První certifikační autorita, a.s.

ZPRÁVA PRO UŽIVATELE

KVALIFIKOVANÁ ČASOVÁ RAZÍTKA

Stupeň důvěrnosti : veřejný dokument

Verze 3.0

OBSAH :

1 ÚVOD 2

1.1 VÝVOJ DOKUMENTU 2
1.2 PŘEHLED 2
1.3 KONTROLY BEZPEČNOSTNÍ SHODY, AUDITY A JINÉ KONTROLY 2

2 KONTAKTNÍ INFORMACE 3

3 OVĚŘOVACÍ PROCEDURY 3

4 OMEZENÍ POUŽITÍ 3

5 POVINNOSTI KLIENTŮ (ŽADATELŮ O KVALIFIKOVANÉ ČASOVÉ RAZÍTKO) 3

6 POVINNOSTI SPOLÉHAJÍCÍCH SE STRAN 4

7 OMEZENÍ ZÁRUKY A ODPOVĚDNOSTI 4

8 SMLOUVY, PROVÁDĚCÍ SMĚRNICE, POLITIKA 4

9 OCHRANA OSOBNÍCH ÚDAJŮ 5

10 POLITIKA NÁHRAD A REKLAMACE 5

11 PRÁVNÍ PROSTŘEDÍ 6

12 AKREDITACE, AUDIT 6

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)

1.2 Přehled

Tento dokument byl vypracován na základě požadavků platné legislativy (odkazující se na doporučení technické specifikace ETSI[1] TS 102 176-1), vztahující k problematice využívání kryptografických algoritmů v procesu vytváření elektronického podpisu a algoritmů, využívaných k vytvoření otisku dat při vytváření žádosti o časové razítko.

V žádosti o kvalifikované časové razítko jsou podporovány kryptografické algoritmy SHA1, SHA-256 a SHA-512. Certifikáty serverů, elektronicky podepisujících/označujících vydávaná kvalifikovaná časová razítka, lze získat na stránkách společnosti První certifikační autorita, a.s., nebo Ministerstva vnitra České republiky.

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
Kontrola I.CA dle metodiky NBÚ Slovenské republiky - zpráva ze dne 30.04.2007	VYHOVUJE
Audit systému řízení bezpečnosti informací (ISMS) - zpráva ze dne 30.04.2007	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

[1] European Telecommunications Standards Institute

2 Kontaktní informace

Základní adresy na níž lze nalézt informace o společnosti První certifikační autorita, a.s., výše poskytovaném typu kvalifikované certifikační služby, 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 Ověřovací procedury

Vydávání časových razítek 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 proces identifikace a autentizace žadatele o časové razítko realizován na bázi tzv. „komerčního“ certifikátu, vydaného I.CA.

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

4 Omezení použití

Nejsou definována žádná omezení použitelnosti kvalifikovaného časového razítka[2]. Obecně platí, že kvalifikované časové razítko je datová zpráva, kterou vydal kvalifikovaný 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. Kvalifikovaná časová razítka je možné použít např. v oblastech :

- elektronických podpisů nebo elektronických značek, kdy je třeba ověřit, že byly vytvořeny v době, kdy certifikát veřejného klíče podepisující nebo označující entity byl platný. Tato kontrola je nezbytná z následujících dvou důvodů :
  - během platnosti certifikátu elektronicky podepisující, resp. elektronicky označující entity byl odpovídající soukromý klíč kompromitován
  - elektronický podpis, resp. elektronická značka byly vytvořeny po ukončení doby platnosti příslušného certifikátu
- ochraně spustitelného kódu
- transakcí prováděných na síti

Kvalifikovaná časová razítka nesmí uživatel využívat v rozporu s vydávaným účelem nebo s platnou legislativou.

5 Povinnosti klientů (žadatelů o kvalifikované časové razítko)

Klienti (žadatelé) jsou povinni žádat o kvalifikovaná časová razítka v souladu s odpovídající politikou a platnou legislativou. Žadatelé jsou vždy po obdržení odpovědi na žádost o časové razítko povinni 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 zejména :

- provádět veškeré úkony k ověření, že elektronické značky, resp. elektronické podpisy, vztahující se k vydanému kvalifikovanému časovému razítku jsou platné a jim odpovídající certifikáty nebyly zneplatněny

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

- ověřit platnost elektronické značky/podpisu časového razítka a následně všech certifikátů, vztahujících se k časovému serveru, který tuto elektronickou značku vytvořil
- ověřit, zda vrácený otisk (hash) je totožný s odeslaným v žádosti
- v případě, že žádost obsahovala položku „nonce“ a/nebo „reqPolicy“ ověřit, že její hodnota v odpovědi je totožná

6 Povinnosti spoléhajících se stran

Obecným závazkem spoléhajících se stran je ověření elektronických značek, resp. elektronických podpisů, vztahujících se k vydanému kvalifikovanému časovému razítku. Spoléhající se strana je povinna zejména :

- provádět veškeré úkony k ověření, že elektronické značky, resp, elektronické podpisy, vztahující se k vydanému kvalifikovanému časovému razítku jsou platné a jim odpovídající certifikáty nebyly zneplatněny
- 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 (viz kapitola 11).
- 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, prováděcí směrnice, 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.).

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 kvalifikovaných časových razítek.
- Poskytuje výše uvedené záruky po celou dobu platnosti smlouvy o poskytování certifikačních služeb uzavřené se zákazníkem.
- Pokud nevydá kvalifikované časové razítko v definované kvalitě (uvedeno v aktuálním dokumentu Politika vydávání kvalifikovaných časových razítek), má klient právo na vrácení ceny za dané kvalifikované časové razítko, popř. jeho poskytnutí zdarma. Dále platí obsah kapitoly 7.
- Jiné záruky, než výše uvedené, neposkytuje.

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 aj.

Oprávněnou reklamaci je možné podat těmito způsoby :

- e-mailem na adresu : reklamace@ica.cz
- doporučenou poštovní zásilkou na adresu :

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

Pivinnost 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 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, 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), jak vyplývá ze změn provedených zákonem č. 226/2002 Sb., zákonem č. 517/2002 Sb., a zákonem č. 440/2004 Sb.,

- 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.

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