První certifikační autorita, a.s.

ZPRÁVA PRO UŽIVATELE

KVALIFIKOVANÁ ČASOVÁ RAZÍTKA

Stupeň důvěrnosti : veřejný dokument

Verze 2.1

OBSAH :

1 ÚVOD

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

Tabulka 2 – Kontroly bezpečnostní shody, audity

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

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[1]. 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. Po obdržení odpovědi na žádost o kvalifikované časové razítko jsou klienti vždy povinni zjistit chybový status. V případě chyby není kvalifikované časové razítko v odpovědi obsaženo a žadatel je povinen překontrolovat odpovídající chybovou hlášku. V opačném případě je předplatitel povinen :

- 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, zda vrácený otisk (hash) je totožný s odeslaným
- v případě, že žádost obsahovala položku „nonce“ ověřit, že její hodnota v odpovědi je totožná
- v případě, že žádost obsahovala položku „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 :

- 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
- překontrolovat, zda politika, pod kterou bylo kvalifikované časové razítko vydáno, je akceptovatelná jejím potřebám, popř. potřebám jí provozované aplikace

V případě ověřování kvalifikovaného časového razítka po ukončení platnosti certifikátu relevantního TSS, jsou spoléhající se strany povinny :

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

- ověřit, zda certifikát relevantního serveru, generujícího kvalifikovaná časová razítka nebyl v době vydání kvalifikovaného časového razítka odvolán – uvedeno na adrese http://www.ica.cz
- ověřit, zda kryptografická funkce pro tvorbu otisku (hash) v kvalifikovaném časovém razítku je stále bezpečná – uvedeno na adrese http://www.ica.cz
- ujistit se, zda délka kryptografického klíče a algoritmus jsou stále považovány za bezpečné - uvedeno na adrese http://www.ica.cz

7 Omezení záruky a odpovědnosti

Společnost První certifikační autorita, a.s. :

- Prohlašuje, že splní všechny povinnosti, které jí vyplývají jak z politik, podle kterých vydává kvalifikovaná časová razítka, tak z relevantních 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.
- Neodpovídá za :
    - **vady poskytovaných certifikačních služeb v oblasti kvalifikovaných časových razítek, které vzniknou jejich používáním v rozporu s příslušnýnou politikou, a dále za vady, které vznikly z důvodu vyšší moci, včetně dočasného výpadku telekomunikačního spojení atd.**
    - **škodu, vyplývající z použití kvalifikovaných časových razítek v období po zveřejnění zneplatněného kvalifikovaného systémového certifikátu serveru vydávajícího kvalifikovaná časová razítka 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 právních předpisů) upraven smlouvou.

Vztah mezi spoléhající se stranou a společností První certifikační autorita, a.s. je upraven příslušnými ustanoveními platné politiky. Vztah společnostI První certifikační autorita, a.s. a spoléhajících se stran není upraven smlouvou.

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

9 Ochrana osobních údajů

Ochrana osobních údajů a dalších neveřejných informací je v I.CA řešena v souladu s požadavky příslušné zákonné normy (zákony ČR č. 101/2000 Sb. a SR č. 428/2002 Z.z. v aktuálních zněních).

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

Reklamující osoba 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.

11 Právní prostředí

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

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 certifikátů a časových razítek také řídí :

- 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

- vyhláškou Národného bezpečnostního úradu Slovenské republiky č. 132/2009 Z.z., o podmienkach na poskytovanie akreditovaných certifikačných služieb a o požiadavkách na audit, rozsah auditu a kvalifikáciu audítorov
- 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