První certifikační autorita, a.s.

Zpráva pro uživatele TSA

Verze 3.9

OBSAH

1 ÚVOD

Tento dokument - Zpráva pro uživatele TSA, vydaný společností První certifikační autorita, a.s. (dále též I.CA), podává základní přehled o poskytované službě vydávání kvalifikovaných elektronických časových razítek, včetně práv a povinnostech žadatelů o kvalifikovaná elektronická časová razítka (dále též časová razítka).

Tento dokument je pouze zjednodušeným výběrem informací uvedených v plném rozsahu v politice služby, v prováděcí směrnici a ve smlouvě o vydávání časových razítek. Slouží pro zjednodušení orientace uživatelů časových razítek.

1.1 Vývoj dokumentu

Tabulka 1 - Vývoj dokumentu

Verze	Datum vydání	Poznámka
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.
3.7	21.12.2015	• Provedení auditu stavu bezpečnosti poskytovaných certifikačních služeb dle požadavků platné legislativy Slovenské republiky. • Provedení auditu ISMS dle požadavků platné legislativy České republiky na poskytovatele kvalifikovaných certifikačních služeb. • Provedení kontroly bezpečnostní shody.
3.8	18.04.2017	Aktualizace údajů o kontrolách a auditech. Aktualizace vyplývající z legislativy pro služby vytvářející důvěru.
3.9	16.11.2017	Aktualizace typů certifikačních autorit a údajů o provedených auditech.

1.2 Audity a kontroly I.CA

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 30th, 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 30th, 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

Audit systému řízení bezpečnosti informací společnosti První certifikační autorita, a.s. (akreditovaný poskytovatel kvalifikovaných certifikačních služeb) – Závěrečná zpráva ze dne 14.5.2015	VYHOVUJE
Audit stavu bezpečnosti certifikačnej autority společnosti První certifikační autorita, a.s. – Záverečná správa, máj 2015 (ze dne 20.5.2015)	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 2015	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 102 042 (policies DVCP, OVCP, NCP) - Audit Statement Report, August 2015	VYHOVUJE
Kontrola bezpečnostní shody (celková) - zpráva ze dne 27.8.2015	VYHOVUJE
Celková kontrola bezpečnostní shody – 2015, ze dne 27.8.2015	VYHOVUJE
AUDIT STATEMENT REPORT- Root CA/RSA: ETSI TS 101 456 V1.4.3 (2007-05): "Electronic Signatures and Infrastructures (ESI); Policy requirements for certification authorities issuing qualified certificates", policies QCP public + SSCD, QCP public and ETSI TS 102 042V2.4.1 (2013-02): "Electronic Signatures and Infrastructures (ESI); Policy requirements for certification authorities issuing public key certificates", policies NCP, NCP+, DVCP, OVCP Audit Statement Report, ze dne 18.5. 2016.	VYHOVUJE
Kontrola bezpečnostní shody (částečná) - zpráva ze dne 27.8.2016	VYHOVUJE
Audit požadovaný Microsoft Trusted Root Certificate Program - AUDIT STATEMENT REPORT – I.CA Root CA/RSA, 18.5.2017 **ETSI EN 319 411-2 V2.1.1 (2016-02)** Electronic Signatures and Infrastructures (ESI); Policy and security requirements for Trust Service Providers issuing certificates; Part 2: Requirements for trust service providers issuing EU qualified certificates, policies:	VYHOVUJE

a) QCP-n Policy for EU qualified certificate issued to a natural person b) QCP-n-qscd Policy for EU qualified certificate issued to a natural person where the private key and the related certificate reside on a QSCD c) QCP-l Policy for EU qualified certificate issued to a legal person d) QCP-l-qscd Policy for EU qualified certificate issued to a legal person where the private key and the related certificate reside on a QSCD **ETSI EN 319 411-1 V1.1.1 (2016-02)** Electronic Signatures and Infrastructures (ESI); Policy and security requirements for Trust Service Providers issuing certificates; Part 1: General requirements, policies: a) NCP: Normalized Certificate Policy b) NCP+: Normalized Certificate Policy requiring a secure cryptographic device c) DVCP: Domain Validation Certificate Policy d) OVCP: Organizational Validation Certificate Policy	
Audit požadovaný eIDAS/ČR pro služby: a) Vydávání kvalifikovaných elektronických časových razítek, 26.05.2017	SHODA
Audit požadovaný eIDAS/SR pro služby: a) Kvalifikovaná dôveryhodná služba vyhotovovania kvalifikovaných elektronických časových pečiatok, 13.06.2017	SHODA

2 KONTAKTNÍ INFORMACE

2.1 Sídlo společnosti

Adresa sídla společnosti je:

První certifikační autorita, a.s.

Podvinný mlýn 2178/6

190 00 Praha 9

Česká republika.

Telefonické a mailové spojení do sídla společnosti je:

tel.: +420 284 081 940

fax.: +420 284 081 965

e-mail: info@ica.cz

2.2 Zveřejňování informací

Veškeré veřejné informace lze nalézt na internetové adrese: http://www.ica.cz.

2.3 Komunikace s veřejností

Komunikace s veřejností je možná těmito způsoby:

- obecný kontakt: info@ica.cz,
- pracoviště registračních autorit: http://www.ica.cz,
- technická podpora:
  - tel.: +420 284 081 930 – 33,
  - e-mail: support@ica.cz,
- reklamace: reklamace@ica.cz,
- obchodní oddělení: sales@ica.cz,
- informace o TSA: tsa@ica.cz.

3 VYDÁVÁNÍ ČASOVÝCH RAZÍTEK

3.1 Typy vydávaných časových razítek

I.CA vydává časová razítka dle platné legislativy pro služby vytvářející důvěru.

Při vydávání časových razítek se I.CA řídí vlastní politikou s OID= 1.3.6.1.4.1.23624.10.1.50.x.y (x.y označuje verzi.podverzi politiky), která zahrnuje všechny požadavky politiky BTSP (Best practices Time-Stamp Policy) specifikované v ETSI EN 319421 verze 1.1.1.

Předpokládaná doba životnosti časového razítka je dána dobou platnosti certifikátu serveru vydávajících časová razítka (TSU), která je stanovena s ohledem na použité kryptografické algoritmy v souladu s doporučeními ETSI TS 119312 platnými v době vydání časového razítka. Vzhledem k možnému pokroku v kryptoanalýze v průběhu předpokládané životnosti časového razítka však nelze dobu životnosti zaručit.

3.2 Ověřovací procedury

Vydávání časových razítek je v 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 autentizován výběrem jedné 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.

3.3 Žádost o časové razítko

Po úspěšně provedené identifikaci a autentizaci, vytvoří žadatel v souladu s příslušnou politikou žádost o časové razítko (v souladu s RFC 3161). 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.

3.4 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) vkládaný do časového razítka, jehož maximální odchylka při vytváření časového razítka je 1 sekunda od UTC (uvedeno v položce accuracy časového razítka), je synchronizován se zdrojem důvěryhodného času.

Odpověď je elektronicky označena, resp. opatřena elektronickou pečetí vytvořenou soukromým klíčem časového serveru, který časové razítko vydal.

Každá odpověď na žádost o časové razítko je předána žadateli o časové razítko a taktéž umístěna v příslušném úložišti systému TSA.

Certifikáty serverů vydávajících časová razítka lze získat na stránkách společnosti První certifikační autorita, a.s., nebo Ministerstva vnitra České republiky, případně v příslušném TSL (Trust Service List).

3.5 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 zprávu. V případě časového razítka obsaženého v bezchybné odpovědi je žadatel povinen ověřit zejména:

- zda vrácený otisk (hash) je totožný s odeslaným v žádosti,
- platnost elektronické značky/pečetě časového razítka,
- platnost celé certifikační cesty certifikátu TSU včetně kontroly odvolání,
- 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[1] vydaného v souladu s politikou vydávání časových razítek. Obecně platí, že časové razítko je datová zpráva, 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 ŽADATELŮ O ČASOVÉ RAZÍTKO

Klienti (žadatelé) jsou povinni žádat o časová razítka v souladu s odpovídající politikou. Povinnosti při ověření platnosti vráceného časového razítka jsou uvedeny v kapitole 3.5.

6 POVINNOSTI SPOLÉHAJÍCÍCH SE STRAN

Spoléhající se strana je povinna zejména:

- získat z bezpečného zdroje relevantní certifikáty, vztahující se k časovému razítku a ověřit kontrolní součet těchto certifikátů,
- ověřit platnost elektronické značky/pečetě časového razítka a následně všech certifikátů, vztahujících se k časovému serveru, který tuto elektronickou značku/pečeť vytvořil,
- ověřit obsah vydaného časového razítka - konkrétně se jedná o hash ověřovaných dat a zda politika, pod kterou bylo časové razítko vydáno, je akceptovatelná její potřebám, popř. potřebám provozovaných aplikací.

7 OMEZENÍ ZÁRUKY A ODPOVĚDNOSTI

Společnost První certifikační autorita, a.s.:

- Prohlašuje, že splní všechny povinnosti, které jí vyplývají z politik a legislativních předpisů.
- Poskytuje výše uvedené záruky po celou dobu platnosti smlouvy o poskytování 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 služeb, které vzniknou jejich používáním v rozporu s příslušnou politikou služby, a dále za vady, které vznikly z důvodu vyšší moci včetně dočasného výpadku telekomunikačního spojení atd.

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

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 příslušné politiky služby.

Vztah mezi spoléhající se stranou a společností První certifikační autorita, a.s., je upraven příslušnými ustanoveními příslušné politiky služby.

Veškeré zveřejňované informace je možné získat na kontaktní adrese, uvedené v kapitole 2.2 tohoto dokumentu, případně na dalších adresách uvedených v kap. 2.3.

Doplňující detailnější informace ohledně vydávání časových razítek je též možné zjistit z příslušné prováděcí směrnice služby (její veřejné části).

9 OCHRANA OSOBNÍCH ÚDAJŮ

Ochrana osobních údajů je ve společnosti První certifikační autorita, a.s., řešena v souladu s požadavky aktuální legislativy týkající se ochrany osobních údajů, tj. zákona č. 101/2000 Sb., o ochraně osobních údajů a o změně některých zákonů do 25.5.2018, resp. nařízení Evropského parlamentu a Rady (EU) 2016/679 o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a o volném pohybu těchto údajů a o zrušení směrnice 95/46/ES (obecné nařízení o ochraně osobních údajů) od 25.5.2018.

10 POLITIKA NÁHRAD A REKLAMACE

Reklamaci je možné podat těmito způsoby:

- e-mailem na adresu reklamace@ica.cz,
- doporučenou poštovní zásilkou na adresu sídla společnosti I.CA,
- zasláním zprávy do datové schránky společnosti I.CA,
- osobně v sídle společnosti I.CA.

Reklamující osoba (držitel časového razítka nebo spoléhající se strana) je povinna uvést:

- co nejvýstižnější popis závady,
- sériové číslo reklamovaného produktu,
- požadovaný způsob vyřízení reklamace.

O reklamaci rozhodne I.CA nejpozději do tří pracovních dnů od doručení reklamace. Vyrozumí o tom reklamujícího (formou elektronické pošty, zprávy do datové schránky nebo doporučenou zásilkou), pokud se strany nedohodnou na jiném způsobu.

Reklamace, včetně vady, bude vyřízena bez zbytečných odkladů, a to nejpozději do třiceti dnů ode dne uplatnění reklamace, pokud se strany nedohodnou jinak.

11 PRÁVNÍ PROSTŘEDÍ

Společnost První certifikační autorita, a.s. se při své činnosti řídí zákonnými požadavky, zejména:

- nařízením Evropského parlamentu a Rady (EU) č. 910/2014 o elektronické identifikaci a službách vytvářejících důvěru pro elektronické transakce na vnitřním trhu a o zrušení směrnice 1999/93/ES (eIDAS),
- zákonem České republiky č. 297/2016 Sb., o službách vytvářejících důvěru pro elektronické transakce.
- zákonem Slovenské republiky č. 272/2016 Z.z. o dôveryhodných službách pre elektronické transakcie na vnútornom trhu a o zmene a doplnení niektorých zákonov (zákon o dôveryhodných službách),
- zákonem České republiky č. 90/2012 Sb., o obchodních korporacích,
- zákonem České republiky č. 101/2000 Sb., o ochraně osobních údajů a o změně některých zákonů - do 25.5.2018,
- nařízením Evropského parlamentu a Rady (EU) 2016/679 o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a o volném pohybu těchto údajů a o zrušení směrnice 95/46/ES (obecné nařízení o ochraně osobních údajů) - po 25.5.2018.

12 KVALIFIKACE, AUDITY A KONTROLY

Společnost První certifikační autorita, a.s., je kvalifikovaným poskytovatelem služeb vytvářejících důvěru. Poskytování těchto služeb je pravidelně podrobováno auditům a kontrolám v souladu se zákonnými požadavky vyjmenovanými v kapitole 11.

Společnost První certifikační autorita, a.s., je členem programu Microsoft Trusted Root Certificate Program (zařazení kořenového certifikátu I.CA do důvěryhodných kořenových certifikačních autorit společnosti Microsoft), proto jsou poskytované služby podrobovány také pravidelným auditům vyžadovaným touto společností.

Za společnost První certifikační autorita, a.s.

Ing. Petr Budiš Ph.D., MBA, v.r.