklamace atd.,
- jsou oprávněny z naléhavých provozních nebo technických důvodů pozastavit zcela nebo zčásti výkon své činnosti - toto opatření jsou povinny neprodleně hlásit řediteli I.CA, který je potvrdí, zruší nebo změní,
- jsou zmocněny jménem I.CA uzavírat smlouvy o poskytování 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 Osoby, které požádaly o vydání certifikátu a kterým byl certifikát vydán

Osobami, které mohou požádat o vydání certifikátu a kterým bude certifikát vydán, mohou být fyzická osoba, právnická osoba nebo organizační složka státu.

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. v oblastech elektronického podpisu, šifrování, autentizace atd.

1.3.5 Jiné participující subjekty

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

1.4 Použití certifikátu

1.4.1 Přípustné použití certifikátu

Certifikáty, které vydává I.CA klientům, mohou být používány v aplikacích zejména pro účely elektronických podpisů, šifrování a autentizace. Tyto certifikáty, vydávané v souladu s dále uvedenými pravidly, jsou určené pro osobní použití, serverových aplikacích apod.

1.4.2 Omezení použití certifikátu

Certifikáty vydávané dle této CPS společností První certifikační autorita, a.s. nesmí být využívány v rozporu s vydávaným účelem definovaným touto CPS.

1.5 Správa politiky

1.5.1 Organizace spravující certifikační politiku nebo certifikační prováděcí směrnici

Tuto CPS, resp. jí odpovídající CP, 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 podle bodu 1.5.3

V případě, že je potřebné provést změny v této CPS 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 předchází její schválení ředitelem společnosti První certifikační autorita, a.s. Proces změny je popsán v interní dokumentaci „***Změnové řízení***".

1.6 Přehled použitých pojmů a zkratek

Dále uvedený přehled pojmů a zkratek 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
Autentizace	vytvoření podpisu k náhodně vygenerovaným datům, přičemž tento úkon slouží pouze k určení identity dané osoby a nemá žádné následky vzhledem k obsahu náhodně vygenerovaných dat
Bit	z anglického *binary digit* - číslice dvojkové soustavy je základní a současně nejmenší jednotkou informace používanou především v číslicové a výpočetní technice
Certifikát	datová zpráva, která je vydána poskytovatelem certifikačních služeb, spojuje veřejný klíč s podepisující, šifrující nebo autentizující se osobou a umožňuje ověřit její identitu
CRL (Certificate Revocation List)	seznam zneplatněných certifikátů
Čas	světový čas UTC
Elektronický podpis	Údaje v elektronické podobě, které jsou připojené k datové zprávě nebo jsou s ní logicky spojené a které slouží jako metoda k jednoznačnému ověření identity podepsané osoby ve vztahu k datové zprávě
I.CA	První certifikační autorita, a.s.
Následný certifikát	certifikát, který byl v souladu se smlouvou o poskytování certifikační služby, uzavřenou mezi žadatelem a I.CA vydán žadateli na základě nové žádosti o certifikát (struktura PKCS#10) v období platnosti certifikátu, ke kterému je vydáván tento následný certifikát

Párová data	jedinečná data pro vytváření elektronického podpisu, resp. elektronické značky spolu s odpovídajícími daty pro ověřování elektronického podpisu, resp. elektronické značky
Podepisující osoba	fyzická osoba, která je držitelem prostředku pro vytváření elektronických podpisů a jedná jménem svým nebo jménem jiné fyzické či právnické osoby
RA	registrační autorita
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, šifrování nebo autentizaci
Spoléhající se strana	subjekt, spoléhající se při své činnosti na certifikát, vydaný I.CA
TWINS	produkt I.CA, obsahující dvojici certifikátů: • kvalifikovaný certifikát – vydaný v souladu s platnou legislativou vztahující se k problematice elektronického podpisu, • komerční certifikát – vydaný výhradně na základě smluvního vztahu mezi I.CA a koncovým uživatelem
Veřejný klíč	jedinečná data pro ověřování elektronického podpisu, dešifrování, autentizace
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

2 Odpovědnosti za zveřejňování a úložiště informací a dokumentace

2.1 Úložiště informací a dokumentace

Společnost První certifikační autorita, a.s., zřizuje a provozuje úložiště informací a dokumentace, 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, ostatní veřejné a aktuální informace a dokumenty atd.), případně odkazy pro zjištění dalších informací, jsou:

a) 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, pracovištích RA. Pracovníci I.CA a smluvních partnerů jsou rovněž povinni tyto informace na vyžádání sdělit veřejnosti.

Informace o veřejných certifikátech lze získat na adrese http://www.ica.cz/. 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).

Informace o CRL lze získat na adrese http://www.ica.cz/. 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. 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 vzniku důvodné obavy ze zneužití dat pro vytváření elektronických podpisů vydávaných certifikátů nebo seznamů zneplatněných certifikátů, oznámí I.CA tuto skutečnost na své internetové informační adrese.

2.3 Periodicita zveřejňování informací

- 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) – neprodleně po zneplatnění, nejvýše do 24 hodin od vydání předchozího CRL,
- informace o 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 certifikačních služeb.

2.4 Řízení přístupu k jednotlivým typům úložišť

Veškeré veřejné informace (viz kapitoly 2.2, 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, zejména:

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

3 Identifikace a autentizace

3.1 Pojmenovávání

3.1.1 Typy jmen

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 CountryName (např. CZ) může obsahovat pouze kód státu, v němž má žadatel o certifikát:

- místo trvalého pobytu (uvedeno v osobním dokladu - pokud není kód státu trvalého pobytu explicitně uveden, uvede se kód státu, který předkládaný doklad vydal), nebo
- sídla/pracoviště (uvedeno ve výpisu z obchodního rejstříku, živnostenského listu, zřizovací listiny atd.) .

V procesu kontroly žádosti o prvotní certifikát pracovník RA ověřuje správnost podle výše uvedených dokladů[2] a pokud zjistí neshodu, 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 podkapitola mi.

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:

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

V případě žádosti o prvotní certifikát pracovník RA ověřuje správnost dle výše uvedených dokumentů a pokud zjistí neshodu, žádost odmítne. Pracovník RA taktéž rozhoduje o přípustnosti konkrétního obsahu údaje - kontroluje, zda se nejedná o nepovolené výrazy (vulgární, propagující fašismus, rasovou a třídní nenávist)a zda nejsou dotčena práva jiných subjektů - registrované známky apod.

[2] Akceptovatelné 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 označení nižšího územně správního celku, do něhož spadá:

- fyzická osoba nepodnikající – místo trvalého bydliště podle primárního osobního dokladu žadatele o 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 jinou správní jednotku, 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 Organization (povinnost/nepovinnost naplnění závisí 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.

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

[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.

3.1.1.6 OrganizationalUnitName (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 email Address (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 3.1.1.12 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 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.

3.1.1.10 SerialNumber (sériové číslo předmětu)

Sériové číslo předmětu, sloužící k rozlišení různých subjektů v rámci klientely I.CA, obecně vyplňuje I.CA a je naplněno řetězcem „ICA - “ a za něj připojeno na řetězec převedené identifikační číslo žadatele o certifikát. V žádosti o prvotní certifikát se nesmí vyskytnout, v žádosti o následný certifikát a v jí odpovídajícím vydaném certifikátu se může vyskytnout právě jednou.

[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.

3.1.1.11 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.

3.1.1.12 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),
- ***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] 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

I.CA vydává své certifikáty s řetězci v položce Subject (DN) podle požadavků obsažených v žádosti o certifikát s tím, že při vydávání certifikátů dochází v polích DN k odstranění úvodních a koncových bílých znaků („whitespaces“) a všechny skupiny těchto znaků uprostřed řetězců jsou nahrazeny jedinou mezerou. Bílými znaky se rozumí znaky 0x09 až 0x0D a 0x20 v kódování ASCII, mezerou pak znak 0x20 ve stejném kódování.

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

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

3.1.3 Anonymita a používání pseudonymu

Služba anonymity a používání pseudonymu není poskytována.

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. Pro kódování základních položek lze použít typ UTF8String nebo PrintableString s výjimkou položek Country a SerialNumber (typ PrintableString), položky otherName (UTF8String), 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 3.1.1.10). 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 certifikátu, I.CA upozorní žadatele a požádá ho, aby některý z požadovaných údajů změnil či doplnil. Pokud žadatel toto neučiní, 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.

3.2 Počáteční ověření identity

Postup ověřování identity je detailně uveden v interní dokumentaci ***„Operátor RA“***.

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

Vlastnictví dat pro vytváření elektronických podpisů, odpovídajících datům pro ověřování elektronických podpisů, která daná žádost o certifikát (struktura PKCS#10) obsahuje a která budou obsažena ve vydaném certifikátu, se prokazuje předložením této žádosti ověřujícímu subjektu, kterým může být pracovník registrační nebo certifikační autority. S ohledem na skutečnost, že tato žádost je elektronicky podepsána daty pro vytváření elektronických podpisů (tzv. soukromý klíč), odpovídajících datům pro ověřování elektronických podpisů (tzv. veřejný klíč) obsažených v žádosti, dokazuje tímto způsobem žadatel o certifikát, že v době tvorby elektronického podpisu 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 osobního dokladu. Osobní doklad pro občany České republiky musí být občanský průkaz, platný cestovní pas, popř. obdobný doklad stejné právní váhy. Osobní doklad pro cizince je platný cestovní pas, popř. obdobný doklad stejné právní váhy. Občané Slovenské republiky mohou jako osobní doklad použít občanský průkaz.

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

- Originál osobního dokladu zmocněnce (kvalita dokladu je uvedena výše).
- Originál, případně úředně ověřenou kopie osobního dokladu žadatele o certifikát (kvalita dokladu je uvedena výše).
- Plnou 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.

[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] V 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.

- 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 osobu 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),
  - 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 3.2.2. 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).

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 certifikát je její zaměstnanec, je postupováno v souladu s kapitolou 3.2.3.2.

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 podepisující 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 v certifikátu

3.3.1 Identifikace a autentizace při rutinní výměně párových dat

Identifikace a autentizace žadatele o vydání následného certifikátu (struktura PKCS#10) je prováděna ověřením elektronického podpisu žádosti o vydání následného certifikátu – v procesu ověřování elektronického podpisu žádosti o následný certifikát musí být použit platný certifikát, ke kterému je vydáván

[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).

tento následný certifikát nebo musí být použit platný certifikát pro obnovu (tzv. „podpisový certifikát“, volitelně vydávaný např. v procesu žádosti o serverový certifikát). V obou případech se jedná o certifikáty, vydané v souladu s dokumentem Certifikační politika vydávání komerčních 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 uveden v kapitole 4.2.1.

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 podepsaná elektronická zpráva - (revoke@ica.cz), elektronický podpis musí být realizován daty pro vytváření elektronického podpisu 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 certifikátu pro obnovu k tomuto zneplatňovanému certifikátu,
- elektronicky nepodepsaná elektronická zpráva, obsahující heslo pro zneplatnění certifikátu - (revoke@ica.cz),
- prostřednictvím formuláře na internetové informační adrese (http://www.ica.cz).

V případě použití **listovní zásilky pro předání žádosti 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.

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 certifikační služby, tak žadatele o tuto službu, jsou uvedeny v následujících kapitolách.

4.2 Zpracování žádosti o certifikát

Proces zpracování žádosti o certifikát je detailně popsané v interní dokumentaci:

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

4.2.1 Identifikace a autentizace

Podporované hashovací funkce, využívané při tvorbě elektronického podpisu žádosti o certifikát a hashovací funkce použité v procesu tohoto certifikátu, jsou uvedeny v následujícím seznamu:

- Produkt TWINS: žádost SHA-1 -> vydaný certifikát SHA-256, žádost SHA-256 -> vydaný certifikát SHA-256, žádost SHA-512 -> vydaný certifikát SHA-512 .
- Ostatní komerční certifikáty: 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 podpisů (viz kapitola 3.2.1) – pracovník RA tuto skutečnost kontroluje prostřednictvím speciálního aplikačního programového vybavení takovým způsobem, že pomocí dat pro ověřování elektronických podpisů, uvedených v žádosti o certifikát, ověří platnost elektronického podpisu na této žádosti. Pokud je ověření platnosti elektronického podpisu negativní, RA žádost nepřijme a řízení k vydání certifikátu ukončí.
2. Kontrola předloženého osobního dokladu žadatele o certifikát, popř. zmocněnce (viz kapitola 3.2.3.1). V případě pochybností o pravosti předloženého osobního dokladu žadatele o certifikát, popř. zmocněnce odmítne je proces vydávání certifikátu ukončen..
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 certifikátu (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 (ve formátu PKCS#10) o vydání certifikátu, splňující následující požadavky:

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 také využívána 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, vyřizující předmětnou žádost, vytiskne dokument „Protokol o podání žádosti na vydání certifikátu I.CA“, který nechá žadateli o certifikát, popř. zmocněnci, podepsat. Pokud žadatel o certifikát, popř. zmocněnec odmítne tento protokol podepsat, je pracovník, vyřizující předmětnou žádost, povinen proces vydávání certifikátu ukončit.

V případě požadavku na certifikát typu „codeSigning“ je žadatel o tento typ certifikátu, popř. zmocněnec povinen písemně potvrdit, že je společnost První certifikační autorita, a.s. oprávněna uchovávat pořízené kopie veškerých dokladů, jimiž se identifikoval. Nařízením ředitele I.CA mohou být definovány další rozšiřující podmínky.

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

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

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

4.2.3 Doba zpracování žádosti o certifikát

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 certifikační autority nezbytné kontroly a další činnosti, popsané v interním dokumentu:

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

4.3.2 Oznámení o vydání certifikátu držiteli certifikátu, podepisující 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 certifikát na 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.

Uvedené postupy jsou detailně popsány v interní dokumentaci:

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

4.4 Převzetí vydaného certifikátu

4.4.1 Úkony spojené s převzetím certifikátu

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 podpisů odpovídající datům pro ověřování elektronických podpisů, 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.

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.

Proces převzetí vydaného certifikátu je detailně popsán v interní dokumentaci:

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

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, resp. následného certifikátu při osobním dostavení se žadatele/zmocnitele, získá oznámení o vydaném certifikátu pracovník vyřizující předmětnou žádost.

4.5 Použití párových dat a certifikátu

4.5.1 Použití soukromého klíče a certifikátu držitelem, podepisující, resp. autentizující se nebo šifrující 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 certifikační služby,
- seznámit s relevantními ustanoveními příslušné smlouvy o poskytování 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 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,
- využívat data pro vytváření elektronických podpisů související s vydaným certifikátem v souladu s ustanoveními této CP,
- při činnostech souvisejících s daty pro vytváření elektronického podpisu dodržovat veškerá ustanovení této CP.

Uživatel, který nedodržuje či nedodržel své povinnosti, nemá nárok na případnou náhradu škody. I.CA a smluvní partneři jsou povinni upozornění na povinnosti uživatelů zveřejnit prostřednictvím svých kontaktních adres.

4.5.2 Použití veřejného klíče a certifikátu spoléhající se stranou

Spoléhající se strany jsou zejména povinny:

- provádět veškeré úkony potřebné k tomu, aby si ověřily, že elektronický podpis je platný 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 ustanovení této CP.

Uživatel, který nedodržuje či nedodržel své povinnosti, nemá nárok na případnou náhradu škody. I.CA a smluvní partneři jsou povinni upozornění na povinnosti uživatelů zveřejnit prostřednictvím svých kontaktních adres.

4.6 Obnovení certifikátu

Službou obnovení certifikátu je v kontextu tohoto dokumentu myšleno obnovení již zneplatněného certifikátu a/nebo vydání následného certifikátu se stejnými daty pro ověřování elektronických podpisů 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 nebo podepisující 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 veřejného klíče 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 veřejného klíče v certifikátu

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

4.7.2 Subjekty oprávněné požadovat výměnu veřejného klíče v certifikátu

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

4.7.3 Zpracování požadavku na výměnu veřejného klíče

Pokud je ověření elektronických podpisů pozitivní (viz relevantní části kapitol 3.3.1, 4.2.1) a obsah položek žádosti o výměnu dat pro ověřování elektronických podpisů 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 vyměněným veřejným klíčem

Viz relevantní části kapitoly 4.3.2.

4.7.5 Úkony spojené s převzetím certifikátu s vyměněným veřejným klíčem

Viz relevantní části kapitoly 4.4.1.

4.7.6 Zveřejnění vydaných certifikátů s vyměněným veřejným klíčem

Viz kapitola 4.4.2.

4.7.7 Oznámení o vydání certifikátu s vyměněným veřejným klíčem 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 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 zejména na základě následujících okolností:

- jeho držitel poruší závažným způsobem ustanovení smlouvy o poskytování certifikační služby nebo dokumentů, které jsou přílohou této smlouvy,
- dojde ke kompromitaci, resp. existuje důvodné podezření, že došlo ke kompromitaci dat pro vytváření elektronických podpisů,
- je důvodné podezření, že došlo ke kompromitaci dat pro vytváření elektronických podpisů držitele certifikátu, podepisující, resp. autentizující se nebo šifrující osoby,
- držitel certifikátu nebo jím oprávněná osoba požádá o jeho zneplatnění,
- na základě klientova sdělení, resp. zjištění I.CA nebo spolupracujících subjektů se věcný obsah certifikátu stane neplatným,
- držitel certifikátu byl usvědčen ze závažného porušení povinností vyplývajících z této CPS,
- nařídí tak soud ve svém rozsudku nebo předběžném opatření,
- držitel certifikátu zemřel.

4.9.2 Subjekty oprávněné žádat o zneplatnění certifikátu

Žádost o zneplatnění mohou podat zejména:

- podepisující osoba, držitel certifikátu nebo subjekt, který k tomu byl explicitně určen ve smlouvě o poskytování 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.

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 hexadecimálním 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 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 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 musí být 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]. Po dobu zablokování je certifikát platný a případná odpovědnost za škodu vzniklou použitím takového certifikátu v době jeho zablokování nelze nárokovat na I.CA.

Maximální prodlení mezi zneplatněním certifikátu a zveřejněním seznamu zneplatněných certifikátů, na kterém je tento certifikát poprvé uveden, je nejvýše 24 hodin.

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

Detailní postupy jsou uvedeny v interní dokumentaci ***„Operátor CA“***.

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

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

4.9.7 Periodicita vydávání seznamu zneplatněných certifikátů

Seznam zneplatněných certifikátů je společností První certifikační autorita, a.s. vydáván neprodleně po úspěšném přijetí požadavku na zneplatnění certifikátu, nejvýše do 24 hodin od vydání předchozího CRL.

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

4.9.8 Maximální zpoždění při vydávání seznamu zneplatněných certifikátů

V procesu vydávání CRL je vždy dodrženo ustanovení kapitoly 4.9.5.

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

Služba může být poskytována smluvním partnerům za specifických podmínek.

[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.

4.9.10 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 soukromého klíče

Služba není poskytována.

4.9.13 Podmínky pro pozastavení platnosti certifikátu

Služba není poskytována.

4.9.14 Subjekty oprávněné požadovat pozastavení platnosti certifikátu

Služba není poskytována.

4.9.15 Zpracování požadavku na pozastavení platnosti certifikátu

Služba není poskytována.

4.9.16 Omezení doby pozastavení platnosti certifikátu

Služba není poskytována.

4.10 Služby související s ověřováním statutu certifikátu

4.10.1 Funkční charakteristiky

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

4.10.2 Dostupnost služeb

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

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

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

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

- *„**Přemístění provozního pracoviště**“.*

4.10.3 Další charakteristiky služeb statutu certifikátu

Další charakteristiky služeb statutu certifikátu nejsou poskytovány. I.CA může bez udání důvodu poskytování charakteristik služeb statutu certifikátu rozšířit.

4.11 Ukončení poskytování služeb pro držitele certifikátu, podepisující osobu

I.CA ukončí poskytování služeb držiteli certifikátu, resp. podepisující 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 soukromého klíče u důvěryhodné třetí strany a jejich obnova

Služba není poskytována.

5 Management, provozní a fyzická bezpečnost

Management bezpečnosti poskytovaných certifikačních služeb v oblasti vydávání certifikátů je zaměřen především na systémy, které vydávají a elektronicky podepisují certifikáty a seznamy zneplatněných certifikátů.

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

- ***„Řízení fyzického přístupu do místností I.CA“,***
- ***„Požární bezpečnost“,***
- ***„Bezpečnostní incidenty“,***
- ***„Příručka administrátora“,***
- ***„Příprava uchovávaných informací“,***
- ***„Záloha dat provozních systémů“,***
- ***„Obnova komponenty provozního pracoviště“,***
- ***„Přemístění provozního pracoviště“,***
- ***„HSM/Private Server“.***

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) provozních pracovišť jsou uvedeny v interní dokumentaci společnosti. Ochrana objektů je řešena elektronickým zabezpečovacím systémem (EZS), připojením na pult centrální ochrany (PCO) a případně speciálním systémem pro snímání, přenos a zobrazování pohybu osob a dopravních prostředků.

5.1.3 Elektřina a klimatizace

V prostorách, určených k výkonu hlavních certifikačních služeb v oblasti vydávání 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 provozních pracovišť jsou umístěny takovým způsobem, aby nemohly být zaplaveny ani stoletou vodou. Provozní pracoviště jsou dle potřeby vybavena čidly průniku vody pro případ zaplavení vodou z topení, nebo vodou ze střechy při prudkém dešti.

5.1.5 Protipožární opatření a ochrana

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

5.1.6 Ukládání médií

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

5.1.7 Nakládání s odpady

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

5.1.8 Zálohy mimo budovu

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

5.2 Procesní bezpečnost

5.2.1 Důvěryhodné role

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

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

5.2.2 Počet osob požadovaných na zajištění jednotlivých činností

Ve společnosti První certifikační autorita, a.s. jsou pro procesy poskytování 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 elektronického podpisu I.CA vydávaných certifikátů a seznamů zneplatněných certifikátů,
- ničení dat pro vytváření elektronického podpisu I.CA vydávaných certifikátů a seznamů zneplatněných certifikátů,
- zálohování/obnovu dat pro vytváření elektronického podpisu I.CA vydávaných certifikátů a seznamů zneplatněných certifikátů,
- aktivace kryptografického modulu, obsahujícího data pro vytváření elektronického podpisu I.CA vydávaných certifikátů a seznamů zneplatněných certifikátů.

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

5.2.3 Identifikace a autentizace pro každou roli

Pracovníkům každé role jsou přiděleny prostředky pro řádnou identifikaci (jméno, certifikát) a autentizaci (heslo, soukromý klíč) k těm komponentám, které jsou pro jejich činnost nezbytné - upraveno interními směrnicemi, zejména:

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

5.2.4 Role vyžadující rozdělení povinností

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

5.3 Personální bezpečnost

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

5.3.1 Požadavky na kvalifikaci, zkušenosti a bezúhonnost

Pracovníci 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 důvěryhodné funkce.

Ostatní pracovníci 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)

Problematika spojená s vytvářením, zpracováním a uchováváním auditních logů je detailně řešena v interní dokumentaci, zejména:

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

5.4.1 Typy zaznamenávaných událostí

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

Doba, po kterou se uchovávají auditní záznamy, je stanovena na minimálně 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

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

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

- ***„Dokumenty agendy certifikačních služeb“.***

5.5.1 Typy informací a dokumentace, které se uchovávají

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

- smlouvy o poskytování certifikační služby, včetně žádosti o poskytování služby,
- případné kopie předložených dokladů, předkládaných při uzavření smlouvy o poskytování certifikační služby,
- potvrzení o převzetí certifikátu držitelem, popř. zmocněncem, případně souhlas držitele se zveřejněním certifikátu v seznamu vydaných certifikátů,
- dokumenty a záznamy související s životním cyklem vydaného certifikátu včetně tohoto certifikátu,
- aplikační programové vybavení a veškerou dokumentaci společnosti, která je nutná pro provádění kontrol,
- 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.

Tyto informace a dokumenty jsou konkretizovány v interních dokumentech ***„Dílčí spisový a skartační řád pro agendy certifikačních služeb“***.

5.5.2 Doba uchovávání uchovávaných informací a dokumentace

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

5.5.3 Ochrana úložiště uchovávaných informací a dokumentace

Uchovávané informace a dokumentace obsahují i osobní data klientů, a proto je vzhledem k 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 výše uvedenými 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 veřejného klíče v certifikátu poskytovatele

Výměna dat pro ověřování elektronických podpisů v kořenovém certifikátu I.CA je v případě standardních situací (vypršení platnosti certifikátu) s dostatečným časovým předstihem (minimálně jeden rok před uplynutím doby platnosti tohoto certifikátu) prováděna formou vydání nového kořenového certifikátu I.CA. V případě nestandardních situací (např. dojde-li k takovému vývoji kryptoanalytických metod, které by mohly ohrozit bezpečnost procesu tvorby elektronických podpisů, 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 podpisů v kořenovém 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

Postupy jsou uvedeny v interním dokumentech, zejména:

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

5.7.2 Poškození výpočetních prostředků, software nebo dat

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

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

5.7.3 Postup při kompromitaci soukromého klíče poskytovatele

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

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

Obdobný postup bude uplatněn i v případě, že dojde k takovému vývoji kryptoanalytických metod (např. změny kryptografických algoritmů, délky klíčů atd.), že by mohla být bezprostředně ohrožena bezpečnost procesu vydávání certifikátů a seznamu zneplatněných certifikátů.

5.7.4 Schopnosti obnovit činnost po havárii

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

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

5.8 Ukončení činnosti CA nebo RA

V případě plánovaného ukončení činnosti I.CA jako kvalifikovaného poskytovatele certifikačních služeb v oblasti vydávání certifikátů, tzn. z jiných důvodů, než 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:

- zpřístupnění informace o ukončení své činnosti všem osobám spoléhajícím se na certifikát, držitelům a jiným osobám, se kterými má smluvní nebo jiné obdobné vztahy týkající se poskytování certifikačních služeb,
- ukončí vydávání všech typů certifikátů,
- uchování údajů získaných při registraci a záznamů událostí po dobu, nejméně 10 let od ukončení platnosti vydaných certifikátů,
- prokazatelně zničí svůj soukromý klíč,
- vyvine maximální úsilí pro to, aby platné certifikáty byly převzaty jinou certifikační autoritou.

V případě ukončení činnosti konkrétního pracoviště RA je tato skutečnost oznámena na internetové adrese (viz kapitola 2.2), případně formou vývěsky (je-li to možné) na pracovišti této RA.

6 Technická bezpečnost

6.1 Generování a instalace párových dat

6.1.1 Generování párových dat

Generování párových dat I.CA probíhá v zabezpečené zóně a o jeho průběhu je vyhotoven písemný protokol.

I.CA používá pro párová data, sloužící k podepisování vydávaných certifikátů a seznamů zneplatněných certifikátů délku 2048 bitů.

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

- ředitel I.CA nebo jím jmenovaný člen vedení I.CA,
- bezpečnostní manager nebo bezpečnostní administrátor (konkrétně určí ředitel I.CA),
- administrátor systému, nebo jiný pověřený technicky proškolený pracovník I.CA.

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

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

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

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

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

I.CA z principiálních bezpečnostních důvodů neposkytuje službu generování párových dat klienta na svých zařízeních.

6.1.2 Předání soukromého klíče žadateli

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 veřejného klíče poskytovateli certifikačních služeb

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

6.1.4 Poskytování veřejného klíče CA spoléhajícím se stranám

Data pro ověřování elektronických podpisů 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,
- každý žadatel o certifikát obdrží kořenový certifikát I.CA při získání svého prvotního certifikátu na RA.

Způsoby získání dat pro ověřování elektronických podpisů držitelů certifikátů 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 veřejného klíče a kontrola jejich kvality

Algoritmy, použité pro generování celočíselných hodnot nutných pro fungování elektronického podpisu (např. testy prvočíselnosti atd.), musí mít parametry uvedené v relevantních technických standardech nebo normách.

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

6.1.7 Omezení pro použití veřejného klíče

Uvedeno v kapitole 1.4.

6.2 Ochrana soukromého klíče a bezpečnost kryptografických modulů

Konkrétní postupy jsou popsány v interní dokumentaci I.CA:

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

6.2.1 Standardy a podmínky používání kryptografických modulů

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

6.2.2 Sdílení tajemství

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

6.2.3 Úschova dat pro vytváření elektronických podpisů

Služba není poskytována.

6.2.4 Zálohování dat pro vytváření elektronických podpisů

Kryptografický modul použitý pro správu párových dat I.CA umožňuje zálohování soukromého klíče, sloužícího pro vytváření elektronických podpisů 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

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

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

Soukromý klíč, sloužící pro vytváření elektronických podpisů 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 podpisů v kryptografickém modulu

Soukromý klíč, sloužící k vytváření elektronických podpisů je uložen bezpečným způsobem v kryptografickém modulu.

6.2.8 Postup při aktivaci dat pro vytváření elektronických podpisů

Aktivaci soukromého klíče, sloužícího pro vytváření elektronických podpisů 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 elektronickému 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

Deaktivaci soukromého klíče, sloužícího pro vytváření elektronických podpisů 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

Soukromý klíč, sloužící k elektronickému podepisování 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 elektronickému podepisování vydávaných certifikátů a seznamů zneplatněných certifikátů jsou definovány v interní bezpečnostní dokumentaci.

6.2.11 Hodnocení kryptografických modulů

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

6.3 Další aspekty správy párových dat

6.3.1 Uchovávání dat pro ověřování elektronických podpisů

Problematika uchovávání dat pro ověřování elektronických podpisů je popsána v interní dokumentaci.

6.3.2 Maximální doba platnosti certifikátu vydaného podepisující 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 podpisů vydávaných certifikátů a seznamů zneplatněných certifikátů.

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

6.4.2 Ochrana aktivačních dat

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

6.4.3 Ostatní aspekty aktivačních dat

Výše uvedená aktivační data jsou určena výhradně pro procesy poskytování 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

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

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

6.5.2 Hodnocení počítačové bezpečnosti

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

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

6.6 Bezpečnost životního cyklu

6.6.1 Řízení vývoje systému

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

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

6.6.2 Kontroly řízení bezpečnosti

Soulad se standardy je ověřován pravidelnými audity, prováděnými pracovníky nezávislých auditorských firem a kontrolami, prováděnými pracovníky I.CA. Tato problematika je popsána v interním dokumentu ***„Kontrolní činnost, bezúhonnost a odbornost“***.

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

6.6.3 Řízení bezpečnosti životního cyklu

Řízení bezpečnosti životního cyklu je v I.CA je vytvářeno procesním přístupem typu „Plánování-Zavedení-Kontrola-Využití“ (**P**lan-**D**o-**C**heck-**A**ct), 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 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.

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

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

6.8 Časová razítka

Řešení je uvedeno v kapitole 5.5.5.

7 Profily certifikátu, seznamu zneplatněných certifikátů a OCSP

7.1 Profil certifikátu

7.1.1 Základní položky certifikátu

Tabulka 3 – Údaje vydávaného certifikátu

Položka	Obsah	Pozn.
Version	v3 (0x2)	povinná, generuje I.CA
serial Number	jedinečné sériové číslo vydávaného certifikátu (přiděluje I.CA)	povinná, generuje I.CA
SignatureAlgorithm	identifikátor algoritmu, použitého I.CA pro elektronický podpis vydávaného certifikátu (sha256WithRSAEncryption)	povinná, generuje I.CA
Issuer	informace o vydavateli certifikátu - viz Tabulka 4	povinná, generuje I.CA
Validity		povinná, generuje I.CA, jedná se jednoleté certifikáty
• notBefore	počátek platnosti vydávaného certifikátu (UTC[12])	
• notAfter	konec platnosti vydávaného certifikátu (UTC)	
Subject	informace o podepisující osobě/držiteli certifikátu: • CountryName (C), • CommonName (CN), • StateOrProvinceName (S), • LocalityName (L), • OrganizationName (O), • OrganizationalUnitName (OU), • emailAddress (E), • Initials (I), • Title (T), • SerialNumber, • GenerationQualifier	viz kapitola 3.1
subjectPublicKeyInfo		povinná, generuje I.CA
• algorithm	rsaEncryption	
• subjectPublicKey	veřejný klíč ve vydávaném certifikátu (2048 bitů)	
Extensions	rozšíření vydávaného certifikátu	viz Tabulka 5

[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 (BIH)

Tabulka 4 – Issuer

Položka	Obsah
Organization (O)	První certifikační autorita, a.s.
OrganizationUnitName(OU)	I.CA - Provider of Certification Services
CommonName (CN)	I.CA - Standard Certification Authority, MM/RRRR
Country (C)	CZ

Pozn.: MM/RRRR je měsíc a rok počátku platnosti certifikátu CA.

7.1.2 Číslo verze

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

7.1.3 Rozšiřující položky v certifikátu

Tabulka 5 – Rozšiřující položky certifikátu

Položka	Obsah	Upřesnění
SubjectAlternativeName	otherName, rfc822Name, dNSName, URI, iPAddress	nekritická a nepovinná položka
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 • Policy	viz kapitola 7.1.7	nekritická a povinná položka, generuje I.CA
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.
• **Produkt TWINS**	digitalSignature, nonRepudiation	(generuje I.CA)
• **Ostatní**	**v případě neuvedení položky v žádosti:** digitalSignature, nonRepudiation, keyEncipherment, dataEncipherment, keyAgreement **v případě uvedení položky v žádosti:** nastavení bitů přebíráno výhradně ze žádosti - v případě používání elektronického podpisu doporučuje I.CA s ohledem na kompatibilitu s produkty třetích stran nastavení bitu digitalSignature	(generuje I.CA) (přebíráno ze žádosti) Pozn. Uplatnění, resp. neuplatnění bitů digitalSignature, nonRepudiation, keyEncipherment, dataEncipherment, keyAgreement lze modifikovat - za škodu způsobenou touto modifikací je odpovědný žadatel o certifikát.
Extended Key Usage	anyExtendedKeyUsage, id-kp-serverAuth, id-kp-clientAuth, id-kp-codeSigning, id-kp-emailProtection, Microsoft SmartCard Logon	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
OID: 1.3.6.1.4.1.23624.4.3	číslo žádosti o certifikát	nekritická položka a pouze v případě vydávání produktu TWINS, 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 certifikačních služeb je využívány OID algoritmů, odkazované příslušnými technickými standardy.

7.1.5 Způsoby zápisu jmen a názvů

Uvedeno v kapitole 3.1.

7.1.6 Omezení jmen a názvů

Pro jméno subjektu (Subject) není žádné omezení s výjimkou omezení vyplývajících z kapitoly 3.1.2. O přípustnosti konkrétního obsahu jednotlivých atributů jména subjektu (atributů položky Subject) 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 certifikátů a je jí přiděleno OID, uvedené v kapitole 1.2.

7.1.8 Rozšiřující atribut „Policy Constrainsts"

Není aplikováno.

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

Položka je nekritická.

7.2 Profil seznamu zneplatněných certifikátů

Tabulka 6 – Základní položky CRL

Položka	Obsah
Version	Verze v2
SignatureAlgorithm	algoritmus pro elektronický podpis vydávaného CRL (

	sha256WithRSAEncryption)
Issuer	vydavatel CRL
thisUpdate	datum a UTC čas vydání CRL
nextUpdate	datum a předpokládaný UTC čas vydání následujícího CRL
revokedCertificates	seznam zneplatněných certifikátů
userCertificate	sériové číslo zneplatněného certifikátu
revocationDate	datum a čas zneplatnění certifikátu
crlEntryExtension.CRL.Reason	důvod zneplatnění certifikátu
crlExtensions	rozšíření CRL - viz 7
signatureValue	elektronický podpis vydaného CRL

7.2.1 Číslo verze

Seznamy zneplatněných certifikátů jsou vydávány dle X 509 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

7.3 Profil OCSP

Viz kapitola 4.9.9.

8 Hodnocení shody a jiná hodnocení

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

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

8.1 Periodicita hodnocení nebo okolnosti pro provedení hodnocení

Audit systému, poskytujícího certifikační služby je prováděn po 2 letech od předchozího auditu. I.CA si vyhrazuje právo provádění i jiných forem kontrol.

8.2 Identita a kvalifikace hodnotitele

Hodnotitelem je fyzická/právnická osoba s příslušnou certifikací, pověřená ředitelem společnosti První certifikační autorita, a.s.

8.3 Vztah hodnotitele k hodnocenému subjektu

Vztah hodnotitele k I.CA je dán standardy, dle kterých je hodnocení prováděno.

8.4 Hodnocené oblasti

Hodnocené oblasti jsou 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 povinen určit, jaká opatření k odstranění případných nedostatků je I.CA povinna přijmout.

8.6 Sdělování výsledků hodnocení

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

V nejbližším možném termínu svolá bezpečnostní manager schůzi bezpečnostního výboru, na které budou mimo vedení společnosti přítomni vedoucí jednotlivých oddělení, na které přítomné s výsledky hodnocení seznámí.

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 (v elektronické verzi 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 certifikačních služeb 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 podpisů, příslušná k datům pro ověřování elektronických podpisů, obsažených v kořenových certifikátech I.CA,
- data pro vytváření elektronických podpisů příslušná k datům pro ověřování elektronických podpisů 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 certifikačních služeb,
- veškeré osobní údaje.

9.3.2 Informace mimo rámec citlivých informací

Za veřejné se považují 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 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 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 elektronickému podepisování vydávaných certifikátů a seznamu zneplatněných certifikátů,
- vydávané certifikáty splňují náležitosti, požadované touto CP,
- 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 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 vyřízení žádostí (viz kapitola 1.3.2). RA nevyřídí kladně žádost, pokud žadatel hodnověrným způsobem neprokázal svoji identitu, nedoložil údaje uvedené v žádosti o službu, odmítá potřebné údaje sdělit nebo odmítne podepsat příslušné dokumenty. Postup je popsán v 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 osoby

Držitel certifikátu nebo podepisující osoba ručí za informace, jimi uvedené ve smlouvě o poskytování certifikační služby a postupují v souladu s platnou legislativou.

9.6.4 Zastupování a záruky spoléhajících se stran

Spoléhající se strany postupují v souladu s touto CP.

9.6.5 Zastupování a záruky ostatních zúčastněných subjektů

Služba není poskytována.

9.7 Zřeknutí se záruk

Společnost První certifikační autorita, a.s., se striktně řídí platnou legislativou a nemůže se zříci záruk v ní určených.

9.8 Omezení odpovědnosti

Hranice odpovědnosti společnosti První certifikační autorita, a.s., se v oblasti poskytování certifikačních služeb řídí touto CP a 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 (tzn. držitel certifikátu, podepisující osoba) 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 podpisů, popř. samotné kompromitace dat pro vytváření elektronických podpisů, kterými I.CA elektronicky podepisuje vydávané certifikáty a seznamy zneplatněných certifikátů, nabídne I.CA držitelům bezplatné vydání nového certifikátu - případné náklady na vydání nových certifikátů hradí I.CA, která po dobu zablokování certifikátů nese veškerou odpovědnost za případné škody vzniklé v souvislosti se zneužitím těchto certifikátů,
- v případě, že I.CA při příjmu žádosti o vydání certifikátu zjistí, že existuje jiný certifikát se stejným veřejným klíčem, je žadatel o certifikát vyzván k vygenerování nové žádosti, a tedy i nových párových dat - držitel již existujícího certifikátu, který vlastní veřejný klíč stejný jako žadatel o vydání certifikátu, je vyzván k vygenerování nových párových dat, jeho původní certifikát je okamžitě zneplatněn a držitel je o této skutečnosti informován.

9.10 Doba platnosti, ukončení platnosti

9.10.1 Doba platnosti

Tento dokument zůstává platnosti do skončení platnosti posledního certifikátu, který byl dle odpovídající CP vydán.

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 držiteli certifikátů může I.CA využít jimi dodané e-mailové adresy, poštovní adresy, telefonická čísla nebo osobní jednání.

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

9.12 Změny

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

9.12.1 Postup při změnách

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

9.12.2 Postup při oznamování změn

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

9.12.3 Okolnosti, při kterých musí být změněno OID

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

9.13 Řešení sporů

V případě, že držitel certifikátu, spoléhající se strana, žadatel o certifikát 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 certifikačních služeb v oblasti vydávání certifikátů je provozován ve shodě s požadavky platné legislativy.

9.16 Další ustanovení

9.16.1 Rámcová shoda

Tyto skutečnosti jsou pro aplikaci vydání tohoto dokumentu irelevantní.

9.16.2 Postoupení práv

Tyto skutečnosti jsou pro aplikaci vydání tohoto dokumentu irelevantní.

9.16.3 Oddělitelnost ustanovení

Tyto skutečnosti jsou pro aplikaci vydání tohoto dokumentu irelevantní.

9.16.4 Zřeknutí se práv

Tyto skutečnosti jsou pro aplikaci vydání tohoto dokumentu irelevantní.

9.16.5 Vyšší moc

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

9.17 Další opatření

Tyto skutečnosti jsou pro aplikaci vydání tohoto dokumentu irelevantní.

10 Závěrečná ustanovení

Tato CPS vydaná, společností První certifikační autorita, a.s., nabývá platnosti a účinnosti dnem 22.09. 2015.