První certifikační autorita, a.s.

ZPRÁVA PRO UŽIVATELE

KVALIFIKOVANÉ CERTIFIKÁTY
KVALIFIKOVANÉ SYSTÉMOVÉ CERTIFIKÁTY

Stupeň důvěrnosti: veřejný dokument

Verze 3.6

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
3.2	14.5.2012	• Provedení auditu stavu bezpečnosti poskytovaných certifikačních služeb dle požadavků platné legislativy Slovenské republiky • Provedení auditu dle požadavků Microsoft Root Certificate Program
3.3	10.9.2012	Doplnění provedení celkové kontroly bezpečnostní shody
3.4	11.6.2013	• 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 (ETSI 101 456)
3.5	10.9.2013	Doplnění kontroly bezpečnostní shody, aktualizace dokumentu
3.6.	19.11.2014	• Provedení auditu stavu bezpečnosti poskytovaných certifikačních služeb dle požadavků platné legislativy Slovenské republiky • Provedení auditu dle požadavků Microsoft Root Certificate Program (ETSI 101 456) • Provedení kontroly bezpečnostní shody • Kontrola MV ČR dle ustanovení § 4 zákona č. 255/2012 Sb., o kontrole (kontrolní řád), a s ustanovením § 9 odst. 2 písm. b) a odst. 3 a 4 zákona č. 227/2000 Sb., o elektronickém podpisu a o změně některých dalších zákonů, ve znění pozdějších předpisů

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 držitelů certifikátů a spoléhajících se stran.

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
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 - Final Report, May 2012	VYHOVUJE
Audit stavu bezpečnosti poskytovania certifikačných činností – Záverečná správa, máj 2012	VYHOVUJE
Kontrola bezpečnostní shody (celková) - zpráva ze dne 31.8.2012	VYHOVUJE
Audit systému řízení bezpečnosti informací společnosti První certifikační autorita, a.s. (akreditovaný poskytovatel kvalifikovaných certifikačních služeb) – Závěrečná zpráva ze dne 14.5.2013	VYHOVUJE

Audit stavu bezpečnosti poskytovania certifikačných činností – Závěrečná zpráva ze dne 14.5.2013	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 - Final Report, May 2013	VYHOVUJE
Kontrola bezpečnostní shody (částečná) - zpráva ze dne 28.8.2013	VYHOVUJE
Audit stavu bezpečnosti poskytovania certifikačných činností – Záverečná správa, máj 2014 (ze dne 20.5.2014)	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 - Final Report, May 2014 (ze dne 20.5.2014)	VYHOVUJE
Kontrola bezpečnostní shody (částečná) - zpráva ze dne 27.8.2014	VYHOVUJE
Protokol o plnění ustanovení § 6 odst. 1 písm. d) zákona 227/2000 Sb. (zákon o elektronickém podpisu) ve vazbě na odst. 1 písm. c). Plnění ustanovení § 6 odst. 5 a 6 zákona 227/2000 Sb. ve vazbě na plnění povinností stanovených vyhláškou č. 378/2006 Sb. (vyhláška o postupech kvalifikovaných poskytovatelů certifikačních služeb) - ze dne 6.11.2014	Kontrolou bylo ověřeno, že akreditovaný poskytovatel certifikačních služeb I.CA dodržuje uvedená ustanovení

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) adresa sídla společnosti:

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

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

c) sídla registračních autorit

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

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

b) elektronická poštovní adresa info@ica.cz

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.

Kvalifikované certifikáty jsou vydávány v souladu s legislativou České republiky (aktuální znění zákona č. 227/2000 Sb., o elektronickém podpisu) a Slovenské republiky (zákona č. 215/2002 Z.z., o elektronickom podpise), kvalifikované systémové certifikáty pak v souladu s legislativou České republiky.

Výše uvedené typy certifikátů (délka RSA klíče 2048 bitů) jsou vydávány fyzickým osobám, právnickým osobám nebo organizačním složkám státu.

Společností První certifikační autorita, a.s. podporované hashovací funkce využívané v procesu tvorby žádosti (PKCS#10) o kvalifikovaný certifikát nebo kvalifikovaný systémový certifikát a hashovací funkce použité v procesu vydávání tohoto certifikátu, jsou uvedeny v následujícím seznamu:

- žádost SHA-256 -> vydaný certifikát SHA-256
- žádost SHA-512 -> vydaný certifikát SHA-512
- žádost SHA-1 -> vydaný certifikát SHA-256

V případě, že žádost bude využívat jinou hashovací funkci, nebude certifikát vydán.

Pro koncové uživatele nedefinuje legislativa **České republiky** 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 musí** být výhradně produkty, certifikované Národním bezpečnostním úřadem Slovenské republiky.

Certifikáty certifikačních autorit I.CA (délka RSA klíče 2048 bitů a podporovaný kryptografický algoritmus SHA-256) lze získat na stránkách společnosti První certifikační autorita, a.s., Ministerstva vnitra České republiky (akreditace v souladu s legislativou České republiky) nebo NBÚ Slovenské republiky (akreditace v souladu s legislativou Slovenské republiky).

3.2 Ověření žadatele o certifikát

3.2.1 Vydání prvotního certifikátu

V procesu vydávání prvotního certifikátu[1] je vždy ověřována totožnost žadatele o certifikát na základě jeho osobních dokladů. V případě, že certifikát bude vydán fyzickým osobám podnikajícím, právnickým osobám nebo organizačním složkám státu, je ověřován i vztah žadatele na tuto osobu. V případě, že žadatel o certifikát je zastupován zmocněncem, pak jsou ověřovány i jeho osobní doklad a požadována platná plná moc.

Podrobný popis ověřovacího procesu získání prvotního certifikátu je uveden v příslušných certifikačních politikách.

[1] není-li uveden typ certifikátu, jedná se jak o kvalifikovaný certifikát a/nebo kvalifikovaný systémový certifikát

3.2.2 Vydání následného certifikátu

V procesu vydávání následného certifikátu (certifikát, který bude vydán žadateli na základě nové žádosti o certifikát v období platnosti certifikátu, ke kterému je vydáván tento následný certifikát) je totožnost žadatele o následný certifikát ověřována kontrolou elektronického podpisu (jsou využívána párová data, která jsou předmětem výměny) žádosti (PKCS#10) o tento následný certifikát.

Podrobný popis ověřovacího procesu získání následného certifikátu je uveden v příslušných certifikačních politikách.

3.3 Zpracování požadavku 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 relevantní ustanovení kapitoly 3.2.1. 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)
- prostřednictvím datové schránky

V případě použití **listovní zásilky o zneplatnění certifikátu** musí být tato zaslána doporučeně na adresu sídla společnosti.

Podrobný popis zpracování požadavku o zneplatnění certifikátu je uveden v příslušných certifikačních politikách.

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.

Podrobný popis použití certifikátů je uveden v příslušných certifikačních politikách.

5 Povinnosti klientů

Z pohledu společnosti První certifikační autorita, a.s. je klientem každá osoba, která uzavřela se společností První certifikační autorita, a.s. smlouvu o vydání certifikátu.

Klient musí zejména:

- seznámit se s relevantní certifikační politikou a ustanoveními příslušné smlouvy o vydání a používání certifikátu (resp. seznámit s nimi případné podepisující 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 I.CA o tom, že hrozí nebezpečí zneužití jeho dat pro vytváření elektronického podpisu/značky
- bez zbytečného odkladu podávat I.CA přesné, pravdivé a úplné informace, vztahující se k vydávanému/vydanému certifikátu

6 Povinnosti spoléhajících se stran

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

- užívat certifikáty v souladu s platnou legislativou a relevantní certifikační politikou
- ověřit platnost elektronického podpisu/značky s ohledem na integritu
- získat certifikáty certifikačních autorit 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 jak relevantních certifikátů certifikačních autorit, tak i vydaného certifikační autoritou společnosti První certifikační autorita, a.s. koncovému uživateli

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.
- 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.

Společnost První certifikační autorita, a.s. 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 je dodržena definovaná lhůta pro zveřejnění zneplatněného certifikátu na seznamu zneplatněných certifikátů (CRL).

8 Smlouvy a certifikační politika

Vztah mezi držitelem certifikátu a poskytovatelem 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 poskytovatelem certifikačních služeb - společností První certifikační autorita, a.s., je upraven příslušnými ustanoveními platných certifikačních politik. Vztah společnosti První certifikační autorita, a.s. a spoléhajících se stran smlouvou upraven není.

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.

Žadatel o kvalifikovaný certifikát, resp. kvalifikovaný systémový 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 certifikátů bezplatné vydání nového certifikátu - případné náklady na vydání nových certifikátů hradí I.CA, která po dobu zablokování certifikátu (stav, ve kterém se certifikát nachází od doby, kdy jej I.CA zneplatnila, do doby, kdy I.CA zveřejnila CRL, ve kterém je tento certifikát poprvé zařazen) 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 v oblasti kvalifikovaných certifikačních služeb řídí příslušnými aktuálními 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.,
- 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

S ohledem na získání akreditace na poskytování kvalifikovaných certifikačních služeb na území Slovenské republiky se společnost První certifikační autorita, a.s. se při své činnosti řídí příslušnými aktuálními ustanoveními právního řádu Slovenské republiky, 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

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 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 podrobováno pravidelným auditům v souladu s požadavky Microsoft Root Certificate Program.

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