První certifikační autorita, a.s.

ZPRÁVA PRO UŽIVATELE

KVALIFIKOVANÁ ČASOVÁ RAZÍTKA

Verze 2.0

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

Tabulka 2 – 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

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 a použití

Vydávání kvalifikovaných časových razítek je I.CA komerčně nabízenou službou fyzické osobě, právnické osobě nebo organizační složce státu, která se smluvně zaváže jednat podle odpovídající politiky.

Pro žadatele, který podepisuje s I.CA smlouvu o poskytování kvalifikovaných časových razítek je požadován minimální věk 15 let. Osoby od 15 do 18 let musí mít svého zákonného zástupce.

V případě fyzické osoby může být osobou, podepisující smlouvu pouze ta, která je způsobilá k právním úkonům dle příslušné právní normy. Pokud osoba, podepisující smlouvu o poskytování kvalifikovaných certifikačních služeb nepožaduje služby přímo pro sebe, ale zastupuje jinou osobu, musí mít oprávnění tuto osobu zastupovat.

Při registraci nového žadatele o službu poskytování kvalifikovaných časových razítek je dle předložených dokladů ověřena jeho identita a případně jeho oprávnění k zastupování. Při registraci nového žadatele se vyžaduje :

a) předložení platného osobního dokladu žadatele

b) způsobilost žadatele k právním úkonům;

c) doklady, prokazující právo žadatele jednat za jinou fyzickou nebo právnickou osobu, organizační složku státu jako zástupce na základě plné moci s úředně ověřeným podpisem zastupovaného subjektu.

Postup ověřování identity fyzické osoby je detailně uveden v odpovídající politice (umístěná na adrese http://www.ica.cz) a v interní dokumentaci I.CA .

V případě, kdy žadatel vystupuje jako zástupce právnické osoby nebo organizační složky státu, vyžaduje I.CA při uzavírání smlouvy o vydání jednoho nebo více kvalifikovaných časových razítek :

- originál nebo notářsky ověřenou kopii výpisu z obchodního rejstříku, živnostenského listu nebo jiného dokumentu, na jejichž základě byla právnická osoba nebo organizační složka státu vytvořena a které musí obsahovat úplné obchodní jméno, identifikační číslo (IČO), statutární orgán a sídlo
- doklad opravňující žadatele jednat jménem této právnické osoby nebo organizační složky státu – viz odstavec c)
- žadatel se musí prokázat způsobem, uvedeným v následujícím odstavci

V případě, kdy žadatel vystupuje jako fyzická osoba, vyžaduje I.CA při uzavírání smlouvy o vydání jednoho nebo více kvalifikovaných časových razítek :

- celé občanské jméno žadatele;
- datum narození žadatele;
- číslo předloženého osobního dokladu;
- adresa trvalého bydliště žadatele.

Pokud dojde během trvání smluvního vztahu k I.CA ke změnám ve výše uvedených vyžadovaných osobních údajích, je klient povinen tyto změny ohlásit I.CA.

Vydávání kvalifikovaných časových razítek probíhá následujícím způsobem :

- S ohledem na komerční bázi a nadstandardní služby v procesu vydávání kvalifikovaných časových razítek vytvoří žadatel bezpečné autentizované spojení s TSA (s využitím komerčních certifikátů vydaných I.CA). V případě neúspěšného spojení je transakce ukončena a klient vhodným způsobem informován.
- Klientská aplikace vytvoří pro jakákoli elektronická data (zpráva, dokument, transakce, atd.) jejich otisk (hash), který je následně v uložen v žádosti na vytvoření kvalifikovaného časového razítka (v normovaném formátu dle RFC 3161). Takto vytvořená datová struktura je s využitím Internetu předána TSA.
- V rámci TSA je žádost předána archivačnímu serveru a následně zaslána jednomu ze serverů, generujícího kvalifikovaná časová razítka (TSS). Vzhledem ke skutečnosti, že je zasílán pouze otisk (hash), je obsah elektronických dat (zpráva, dokument, transakce, atd.) pro TSS naprosto neznámý (včetně identity klienta).
- TSS :
    - provede veškeré kontroly formální správnosti žádosti a následně vytvoří novou datovou strukturu v normovaném formátu dle RFC 3161, obsahující odpovídající chybový status
    - v případě kladného výsledku kontrol žádosti přidá k otisku (hash), obsaženém v žádosti, časový údaj, který je získán z měřidla důvěryhodného času (včetně informace o tomto měřidlu)
    - nově vytvořenou datovou strukturu elektronicky označí, resp. elektronicky podepíše (tím se TSS nezpochybnitelným způsobem zaručuje za správnost informací uvedených ve vygenerovaném kvalifikovaném časovém razítku)
- Výše uvedená datová struktura, obsahující časové razítko, certifikát TSS a certifikát synchronizačního zdroje (odpověď na žádost o kvalifikované časové razítko), je odeslána archivačnímu serveru TSA
- Poté, co jsou provedeny výše uvedené činnosti, odešle TSA odpověď klientovi

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 :

- ověřit, zda certifikát relevantního serveru, generujícího kvalifikovaná časová razítka nebyl v době vydání kvalifikovaného časového razítka odvolán – uvedeno na adrese http://www.ica.cz

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

- 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

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

- zákonem 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 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 Slovenské republiky č. 540/2002 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 od :

- 18.03.2002 **prvním akreditovaným** poskytovatelem certifikačních služeb v ČR pro oblast vydávání **kvalifikovaných certifikátů** 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.
- je od 01.02.2006 **akreditovaným** poskytovatelem certifikačních služeb v ČR pro oblast vydávání **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.,.
- je od 21.09.2006 **prvním zahraničním kvalifikovaným poskytovatelem certifikačních služeb v SR, kterému byla udělena akreditace v oblasti poskytování kvalifikovaných certifikátů a časových razítek** podle aktuálního znění zákona č. 215/2002 o elektronickom podpise a o zmene a doplnení niektorých zákonov v platnom znení a s ním spojených vykonávacích vyhlášok

S ohledem na výše uvedené skutečnosti je dle příslušných legislativ vykonáván dozor nad její činností akreditačními úřady, konkrétně Ministerstvem vnitra České republiky a Národním bezpečnostním úřadem Slovenské republiky.

Dále je poskytování kvalifikovaných certifikačních služeb společnosti První certifikační autorita, a.s., **pravidelně** podrobováno následujícím typům kontrol :

- každé čtyři let roky je prováděna celková kontrola bezpečnostní shody - během těchto čtyř let jsou prováděny roční částečné kontroly bezpečnostní shody¨

- každé dva roky je prováděn audit systému řízení bezpečnosti informací, jehož cílem je objektivní a na společnosti První certifikační autorita, a.s nezávislé ověření, že má zaveden a uplatňován systém řízení bezpečnosti informací.

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