První certifikační autorita, a.s.

ZPRÁVA PRO UŽIVATELE

KVALIFIKOVANÁ ČASOVÁ RAZÍTKA

Stupeň důvěrnosti: veřejný dokument

Verze 3.6

OBSAH :

1 ÚVOD

1.1 Vývoj dokumentu

Tabulka 1 – Vývoj dokumentu

Verze	Datum vydání	Shrnutí změn
1.0	25.01.2006	První vydání
1.1	14.10.2006	Změna vyhlášky, provedení kontroly bezpečnostní shody, auditu, akreditace v SR
2.0	01.11.2007	Audit ISMS, upřesnění problematiky záruk, odpovědností, náhrad a reklamací, použití více vyhrazených serverů pro vydávání kvalifikovaných časových razítek
2.1	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
3.0	01.03.2010	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
3.2.	14.5.2012	Provedení auditu stavu bezpečnosti poskytovaných certifikačních služeb dle požadavků platné legislativy Slovenské republiky
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
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 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 časových razítek, včetně práv a povinnostech žadatelů o kvalifikovaná časová razítka.

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 stavu bezpečnosti poskytovania certifikačných činností – Závěrečná zpráva ze dne 30.04.2010	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 - April 30rd, 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
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
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
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

Základní adresy na nichž lze nalézt informace o společnosti První certifikační autorita, a.s., jí poskytované certifikační službě vydávání kvalifikovaných časových razítek, případně odkazy pro zjištění dalších informací, jsou:

- První certifikační autorita, a.s.
  Podvinný mlýn 2178/6
  190 00 Praha 9
  Česká republika
- internetová adresa http://www.ica.cz
- sídla registračních autorit
- elektronické poštovní adresy tsa@ica.cz, info@ica.cz

3 Vydávání časových razítek

3.1 Ověřovací procedury

Vydávání časových razítek[1] je I.CA komerčně nabízenou službou, uzavíranou způsobem běžným v obchodním styku.

S ohledem na komerční bázi a nadstandardní služby v procesu vydávání časových razítek je žadatel o časové razítko identifikován a autentizovám výběrem jednou z níže uvedených možností:

- komerčním certifikátem vydaným I.CA
- jménem a heslem
- IP adresou

I.CA si vyhrazuje právo na využití jiného způsobu implementace procesu identifikace a autentizace žadatele o časové razítko.

3.2 Žádost o časové razítko

Po úspěšně provedené identifikaci a autentizaci, vytvoří žadatel v souladu s příslušnou politikou žádost o časové razítko (v souladu s RFC3161). Tato žádost je předána systému TSA, který ji následně předá jednomu ze serverů, vydávajících časová razítka. V žádosti o časové razítko jsou podporovány kryptografické algoritmy SHA1, SHA-256 a SHA-512.

3.3 Vydání časového razítka

Systém TSA provádí veškeré kontroly formální správnosti žádosti o časové razítko a na základě jejich výsledku vytvoří konkrétní časový server odpověď, obsahující v případě kladného výsledku kontrol časové razítko (viz RFC 3161). Časový údaj (UTC), jehož přesnost při vytváření časového razítka je 1 sekunda, je získán z měřidla důvěryhodného času. Odpověď je elektronicky označena/podepsána daty pro vytváření elektronické značky/podpisu časového serveru, který časové razítko vydal (tím se tento server nezpochybnitelným způsobem zaručuje za správnost informací uvedených ve vygenerovaném časovém razítku).

Každá odpověď na žádost o časové razítko, obsahující mimo výše uvedených údajů i další potřebné informace (mimo jiné o měřidlu důvěryhodného času), je předána žadateli o časové razítko a taktéž umístěna v příslušném úložišti systému TSA.

Certifikáty serverů, elektronicky podepisujících/označujících vydávaná časová razítka, lze získat na stránkách společnosti První certifikační autorita, a.s., nebo Ministerstva vnitra České republiky.

[1] není-li uvedeno jinak, jedná se o kvalifikované časové razítko

3.4 Ověření časového razítka

Po obdržení odpovědi na žádost o časové razítko je žadatel povinen zjistit status odpovědi. V případě chyby není časové razítko v odpovědi obsaženo a žadatel je povinen překontrolovat odpovídající chybovou hlášku. V opačném případě je žadatel povinen ověřit zejména:

- zda vrácený otisk (hash) je totožný s odeslaným v žádosti
- platnost elektronické značky/podpisu časového razítka
- platnost všech certifikátů v certifikační cestě, vztahujících se k vydanému časovému razítku
- v případě, že žádost obsahovala položku „nonce“ a/nebo „reqPolicy“ ověřit, že její hodnota v odpovědi je totožná

4 Omezení použití

Nejsou definována žádná omezení použitelnosti časového razítka[2]. Obecně platí, že časové razítko je datová zpráva, kterou vydal poskytovatel certifikačních služeb a která důvěryhodným způsobem spojuje data v elektronické podobě s časovým okamžikem a zaručuje, že uvedená data v elektronické podobě existovala před daným časovým okamžikem.

5 Povinnosti klientů (žadatelů o časové razítko)

Klienti (žadatelé) jsou povinni žádat o časová razítka v souladu s odpovídající politikou a legislativou, vztahující se k problematice elektronického podpisu. Povinnosti jsou uvedeny v kapitole 3.4.

6 Povinnosti spoléhajících se stran

Obecným závazkem spoléhajících se stran je ověření elektronické značky/ podpisu vydaného časového razítka. Spoléhající se strana je povinna zejména:

- ověřit platnost elektronické značky/podpisu časového razítka a následně všech certifikátů, vztahujících se k časovému serveru, který tuto elektronickou značku/podpis vytvořil
- ověřit vydané časové razítko - konkrétně se jedná o hash ověřovaných dat a zda politika, pod kterou bylo časové razítko vydáno, je akceptovatelná její potřebám, popř. potřebám provozovaných aplikací
- ověřit bezpečnost procesu vytváření časového razítka s důrazem na kryptografická funkce pro tvorbu otisku (hash), délku kryptografického klíče a algoritmus pro tvorbu elektronického podpisu/značky

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.

[2] časová razítka vydaná lze využívat jak v otevřených systémech veřejných služeb (např. státní správy), tak v uzavřených systémech soukromých společností.

- 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.

8 Smlouvy, prováděcí směrnice, politika

Vztah mezi klientem a 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 společností První certifikační autorita, a.s., je upraven příslušnými ustanoveními platných certifikačních politik.

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.

10 Politika náhrad a reklamace

Společnost První certifikační autorita, a.s. :

- se zavazuje, že splní veškeré povinnosti definovanými jak příslušnými právními předpisy, tak politikami, reflektující problematiku vydávání časových razítek.
- poskytuje výše uvedené záruky po celou dobu platnosti smlouvy o poskytování certifikačních služeb uzavřené se zákazníkem.

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 zákazníkem, zejména za provozování v rozporu s podmínkami uvedenými v politice, jakož i za vady vzniklé z důvodu vyšší moci, včetně dočasného výpadku telekomunikačního spojení apod.

Oprávněnou reklamaci je možné podat těmito způsoby:

- e-mailem na adresu : reklamace@ica.cz
- doporučenou poštovní zásilkou na adresu sídla společnosti (První certifikační autorita, a.s. Podvinný mlýn 2178/6, 190 00 Praha 9, Česká republika)
- osobně v sídle společnosti

Povinnost reklamující osoby :

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

Povinnost společnosti První certifikační autorita, a.s. :

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.

11 Právní prostředí

Společnost První certifikační autorita, a.s. se při své činnosti 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.,
- 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. 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, audit

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