První certifikační autorita, a.s.

ZPRÁVA PRO UŽIVATELE

KVALIFIKOVANÉ CERTIFIKÁTY
KVALIFIKOVANÉ SYSTÉMOVÉ CERTIFIKÁTY

Stupeň důvěrnosti : veřejný dokument

Verze 3.1

OBSAH :

1 ÚVOD

1.1 Vývoj dokumentu

Tabulka 1 – Vývoj dokumentu

Verze	Datum vydání	Pozn.
1.0	27.04.2006	První vydání
1.1	14.10.2006	Změna legislativy (vyhláška České republiky č. 378/2006 Sb.,), provedení kontroly bezpečnostní shody, auditu, akreditace v SR
2.0	14.06.2007	Audit ISMS, upřesnění problematiky záruk, odpovědností, náhrad a reklamací
2.1	04.08.2008	Splnění podmínek Microsoft Root Certificate Program - zařazení root certifikátu do důvěryhodných kořenových certifikačních úřadů
2.2	21.10.2009	• Provedení auditu ISMS dle požadavků platné legislativy České republiky na poskytovatele kvalifikovaných certifikačních služeb • Provedení auditu stavu bezpečnosti poskytovaných certifikačních služeb dle požadavků platné legislativy Slovenské republiky • Provedení auditu dle požadavků Microsoft Root Certificate Program
3.0	11.01.2010	Vydávání certifikátů s parametry, splňujícími požadavky platné legislativy na problematiku hashovacích funkcí (využívání algoritmů rodiny SHA-2) a minimální přípustné délky kryptografického klíče pro algoritmus RSA (2048 bitů)
3.1	15.09.2011	Doplnění provedených kontrol za minulá období, upřesnění podporovaných hashovacích funkcí

1.2 Přehled

Tento dokument, vydaný společností První certifikační politika, a.s., (dále též I.CA), podává základní přehled o poskytované certifikační službě vydávání kvalifikovaných certifikátů a kvalifikovaných systémových certifikátů, právech a povinnostech uživatelů této služby, byl vypracován na základě požadavků platné legislativy, vztahující k problematice využívání kryptografických algoritmů v procesu vytváření elektronického podpisu. V souladu s požadavky této legislativy (odkazující se na doporučení technické specifikace ETSI[1] TS 102 176-1) stanovil příslušný akreditační a dozorový orgán[2] kvalifikovaným poskytovatelům certifikačních služeb povinnost ukončit vydávání kvalifikovaných certifikátů, resp. kvalifikovaných systémových certifikátů s algoritmem SHA-1 nejpozději k 31. 12. 2009 a nejpozději od 1. 1. 2010 zahájit vydávání kvalifikovaných certifikátů, resp. kvalifikovaných systémových certifikátů, podporující některý z algoritmů rodiny SHA-2. Zároveň je od uvedeného data stanovena minimální přípustná délka kryptografického klíče pro algoritmus RSA na 2048 bitů.

Kořenový certifikát I.CA (délka RSA klíče 2048 bitů a podporovaný kryptografický algoritmus SHA-256) lze získat na stránkách společnosti První certifikační autorita, a.s. nebo Ministerstva vnitra České republiky.

Společností První certifikační autorita, a.s. podporované hashovací funkce, využívané v procesu žádosti o prvotní, resp. následný kvalifikovaný certifikát a hashovací funkce použité v procesu vydávání tohoto certifikátu, jsou uvedeny v následujícím seznamu :

[1] European Telecommunications Standards Institute
[2] S ohledem na skutečnost, že I.CA je akreditovaným poskytovatelem certifikačních služeb na území České republiky a Slovenské republiky, jedná se o Ministerstvo vnitra České republiky a Národní bezpečnostní úřad Slovenské republiky

- Produkt TWINS (současně vydávaný pár certifikáů – kvalifikovaný a „nekvalifikovaný“):
    - žádost SHA-1 -> vydaný certifikát SHA-256
    - žádost SHA-256 -> vydaný certifikát SHA-256
    - žádost SHA-512 -> vydaný certifikát SHA-512
- Ostatní kvalifikované certifikáty :
    - žádost SHA-256 -> vydaný certifikát SHA-256
    - žádost SHA-512 -> vydaný certifikát SHA-512

Společností První certifikační autorita, a.s. podporované hashovací funkce, využívané v procesu žádosti o prvotní, resp. následný o kvalifikovaný systémový certifikát a hashovací funkce použité v procesu vydávání tohoto certifikátu, jsou uvedeny v následujícím seznamu : :

- žádost SHA-256 -> vydaný certifikát SHA-256, nebo
- žádost SHA-512 -> vydaný certifikát SHA-512.

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

1.3 Kontroly bezpečnostní shody, audity a jiné kontroly

Tabulka 2 – Provedené kontroly bezpečnostní shody, audity, jiné kontroly

Typ	Výrok kontrolora/auditora
Kontrola bezpečnostní shody - zpráva ze dne 26.06.2006	VYHOVUJE
Audit bezpečnosti poskytovania certifikačných činností - zpráva ze dne 09.08.2006	VYHOVUJE
Audit systému řízení bezpečnosti informací (ISMS) - zpráva ze dne 30.04.2007	VYHOVUJE
Kontrola bezpečnostní shody - zpráva ze dne 28.06.2007	VYHOVUJE
Audit of the company První certifikační autorita, a.s. for compliance with policy requirements for certification authorities issuing certificates in accordance with ETSI TS 101 456 - March 3rd, 2008	VYHOVUJE
Kontrola bezpečnostní shody - zpráva ze dne 18.6.2008	VYHOVUJE
Audit systému řízení bezpečnosti informací společnosti První certifikační autorita, a.s. (akreditovaný poskytovatel kvalifikovaných certifikačních služeb) – Závěrečná zpráva ze dne 30.04.2009	VYHOVUJE
Audit stavu bezpečnosti poskytovania certifikačných činností – Závěrečná zpráva ze dne 30.04.2009	VYHOVUJE
Audit of the company První certifikační autorita, a.s. for compliance with policy requirements for certification authorities issuing certificates in accordance with ETSI TS 101 456 - April 30rd, 2009	VYHOVUJE
Kontrola bezpečnostní shody - zpráva ze dne 18.6.2009	VYHOVUJE
Audit of the company První certifikační autorita, a.s. for compliance with policy requirements for certification authorities issuing certificates in accordance with ETSI TS 101 456 - April 28th, 2010	VYHOVUJE
Audit stavu bezpečnosti poskytovania certifikačných činností – Závěrečná zpráva ze dne 30.04.2010	VYHOVUJE
Kontrola bezpečnostní shody - zpráva ze dne 30.06.2010	VYHOVUJE
Audit of the company První certifikační autorita, a.s. for compliance with policy requirements for certification authorities issuing certificates in accordance with ETSI TS 101 456 - May 2nd, 2011	VYHOVUJE

Audit stavu bezpečnosti poskytovania certifikačných činností – Závěrečná zpráva ze dne 2.5.2011	VYHOVUJE
Audit systému řízení bezpečnosti informací společnosti První certifikační autorita, a.s. (akreditovaný poskytovatel kvalifikovaných certifikačních služeb) – Závěrečná zpráva ze dne 2.5.2011	VYHOVUJE
Kontrola bezpečnostní shody - zpráva ze dne 1.9.2011	VYHOVUJE

2 Kontaktní informace

Základními adresami (dále též informační adresy), na nichž lze nalézt veřejné informace o I.CA (certifikační politiky, zprávy pro uživatele, další informace dle platné legislativy, ostatní veřejné dokumenty, případně odkazy pro zjištění dalších informací, atd.) jsou :

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

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

c) sídla registračních autorit

Kontaktní adresy, které slouží pro kontakt uživatelů s I.CA, jsou :

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

b) elektronická poštovní adresa info@ica.cz

3 Typy certifikátů, ověřovací procedury

3.1 Typy certifikátů

Společnost První certifikační autorita, a.s. vydává kvalifikované certifikáty a kvalifikované systémové certifikáty, jejich struktura vyhovuje standardu X.509 verze 3.

Legislativa **České republiky** nedefinuje úložiště soukromého klíče. V případě, že úložištěm soukromého klíče je bezpečné zařízení pro tvorbu elektronického podpisu (**S**ecure **S**ignature **C**reation **D**evice - SSCD), musí splňovat požadavky standardu CWA 14169 – Secure signature-creation devices "EAL 4+" .

Úložištěm soukromého klíče koncovým uživatelům vydávaných kvalifikovaných certifikátů v souladu s legislativou **Slovenské republiky** vztahující se k problematice elektronického podpisu **musí** být pouze produkty, certifikované Národním bezpečnostním úřadem Slovenské republiky.

Není-li uvedeno jinak, je dále v tomto dokumentu pod pojmem certifikát míněn kvalifikovaný certifikát a/nebo kvalifikovaný systémový certifikát.

3.2 Počáteční ověření identity

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

Vlastnictví dat pro vytváření elektronických podpisů/značek, odpovídajících datům pro ověřování elektronických podpisů/značek, která daná žádost o certifikát obsahuje a která budou obsažena ve vydaném certifikátu, se prokazuje předložením žádosti o certifikát. S ohledem na skutečnost, že tato žádost je elektronicky podepsána/označena daty pro vytváření elektronických podpisů/značek, odpovídajících datům pro ověřování elektronických podpisů/značek obsažených v žádosti, dokazuje tímto způsobem žadatel o certifikát, že v době tvorby elektronického podpisu/značky vlastnil soukromý klíč, odpovídající veřejnému klíči, který je v žádosti uveden.

3.2.2 Ověřování identity právnické osoby nebo organizační složky státu

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

3.2.3 Ověřování identity fyzické osoby

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

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

3.2.3.1 Fyzická osoba nepodnikající

3.2.3.1.1 Předkládané doklady na RA (registrační autorita)

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

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

  Údaje požadované v sekundárním osobním dokladu musí být shodné s těmito údaji v primárním osobním dokladu. O shodnosti rozhoduje pracovník RA. Pokud žadatel nepředloží dva osobní doklady výše popsané kvality, nebude žádost přijata. Příkladem akceptovatelného sekundárního osobního dokladu jsou např. cestovní pas, řidičský průkaz, služební průkazy státních úřadů, průkaz poslance, služební průkaz policie, zbrojní průkaz, vojenská knížka, průkaz zdravotního pojištění, průkazka hromadné dopravy, firemní průkazky, studentský průkaz atd.
- Pokud bude certifikát obsahovat doplňující identifikátor (certifikáty vydávané v souladu s legislativou Slovenské republiky), je požadován platný originál, resp. úředně ověřená kopie relevantního dokladu.

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

- Originály platného primárního osobního dokladu a dalšího osobního dokladu (sekundárního) zmocněnce (kvalita primárního a sekundárního dokladu je uvedena výše)
- Originály primárního a sekundárního osobního dokladu žadatele o certifikát (kvalita primárního a sekundárního dokladu je uvedena výše)
- Pokud bude certifikát obsahovat doplňující identifikátor (certifikáty vydávané v souladu s legislativou Slovenské republiky), je požadován platný originál, resp. úředně ověřená kopie relevantního dokladu.
- Plná moc (nerozhodne-li ředitel I.CA jinak) s úředně ověřeným podpisem zmocnitele - pokud je plná moc v cizím jazyce (kromě slovenštiny), musí být přeložena do češtiny úředním překladatelem (v zahraničí[3] provedené úřední ověření podpisů musí být tzv. „superlegalizováno“, tj. potvrzeno zastupitelským úřadem České republiky v zemi původu plné moci; v případě dokladů, ověřených v zemích, uvedených na http://www.hcch.net/, nemusí být superlegalizace provedena[4]
- Pokud je žadatel zákonným zástupcem[5] klienta, požaduje se o tom úřední doklad :

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

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

[5] zákonným zástupcem dítěte není pro účely ZoEP pěstoun

- 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.

- Poručník nebo opatrovník je osobám bez plné způsobilosti k právním úkonům, včetně dospělých, ustanoven soudem. Dokladem je soudní rozhodnutí.
  - Opatrovníkem nebo poručníkem dítěte může být ustanoven také orgán sociálně-právní ochrany dítěte (zpravidla obec nebo obcí zřízený veřejný opatrovník). V tom případě jde o právnickou osobou a vedle usnesení soudu dokládá ještě skutečnosti, vztahující se k právnickým osobám.
  - Opatrovník může být ustanoven také osobám s tělesným postižením, které nemají omezenou svéprávnost, ale potřebují při právních úkonech asistenci (např. nevidomým).

3.2.3.1.2 Kontrolované a ověřované doklady na RA

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

- Zda osoba, která je uvedena v žádosti o certifikát, je totožná s osobou žadatele (dle platného primárního dokladu), a že údaje uvedené v žádosti odpovídají údajům v předložených dokladech. Shoda je nutná u těchto údajů :
  - příjmení, jméno
  - bydliště (město)
  - oblast (ulice, pokud je uvedena)
- Plnoletost žadatele
- Platnost předkládaných dokladů
- Pokud se žadatel prokazuje cestovním pasem, kontrola na shodu bydliště se neprovádí
- Příslušník cizího státu musí splňovat podmínky pro právní subjektivitu a svéprávnost alespoň podle práva CZ - pokud je nesplňuje, je třeba ověřit, zda splňuje podmínky podle práva státu jehož je příslušníkem. V takovém případě je třeba postupovat individuálně, ve spolupráci s žadatelem a I.CA.

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

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

3.2.3.2 Fyzická osoba podnikající, zaměstnanec

3.2.3.2.1 Předkládané doklady na RA

Žadatel o certifikát předkládá následující typy dokladů :

- Doklady ve stejném rozsahu, jako v kapitole 3.2.3.1.1.
- Doklad, uvedený v kapitole 3.2.2. Pokud je tento doklad v cizím jazyce, platí pro ověření pravidla, uvedená v kapitole 3.2.3.1.

- V případě zaměstnance - potvrzení o zaměstnaneckém poměru k danému zaměstnavateli, pokud není uzavřena s I.CA rámcová smlouva. Potvrzení musí být opatřeno podpisem osoby s právem jednání za příslušného zaměstnavatele. Pokud tato osoba není osobou oprávněnou k zastupování zaměstnavatele, tj. není statutárním zástupcem (není uveden na výpisu z obchodního rejstříku nebo jiného zákonem určeného rejstříku nebo registru, živnostenský list, zřizovací listina, atd. jako osoba oprávněná jednat), požaduje se navíc úředně ověřený doklad (plná moc, pověření, doklad o zákonném zastupování) podepsaný statutárním zástupcem zaměstnavatele, potvrzující oprávněnost této osoby jednat za zaměstnavatele.

3.2.3.2.2 Kontrolované a ověřované doklady na RA

Pracovníkem RA je kontrolováno a ověřováno :

- Zda údaje, uvedené v žádosti o certifikát, se shodují s údaji v dokladech předložených žadatelem, resp. zmocněncem - při kontrole postupuje pracovník RA stejně jako u fyzické osoby nepodnikající.
- Potvrzení o zaměstnaneckém poměru k danému zaměstnavateli.
- Zda je osoba, podepisující potvrzení o zaměstnaneckém poměru, uvedená v úředně ověřeném dokladu (plná moc, pověření, doklad o zákonném zastupování), oprávněna zastupovat zaměstnavatele - pracovník RA musí zkontrolovat, zda tato osoba má právo takovéto pověření provést, popřípadě, zda uděluje plnou moc oprávněné osobě v souladu s výpisem výše uvedených dokumentů[6] (v případě fyzické/právnické osoby se jedná o výpis z obchodního nebo jiného zákonem předepsaného rejstříku, živnostenského listu, zřizovací listiny, zákona, atd., v případě organizační složky státu/orgánu veřejné moci se jedná o zvláštní právní předpisy)

Pokud dojde během trvání smluvního vztahu k I.CA ke změnám ve výše uvedených údajích nebo v údajích, uvedených v certifikátu, je držitel certifikátu, resp. podepisující osoba povinen tyto změny ohlásit I.CA.

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“)

3.3.1.1 Kvalifikovaný certifikát

Identifikace a autentizace žadatele o vydání následného certifikátu (struktura PKCS#10) je prováděna ověřením zaručeného elektronického podpisu žádosti o vydání následného certifikátu. V procesu ověřování elektronického podpisu žádosti o následný certifikát musí být použit platný certifikát (vydaný dle dokumentu Certifikační politika vydávání kvalifikovaných certifikátů - verze 3.0 a vyšší), ke kterému je vydáván tento následný certifikát.

[6] 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)

3.3.1.2 Kvalifikovaný systémový certifikát

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

3.4 Identifikace a autentizace při zpracování požadavků na zneplatnění certifikátu

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

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

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

V případě použití **listovní zásilky o zneplatnění certifikátu** musí být tato zaslána doporučeně na adresu sídla společnosti (viz kapitola 2).

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

4 Omezení použití

Certifikáty, vydávané společností První certifikační autorita, a.s., smí být používány k ověření elektronického podpisu, resp. elektronické značky v souladu s platnou legislativou a vydávaným účelem, uvedeným v písemné smlouvě mezi I.CA a držitelem certifikátu, resp. podepisující osobou.

5 Povinnosti klientů

Z hlediska společnosti První certifikační autorita, a.s. je jejím klientem každá fyzická nebo právnická osoba, která uzavřela smlouvu o využívání kvalifikovaných certifikačních služeb I.CA s provozovatelem jejích služeb.

Klient musí zejména :

- seznámit se s relevantní certifikační politikou a ustanoveními příslušné smlouvy o vydání a používání certifikátu (resp. seznámit s nimi případné podepisující osoby nebo označující osoby) a dbát na jejich dodržování
- zacházet s prostředky jakož i s daty pro vytváření elektronického podpisu/značky s náležitou péčí tak, aby nemohlo dojít k jejich neoprávněnému použití,
- uvědomit neprodleně poskytovatele certifikačních služeb, který certifikát vydal, o tom, že hrozí nebezpečí zneužití jeho dat pro vytváření zaručeného elektronického podpisu/značky
- bez zbytečného odkladu podávat přesné, pravdivé a úplné informace poskytovateli certifikačních služeb
- v případě, že je označující osobou zajistit, aby prostředek pro vytváření elektronických značek, který používá, splňoval požadavky stanovené platnou legislativou

6 Povinnosti spoléhajících se stran

Z hlediska společnosti První certifikační autorita, a.s. je spoléhající se stranou subjekt, spoléhající se při své činnosti na společností I.CA vydané kvalifikované certifikáty a kvalifikované systémové certifikáty. Spoléhající se strana je zejména povinna :

- užívat certifikáty v souladu s platnou legislativou a relevantní certifikační politikou
- získat certifikát certifikační autority společnosti První certifikační autorita, a.s. z bezpečného zdroje a ověřit otisk (miniatura, fingerprint, …) tohoto certifikátu
- před použitím certifikátu vydaného certifikační autoritou společnosti První certifikační autorita, a.s. ověřit platnost certifikátu certifikační autority společnosti První certifikační autorita, a.s.
- provádět veškeré úkony k ověření, že elektronický podpis/ značka jsou platné a odpovídající certifikát nebyl zneplatněn

7 Omezení záruky a odpovědnosti

Společnost První certifikační autorita, a.s. :

- prohlašuje, že splní všechny povinnosti, které jí vyplývají z certifikačních politik a legislativních předpisů (viz kapitola 0).
- poskytuje výše uvedené záruky po celou dobu platnosti smlouvy o poskytování certifikačních služeb, uzavřené s klientem. Pokud bylo zjištěno porušení povinností klienta, mající souvislost s uváděnou škodou, záruční plnění se neposkytne. Tato skutečnost musí být klientovi oznámena a zaprotokolována. Další možné náhrady škody vycházejí z ustanovení příslušných zákonů a o jejich výši může rozhodnout soud.
- neodpovídá za :
  - vady poskytovaných certifikačních služeb, které vzniknou jejich používáním v rozporu s příslušnými certifikačními politikami, a dále za vady, které vznikly z důvodu vyšší moci včetně dočasného výpadku telekomunikačního spojení atd.
  - 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).

8 Smlouvy a certifikační politika

Vztah mezi klientem a akreditovaným poskytovatelem kvalifikovaných certifikačních služeb, společností První certifikační autorita, a.s., je (kromě příslušných ustanovení povinných právních předpisů) upraven smlouvou a příslušnými ustanoveními platných certifikačních politik.

Vztah mezi spoléhající se stranou a akreditovaným poskytovatelem kvalifikovaných certifikačních služeb, společností První certifikační autorita, a.s., je upraven příslušnými ustanoveními platných certifikačních politik. Vztah společnost První certifikační autorita, a.s. a spoléhajících se stran není upraven smlouvou.

Veškeré veřejné informace je možné získat na kontaktních adresách, uvedených v kapitole 2 tohoto dokumentu.

9 Ochrana osobních údajů

Ochrana osobních údajů a dalších neveřejných informací je v I.CA řešena v souladu s požadavky příslušných zákonných norem (zákon ČR č. 227/2000 Sb., o elektronickém podpisu a o změně některých dalších zákonů, zákon ČR č. 101/2000 Sb. o ochraně osobních údajů a o změně některých zákonů, zákon SR č. 215/2002 Z.z. o elektronickom podpise a o zmene a doplnení niektorých zákonov, zákon SR č. 428/2002 Z. z. o ochrane osobných údajov vrátane Zákona č. 90/2005 Z. z.).

Žadatel o certifikát dává společnosti První certifikační autorita, a.s. písemný souhlas se zpracováním a uchováváním osobních údajů v rozsahu požadavků platné legislativy, vztahující se k problematice elektronickém podpisu.

10 Politika náhrad a reklamace

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.

11 Právní prostředí

Společnost První certifikační autorita, a.s. se při své činnosti řídí příslušnými ustanoveními právního řádu České republiky, zejména :

- 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.,
- nařízením vlády České republiky č. 495/2004 Sb., kterým se provádí zákon č. 227/2000 Sb.
- vyhláškou 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)
- zákonem České republiky č. 101/2000 Sb. o ochraně osobních údajů a o změně některých zákonů
- zákonem České republiky č. 300/2008 Sb., o elektronických úkonech a autorizované konverzi dokumentů

S ohledem na získání akreditace na poskytování kvalifikovaných certifikačních služeb na území Slovenské republiky se společnost První certifikační autorita, a.s. v oblastech vydávání kvalifikovaných certifíkátů a časových razítek dále řídí zejména :

- zákonem 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
- zákonem Slovenské republiky č. 428/2002 Z.z. o ochrane osobných údajov

12 Akreditace, audity a kontroly

Společnost **První certifikační autorita, a.s.,** je akreditovaným poskytovatelem certifikačních služeb v České republice pro oblast vydávání **kvalifikovaných certifikátů, 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) a 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.

Poskytování kvalifikovaných certifikačních služeb společností První certifikační autorita, a.s., je pravidelně podrobováno auditům a kontrolám, požadovaných legislativou České republiky a Slovenské republiky. S ohledem na zařazení kořenových certifikátů I.CA do důvěryhodných kořenových certifikačních úřadů společnosti Microsoft, je poskytování certifikačních služeb také auditováno dle požadavků Microsoft Root Certificate Program.

Ing. Petr Budiš, Ph.D., v.r.
předseda představenstva
a ředitel společnosti