První certifikační autorita, a.s.

CERTIFIKAČNÍ PROVÁDĚCÍ SMĚRNICE

VYDÁVÁNÍ KVALIFIKOVANÝCH CERTIFIKÁTŮ A/NEBO KVALIFIKOVANÝCH SYSTÉMOVÝCH CERTIFIKÁTŮ

Verze 2.6

Tabulka 1 – Identifikace

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

Tabulka 2 – Vývoj dokumentu

Verze	Datum vydání	Shrnutí změn
1.00	18.12.2001	První verze dokumentu
1.01	27.12.2001	Zapracování připomínek
1.02	18.02.2002	Inovace kapitoly 7
1.03	15.03.2002	Úprava profilu kvalifikovaného certifikátu
1.04	10.06.2005	Aktualizace podle zákona č. 227/2000 Sb., o elektronickém podpisu a o změně některých dalších zákonů (zákon o elektronickém podpisu), jak vyplývá ze změn provedených zákonem č. 226/2002 Sb., zákonem č. 517/2002 Sb., a zákonem č. 440/2004 Sb., aktualizace norem, procedur auditu
2.0	09.12.2005	Vytvoření struktury striktně dle RFC 3647 Zaměření na problematiku kvalifikovaných certifikátů nebo kvalifikovaných systémových certifikátů
2.1	10.04.2006	Úprava kapitol 3, 7
2.2	14.10.2006	Akreditace SK
2.3	01.08.2007	Vyhláška 378/2006, sjednocení názvu nadřízený QSC a certifikát I.CA,
2.4	02.08.2008	Úprava dokumentu s ohledem na splnění podmínek Microsoft Root Certificate Program - zařazení root certifikátu do důvěryhodných kořenových certifikačních úřadů.
2.5	22.12.2008	Aktualizace s ohledem na novelu slovenské legislativy č. 214/2008 Z.z.
2.6	22.09.2015	Aktualizace a revize dokumentu

Obsah

1 Úvod

Společnost **První certifikační autorita, a.s.,** je od:

- 18.03.2002 prvním akreditovaným poskytovatelem certifikačních služeb v České republice pro oblast vydávání **kvalifikovaných certifikátů** podle zákona č. 227/2000 Sb., o elektronickém podpisu a o změně některých dalších zákonů (zákon o elektronickém podpisu), jak vyplývá ze změn provedených zákonem č. 226/2002 Sb., zákonem č. 517/2002 Sb., a zákonem č. 440/2004 Sb.,
- 01.02.2006 akreditovaným poskytovatelem certifikačních služeb v České republice pro oblast vydávání **kvalifikovaných systémových certifikátů a kvalifikovaných časových razítek** podle zákona č. 227/2000 Sb., o elektronickém podpisu a o změně některých dalších zákonů (zákon o elektronickém podpisu), jak vyplývá ze změn provedených zákonem č. 226/2002 Sb., zákonem č. 517/2002 Sb., a zákonem č. 440/2004 Sb.,.
- 21.09.2006 prvním zahraničním kvalifikovaným poskytovatelem certifikačních služeb ve Slovenské republice, kterému byla udělena akreditace v oblasti poskytování **kvalifikovaných certifikátů a kvalifikovaných časových razítek** podle aktuálního znění zákona č. 215/2002 Z.z., o elektronickom podpise a o zmene a doplnení niektorých zákonov v platnom znení a s ním spojených vykonávacích vyhlášok

Tento dokument, **Certifikační politika vydávání kvalifikovaných certifikátů** (dále též CP), vypracovaný společností První certifikační autorita, a. s. (dále též I.CA):

- je v souladu se zákonem České republiky č. 227/2000 Sb., o elektronickém podpisu a o změně některých dalších zákonů (zákon o elektronickém podpisu), jak vyplývá ze změn provedených zákonem č. 226/2002 Sb., zákonem č. 517/2002 Sb., a zákonem č. 440/2004 Sb., a s ním souvisejících předpisů a vyhlášek,
- je v souladu s aktuálním zněním zákona Slovenské republiky č. 215/2002 Z.z., o elektronickom podpise a o zmene a doplnení niektorých zákonov v platnom znení a s ním spojených vykonávacích vyhlášok,
- se zabývá skutečnostmi, které se vztahují na I.CA, podepisující osoby, držitele, spoléhající se strany, jiné účastníky PKI a smluvní partnery a které souvisejí s vydáváním **kvalifikovaných certifikátů**, jejich další správou, použitím, akceptací, ukončením platnosti, zneplatněním a všemi aspekty souvisejícími s nakládáním s párovými daty,
- striktně dodržuje členění dokumentu navržené v RFC 3647, s přihlédnutím k doporučením orgánů EU a k právu České republiky a Slovenské republiky v dané oblasti. Jednotlivé kapitoly jsou proto v této CP zachovány i v případě, že jsou ve vztahu k ní irelevantní.

S ohledem na skutečnost, že společnost První certifikační autorita, a.s. vydává více druhů certifikátů dle různých politik, překontrolujte a ujistěte se o tom, že tento dokument odpovídá Vašim požadavkům na kvalifikovaný certifikát.

1.1 Přehled

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

Pro oblast kvalifikovaných certifikátů, vydávaných v souladu s aktuálním zněním zákona České republiky č. 227/2000 Sb., o elektronickém podpisu, je pro sestavení certifikační cesty stanoven jako důvěryhodná kotva certifikát, vydaný společností První certifikační autorita, a.s, který ověřilo Ministerstvo vnitra České republiky (viz písm. d) odst. 2 §9 zákona č. 227/2000 Sb.,). Tento nadřízený kvalifikovaný systémový certifikát je umístěn jak na stránkách Ministerstva vnitra České republiky, tak společnosti První certifikační autorita, a.s. a obsahuje data pro ověřování elektronického podpisu, odpovídající datům pro tvorbu elektronického podpisu, kterými společnost První certifikační autorita, a.s. podepisuje vydávané

kvalifikované certifikáty, kvalifikované systémové certifikáty a seznamy zneplatněných certifikátů. Vydávání a správa tohoto certifikátu je v I.CA řízena speciálními dokumenty.

Pro oblast kvalifikovaných certifikátů, vydávaných v souladu s aktuálním znění zákona Slovenské republiky č. 215/2002 Z.z. o elektronickém podpisu, je pro sestavení certifikační cesty důvěryhodnou kotvou kořenový certifikát Národního bezpečnostního úřadu Slovenské republiky, vydaný kořenovou certifikační autoritou, spravovanou Národním bezpečnostním úřadem Slovenské republiky (NBÚ SK). Tato kořenová certifikační autorita, v souladu se slovenskou legislativou, vydává a ověřuje certifikáty akreditovaným certifikačním autoritám. Teprve tyto certifikáty, umístěné na stránkách NBÚ SK, obsahují data pro ověřování elektronického podpisu, odpovídající datům pro tvorbu elektronického podpisu, kterými akreditované certifikační autority, a tedy i společnost První certifikační autorita, a.s. podepisuje uživatelům vydávané kvalifikované certifikáty, resp. seznamy zneplatněných certifikátů. Vygenerování žádosti o tento certifikát se v I.CA řídí speciálními dokumenty.

V procesu poskytování kvalifikovaných certifikačních služeb v oblasti vydávání certifikátů provozuje společnost První certifikační autorita, a.s jedinou certifikační autoritu – viz kapitola 1.3.1.

Informace o vydaných certifikátech, certifikátech CA, dalších poskytovaných certifikačních službách atd. je možno získat na internetové informační adrese, uvedené v kapitole 2.

Legislativa České republiky nekonkretizuje úložiště soukromého klíče, úložištěm soukromého klíče dle legislativy Slovenské republiky smí být pouze produkty, certifikované NBÚ SK.

Není-li uvedeno jinak, je dále v tomto dokumentu pod pojmy:

- **certifikát** míněn kvalifikovaný certifikát a/nebo kvalifikovaný systémový certifikát ,
- **certifikát CA** míněn nadřízený kvalifikovaný systémový certifikát I.CA, resp. kvalifikovaný certifikát I.CA – obsahuje data pro ověřování elektronických značek, resp. podpisů, odpovídající datům pro vytváření elektronických značek, resp. podpisů, kterými I.CA elektronicky označuje, resp. podepisuje vydávané certifikáty a seznamy zneplatněných certifikátů.

1.2 Název a identifikace dokumentu

Název tohoto dokumentu: Certifikační prováděcí směrnice vydávání kvalifikovaných certifikátů a/nebo kvalifikovaných systémových certifikátů, verze 2.6

OID dokumentu: není přiřazeno

Tato CPS se vztahuje k následujícím CP:

OID	CP
1.3.6.1.4.1.23624.1.4.10.5	Certifikační politika vydávání kvalifikovaných certifikátů
1.3.6.1.4.1.23624.1.4.11.3	Certifikační politika vydávání kvalifikovaných systémových certifikátů

1.3 Participující subjekty

1.3.1 Certifikační autority (dále „CA“)

I.CA je akreditovaným poskytovatelem certifikačních služeb. Podřízené certifikační autority, poskytující kvalifikované certifikační služby, související s vydáváním certifikátů I.CA nezřizuje, ani nepodporuje.

1.3.2 Registrační autority (dále „RA“)

Poskytování služeb I.CA se realizuje prostřednictvím registračních autorit. RA jsou buď vlastní nebo smluvních partnerů. I.CA podporuje níže uvedené typy registračních autorit.

Vlastní stacionární registrační autorita (VSRA):

- je základní decentralizovanou složkou výkonného aparátu I.CA,
- přijímá žádosti o služby dle této CP, zejména přijímá žádosti o certifikáty, zprostředkovává předání certifikátů a seznamů zneplatněných certifikátů, poskytuje potřebné informace, vyřizuje reklamace atd.,
- je oprávněna z naléhavých provozních nebo technických důvodů pozastavit zcela nebo zčásti výkon své činnosti - toto opatření je povinna neprodleně hlásit řediteli I.CA, který je potvrdí, zruší nebo změní,
- je zmocněna jménem I.CA uzavírat smlouvy o poskytování kvalifikované certifikační služby
- zajišťuje zpoplatňování služeb I.CA, pokud není stanoveno smlouvou jinak.

Vlastní mobilní registrační autorita (VMRA):

- je zvláštní decentralizovanou mobilní složkou výkonného aparátu I.CA.
- přijímá žádosti o služby dle této CP, zejména přijímá žádosti o certifikáty, zprostředkovává předání certifikátů a seznamů zneplatněných certifikátů, poskytuje potřebné informace, vyřizuje reklamace atd.,
- je oprávněna z naléhavých provozních nebo technických důvodů pozastavit zcela nebo zčásti výkon své činnosti - toto opatření je povinna neprodleně hlásit řediteli I.CA, který je potvrdí, zruší nebo změní,
- je zmocněna jménem I.CA uzavírat smlouvy o poskytování kvalifikovaných certifikačních služeb,
- zajišťuje zpoplatňování služeb I.CA, pokud není stanoveno smlouvou jinak.

Smluvní registrační autorita (SRA):

- plní jménem I.CA obdobné funkce jako vlastní RA na základě písemné smlouvy mezi I.CA a provozovatelem SRA.

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

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

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

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

1.3.4 Spoléhající se strany

Spoléhající se stranou jsou subjekty, spoléhající se při své činnosti na kvalifikovaný certifikát nebo kvalifikovaný systémový certifikát vydaný I.CA, tzn. fyzické osoby, právnické osoby, organizační složky státu apod.

1.3.5 Jiné participující subjekty

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

1.4 Použití certifikátu

Certifikáty vydané dle této CPS lze použít ve shodě s ZoEP.

1.4.1 Přípustné použití certifikátu

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

1.4.2 Omezení použití certifikátu

Certifikáty nesmí být využívány v rozporu s vydávaným účelem a platnou legislativou. Dále platí ustanovení, uvedené v kapitole 1.4.1.

1.5 Správa politiky

1.5.1 Organizace spravující certifikační politiku nebo certifikační prováděcí směrnici

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

1.5.2 Kontaktní osoba organizace spravující certifikační politiku nebo certifikační prováděcí směrnici

Ředitel společnosti První certifikační autorita, a.s. určuje kontaktní osobu, jejíž e-mail, telefonní číslo a fax jsou uvedeny na internetové informační adrese.

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

Jedinou osobou, která je odpovědná za rozhodování o souladu postupů I.CA s postupy jiných poskytovatelů certifikačních služeb, je ředitel společnosti První certifikační autorita, a.s. Déle platí ustanovení kapitoly 3.2.6.

1.5.4 Postupy při schvalování souladu s bodem 1.5.3

V případě, že je potřebné s ohledem na kapitolu 1.5.3 provést změny v odpovídající CP a této CPS, určuje ředitel I.CA osobu, která je oprávněna změny provádět.

1.6 Přehled použitých pojmů a zkratek

Dále uvedený přehled pojmů a zkratky je platný pro tento dokument. V případě pojmu může být na pravé straně v závorkách uveden zdroj, v němž se nachází původní pojem včetně definice. Použité zkratky

mají alternativní charakter, tzn. v textu může být použita jak plný text, tak i jeho zkratka, přičemž obojí má totožnou obsahovou hodnotu.

Tabulka 3 – Pojmy a zkratky

Pojem	Vysvětlení
CA	centrální pracoviště certifikační autority společnost První certifikační autorita, a.s.
Certifikát	datová zpráva, která je vydána poskytovatelem certifikačních služeb, spojuje data pro ověřování elektronických podpisů (CZ, SK) s podepisující osobou a umožňuje ověřit její identitu, nebo spojuje data pro ověřování elektronických značek (CZ) s označující osobou a umožňuje ověřit její identitu
CP	certifikační politika (veřejný dokument)
CPS	certifikační prováděcí směrnice (neveřejný dokument)
CRL (Certification Revocation List)	Seznam zneplatněných certifikátů
Čas	světový čas UTC
CZ	mezinárodní kód pro Českou republiku
Držitel certifikátu	• česká legislativa - fyzická osoba, právnická osoba nebo organizační složka státu, která požádala o vydání kvalifikovaného certifikátu nebo kvalifikovaného systémového certifikátu pro sebe nebo pro podepisující osobu nebo pro označující osobu a které byl kvalifikovaný certifikát nebo kvalifikovaný systémový certifikát vydán • slovenská legislativa - fyzická osoba, které byl na základě slovenské legislativy certifikát vydán
Elektronický podpis	údaje, resp. informace, které splňují požadavky české, resp. slovenské legislativy
Elektronická značka (CZ)	údaje v elektronické podobě, které jsou připojené k datové zprávě nebo jsou s ní logicky spojené a které splňují následující požadavky: • jsou jednoznačně spojené s označující osobou a umožňují její identifikaci prostřednictvím kvalifikovaného systémového certifikátu • byly vytvořeny a připojeny k datové zprávě pomocí prostředků pro vytváření elektronických značek, které označující osoba může udržet pod svou výhradní kontrolou • jsou k datové zprávě, ke které se vztahují, připojeny takovým způsobem, že je možné zjistit jakoukoli následnou změnu dat
ETSI	**E**uropean **T**elecommunications **S**tandards **I**nstitute
IETF	**I**nternet **E**ngineering **T**ask **F**orce
EPS	Elektrická požární signalizace
I.CA	První certifikační autorita, a.s. – akreditovaný poskytovatel certifikačních služeb
Kvalifikovaný certifikát (QC)	certifikát, který má náležitosti podle platné legislativy a byl vydán kvalifikovaným poskytovatelem certifikačních služeb
MV CZ	Ministerstvo vnitra České republiky
Nadřízený kvalifikovaný systémový certifikát (CZ)	kvalifikovaný certifikát poskytovatele certifikačních služeb, který se řídí speciálními dokumenty vydanými I.CA • „Certifikační politika vydávání certifikátů CA/TSU“ • „Certifikační prováděcí směrnicí vydávání certifikátů CA/TSU“
Následný kvalifikovaný certifikát	kvalifikovaný certifikát, který byl v souladu se smlouvou o poskytování kvalifikované certifikační služby, uzavřenou mezi koncovým uživatelem a I.CA, vydán koncovému uživateli na základě nové žádosti o kvalifikovaný certifikát elektronicky podepsané platnými daty pro vytváření elektronických podpisů souvisejícími s již vydaným kvalifikovaným certifikátem, ke kterému je vydáván tento následný

	kvalifikovaný certifikát ať již z důvodu výměny dat pro ověřování elektronických podpisů
NIST	**N**ational **I**nstitute of **S**tandards and **T**echnology
OID	(Object Identifier) číselná identifikace objektu v rámci jednotné klasifikace objektů podle ISO/ITU
Párová data (dvojice soukromý a veřejný klíč)	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 Certifikační autority I.CA – souhrnný název pro VSRA, VMRA, SRA. Používá se v případech, kdy není podstatný majitel registrační autority ani její forma
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 (ČZ, SK) nebo elektronické značky (CZ)
SK	mezinárodní kód pro Slovenskou republiku
SRA	smluvní registrační autorita Certifikační autority I.CA - plní obdobné funkce jako VSRA nebo VMRA na základě písemné smlouvy mezi I.CA a provozovatelem SRA
Statut kvalifikovaného certifikátu	stav, ve kterém se kvalifikovaný certifikát nachází, tzn. ve stavech platnosti, neplatnosti, zneplatnění, zablokování
Spoléhající se strana	subjekt, spoléhající se při své činnosti na certifikát, vydaný I.CA
UPS	Uninterruptible Power Supply
UTC	**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)
Veřejný klíč	jedinečná data pro ověřování elektronického podpisu (CZ, SK) nebo elektronické značky (CZ)
VMRA	vlastní mobilní registrační autorita Certifikační autority I.CA
VoEP	• vyhláška České republiky č. 378/2006 Sb., o postupech kvalifikovaných poskytovatelů certifikačních služeb, o požadavcích na nástroje elektronického podpisu a o požadavcích na ochranu dat pro vytváření elektronických značek (vyhláška o postupech kvalifikovaných poskytovatelů certifikačních služeb), • sada vyhlášek Slovenské republiky, vztahujících se k problematice aktuálního znění zákona Slovenské republiky č. 215/2002 Z.z., o elektronickom podpise a o zmene a doplnení niektorých zákonov
VSRA	vlastní stacionární registrační autorita Certifikační autority I.CA
Zablokování	stav, ve kterém se kvalifikovaný certifikát nebo kvalifikovaný systémový certifikát nachází od doby, kdy jej I.CA zneplatnila, do doby, kdy I.CA zveřejnila CRL, ve kterém je tento kvalifikovaný certifikát nebo kvalifikovaný systémový certifikát poprvé zařazen.
Zaručený elektronický podpis	elektronický podpis, splňující požadavky české, resp. slovenské legislativy
Zneplatnění	stav kvalifikovaného certifikátu, který byl I.CA zneplatněn – tomuto certifikátu nelze již platnost obnovit
ZoEP	• aktuální znění zákona České republiky č. 227/2000 Sb., o elektronickém podpisu a o změně některých dalších zákonů (zákon o elektronickém podpisu), jak vyplývá ze změn

	provedených zákonem č. 226/2002 Sb., zákonem č. 517/2002 Sb., a zákonem č. 440/2004 Sb.. • aktuální znění zákona Slovenské republiky č. 215/2002 Z.z., o elektronickom podpise a o zmene a doplnení niektorých zákonov
Žádost o službu (Žádost)	formální dokument žádosti o některou ze služeb poskytovaných I.CA např. žádost o vydání kvalifikovaného certifikátu, žádost o zneplatnění kvalifikovaného certifikátu atd.
Žádost o vydání kvalifikovaného certifikátu	formální, standardní dokument elektronické žádosti o vydání kvalifikovaného certifikátu dle přípustných norem a směrnic definovaných v této CP

2 Odpovědnosti za zveřejňování, úložiště informací a dokumentace

2.1 Úložiště informací a dokumentace

S ohledem na požadavky ZoEP zřizuje I.CA úložiště informací a dokumentace.

2.2 Zveřejňování informací a dokumentace

Základní adresy, na nichž lze nalézt veřejné informace o I.CA, tzn. certifikační politiky, zprávy pro uživatele, další informace dle ZoEP, ostatní veřejné dokumenty atd., (dále též informační adresy), 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 (dále též internetová informační adresa)

c) sídla registračních autorit

Adresy, které slouží pro kontakt veřejnosti s I.CA (dále též kontaktní adresy), 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 informační adrese, pracovištích SRA a VSRA. Pracovníci I.CA a smluvních partnerů (SRA) jsou rovněž povinni tyto informace na vyžádání sdělit všem uživatelům. Totéž platí i v případě, že dojde ke změně kontaktních adres.

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 atributu 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).

I.CA garantuje zajištění nepřetržité dostupnosti a integrity seznamu vydaných veřejných certifikátů.

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 informacím o:

- konkrétních CP a Zprávě pro uživatele - HTTP,
- vydaných veřejných certifikátech - HTTP, HTTPS, FTP,
- seznamech zneplatněných certifikátů - HTTP, HTTPS, FTP.

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

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

2.3 Periodicita zveřejňování informací

I.CA zveřejňuje informace s následující periodicitou:

- Certifikační politika vydávání kvalifikovaných certifikátů, resp. Certifikační politika vydávání kvalifikovaných systémových certifikátů - před prvním vydáním certifikátu v souladu s danou CP.
- Zpráva pro uživatele – při zahájení poskytované certifikační služby v oblasti vydávání certifikátů, popř. při její změně.
- Získání nebo odejmutí akreditace dle ZoEP – okamžitě.
- informace o zneplatnění certifikátu CA s uvedením důvodu zneplatnění (v případě zneužití nebo vzniku důvodné obavy ze zneužití dat pro vytváření elektronických značek, resp. elektronických podpisů, určených pro označování, resp. podepisování vydávaných certifikátů a seznamů zneplatněných certifikátů) – bezodkladně.
- Aktualizace seznamu vydaných certifikátů – okamžitě při každém vydání nového certifikátu.
- Vydávání seznamu zneplatněných certifikátů - tato povinnost je realizována periodickým vydáváním CRL minimálně jedenkrát za 24 hodin (zpravidla po 8 hodinách). Vydávání CRL je nepřetržité – 7 dní v týdnu. Internetové adresy, na kterých lze získat CRL dálkovým přístupem, jsou uvedeny na internetové informační adrese I.CA a jsou rovněž uvedeny v každém certifikátu. I.CA zveřejňuje seznamy zneplatněných certifikátů nejméně dvěma na sobě nezávislými způsoby dálkového přístupu.
- Ostatní veřejné informace – není předem určeno, obecně však platí, že tyto informace musí odrážet aktuální stav poskytovaných kvalifikovaných certifikačních služeb.

2.4 Řízení přístupu k jednotlivým typům úložišť

Přístup ke konkrétním typům úložišť pověřenými pracovníky I.CA je definován interní dokumentací:

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

3 Identifikace a autentizace

3.1 Pojmenovávání

3.1.1 Typy jmen

Tabulka 4 – QC: základní atributy předmětu (Subject)

Pořadí/Atribut	Kódování Min/Max	Žádost	Certifikát	Význam	Příklad	Doložení[1]
1./CountryName	PS 2/2	=1	=1	kap. 3.1.2.1	CZ	primární doklad
2./CommonName	U8,(BMP)[2] 1/64	=1	=1	kap. 3.1.2.2, popř. pseudonym, následovaný řetězcem „ – PSEUDONYM “	Ing. Petr Jan Holoubek PhD, popř. Kokoška – PSEUDONYM	primární doklad
3./StateOrProvinceName	U8,(BMP) 1/128	1	1	kap. 3.1.2.3	Praha	primární doklad
4./LocalityName	U8,(BMP) 1/128	1	1	kap. 3.1.2.4	Praha 7 Ovenecká 1047/17 17000	primární doklad
5./OrganizationName	U8,(BMP) 1/64	1	1	kap. 3.1.2.5	Společnost, a.s.	VOR[3], ŽL[4]
6./OrganizationalUnitName	U8,(BMP) 1/64	M	M	kap. 3.1.2.6	Odbor systému a sítě	POZ[5]
7./Pkcs9_EmailAddress	IA5 1/64	1	1	kap. 3.1.2.7	holy@quick.cz	
8./GivenName	U8,(BMP) 1/64	1r	1	kap. 3.1.2.8	Petr Jan	primární doklad
9./Initials	U8,(BMP) 1/64	1	1	kap. 3.1.2.9	PJH	primární doklad
10./Name	U8,(BMP) 1/64	1r	1	kap. 3.1.2.10	Ing. Petr Jan Holoubek PhD	primární doklad
11./Surname	U8,(BMP) 1/64	1r	1	kap. 3.1.2.11	Holoubek	primární doklad
12./Title	U8,(BMP) 1/64	M	M	kap. 3.1.2.12	specialista systému a sítě	POZ
13./SerialNumber	PS 1/64	CZ:1r SK:2r	CZ:=1 SK:1-2	kap. 3.1.2.13	CZ:ICA – 10020184 SK: rodné číslo, číslo pasu, nebo číslo průkazu	SK: kontrolovaný doklad

[1] Viz uvedené kapitoly ve sloupci „Význam“
[2] Pro certifikáty dle ZoEP SK je použito pouze kódování U8 – UTF8String
[3] Výpis z obchodního rejstříku
[4] Živnostenský list
[5] Potvrzení o zaměstnání

					totožnosti v definovaném tvaru	
14./GenerationQualifier	U8,(BMP) 1/64	1	1	kap. 3.1.2.14	Ml.	primární doklad
15./Pseudonym	U8,(BMP) 1/128	1r	1	kap. 3.1.2.15	Kokoska	-

Tabulka 4a – QSC: základní atributy předmětu (Subject)

Pořadí/Atribut	Kódování Min/Max	Žádost	Certifikát	Význam	Příklad	Doložení
1./CountryName	PS 2/2	=1	=1	kap. 3.1.2.1	CZ	primární doklad
2./CommonName	U8,BMP 1/64	=1	=1	kap. 3.1.2.2, popř. pseudonym, následovaný řetězcem „ – PSEUDONYM “	Ing. Petr Jan Holoubek PhD, popř. Kokoška – PSEUDONYM	primární doklad
3./StateOrProvinceName	U8,BMP 1/128	1	1	kap. 3.1.2.3	Praha	primární doklad
4./LocalityName	U8,BMP 1/128	1	1	kap. 3.1.2.4	Praha 7 Ovenecká 1047/17 17000	primární doklad
5./OrganizationName	U8,BMP 1/64	1	1	kap. 3.1.2.5	Společnost, a.s.	VOR, ŽL
6./OrganizationalUnitName	U8,BMP 1/64	M	M	kap. 3.1.2.6	Odbor systému a sítě	POZ
7./Pkcs9_EmailAddress	IA5 1/64	1	1	kap. 3.1.2.7	holy@quick.cz	
8./Initials	U8,BMP 1/64	1	1	kap. 3.1.2.9	PJH	primární doklad
9./Name	U8,BMP 1/64	1	1	kap. 3.1.2.10	Ing. Petr Jan Holoubek PhD	primární doklad
10./Title	U8,BMP 1/64	M	M	kap. 3.1.2.12	specialista systému a sítě	POZ
11./SerialNumber	PS 1/64	1r	=1	kap. 3.1.2.13	CZ:ICA – 10020184	
12./GenerationQualifier	U8,BMP 1/64	1	1	kap. 3.1.2.14	Ml.	primární doklad

Tabulka 5 – Rozšiřující atributy žádosti o certifikát, resp. certifikátu

Atribut	Kódování	Žádost	Certifikát	Význam	Příklad	Doložení
SubjectAlternativeName						
• otherName	Dle RFC3280, resp. RFC 5280	M	M	kap. 3.1.2.16		
• rfc822Name	IA5	M	M	kap. 3.1.2.16	holy@quick.cz	
• dNSName	IA5	M	M	kap. 3.1.2.16	www.moje.cz	čestné prohlášení

• uniformResourceIdentifier	IA5	M	M	kap. 3.1.2.16	http:// www.moje.cz	čestné prohlášení
• iPAddress	Dle RFC3280, resp. RFC 5280	M	M	kap. 3.1.2.16	172.17.5.3	čestné prohlášení

Legenda:

- **Pořadí** určuje pořadí atributů v předmětu vydávaných certifikátů. Jestliže je některý z atributů v certifikátu obsažen vícekrát, pak pořadí těchto stejných atributů je dáno pořadím, uvedeným v žádosti o certifikát.
- **Kódování** určuje množinu povolených kódování dle ASN.1 pro daný atribut předmětu. Použité typy kódování jsou **PS** - PrintableString, **IA5** - IA5String, **U8** - UTF8String, **BMP** – BMPString a mohou být v rámci jednotlivých obchodních produktů omezeny.
- **Min** a **Max** určují minimální a maximální povolenou délku ve znacích v daném atributu předmětu
- **Žádost** a **Certifikát** udává výskyt daného atributu předmětu v žádosti o certifikát, resp. v certifikátu. Použité zkratky mají následující význam:
  - **=1** : právě jedna,
  - **1** : maximálně jedna,
  - **1r** : maximálně jedna v žádosti o následný certifikát, jinak nula,
  - **1-2** : minimálně jedna, maximálně dvě,
  - **2r** : maximálně dvě v žádosti o následný certifikát, jinak maximálně jedna,
  - **M** : libovolný počet.

3.1.2 Požadavek na významovost jmen

Společnost První certifikační autorita, a.s. vydává certifikáty s atributy předmětu podle požadavků obsažených v žádosti o certifikát s následujícími výjimkami:

- v atributech dochází 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,
- atribut SerialNumber je naplněn řetězcem „ICA - “ a za něj je připojeno na řetězec převedené identifikační číslo klienta.

Při kontrole rozdílnosti či shodnosti atributů je použitý následující způsob porovnávání:

- jestliže jsou obsahy dvou stejných atributů různě kódovány, jsou tyto atributy považovány za shodné
- porovnávání obsahů atributů ve všech kódováních je závislé na velikosti písma
- při porovnávání obsahu atributů ve všech kódováních jsou odstraňovány mezerové znaky (např. řetězce „Martin“ a „ Martin“ jsou shodné)

Dva předměty jsou shodné, jestliže platí:

- ke všem atributům prvního předmětu (kromě Pkcs9_EmailAddress a SerialNumber) byly nalezeny odpovídající atributy v druhém předmětu
- ke všem atributům druhého předmětu (kromě Pkcs9_EmailAddress a SerialNumber) byly nalezeny odpovídající atributy v prvním předmětu
- shodné atributy předmětů (kromě Pkcs9_EmailAddress a SerialNumber) obsahující shodné hodnoty
- pokud atribut SerialNumber obsahují oba předměty a hodnota atributů má stejný prefix, tak tyto atributy musí mít shodnou hodnotu

Kontroly na RA/CA:

- přítomnost nepovolených znaků (v závislosti na typu pole) - v případě výskytu nepovolených znaků se žádost nepřijme
- přítomnost všech povinných atributů - pokud některý z povinných atributů není vyplněn, žádost se nepřijme (povinnými atributy pro veškeré fyzické osoby jsou CommonName a CountryName, pro fyzické osoby podnikajících nebo zaměstnance je přidáno navíc OrganizationName)

Dále se kontroluje věcná správnost jmen. Rozsah kontrol je uveden v následujících podkapitolách.

3.1.2.1 CountryName (Stát)

- **QC**: Atribut může obsahovat pouze kód státu (musí odpovídat normě ISO 3166), v němž má žadatel o certifikát uvedeno místo trvalého pobytu nebo sídla - uvedeno v primárním osobním dokladu. RA kontroluje správnost podle primárního dokladu (pokud není stát explicitně uveden, uvede se stát, který předkládaný doklad vydal), v případě neshody žádost odmítne.
- **QSC** Atribut může obsahovat pouze kód státu (musí odpovídat normě ISO 3166), v němž má žadatel o certifikát v případě fyzické osoby nepodnikající trvalé bydliště podle primárního osobního dokladu, v případě fyzické osoby podnikající, právnické osoby, organizační složky státu nebo zaměstnanec název firmy, pracoviště podle VOR, ŽL, zřizovací listiny atd. RA kontroluje správnost podle výše uvedeného dokladu (fyzická osoba nepodnikající - pokud není explicitně uveden v primárním osobním dokladu, uvede se stát, který předkládaný průkaz vydal) nebo podle VOR, ŽL, zřizovací listiny atd. V případě neshody žádost odmítne.

3.1.2.2 CommonName (Obecné jméno)

Atribut může obsahovat znaky s diakritikou a je vytvářen dle následujícího schématu:

- **QC**:
  - jméno a příjmení, případně další jméno/jména a tituly, uvedené v primárním dokladu žadatele o certifikát - RA kontroluje správnost podle primárního osobního dokladu, v případě neshody žádost odmítne, nebo
  - název pseudonymu, doplněný řetězcem „ – PSEUDONYM“. Problematika doložení názvu pseudonymu a procesy RA jsou uvedeny v kapitole 3.1.2.15
- **QSC**:
  - název zařízení, nebo
  - název organizace (kapitola 3.1.2.5), nebo
  - celé jméno (viz QC této kapitoly).

3.1.2.3 StateorProvinceName (Kraj)

- **QC**: Atribut může obsahovat pouze označení nižšího územně správního celku, do něhož spadá místo trvalého bydliště podle primárního dokladu žadatele o certifikát, tedy město, obec nebo jinou správní jednotku, která je v primárním osobním dokladu uvedena. Z obsahu musí být zřejmé, zda se jedná o kraj nebo jiný celek. RA přijímající předmětnou žádost správnost tohoto údaje v případě, že byl uveden, kontroluje, v případě neshody danou žádost odmítne. Atribut může obsahovat znaky s diakritikou.
- **QSC**: V případě fyzické osoby nepodnikající může atribut obsahovat pouze označení nižšího územně správního celku, do něhož spadá trvalé bydliště podle primárního osobního dokladu žadatele o kvalifikovaný systémový certifikát, tedy město, obec nebo jinou správní jednotku, která je v primárním osobním dokladu uvedena. V případě fyzické osoby podnikající, právnické osoby, organizační složky státu, zaměstnance může atribut obsahovat pouze označení nižšího územně

správního celku, do něhož spadá místo sídla podle VOR, ŽL, zřizovací listiny atd., tedy město, obec nebo jinou správní jednotku, která je v dokladu uvedena. Z obsahu musí být zřejmé, zda se jedná o kraj nebo jiný celek. RA přijímající předmětnou žádost správnost tohoto údaje v případě, že byl uveden, kontroluje, v případě neshody danou žádost odmítne. Položka může obsahovat znaky s diakritikou.

3.1.2.4 LocalityName (Místo)

- **QC**: Atribut může obsahovat místo trvalého bydliště podle primárního osobního dokladu žadatele o certifikát, tedy město, obec nebo jinou správní jednotku, která je v primárním osobním dokladu uvedena. RA přijímající předmětnou žádost správnost tohoto údaje v případě, že byl uveden, kontroluje, v případě neshody danou žádost odmítne. Atribut může obsahovat znaky s diakritikou.
- **QSC:** V případě fyzické osoby nepodnikající může atribut obsahovat trvalé bydliště podle primárního osobního dokladu, tedy město, obec nebo jinou správní jednotku, která je v primárním osobním dokladu žadatele o kvalifikovaný systémový certifikát uvedena. V případě fyzické osoby podnikající, právnické osoby, organizační složky státu, zaměstnance může obsahovat místo sídla podle VOR, ŽL, zřizovací listiny atd., tedy město, obec nebo jinou správní jednotku, která je v dokladu uvedena. RA přijímající předmětnou žádost správnost tohoto údaje v případě, že byl uveden, kontroluje, v případě neshody danou žádost odmítne. Položka může obsahovat znaky s diakritikou.

3.1.2.5 OrganizationName (Organizace)

- **QC**: Atribut může obsahovat pouze obchodní název podle VOR nebo jiného zákonem určeného rejstříku/registru, živnostenského listu, zřizovací listiny atd. Žadatel o certifikát je povinen doložit oprávněnost použití obsahu dané položky nezpochybnitelným způsobem[6]. RA přijímající předmětnou žádost správnost tohoto údaje v případě, že byl uveden, kontroluje, v případě neshody danou žádost odmítne. Atribut může obsahovat znaky s diakritikou.
- **QSC:** Atribut může obsahovat pouze obchodní název podle VOR nebo jiného zákonem určeného rejstříku/registru, živnostenského listu, zřizovací listiny atd. Žadatel o kvalifikovaný systémový certifikát je povinen doložit oprávněnost použití obsahu dané položky nezpochybnitelným způsobem. RA přijímající předmětnou žádost správnost tohoto údaje v případě, že byl uveden, kontroluje, v případě neshody danou žádost odmítne. Položka může obsahovat znaky s diakritikou.

3.1.2.6 OrganizationalUnitName (Organizační jednotka)

- **QC, QSC**:Atribut může obsahovat pouze název organizační jednotky a to výhradně v tom případě, že byl použit atribut Organization. Žadatel o certifikát je povinen doložit oprávněnost použití obsahu dané položky nezpochybnitelným způsobem. RA přijímající předmětnou žádost správnost tohoto údaje v případě, že byl uveden, kontroluje, v případě neshody danou žádost odmítne. Atribut může obsahovat znaky s diakritikou a může se vyskytovat vícekrát.

3.1.2.7 pkcs9Email Address

- **QC, QSC**: Atribut může obsahovat pouze elektronickou poštovní adresu žadatele o certifikát (dle RFC 822). Vyžaduje se hodnověrně doložené vlastnictví této elektronické poštovní adresy nebo čestné prohlášení[7] žadatele o certifikát certifikátu, v němž toto vlastnictví potvrzuje. V případě nesplnění této podmínky má RA právo danou žádost odmítnout. Atribut nesmí obsahovat znaky s diakritikou.

[6] 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

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

3.1.2.8 GivenName (Křestní jméno/jména)

- **QC:** Atribut může obsahovat pouze následující:
    - křestní jméno, nebo
    - křestní jméno a další křestní jméno/jména, nebo
    - křestní a rodné jméno.

žadatele o certifikát osoby tak, jak je uvedeno v jejím primárním osobním dokladu. RA, přijímající předmětnou žádost, obsah této položky pokud je vyplněna kontroluje oproti předloženém primárnímu osobnímu dokladu. V případě neshody danou žádost odmítne. Atribut může obsahovat znaky s diakritikou.

3.1.2.9 Initials (Iniciály)

- **QC, QSC**: Atribut může obsahovat pouze iniciály celého jména žadatele o certifikát. RA přijímající předmětnou žádost, pokud je atribut Initials vyplněna, shodu iniciál s jménem žadatele o certifikát kontroluje, v případě neshody danou žádost odmítne. Atribut může obsahovat znaky s diakritikou.

3.1.2.10 Name (Celé jméno)

- **QC, QSC**: Atribut může obsahovat pouze celé jméno žadatele o certifikát včetně titulů tak, jak je uvedeno v jeho primárním osobním dokladu, popř. v dalších dokumentech, jedná-li se o titul (doklad o získaném titulu). Pokud je atribut vyplněn, RA přijímající předmětnou žádost, obsah této položky kontroluje a v případě neshody danou žádost odmítne. Pokud žádost obsahuje titul, který není uveden, popř. nekoresponduje s titulem uvedeným v předloženém primárním osobním dokladu, je žadatele o certifikát povinen doložit oprávněnost použití uvedeného titulu nezpochybnitelným způsobem[8]. Atribut může obsahovat znaky s diakritikou.

3.1.2.11 Surname (Příjmení)

- **QC:** Atribut může obsahovat pouze příjmení žadatele o certifikát, které je ve shodě s jeho primárním osobním dokladem. RA, přijímající předmětnou žádost, obsah této položky, pokud je vyplněn, kontroluje oproti jeho primárnímu osobním dokladu. V případě neshody danou žádost odmítne. Atribut může obsahovat znaky s diakritikou.

3.1.2.12 Title (Titul)

- **QC, QSC**: Obsahem atributu zpravidla bývá postavení žadatele o certifikát v určité (zpravidla firemní) hierarchii. Obsah této položky se kontroluje v závislosti na skutečnostech, které jsou v něm obsaženy[9]. Atribut může obsahovat znaky s diakritikou a může se vyskytovat vícekrát.

[8] např. diplomem, ve kterém je uvedeno, že žadatel má právo daný titul používat

[9] např. 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.

3.1.2.13 SerialNumber (Sériové číslo předmětu)

- **QC**: Sériové číslo předmětu, sloužící k rozlišení různých subjektů v rámci klientely I.CA, obecně vyplňuje CA a je naplněno řetězcem „ICA - " a za něj je připojeno na řetězec převedené identifikační číslo žadatele o certifikát. Pro oblast legislativy Slovenské republiky může další sériové číslo předmětu (struktura definována slovenskou legislativou) obsahovat jedno z následujících čísel: číslo pasu, číslo průkazu totožnosti, nebo rodné číslo. Atribut se může vyskytovat vícekrát.
- **QSC:** Sériové číslo předmětu, sloužící k rozlišení různých subjektů v rámci klientely I.CA, obecně vyplňuje CA a je naplněno řetězcem „ICA - " a za něj je připojeno na řetězec převedené identifikační číslo žadatele o certifikát.

3.1.2.14 GenerationQualifier (Generační rozlišení)

- QC, QSC: Atribut se používá pro označení umístění v rodinném stromu. RA přijímající předmětnou položku v žádosti neověřuje, nejsou však povoleny výrazy vulgární, propagující fašismus, rasovou a třídní nenávist. Atribut může obsahovat znaky s diakritikou.

3.1.2.15 Pseudonym (Pseudonym)

- QC: Pokud žadatel o certifikát použil atribut Pseudonym, může tento atribut obsahovat jakoukoli sekvenci povolených znaků. V případě, že se jedná o ověřitelnou položku, je žadatel o certifikát povinen tuto skutečnost v rámci ověřovací procedury na RA doložit - pracovník RA provádí ověření obsahu této položky a v případě neshody danou žádost odmítne. V případě neověřitelné položky pracovník RA pouze kontroluje, zda se nejedná o nepovolené výrazy (vulgární, propagující fašismus, rasovou a třídní nenávist). O přípustnosti konkrétního obsahu položky pseudonym (kterým bude naplněn atribut CommonName ve vydávaném certifikátu – viz kapitola 3.1.2.2) rozhoduje pracovník RA, který vyřizuje žádost o vydání certifikátu. Rovněž nesmí být dotčena práva jiných subjektů (registrované známky apod.). Atribut může obsahovat znaky s diakritikou.

3.1.2.16 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):***
  - ***QC:***
    - číselný identifikátor podepisující osoby, vedený v centrální databázi MPSV[10] (IK MPSV),
    - číselný identifikátor úřadu, vedený v centrální databázi MPSV (IDS MPSV),
    - Microsoft universal principal name,
  - ***QSC:***
    - Microsoft universal principal name,
- ***rfc822Name (elektronická adresa)*:**
  - ***QC, QSC:*** v případě naplnění má tento atribut (žádost musí obsahovat @) přednost před „pkcs9EmailAddress" a certifikát je přednostně spojen s touto adresou, pro hodnověrné doložení vlastnictví této elektronické poštovní adresy platí ustanovení kapitoly 3.1.2.7,
- ***dNSName (jméno doménového serveru)***:
  - ***QC, QSC:*** pokud je doménové jméno registrováno, vyžaduje se hodnověrně doložený souhlas vlastníka nebo čestné prohlášení žadatele o certifikát, potvrzující vlastnictví doménového jména,
- ***uniformResourceIdentifier - URI (identifikátor zdroje v Internetu)***:
  - ***QC, QSC:*** pokud je URI registrováno, vyžaduje se hodnověrně doložený souhlas vlastníka nebo čestné prohlášení žadatele o certifikát, v němž vlastnictví URI potvrzuje,

[10] Ministerstvo práce a sociálních věcí České republiky

- ***iPAddress (IP adresa)***:
  - ***QC, QSC:*** pokud je IP adresa registrována, vyžaduje se hodnověrně doložený souhlas vlastníka nebo čestné prohlášení žadatele o certifikát, v němž vlastnictví IP adresy potvrzuje. RA přijímající předmětnou žádost je povinna, pokud je atribut vyplněn, tento atribut zkontrolovat, v případě neshody je RA povinna danou žádost odmítnout.

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

3.1.3 Anonymita a používání pseudonymu

- **QC**: viz kapitola 3.1.2.15,
- **QSC**: neposkytováno.

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.

3.1.5 Jedinečnost jmen

Jednoznačnost jména subjektu je zaručena použitím výše definovaného postupu pro tvorbu atributu SerialNumber a jména vydavatele certifikátu.

3.1.6 Obchodní značky

Ve vydaném certifikátu musí ověřitelné údaje odpovídat fyzické nebo právnické osobě. Tyto ověřitelné údaje ověřují pracovníci RA.

3.2 Počáteční ověření identity

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

3.2.1 Ověření souladu dat

- **Kvalifikovaný certifikát** - vlastnictví dat pro vytváření elektronických podpisů, odpovídající datům pro ověřování elektronických podpisů, která bude daný kvalifikovaný certifikát obsahovat, se prokazuje předložením žádosti o vydání kvalifikovaného certifikátu, elektronicky podepsané těmito daty. Pracovník RA toto kontroluje tím, že pomocí dat pro ověřování elektronických podpisů, uvedených v žádosti o kvalifikovaný certifikát, ověří platnost elektronického podpisu na této žádosti. Pokud je ověření platnosti elektronického podpisu negativní, I.CA kvalifikovaný certifikát nevydá a řízení k vydání kvalifikovaného certifikátu zastaví.

- **Kvalifikovaný systémový certifikát** - vlastnictví dat pro vytváření elektronických značek odpovídající datům pro ověřování elektronických značek, která bude daný kvalifikovaný systémový certifikát obsahovat, se prokazuje předložením žádosti o vydání kvalifikovaného systémového certifikátu elektronicky označené těmito daty, resp. elektronicky podepsané platnými daty pro vytváření elektronických podpisů, souvisejícími s vydaným kvalifikovaným certifikátem k tomuto kvalifikovanému systémovému certifikátu. Pracovník RA prostřednictvím aplikace RA toto kontroluje tím, že pomocí dat pro ověřování elektronických značek uvedených v žádosti o kvalifikovaný systémový certifikát, resp. pomocí dat pro ověřování elektronických podpisů souvisejícími s vydaným kvalifikovaným certifikátem k tomuto kvalifikovanému systémovému certifikátu, ověří platnost elektronické značky, resp. elektronického podpisu na této žádosti. Pokud je ověření platnosti elektronické značky, resp. elektronického podpisu negativní, RA žádost nepřijme a řízení k vydání kvalifikovaného systémového certifikátu zastaví.

3.2.2 Ověřování identity právnické osoby nebo organizační složky státu

I.CA vyžaduje originál nebo notářsky ověřenou kopii výpisu z obchodního, nebo jiného zákonem určeného rejstříku/registru, živnostenského listu, zřizovací listiny a který/která musí obsahovat úplné obchodní jméno, identifikační číslo (IČO), 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 CZ nebo SK),
- číslo předloženého primárního osobního dokladu,
- adresa trvalého bydliště.

Pokud dojde během trvání smluvního vztahu k I.CA ke změnám ve výše uvedených údajích nebo v údajích, uvedených v certifikátu, je žadatel, popř. držitel povinen tyto změny ohlásit I.CA. Požadavky při registraci nového žadatele/držitele o certifikát jsou uvedeny v kapitolách 3.2.3.1 až 3.2.3.3.

3.2.3.1 Fyzická osoba nepodnikající

Doklady předkládané na RA:

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

    Údaje požadované v sekundárním osobním dokladu musí být shodné s těmito údaji v primárním osobním dokladu. O shodnosti rozhoduje pracovník RA. Pokud žadatel nepředloží dva osobní doklady výše popsané kvality, nebude žádost přijata. Příkladem

akceptovatelného sekundárního osobního dokladu jsou např. cestovní pas, řidičský průkaz, služební průkazy státních úřadů, průkaz poslance, služební průkaz policie, zbrojní průkaz, vojenská knížka, průkaz zdravotního pojištění, průkazka hromadné dopravy, firemní průkazky, studentský průkaz atd.

- pro účely slovenské legislativy a pokud žadatel o certifikát požaduje uvádět v certifikátu rodné číslo, číslo pasu, nebo číslo průkazu totožnosti - relevantní originál platného dokladu

- Žadatel je na RA zastupován zmocněncem:
  - originály platného primárního osobního dokladu a dalšího osobního dokladu (sekundárního) zmocněnce (kvalita primárního a sekundárního dokladu je uvedena výše)
  - originály, případně úředně ověřené kopie primárního a sekundárního osobního dokladu žadatele o certifikát (kvalita primárního a sekundárního dokladu je uvedena výše)
  - pro účely slovenské legislativy a pokud žadatel o certifikát požaduje uvádět v certifikátu rodné číslo, číslo pasu, nebo číslo průkazu totožnosti - relevantní originál, resp. úředně ověřená kopie platného dokladu
  - doklad, prokazující právo jednat jako zmocněnec - plné moc s úředně ověřeným podpisem zmocnitele, splňující následující požadavky:
    - Pokud je plná moc v cizím jazyce (kromě slovenštiny), musí být přeložena do češtiny úředním překladatelem. V zahraničí[11] provedené úřední ověření podpisů musí být tzv. „superlegalizováno“, tj. potvrzeno zastupitelským úřadem ČR v zemi původu plné moci. V případě dokladů, ověřených v zemích, uvedených na http://www.hcch.net/, nemusí být superlegalizace provedena[12].
  - pokud je žadatel zákonným zástupcem klienta, požaduje se o tom úřední doklad:
    - Rodiče nebo osvojitelé zastupují své nezletilé děti - přestože 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.

      Pozn.: 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 osobou a vedle usnesení soudu dokládá ještě skutečnosti, vztahující se k právnickým osobám.
      - Opatrovník může být ustanoven také osobám s tělesným postižením, které nemají omezenou svéprávnost, ale potřebují při právních úkonech asistenci (např. nevidomým).

Doklady, kontrolované na RA:

V případě, že se žadatel o certifikát se osobně dostaví na RA:

- 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 v položce uvedena).
- plnoletost žadatele,
- platnost předkládaných dokladů (viz odstavec „Doklady předkládané na RA“),
- pokud se žadatel prokazuje cestovním pasem, kontrola na shodu bydliště se neprovádí

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

[12] v tomto případě je třeba postupovat individuálně, ve spolupráci s žadatele o certifikát , resp. pracovníka RA s I.CA

- 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, resp. dokladu o zákonném zastupování
- platnost a správnost předložených dokladů zástupce s údaji na plné moci, resp. dokladu o zákonném zastupování a oprávněnost k podání žádané služby

Doklady, u nichž byl výsledek ověření záporný (tzn. údaje nesouhlasily) nebo se nepodařilo je ověřit, jsou v evidenci dokladů vedeny jako neplatné a služba nesmí být poskytnuta.

3.2.3.2 Fyzická osoba podnikající (OSVČ), zaměstnanec

Doklady, předkládané na RA:

- Doklady ve stejném rozsahu, jako v kapitole 3.2.3.1, bod „Žadatel o certifikát se osobně dostaví na RA“.
- 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.

Doklady, kontrolované na RA:

- 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 (viz kapitola 3.2.3.1),
- potvrzení o zaměstnaneckém poměru k danému zaměstnavateli,
- zda je osoba, podepisující potvrzení o zaměstnaneckém poměru, uvedená v úředně ověřeném dokladu (plná moci pověření, doklad o zákonném zastupování), oprávněna zastupovat zaměstnavatele - pracovník RA musí zkontrolovat, zda pověřující osoba má dle výpisu z obchodního nebo jiného zákonem předepsaného rejstříku, živnostenského listu, zřizovací listiny atd. právo takovéto pověření provést, popřípadě, zda uděluje plnou moc oprávněné osobě v souladu s výpisem výše uvedených dokumentů[13].

Doklady, u nichž byl výsledek ověření záporný (tzn. údaje nesouhlasily) nebo se nepodařilo je ověřit, jsou v evidenci dokladů vedeny jako neplatné a služba nesmí být poskytnuta.

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

3.2.3.3 Fyzická osoba - pseudonym

Pro položku CommonName žádosti o kvalifikovaný certifikát platí podmínky, uvedené v kapitole 3.1.2.2.

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

V případě informací, které se nedají ověřit, je postupováno v souladu s kapitolou 3.1.2.

3.2.5 Ověřování specifických práv

Ověřování specifických práv je prováděno v souladu s kapitolami 3.2.2 a 3.2.3.

3.2.6 Kritéria pro interoperabilitu

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

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

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

Kvalifikovaný certifikát - klient vytvoří novou žádost o vydání následného kvalifikovaného certifikátu, elektronicky podepsanou platnými daty pro vytváření elektronických podpisů souvisejícími s již vydaným kvalifikovaným certifikátem, ke kterému je tento následný kvalifikovaný certifikát vydáván.

Kvalifikovaný systémový certifikát - klient vytvoří novou žádost o vydání následného kvalifikovaného systémového certifikátu, elektronicky označenou platnými daty pro vytváření elektronických značek souvisejícími s již vydaným kvalifikovaným systémovým certifikátem, ke kterému je tento následný kvalifikovaný systémový certifikát vydáván, popř. elektronicky podepsané platnými daty pro vytváření elektronických podpisů, souvisejícími s vydaným kvalifikovaným certifikátem k tomuto kvalifikovanému systémovému certifikátu.

3.3.2 Identifikace a autentizace při výměně párových dat po zneplatnění certifikátu

I.CA nepodporuje výměnu párových dat již zneplatněného certifikátu. Z tohoto důvodu nelze ani přijmout žádost o následný certifikát, pokud je elektronicky podepsána, resp. elektronicky označena daty pro vytváření elektronických podpisů, resp. elektronických značek příslušných k certifikátu, který byl již zneplatněn. Jediný způsob, jak získat nový certifikát, je uveden v kapitole 4.2.2.

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 podepisující osobou, resp. označující osobou popř. jeho držitelem. 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, resp. označená elektronická zpráva - (revoke@ica.cz), elektronický podpis, resp. elektronická značka musí být realizován daty pro vytváření elektronického podpisu, resp. elektronické značky příslušnými k předmětnému certifikátu, jenž má být zneplatněn
- elektronicky nepodepsaná, resp. neoznačená 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 o zneplatnění certifikátu** musí být tato zaslána doporučeně.

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.

S pohledem na platnou legislativu může, resp. musí zneplatnit certifikát poskytovatel certifikačních služeb. Oprávněným žadatelem o zneplatnění certifikátu, vydaného I.CA, je v tomto případě ředitel společnosti První certifikační autorita, a.s..

4 Požadavky na životní cyklus certifikátu

4.1 Žádost o vydání certifikátu

4.1.1 Subjekty oprávněné podat žádost o certifikát

Certifikáty jsou I.CA komerčně nabízenou službou a jsou vydávané každému, kdo se smluvně zaváže jednat podle této CP.

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

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

4.1.2 Registrační proces a odpovědnosti poskytovatele a žadatele

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

4.2 Zpracování žádosti o certifikát

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

Žadatel o **prvotní certifikát** vytvoří žádost o vydání certifikátu, elektronicky podepsanou, resp. označenou vygenerovanými daty pro vytváření elektronických podpisů, resp. značek, odpovídající vygenerovaným datům pro ověřování elektronických podpisů, resp. značek. Po vygenerování žádosti o prvotní certifikát a jejím následném uložení na záznamové médium (např. disketu), se žadatel, popř. zmocněnec s touto žádostí a potřebnými doklady (viz kapitola 3.2.3) dostaví na RA. Žadatel o **následný certifikát** vytvoří žádost postupem, uvedeným v kapitole 3.3.1.

Prokazování vlastnictví dat pro vytváření elektronických podpisů, resp. značek, odpovídající datům pro ověřování elektronických podpisů, resp. značek je uvedeno v kapitole 3.2.1.

V procesu zpracovávání žádosti o **prvotní kvalifikovaný certifikát** provede pracovník RA kontrolu předložených originálů osobních dokladů žadatele o certifikát, popř. zmocněnce a v případě pochybností o pravosti předloženého primárního osobního dokladu žadatele o certifikát, popř. zmocněnce odmítne a proces vydávání certifikátu ukončí. V případě pochybností o pravosti předloženého sekundárního osobního dokladu, nebo v případě neshody vyžadovaných údajů s primárním osobním dokladem požádá žadatele o certifikát, popř. zmocněnce o předložení jiného sekundárního osobního dokladu. Pokud žadatel o certifikát, popř. zmocněnec nepředloží sekundární osobní doklad požadovaných vlastností, pracovník RA žadatele o certifikát, popř. zmocněnce odmítne a proces vydávání certifikátu ukončí. V případě, že fyzickou osobou, vyřizující žádost o vydání certifikátu je zmocněnec, provede pracovník RA dále kontrolu předložených úředně ověřených kopií osobních dokladů (primární a sekundární) zmocnitele a v případě neshody vyžadovaných údajů sekundárního osobního dokladu s primárním osobním dokladem zmocnitele odmítne a proces vydávání certifikátu ukončí. Předkládané a kontrolované doklady jsou uvedeny v kapitole 3.2.3.

V procesu zpracovávání žádosti o **následný kvalifikovaný certifikát** je postupováno v souladu s kapitolou 4.7, resp. 4.8.

4.2.2 Přijetí nebo odmítnutí žádosti o certifikát

V případě, že výsledek kontrol, uvedených v kapitole 4.2.1 je pozitivní, pracovník RA okopíruje předložené osobní doklady (není-li smluvně stanoveno jinak) a protokol o podání žádosti na vydání certifikátu I.CA, jehož součástí je věta „**Žadatel souhlasí s tím, aby společnost První certifikační autorita, a.s. skladovala pořízené kopie jeho osobních dokladů v souladu s platnou legislativou.**“ nechá žadateli o certifikát, popř. zmocněnci, podepsat. Pokud žadatel o certifikát, popř. zmocněnec odmítne tento protokol podepsat, je pracovník RA povinen proces vydávání certifikátu ukončit a kopie osobních dokladů zničit – skartovat (není-li smluvně stanoveno jinak).

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 – řádově jednotky minut,
- vydání certifikátu:
  - 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) – řádově jednotky minut.

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 interních dokumentech

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

V případě kladného výsledku je certifikát vydán (formáty PEM, DER, TXT), v opačném případě nikoli.

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

- vydání prvotního certifikátu - klient je informován prostřednictvím pracovníka RA,
- vydání následného certifikátu:
  - klient se dostaví na RA - je informován prostřednictvím pracovníka RA,
  - klient žádá o následný certifikát prostřednictvím e-mail – certifikát zaslán.

Uvedené postupy jsou detailně popsány v interní dokumentaci:

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

4.4 Převzetí vydaného certifikátu

Proces převzetí vydaného certifikátu je detailně popsán v interní dokumentaci:

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

4.4.1 Úkony spojené s převzetím certifikátu

Pokud žadatel splnil podmínky pro vydání **prvotního certifikátu**, tzn.:

- splnil podmínky registrace (kapitoly 3.2 a 3.3),
- zaplatil určený poplatek – viz aktuální ceník na http://www.ica.cz,
- prokázal vlastnictví dat pro vytváření elektronických podpisů, resp. značek, odpovídajících datům pro ověřování elektronických podpisů, resp. značek, která bude vydaný certifikát obsahovat (kapitoly 3.2.1, 4.7.1),
- podepsal příslušnou smlouvu – rozumí se smlouva o poskytování kvalifikované certifikační služby,

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 relevantní CP o jeho zneplatnění.

Pracovník RA předá žadateli záznamové médium (typ uveden na www.ica.cz), obsahující požadovaný certifikát a odpovídající certifikát CA (v předepsaných formátech). V případě, že byla v žádosti uvedena elektronická adresa, jsou vydaný certifikát a certifikát 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 certifikát CA (v předepsaných formátech), v případě vyřizování žádosti na RA, získá žadatel vydaný certifikát, popř. odpovídající certifikát CA (v předepsaných formátech) od pracovníka RA.

Odpovídající CP získá žadatel na RA, popř. ji může stáhnout z informační adresy – viz kapitola 2.2.

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

4.4.2 Zveřejňování vydaných certifikátů poskytovatelem

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

4.4.3 Oznámení o vydání certifikátu jiným subjektům

V případech vydání prvotního certifikátu, popř. následného certifikátu (při dostavení se klienta na RA), získá oznámení o vydaném certifikátu pracovník RA.

4.5 Použití párových dat a certifikátu

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

Držitelé certifikátů jsou povinni:

- bez zbytečného odkladu podávat přesné, pravdivé a úplné informace I.CA ve vztahu k vydanému certifikátu,
- dodržovat veškerá ustanovení smlouvy o poskytování kvalifikované certifikační služby,
- seznámit s relevantními ustanoveními příslušné smlouvy o poskytování kvalifikované certifikační služby o vydání a používání certifikátu případné podepisující osoby a dbát na jejich dodržování ze strany těchto osob.

Podepisující/označující osoba je povinna:

- 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 kvalifikovaný certifikát (I.CA), o tom, že hrozí nebezpečí zneužití jejích dat pro vytváření zaručeného elektronického podpisu,
- dodržovat veškerá ustanovení této CP, v souladu s kterou byl certifikát vydán,
- dodržovat veškerá relevantní ustanovení smlouvy o poskytování kvalifikované certifikační služby, vztahující se ke certifikátu, se kterými byla seznámena jeho případným držitelem.

Označující osoba je povinna:

- zacházet s prostředky jakož i s daty pro vytváření elektronické značky s náležitou péčí tak, aby nemohlo dojít k jejich neoprávněnému použití,
- používat kvalifikované systémové certifikáty výhradně v souladu s odpovídající CP,
- dodržovat veškerá ustanovení odpovídající CP,
- dodržovat veškerá relevantní ustanovení příslušné smlouvy, vztahující se ke kvalifikovanému systémovému certifikátu, se kterými byla seznámena jeho případným držitelem,
- řídit se platnou legislativou.

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

Spoléhající se strany jsou povinny:

- užívat certifikáty vydané dle relevantní CP v souladu s danou CP,
- dodržovat platnou legislativu,
- provádět veškeré úkony potřebné k tomu, aby si ověřily, že elektronický podpis, resp. značka je platný a odpovídající certifikát nebyl zneplatněn,
- kontrolovat elektronickou značku, resp. podpis a důvěrnost certifikátu CA.

4.6 Obnovení certifikátu

4.6.1 Podmínky pro obnovení certifikátu

Služba obnovení již zneplatněného certifikátu není poskytována.

4.6.2 Subjekty oprávněné požadovat obnovení certifikátu

Služba obnovení již zneplatněného certifikátu není poskytována.

4.6.3 Zpracování požadavku na obnovení certifikátu

Služba obnovení již zneplatněného certifikátu není poskytována.

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

Služba obnovení již zneplatněného certifikátu není poskytována.

4.6.5 Úkony spojené s převzetím obnoveného certifikátu

Služba obnovení již zneplatněného certifikátu není poskytována.

4.6.6 Zveřejnění vydaných obnovených certifikátů poskytovatelem

Služba obnovení již zneplatněného certifikátu není poskytována.

4.6.7 Oznámení o vydání obnoveného certifikátu ostatním subjektům

Služba obnovení již zneplatněného certifikátu není poskytována.

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

V případě, že certifikát obsahuje elektronickou adresu podepisující/označující osoby, resp. držitele, je před vypršením platnosti tohoto certifikátu informace o této skutečnosti spolu s návodem, jak postupovat v případě žádosti o tento typ následného certifikátu, na uvedenou adresu zaslána.

Kvalifikovaný certifikát - s ohledem na požadavky slovenské legislativy, resp. požadavky, uvedené v kapitole 3, lze vydat tento typ následného kvalifikovaného certifikátu, který je kombinací výměny dat pro ověřování elektronických podpisů v kvalifikovaném certifikátu (tzn. procesy kapitoly 4.7) a změny údajů v kvalifikovaném certifikátu (viz procesy kapitoly 4.8).

Kvalifikovaný systémový certifikát – jedná se o standardní výměnu dat pro ověřování elektronických značek v certifikátu.

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

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

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

Kvalifikovaný certifikát - jedinou akceptovatelnou formou získání tohoto typu následného certifikátu, je certifikát, vydaný na základě nové žádosti o vydání certifikátu, elektronicky podepsané platnými daty pro vytváření elektronických podpisů, souvisejícími s již vydaným certifikátem, ke kterému je vydáván tento typ následného certifikátu. I.CA si vyhrazuje právo akceptování i jiných forem postupů při vydávání tohoto typu následného certifikátu.

Kvalifikovaný systémový certifikát - akceptovatelnými formami získání následného kvalifikovaného systémového certifikátu jsou žádosti o vydání kvalifikovaného systémového certifikátu elektronicky označené platnými daty pro vytváření elektronických značek, souvisejícími s již vydaným kvalifikovaným systémovým certifikátem, ke kterému je vydáván tento následný kvalifikovaný systémový certifikát, resp. elektronicky podepsané platnými daty pro vytváření elektronických podpisů, souvisejícími s vydaným kvalifikovaným certifikátem k tomuto kvalifikovanému systémovému certifikátu. I.CA si vyhrazuje právo akceptování i jiných forem postupů při vydávání následných certifikátů.

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

Výměnu dat pro ověřování elektronických podpisů/značek jsou oprávněni požadovat držitelé certifikátu, podepisující osoby, popř. jejich zmocněnci.

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

Kvalifikovaný certifikát:

- Pracoviště CA ověřuje údaje žádosti o tento typ následného certifikátu, které až na výjimky (viz úvod kapitoly 4.7) musí být stejné jako údaje v prvotním certifikátu, pouze data pro ověřování elektronických podpisů musí být jiná. Ostatní položky tohoto typu následného certifikátu podléhají aktuálním pravidlům pro certifikáty dle relevantní CP.
- V případě, že je žádost zaslána na I.CA elektronickou cestou, musí být elektronicky podepsána daty pro vytváření elektronických podpisů souvisejících s platným certifikátem, ke kterému je žádáno o tento typ následného certifikátu. Pokud žádost nemá výše uvedené náležitosti, např. je sice elektronicky podepsána, ale tento elektronický podpis nelze ověřit daty pro ověřování elektronických podpisů uvedených v původním a tomto typu následného certifikátu, I.CA následný certifikát nevydá.
- V případě, že se žadatel o tento typ následného certifikátu, popř. zmocněnec dostaví s žádostí na RA, je postupováno obdobně, jako při vydávání prvotního certifikátu.

Kvalifikovaný systémový certifikát:

- Pracoviště CA ověřuje údaje žádosti o tento typ následného certifikátu, které musí být stejné jako údaje v prvotním certifikátu, pouze data pro ověřování elektronických značek musí být jiná. Ostatní položky tohoto typu následného certifikátu podléhají aktuálním pravidlům pro certifikáty dle relevantní CP.
- V případě, že je žádost zaslána na I.CA elektronickou cestou, musí být elektronicky označena daty pro vytváření elektronických značek souvisejících s platným klientovým kvalifikovaným systémovým certifikátem, ke kterému žádá o následný kvalifikovaný systémový certifikát, popř. elektronicky podepsané platnými daty pro vytváření elektronických podpisů, souvisejícími s vydaným certifikátem k tomuto kvalifikovanému systémovému certifikátu. Pokud žádost nemá výše uvedené náležitosti, např. je sice elektronicky označena, ale tato elektronická značka nelze ověřit daty pro ověřování elektronických značek uvedených ve starém a následném kvalifikovaném systémovém certifikátu, I.CA následný kvalifikovaný systémový certifikát nevydá.

- V případě, že se žadatel, popř. zmocněnec se žádostí dostavil na RA, je postupováno obdobně, jako při vydávání prvotního certifikátu.

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

V případě, že se žadatel o tento typ následného certifikátu, popř. zmocněnec se žádostí o vydání tohoto certifikátu dostaví na RA, je informován prostřednictvím pracovníka RA. V případě, že žadatel o tento typ následného certifikátu zaslal žádost prostřednictvím elektronické pošty, je mu následný certifikát na tuto adresu elektronicky zaslán.

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

Pokud žadatel splnil podmínky pro následného vydání **následného certifikátu**, tzn.:

- splnil podmínky uvedené v úvodu kapitoly 4.7 a kapitolách 3.3.1 a 4.7.1,
- zaplatil určený poplatek – viz aktuální ceník na http://www.ica.cz,

je žadatel o certifikát povinen tento certifikát přijmout. Jediným způsobem, jakým může postupovat v případě, že tento certifikát nechce, je zažádat v souladu s touto CP o jeho zneplatnění.

V případě podání žádosti o vydání tohoto typu následného certifikátu elektronickou cestou, zašle I.CA na žadatelovu elektronickou adresu certifikát v předepsaných formátech, v případě vyřizování žádosti na RA, získá žadatel certifikát od pracovníka RA.

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

I.CA je povinna zajistit neprodlené zveřejnění tohoto typu následného certifikátu (veřejného) včetně těch údajů, ke kterým dal jeho držitel souhlas.

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

V případech vydání tohoto typu následného certifikátu při dostavení se žadatele o certifikát, popř. zmocněnce na RA, získá oznámení o vydaném certifikátu pracovník RA.

4.8 Změna údajů v certifikátu

Kvalifikovaný certifikát - s ohledem na požadavky slovenské legislativy, resp. požadavky, uvedené v kapitole 3, lze vydat tento typ následného kvalifikovaného certifikátu, který je kombinací výměny dat pro ověřování elektronických podpisů v kvalifikovaném certifikátu (tzn. procesy kapitoly 4.7) a změny údajů v kvalifikovaném certifikátu (viz procesy kapitoly 4.8).

Kvalifikovaný systémový certifikát – služba není poskytována a proto jsou následující podkapitoly pro problematiku kvalifikovaných systémových certifikátů irelevantní.

4.8.1 Podmínky pro změnu údajů v certifikátu

Jedinou formou získání tohoto typu následného certifikátu je certifikát, vydaný na základě nové žádosti o vydání certifikátu, elektronicky podepsané platnými daty pro vytváření elektronických podpisů, souvisejícími s již vydaným certifikátem, ke kterému je vydáván tento následný certifikát. I.CA si vyhrazuje právo akceptování i jiných forem postupů při vydávání těchto typů následných certifikátů.

4.8.2 Subjekty oprávněné požadovat změnu údajů v certifikátu

Výměnu dat, souvisejících se změnou údajů v certifikátu, jsou oprávněni požadovat držitelé certifikátu, podepisující osoby, popř. jejich zmocněnci.

4.8.3 Zpracování požadavku na změnu údajů v certifikátu

Pracoviště CA ověřuje údaje žádosti o tento typ následného certifikátu, které až na výjimky (viz úvod kapitoly 4.8) musí být stejné jako údaje v prvotním certifikátu, pouze data pro ověřování elektronických podpisů musí být jiná. Ostatní položky tohoto typu následného certifikátu podléhají aktuálním pravidlům pro certifikáty.

V případě, že je žádost zaslána na I.CA elektronickou cestou, musí být elektronicky podepsána daty pro vytváření elektronických podpisů souvisejících s platným certifikátem, ke kterému je žádáno o tento typ následného certifikátu. Pokud žádost nemá výše uvedené náležitosti, např. je sice elektronicky podepsána, ale tento elektronický podpis nelze ověřit daty pro ověřování elektronických podpisů uvedených v původním a tomto typu následného certifikátu, I.CA následný certifikát nevydá.

V případě, že se žadatel o tento typ následného certifikátu, popř. zmocněnec dostaví s žádostí na RA, je postupováno obdobně, jako při vydávání prvotního certifikátu.

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

V případě, že se žadatel o tento typ následného certifikátu, popř. zmocněnec se žádostí o vydání tohoto certifikátu dostaví na RA, je informován prostřednictvím pracovníka RA. V případě, že žadatel o tento typ následného certifikátu zaslal žádost prostřednictvím elektronické pošty, je mu následný certifikát na tuto adresu elektronicky zaslán.

4.8.5 Úkony spojené s převzetím certifikátu se změněnými údaji

Pokud žadatel splnil podmínky pro následného vydání **následného certifikátu**, tzn.:

- splnil podmínky uvedené v úvodu kapitoly 4.8 a kapitolách 3.3.1 a 4.8.1,
- zaplatil určený poplatek – viz aktuální ceník na http://www.ica.cz,

je žadatel o certifikát povinen tento certifikát přijmout. Jediným způsobem, jakým může postupovat v případě, že tento certifikát nechce, je zažádat v souladu s touto CP o jeho zneplatnění.

V případě podání žádosti o vydání tohoto typu následného certifikátu elektronickou cestou, zašle I.CA na žadatelovu elektronickou adresu certifikát v předepsaných formátech, v případě vyřizování žádosti na RA, získá žadatel certifikát od pracovníka RA.

4.8.6 Zveřejnění vydaných certifikátů se změněnými údaji

I.CA je povinna zajistit neprodlené zveřejnění tohoto typu následného certifikátu (veřejného) včetně těch údajů, ke kterým dal jeho držitel souhlas.

4.8.7 Oznámení o vydání certifikátu se změněnými údaji jiným subjektům

V případech vydání tohoto typu následného certifikátu při dostavení se žadatele o certifikát, popř. zmocněnce na RA, získá oznámení o vydaném certifikátu pracovník RA.

4.9 Zneplatnění a pozastavení platnosti certifikátu

4.9.1 Podmínky pro zneplatnění certifikátu

Certifikát může být zneplatněn na základě následujících okolností:

- o jeho zneplatnění požádá:
  - o podepisující/označující osoba, držitel, nebo
  - o subjekt, který k tomu byl explicitně určen ve smlouvě o poskytování kvalifikované certifikační služby v oblasti vydávání certifikátů (např. při vydávání certifikátu pro zaměstnance), nebo
  - o osoba oprávněná z pozůstalostního řízení,
- nastanou-li skutečnosti uvedené v platné legislativě,
- jeho držitel poruší závažným způsobem ustanovení smlouvy o poskytování kvalifikované certifikační služby nebo dokumentů, které jsou přílohou této smlouvy,
- dojde ke kompromitaci soukromého klíče I.CA, používaného k označování, resp. podepisování vydávaných certifikátů a seznamů zneplatněných certifikátů,
- je důvodné podezření, že došlo ke kompromitaci dat pro vytváření elektronických podpisů, resp. elektronických značek držitele nebo podepisující/označující osoby.

Zneplatnění certifikátu provede I.CA na základě podnětu subjektů oprávněných ze zákona.

4.9.2 Subjekty oprávněné žádat o zneplatnění certifikátu

Žádost o zneplatnění mohou podat subjekty, uvedené v kapitole 4.9.1.

4.9.3 Požadavek na zneplatnění certifikátu

Po splnění podmínek na identifikaci a autentizaci (kapitola 3.4), je postupováno následujícím způsobem:

- V případě **osobního předání žádosti o zneplatnění certifikátu na RA** musí žádost obsahovat sériové číslo certifikátu buď v dekadickém tvaru nebo hexadecimální (uvozeno řetězcem „0x“), celé občanské jméno fyzické osoby, které byl certifikát vydán a heslo pro zneplatnění. Pokud si tato osoba heslo pro zneplatnění nepamatuje, musí tuto skutečnost do písemné žádosti explicitně uvést, včetně čísla primárního osobního dokladu předloženého při žádosti o vydání certifikátu. Tímto primárním osobním dokladem se musí pracovníkovi RA prokázat. Pracovník RA předá výše uvedenou žádost (dálkovým přístupem) na CA. 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 CA zároveň datem a časem zneplatnění tohoto certifikátu. V případě, že žádost nelze akceptovat (špatné heslo pro zneplatnění, neprokazatelná identita fyzické osoby),

pokusí se pracovník RA v součinnosti s touto fyzickou osobou tyto skutečnosti napravit a pokud to z libovolného důvodu nebude možné, žádost o zneplatnění certifikátu bude zamítnuta. Pro zmocněnce platí ustanovení podkapitol 3.2.3.

- V případě **předání žádosti o zneplatnění certifikátu elektronickou cestou** jsou přípustné následující možnosti:
  - Elektronicky podepsaná, resp. označená elektronická zpráva - tělo zprávy musí být následujícího tvaru (v českém nebo slovenském jazyce, s diakritikou nebo bez diakritiky):

    Zadam o zneplatneni certifikatu cislo = xxxxxxx

    nebo

    Žádám o zneplatnění certifikátu číslo = xxxxxxx

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

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

    Zadam o zneplatneni certifikatu cislo = xxxxxxx

    Heslo pro zneplatneni = yyyyyy

    nebo

    Žádám o zneplatnění certifikátu číslo = xxxxxxx

    Heslo pro zneplatnění = yyyyyy

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

    Pokud žádost splňuje výše uvedené požadavky, odpovědný pracovník CA 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 je určen okamžikem přijetí platné žádosti o zneplatnění certifikátu serverem I.CA. V případě, že žádost nesplňuje požadavky, je zamítnuta a žadatel je elektronickou cestou o této skutečnosti informován. O kladném vyřízení není žadatel explicitně informován a tuto skutečnost zjistí v nejbližším vydaném seznamu zneplatněných certifikátů

- V případě použití **listovní zásilky** o zneplatnění certifikátu musí být tato zaslána doporučeně na adresu:

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

  V zásilce musí být uvedena žádost v následujícím tvaru (v českém nebo slovenském jazyce):

Žádám o zneplatnění certifikátu číslo = xxxxxxx

Heslo pro zneplatnění = yyyyyy

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

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

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.

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. 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, resp. elektronické značky jsou platné a certifikáty nebyly zneplatněny. Pro tyto účely jsou spoléhající se strany jsou povinny používat CRL, vydaná a označená, resp. podepsaná I.CA. Neověření certifikátu pomocí CRL je bráno jako hrubé porušení odpovídající CP.

4.9.7 Periodicita vydávání seznamu zneplatněných certifikátů

Seznam zneplatněných certifikátů je společností První certifikační autorita, a.s. vydáván v pravidelných intervalech (zpravidla po 8 hodinách), minimálně jedenkrát za 24 hodin. 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 s ohledem na platnou legislativu vždy dodrženo ustanovení kapitoly 4.9.5.

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

Služba není poskytována.

4.9.10 Požadavky při ověřování statutu certifikátu na on-line

Služba není poskytována.

4.9.11 Jiné způsoby oznamování zneplatnění certifikátu

Služba není poskytována.

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

Služba není poskytována.

4.9.13 Podmínky pro pozastavení platnosti certifikátu

Služba není poskytována.

4.9.14 Subjekty oprávněné požadovat pozastavení platnosti certifikátu

Služba není poskytována.

4.9.15 Zpracování požadavku na pozastavení platnosti certifikátu

Služba není poskytována.

4.9.16 Omezení doby pozastavení platnosti certifikátu

Služba není poskytována.

4.10 Služby související s ověřováním statutu certifikátu

4.10.1 Funkční charakteristiky

Seznamy veřejných certifikátů jsou poskytovány formou zveřejňování informací (viz kapitola 2.2), seznamy zneplatněných certifikátů jsou poskytovány jak formou zveřejňování informací, tak uvedením distribučních míst CRL ve vydaném certifikátu.

4.10.2 Dostupnost služeb

I.CA zajišťuje nepřetržitou dostupnost služeb, uvedených v kapitole 4.10.1. Postup je uveden v interních dokumentech I.CA :

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

4.10.3 Další charakteristiky služeb statutu certifikátu

Další služby, kromě těch, které jsou uvedené v kapitole 4.10.1, nejsou poskytovány.

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

Ukončení služeb (obchodní vztah) mezi držitelem a I.CA končí ve chvíli, kdy skončila platnost držitelova certifikátu aniž by držitel předtím požádal o následný certifikát.

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

Služba není poskytována.

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

Služba není poskytována.

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

Služba není poskytována.

5 Management, provozní a fyzická bezpečnost

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

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

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

5.1 Fyzická bezpečnost

Problematika fyzické bezpečnosti je detailně uvedena v interní dokumentaci:

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

5.1.1 Umístění a konstrukce

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

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

5.1.2 Fyzický přístup

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

5.1.3 Elektřina a klimatizace

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

5.1.4 Vliv vody

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

5.1.5 Protipožární opatření a ochrana

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

5.1.6 Ukládání médií

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

5.1.7 Nakládání s odpady

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

5.1.8 Zálohy mimo budovu provozního pracoviště

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

5.2 Procesní bezpečnost

5.2.1 Důvěryhodné role

Pro činnosti, odpovídajícím rolím podle bezpečnostních požadavků standardu pro důvěryhodné systémy (viz vyhláška České republiky č. 378/2006 Sb., o postupech kvalifikovaných poskytovatelů certifikačních služeb), jsou ve společnosti I.CA definovány důvěryhodné role.

Problematikou se zabývají interní dokumenty, zejména:

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

5.2.2 Počet osob požadovaných na zajištění jednotlivých činností

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

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

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

5.2.3 Identifikace a autentizace pro každou roli

Pracovníkům jsou přiděleny prostředky pro řádnou autentizaci k těm komponentám, které jsou pro jejich činnost nezbytné - upraveno interními směrnicemi:

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

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

5.3 Personální bezpečnost

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

5.3.1 Požadavky na kvalifikaci, zkušenost a bezúhonnost

Pracovníci v rolích podle bezpečnostních požadavků standardu pro důvěryhodné systémy (viz vyhláška České republiky č. 378/2006 Sb., o postupech kvalifikovaných poskytovatelů certifikačních služeb) a dále v rolích ředitel společnosti, bezpečnostní manager, manager pro zvládání krizových situací a plánu obnovy, bezpečnostní auditor jsou přijímáni na základě dále popsaných personálních kriterií:

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

Ostatní pracovníci jsou přijímáni na základě následujících kriterií:

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

Jmenování nebo pověřování pracovníků I.CA do rolí podle bezpečnostních požadavků standardu pro důvěryhodné systémy (viz vyhláška České republiky č. 378/2006 Sb., o postupech kvalifikovaných poskytovatelů certifikačních služeb) a dále do rolí bezpečnostní manager, manager pro zvládání krizových situací a plánu obnovy, bezpečnostní auditor podléhá schválení ředitelem I.CA.

5.3.2 Posouzení spolehlivosti osob

Zdrojem informací všech kmenových pracovníků I.CA jsou:

- sami tito pracovníci,

- osoby, které tyto pracovníky znají,
- veřejné zdroje informací,

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

5.3.3 Požadavky na přípravu pro výkon role, vstupní školení

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

5.3.4 Požadavky a periodicita školení

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

5.3.5 Periodicita a posloupnost rotace pracovníků mezi různými rolemi

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

5.3.6 Postihy za neoprávněné činnosti zaměstnanců

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

5.3.7 Požadavky na nezávislé zhotovitele (dodavatele)

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

5.3.8 Dokumentace poskytovaná zaměstnancům

Kmenoví zaměstnanci I.CA mají k dispozici kromě tohoto dokumentu i příslušné politiky, normy, směrnice, příručky a metodické pokyny, potřebné pro výkon jejich činnosti.

5.4 Auditní záznamy (logy)

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

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

5.4.1 Typy zaznamenávaných událostí

Dle požadavků CWA 14167-1 - Security Requirements for Trustworthy Systems Managing Certificates for Electronic Signatures - Part 1: System Security Requirements:

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

- všechny záznamy v auditním souboru obsahují následující parametry:
  - datum (rok, měsíc, den) a čas (hodina, minuta, sekunda) události,
  - typ události,
  - identitu entity, která je za akci odpovědná,
  - úspěšnost/neúspěšnost auditované události.

S ohledem na požadavky:

- CWA 14167-1 - Security Requirements for Trustworthy Systems Managing Certificates for Electronic Signatures - Part 1: System Security Requirements ,
- ETSI TS 101 456 - Electronic Signatures and Infrastructures: Policy requirements for certification authorities issuing qualified certificates,
- ZoEP,

jsou v důvěryhodných systémech I.CA do elektronického auditního logu zaznamenávány následující bezpečnostně relevantní provozní události:

- záznam o registraci žadatele,
- záznam o pokus neoprávněné registrace žadatele (s maximem dosažitelných informací o neoprávněném žadateli),
- záznam o zrušení registrace žadatele (údaje o žadateli se uchovávají),
- vše, co souvisí s životním cyklem klientova certifikátu:
  - záznam o požadavku RA na vydání certifikátu včetně výsledku,
  - záznam o neoprávněném požadavku na vydání certifikátu včetně výsledku,
  - záznam o požadavku na vydání následného certifikátu včetně výsledku,
  - záznam o neoprávněném požadavku na vydání následného certifikátu včetně výsledku,
  - záznam o požadavku na zneplatnění certifikátu včetně údajů o žádající osobě a výsledku,
  - záznam o neoprávněném požadavku na zneplatnění certifikátu včetně údajů o žádající osobě a výsledku,
  - záznam o oznámení možné kompromitace dat pro vytváření elektronických podpisů, resp. značek podepisující/označující osobou,
  - záznam o zneplatnění certifikátu,
  - záznam o pokusu neoprávněného přístupu do systému,
  - záznam o zveřejnění certifikátu, včetně výsledku,
  - záznam o zanesení zneplatněného certifikátu do CRL,
  - záznam o zveřejnění CRL,
- všechny události vztahující se k životnímu cyklu párových dat a certifikátů CA .

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 auditní dat, rezervování dostatečného prostoru pro auditní data, automatické nepřepisování auditního souboru, prezentaci auditních záznamů pro uživatele vhodným způsobem a omezení přístupu k auditnímu souboru pouze pro definované uživatele.

5.4.2 Periodicita zpracování záznamů

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

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

Procesy jsou uvedeny v interní dokumentaci, zejména:

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

5.4.5 Postupy pro zálohování auditních záznamů

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

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

5.4.6 Systém shromažďování auditních záznamů (interní nebo externí)

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

5.4.7 Postup při oznamování události subjektu, který ji způsobil

V případě neoprávněných pokusů není subjekt informován o zapsání události do auditního záznamu.

5.4.8 Hodnocení zranitelnosti

Hodnocení zranitelnosti je ve společnosti První certifikační autorita, a.s. prováděno v periodických intervalech, v případě incidentu, majícího vliv na bezpečnost poskytovaných služeb okamžitě.

5.5 Uchovávání informací a dokumentace

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

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

- ***„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 následující typy informací a dokumentace (viz ***„Dílčí spisový a skartační řád pro agendy certifikačních služeb“*** a ***„Dokumenty agendy certifikačních služeb“***), které související s poskytovanými kvalifikovanými certifikačními službami v oblasti vydávání certifikátů podle ZoEP a obsahují:

- elektronické nebo písemné informace:
    - smlouva o poskytování kvalifikované certifikační služby v oblasti vydávání certifikátů, včetně žádosti o poskytování služby,
    - certifikát vydaný žadateli o certifikát, popř. zmocněnci,
    - certifikát CA,
    - kopie předložených osobních dokladů žadatele o certifikát, popř. zmocněnce, na jejichž základě byla ověřena identita žadatele o certifikát, popř. zmocněnce,
    - potvrzení o převzetí certifikátu držitelem, popř. zmocněncem, případně jeho souhlas se zveřejněním certifikátu v seznamu vydaných certifikátů,
    - prohlášení držitele certifikátu o tom, že mu byly před uzavřením smlouvy o poskytování kvalifikačních služeb v oblasti vydávání certifikátů poskytnuty písemné informace o přesných podmínkách pro využívání kvalifikovaných certifikačních služeb v oblasti vydávání certifikátů, včetně případných omezení pro jejich použití, o podmínkách reklamací a řešení vzniklých sporů, a o tom, zda je, či není akreditován,
    - dokumenty a záznamy související s životním cyklem vydaného certifikátu, certifikátu CA,
    - další záznamy, požadované ZoEP,

- auditní záznamy, aplikační programové vybavení a veškerou dokumentaci společnosti, která je nutná pro provádění informačních auditů a kontrol bezpečnostní shody,
- identifikace místa, kde jsou uloženy informace a dokumentace, jejichž uchování je vyžadováno ZoEP,
- veškeré seznamy zneplatněných certifikátů,
- identifikační údaje osoby, která provedla ověření totožnosti žadatele o certifikát, popř. zmocnitele,
- obchodní název I.CA, nebo 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 dokumentaci.

5.5.2 Doba uchovávání uchovávaných informací a dokumentace

Po celou dobu své existence I.CA zajišťuje uchovávání informací a dokumentace dle kapitoly 5.5.1 po dobu nejméně 10 od jejich vzniku.

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

Postupy při uchovávání informací a dokumentace jsou upraveny interní dokumentací I.CA ***„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 zákonům ČR č. 101/2000 Sb. a SR č. č. 122/2013 Z.z. v aktuálních zněních, dbáno zvýšené ochrany těchto dat. Prostory, ve kterých se uchovávané informace a dokumentace nacházejí, jsou zabezpečeny formou opatření, vycházejících z požadavků objektové a fyzické bezpečnosti.

Uchovávané informace a dokumentace jsou určeny výhradně pro interní potřebu I.CA a jsou přístupné:

- pracovníkům I.CA v důvěryhodných rolích,
- 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.

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 (viz kapitola 5.5.1) jsou upraveny interní dokumentací I.CA., uvedené v kapitole 5.5.

5.5.5 Požadavky na používání časových razítek při uchovávání informací a dokumentace

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

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

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

5.5.7 Postupy pro získání a ověření uchovávaných informací a dokumentace

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

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

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

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

5.7 Obnova po havárii nebo kompromitaci

5.7.1 Postup v případě incidentu a kompromitace

Postupy jsou uvedeny v interních dokumentech, zejména:

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

5.7.2 Poškození výpočetních prostředků, software nebo dat

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

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

5.7.3 Postup při kompromitaci dat pro vytváření elektronických značek poskytovatele

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

- ukončí jejich používání,
- okamžitě a trvale zneplatní vlastní příslušný certifikát CA a jemu odpovídající data pro vytváření elektronických značek, resp. elektronických podpisů,
- zneplatní všechny certifikáty, které byly těmito daty označeny, resp. podepsány
- bezodkladně:
    - o této skutečnosti, včetně důvodu informuje:
        - na své internetové informační adrese,
        - v jednom celostátně distribuovaném deníku – viz kapitola 2.2,
    - pro zpřístupnění této informace je využit i seznam zneplatněných certifikátů, čímž je zajištěna dostupnost této informace minimálně dvěma na sobě nezávislými způsoby, umožňujícími dálkový přístup a jsou nepřetržitě dostupné,

- 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 certifikátu CA,
- oznámí příslušnému úřadu informaci o zneplatnění vlastního příslušného certifikátu CA s uvedením důvodu zneplatnění,
- v případě vzniku důvodné obavy ze zneužití dat pro vytváření elektronických značek, resp. elektronických podpisů pro označování, resp. podepisování vydávaných certifikátů a seznamů zneplatněných certifikátů, nabídne I.CA výše uvedeným držitelům bezplatné vydání nového certifikátu s tím, že případné náklady na vydání nových certifikátů sama hradí. Postup je stejný jako při vydání prvotního certifikátu.

5.7.4 Schopnosti obnovit činnost po havárii

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

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

5.8 Ukončení činnosti CA nebo RA

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

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

- SK:
    - ohlásí příslušnému úřadu záměr ukončit činnost poskytování kvalifikovaných certifikačních služeb v oblasti vydávání certifikátů nejméně 6 měsíců před plánovaným ukončením činnosti,
    - ohlásí každému držiteli platného kvalifikovaného certifikátu záměr ukončit činnost poskytování kvalifikovaných certifikačních služeb v oblasti vydávání certifikátů nejméně 6 měsíců před plánovaným ukončením činnosti,

- může se dohodnout s jiným kvalifikovaným poskytovatelem certifikačních služeb v oblasti vydávání certifikátů o převzetí záznamů o vydaných a zrušených certifikátech a provozní dokumentaci – pokud žádný kvalifikovaný poskytovatel certifikačních služeb v oblasti vydávání certifikátů tyto záznamy nepřevezme:
  - zaniká platnost všech jím vydaných kvalifikovaných certifikátů ode dne zániku tohoto kvalifikovaného poskytovatele certifikačních služeb v oblasti vydávání certifikátů,
  - převezme tyto záznamy úřad.

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

6 Technická bezpečnost

6.1 Generování a instalace párových dat

6.1.1 Generování párových dat

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

V průběhu procesu generování párových dat I.CA, sloužících k označování, resp. podepisování vydávaných certifikátů a seznamů zneplatněných certifikátů, musí být 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, resp. podepisování vydávaných certifikátů a seznamů zneplatněných certifikátů a následné vyhotovení certifikátu CA, příslušného k těmto párovým datům, je popsán v interní dokumentaci I.CA:

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

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

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

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

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

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

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

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

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

- osobně na datovém nosiči,
- zasláním prostřednictvím elektronické pošty.

Vydání prvotního certifikátu je možné pouze osobně. Pro následné certifikáty lze použít obou z výše uvedených způsobů předání. V případě předání prostřednictvím elektronické pošty, musí být zpráva, obsahující data pro ověřování elektronických podpisů/značky, elektronicky podepsána/označena daty pro vytváření elektronických podpisů/značek příslušných k platnému certifikátu, ke kterému je požadováno vydání následného certifikátu.

Data pro ověřování elektronických podpisů/značek jsou součástí žádosti o vydání certifikátu.

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

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

- obdržením na RA (osobní návštěva),
- prostřednictvím internetových informačních adres I.CA a příslušného úřadu,
- prostřednictvím věstníku příslušného úřadu.

Každý žadatel o certifikát obdrží certifikát CA při získání svého prvotního certifikátu na RA.

6.1.5 Délky párových dat

I.CA používá nejprověřenější klasický asymetrický šifrový algoritmus – RSA. Mohutnost klíčů (resp. parametrů daného algoritmu) použitých pro označování, resp. podepisování vydávaných certifikátů a seznamů zneplatněných certifikátů je 2048 bitů. Mohutnost klíčů na straně klienta závisí na klientovi, pro vybraný algoritmus však nesmí být nižší než stanovená hodnota/hodnoty, uvedené v relevantních technických standardech nebo normách.

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

Algoritmy, použité pro generování celočíselných hodnot nutných pro fungování elektronického podpisu (např. testy prvočíselnosti atd.), musí mít parametry uvedené v 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 dat pro ověřování elektronických podpisů nebo dat pro ověřování elektronických značek

Uvedeno v kapitole 7.1.2.

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

Konkrétní postupy jsou popsány v interní dokumentaci I.CA:

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

6.2.1 Standardy a podmínky používání kryptografických modulů

V kryptografickém modulu, který splňuje požadavky české, resp. slovenské legislativy, vztahující se k problematice elektronického podpisu:

- jsou generována párová data I.CA,
- je uložen soukromý klíč I.CA pro elektronické označování, resp. podepisování vydávaných certifikátů a seznamů zneplatněných certifikátů.

6.2.2 Sdílení tajemství

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

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

Služba není poskytována.

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

Kryptografický modul, použitý pro správu párových dat a certifikátu CA, umožňuje zálohování dat pro vytváření elektronických značek, resp. elektronických podpisů. Data v zašifrované podobě jsou zálohována prostřednictvím čipových karet.

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

Po uplynutí doby platnosti dat určených k označování, resp. podepisování vydávaných certifikátů a seznamů zneplatněných certifikátů jsou tato data, včetně jejich záloh zničena a jejich další zálohování se neprovádí. Uchovávání dat, určených k označování, resp. podepisování certifikátů a seznamů zneplatněných certifikátů představuje bezpečnostní riziko, a proto je u I.CA zakázáno.

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

Data pro vytváření elektronických značek, resp. elektronických podpisů příslušná k certifikátu CA, jsou generována přímo v kryptografickém modulu.

Vkládání dat pro vytváření elektronických značek, resp. elektronických podpisů do kryptografického modulu v případě, že se jedná o obnovení těchto dat ze šifrované zálohy, probíhá za přímé osobní účasti nejméně dvou určených pracovníků I.CA. V okamžiku vkládání dat musí být vyhrazená stanice a kryptografický modul odpojeny od počítačové sítě. O vložení dat pro vytváření elektronických značek, resp. elektronických podpisů je pořízen písemný záznam.

6.2.7 Uložení dat pro vytváření elektronických značek v kryptografickém modulu

Data pro vytváření elektronických značek, resp. elektronických podpisů příslušná k certifikátu CA jsou v kryptografickém modulu uložena v šifrovaném tvaru.

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

Aktivaci dat pro vytváření elektronických značek, resp. elektronických podpisů I.CA vydávaných certifikátů a seznamů zneplatněných certifikátů, vygenerovaných v kryptografického modulu, provádí určení pracovníci I.CA prostřednictvím vlastní aktivace kryptografického modulu a aktivační čipové karty podle přesně určeného postupu, který je upraven interní dokumentací. Po aktivaci je systém připraven k označování, resp. podepisování vydávaných certifikátů, seznamů zneplatněných certifikátů a aktivační čipová karta se vyjme. Po aktivaci je zařízení přístupné pouze určeným odpovědným pracovníkům I.CA.

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

Deaktivaci dat pro vytváření elektronických značek, resp. elektronických podpisů I.CA 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 provedení deaktivace dat pro vytváření elektronických značek, resp. elektronických podpisů je pořízen písemný záznam, který podepíší určení pracovníci I.CA.

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

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

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

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

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

6.2.11 Hodnocení kryptografického modulu

Nástroj elektronického podpisu pro elektronické označování, resp. podepisování vydávaných kvalifikovaných certifikátů a seznamů zneplatněných certifikátů, splňuje požadavky na kryptografické moduly dle dokumentu „Standard pro hodnocení bezpečnosti kryptografických modulů vydaný NIST v USA – FIPS PUB 140-1 úroveň 3“.

6.3 Další aspekty správy párových dat

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

Tato data jsou obsažena v certifikátech CA. Na rozdíl od jim příslušných dat pro vytváření elektronických značek, resp. elektronických podpisů, je důležité tato data uchovávat pro případ následné kontroly pravosti vydaných certifikátů a seznamů zneplatněných certifikátů. Se všemi certifikáty CA je nakládáno způsobem, uvedeným v kapitolách 5.4 a 5.5.

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

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

6.4 Aktivační data

6.4.1 Generování a instalace aktivačních dat

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

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

6.4.2 Ochrana aktivačních dat

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

6.4.3 Ostatní aspekty aktivačních dat

Aktivační data jsou určena výhradně pro aktivaci soukromého klíče a nesmí být použita k jiným účelům, ani přenášena nebo uchovávána v otevřené podobě.

6.5 Počítačová bezpečnost

6.5.1 Specifické technické požadavky na počítačovou bezpečnost

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

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

- ***„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 101 456 - Electronic Signatures and Infrastructures (ESI); Policy requirements for certification authorities issuing qualified 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 EN ISO 19011 - Směrnice pro auditování systému managementu jakosti a/nebo systému.

Tato problematika je popsána v interním dokumentu „***Hodnocení bezpečnosti***".

6.6 Bezpečnost životního cyklu

6.6.1 Řízení vývoje systému

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

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

6.6.2 Kontroly řízení bezpečnosti

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

6.6.3 Řízení bezpečnosti životního cyklu

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

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

6.7 Síťová bezpečnost

V prostředí I.CA nejsou prostředky provádějící vlastní kvalifikované certifikační služby přímo dostupné z veřejné sítě Internet. Informační systém je chráněn přístupovým routerem a produktem typu firewall. Veškerá komunikace mezi RA a CA je vedena šifrovaně. Detailní řešení řízení síťové bezpečnosti je popsáno v interní dokumentaci.

Detailní řešení řízení síťové bezpečnosti je popsáno v interní dokumentaci:

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

6.8 Časová razítka

Řešení je uvedeno v kapitole 5.5.5.

7 Profily certifikátu, seznamu zneplatněných certifikátů a OCSP

7.1 Profil certifikátu

Profily certifikátu a seznamu zneplatněných certifikátů jsou vždy uvedeny v konkrétní CP (viz kapitola 7). V následujících kapitolách jsou případně popsány pouze změny, jejichž provedení si I.CA v konkrétní certifikační politice vyhradila.

7.1.1 Číslo verze

Viz kapitola 7.1.

7.1.2 Rozšiřující položky v certifikátu

Viz kapitola 7.1.

7.1.3 Objektové identifikátory (dale OID) algoritmů

Viz kapitola 7.1.

7.1.4 Způsoby zápisu jmen a názvů

Viz kapitola 7.1.

7.1.5 Omezení jmen a názvů

Viz kapitola 7.1.

7.1.6 OID certifikační politiky

Viz kapitola 7.1.

7.1.7 Rozšiřující položka „Policy Constrainst“

Viz kapitola 7.1.

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

Viz kapitola 7.1.

7.1.9 Způsob zápisu kritické rozšiřující položky „Certificate Policies“

Viz kapitola 7.1.

7.2 Profil seznamu zneplatněných certifikátů

Viz kapitola 7.1.

7.2.1 Číslo verze

Viz kapitola 7.1.

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

Viz kapitola 7.1.

7.3 Profil OCSP

Tyto skutečnosti jsou pro aplikaci vydání této CPS irelevantní.

7.3.1 Číslo verze

Tyto skutečnosti jsou pro aplikaci vydání této CPS irelevantní.

7.3.2 Rozšiřující položky OCSP

Tyto skutečnosti jsou pro aplikaci vydání této CPS irelevantní.

8 Hodnocení shody a jiná hodnocení

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

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

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

8.1 Periodicita hodnocení nebo okolnosti pro provedení hodnocení

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

Audit systému bezpečnosti informací je prováděn po 2 letech od předchozího auditu systému bezpečnosti informací a je prováděn podle požadavků normy ČSN EN ISO 19011 - Směrnice pro auditování systému managementu jakosti a/nebo systému environmentálního managementu.

8.2 Identita a kvalifikace hodnotitele

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

8.3 Vztah hodnotitele k hodnocené entitě

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

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

8.4 Hodnocené oblasti

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

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

Předmětem kontroly bezpečnostní shody:

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

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

8.5 Postupy v případě zjištěných nedostatků

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

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

8.6 Sdělování výsledků hodnocení

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

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

Sdělování výsledků hodnocení taktéž podléhá požadavkům ZoEP a VoEP.

9 Ostatní obchodní a právní záležitosti

9.1 Poplatky

9.1.1 Poplatky za vydání nebo obnovení certifikátu

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

9.1.2 Poplatky za přístup k certifikátu a seznamu vydaných certifikátů

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

9.1.3 Poplatky za informace o statutu certifikátu nebo o zneplatnění certifikátu

Přístup k informacím o zneplatněných certifikátech (aktuální CRL) 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 v souladu s požadavky uvedenými v ZoEP a s ohledem na riziko vzniku odpovědnosti za škodu.

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

9.2.3 Pojištění nebo krytí zárukou pro koncové uživatele

Služba není poskytována.

9.3 Citlivost obchodních informací

9.3.1 Výčet citlivých informací

Citlivými informacemi I.CA jsou:

- data pro vytváření elektronických značek, resp. elektronických podpisů, příslušná k datům pro ověřování elektronických značek, resp. elektronických podpisů, obsažených v certifikátech 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,
- vybrané obchodní informace I.CA,
- veškeré informace a dokumentace s ohledem na poskytování kvalifikovaných certifikačních služeb dle ZoEP,
- veškeré osobní údaje.

Chráněnými obchodními informacemi jednotlivých RA jsou:

- data pro vytváření elektronických podpisů příslušná k datům pro ověřování elektronických podpisů obsažených ve vlastních nebo účelových certifikátech RA,
- ostatní kryptograficky podstatné informace sloužící k provozu RA,
- veškeré informace a dokumentace s ohledem na poskytování kvalifikovaných certifikačních služeb dle ZoEP,
- veškeré osobní údaje.

Za chráněné informace se rovněž považují veškeré další informace označené některým ze subjektů jako citlivé.

S chráněnými informacemi, bez ohledu na typ nosiče, je zacházeno tak, aby byla zajištěna jejich důvěrnost a integrita.

9.3.2 Informace mimo rámec citlivých informací

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

9.3.3 Odpovědnost za ochranu citlivých informací

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

Zaměstnanci I.CA, případně jiné fyzické osoby, které přicházejí do styku s osobními údaji, jsou povinni zachovávat mlčenlivost o těchto údajích a datech a o bezpečnostních opatřeních, jejichž zveřejnění

by ohrozilo zabezpečení těchto údajů a dat. Povinnost mlčenlivosti trvá i po skončení pracovního nebo jiného obdobného poměru nebo po provedení příslušných prací.

9.4 Ochrana osobních údajů

9.4.1 Politika ochrany osobních údajů

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

9.4.2 Osobní údaje

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

9.4.3 Údaje, které nejsou považovány za důvěrné

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

9.4.4 Odpovědnost za ochranu osobních údajů

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

9.4.5 Oznámení o používáním důvěrných informací a souhlas s používáním důvěrných 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 Poskytnutí důvěrných 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 náležitosti zpřístupňování osobních údajů

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

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

9.5 Práva duševního vlastnictví

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

9.6 Zastupování a záruky

9.6.1 Zastupování a záruky I.CA

I.CA zaručuje, že:

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

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

- klient neporušil povinnosti plynoucí mu ze smlouvy o poskytování kvalifikované certifikační služby a relevantní CP,
- spoléhající se strana neporušila povinnosti relevantní CP.

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

9.6.2 Zastupování a záruky RA

RA přejímá závazek za správné vyřízení žádostí. RA nevyřídí kladně žádost, pokud žadatel hodnověrným způsobem neprokázal svoji identitu, nedoložil údaje uvedené v o službu, odmítá potřebné údaje sdělit nebo odmítne podepsat příslušné dokumenty. Postup je popsán v této CPS. 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, podepisující nebo označující osoby

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

9.6.4 Zastupování a záruky spoléhajících se stran

Spoléhající se strany postupují v souladu s ZoEP a VoEP.

9.6.5 Zastupování a záruky ostatních zúčastněných subjektů

Služba není poskytována.

9.7 Zřeknutí se záruk

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

9.8 Omezení odpovědnosti

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

9.9 Odpovědnost za škodu, náhrada škody

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

Společnost První certifikační autorita, a.s.:

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

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

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

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

Oprávněnou reklamaci je možné podat těmito způsoby:

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

Reklamující osoba (držitel certifikátu) je povinna uvést:

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

Povinnost I.CA:

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

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

Nový certifikát bude držiteli poskytnut zdarma v následujících případech:

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

9.10 Doba platnosti, ukončení platnosti

9.10.1 Doba platnosti

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

9.10.2 Ukončení platnosti

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

9.10.3 Důsledky ukončení a přetrvání závazků

Uvedeno v kapitole 9.10.1.

9.11 Komunikace mezi zúčastněnými subjekty

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

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

9.12 Změny

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

9.12.1 Postup při změnách

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

9.12.2 Postup při oznamování změn

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

9.12.3 Okolnosti, při kterých musí být změněno OID

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

9.13 Řešení sporů

Tato CPS a odpovídající CP, jejich výklad a aplikace se řídí legislativou ZoEP a VoEP ČR, SR.

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 kvalifikovaných certifikačních služeb v oblasti vydávání certifikátů je provozován ve shodě s požadavky ZoEP.

9.16 Další ustanovení

9.16.1 Rámcová dohoda

Tyto skutečnosti jsou pro aplikaci tohoto vydání dokumentu irelevantní.

9.16.2 Postoupení práv

Tyto skutečnosti jsou pro aplikaci tohoto vydání dokumentu irelevantní.

9.16.3 Oddělitelnost ustanovení

Tyto skutečnosti jsou pro aplikaci tohoto vydání dokumentu irelevantní.

9.16.4 Zřeknutí se práv

Tyto skutečnosti jsou pro aplikaci tohoto vydání dokumentu irelevantní.

9.16.5 Vyšší moc

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

9.17 Další opatření

Tyto skutečnosti jsou pro aplikaci tohoto vydání dokumentu irelevantní.

10 Závěrečná ustanovení

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