První certifikační autorita, a.s.

Zpráva pro uživatele TSA

Verze 4.6

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 právní úpravy České republiky na poskytovatele kvalifikovaných certifikačních služeb. • Provedení auditu stavu bezpečnosti poskytovaných certifikačních služeb dle požadavků platné právní úpravy Slovenské republiky.
3.0	01.03.2010	Vydávání certifikátů s parametry, splňujícími požadavky platné právní úpravy 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	14.05.2012	Provedení auditu stavu bezpečnosti poskytovaných certifikačních služeb dle požadavků platné právní úpravy Slovenské republiky.
3.3	10.09.2012	Doplnění provedení celkové kontroly bezpečnostní shody.
3.4	11.06.2013	• Provedení auditu ISMS dle požadavků platné právní úpravy České republiky na poskytovatele kvalifikovaných certifikačních služeb. • Provedení auditu stavu bezpečnosti poskytovaných certifikačních služeb dle požadavků platné právní úpravy Slovenské republiky.
3.5	10.09.2013	Doplnění kontroly bezpečnostní shody, aktualizace dokumentu.
3.6	19.11.2014	• Provedení auditu stavu bezpečnosti poskytovaných certifikačních služeb dle požadavků platné právní úpravy 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 právní úpravy Slovenské republiky. • Provedení auditu ISMS dle požadavků platné právní úpravy 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 právní úpravy pro služby vytvářející důvěru.
3.9	16.11.2017	Aktualizace typů certifikačních autorit a údajů o provedených auditech.
4.0	08.08.2018	Aktualizace údajů o provedených auditech.
4.1	27.06.2019	Aktualizace údajů o provedených auditech.
4.2	14.07.2020	Revize textu, aktualizace údajů o provedených auditech.
4.3	17.06.2021	Aktualizace údajů o provedených auditech.
4.4	02.12.2022	Seznam auditů a kontrol redukován jen na poslední provedené.
4.5	28.11.2023	Aktualizace údajů o provedených auditech.
4.6	30.07.2024	Aktualizace údajů o provedených auditech.

1.2 Audity a kontroly I.CA

Tabulka 2 – Provedené audity a jiné kontroly

Typ	Výrok kontrolora/auditora
Audit required by Microsoft Trusted Root Program - AUDIT STATEMENT REPORT – I.CA Root CA/RSA: **ETSI EN 319 411-2 V2.5.1 (2023-10)** 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: a) QCP-n Policy for EU qualified certificate issued to a natural person (for electronic signatures) 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 (for qualified electronic signatures) c) QCP-l Policy for EU qualified certificate issued to a legal person (for electronic seals)	COMPLIANCE

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 (for qualified electronic seals) e) QEVCP-w: Policy for EU qualified certificates for website authentication **ETSI EN 319 411-1 V1.4.1 (2023-10)** 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 for TLS/SSL certificates d) OVCP: Organizational Validation Certificate Policy for TLS/SSL certificates e) EVCP: Extended Validation Certificate Policy Auditní závěrečná zpráva z 21.05.2024 Platnost certifikátu: 19.05.2024 - 18.05.2025	
Audit required by Microsoft Trusted Root Program - AUDIT STATEMENT REPORT – I.CA Root CA/RSA 05/2022: **ETSI EN 319 411-2 V2.5.1 (2023-10)** 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: a) QCP-n Policy for EU qualified certificate issued to a natural person (for electronic signatures) 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 (for qualified electronic signatures) c) QCP-l Policy for EU qualified certificate issued to a legal person (for electronic seals) 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 (for qualified electronic seals) **ETSI EN 319 411-1 V1.4.1 (2023-10)** 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 Auditní závěrečná zpráva z 21.05.2024	COMPLIANCE

Platnost certifikátu: 19.05.2024 - 18.05.2025	
Audit požadovaný eIDAS: a) Vydávání kvalifikovaných elektronických časových razítek Auditní závěrečná zpráva z 13.06.2024 Platnost certifikátu: 26.05.2023 - 25.05.2025	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.

Spojení do sídla společnosti je:

tel.:	+420 284 081 940
fax.:	+420 284 081 965
e-mail:	info@ica.cz
ID datové schránky:	a69fvfb

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 právní úpravy 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 319 421 Electronic Signatures and Infrastructures (ESI); Policy and Security Requirements for Trust Service Providers issuing Time-Stamps.

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 119 312 Electronic Signatures and Infrastructures (ESI); Cryptographic Suites 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 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 menší než 1 sekunda, obvykle do 500 ms od UTC (uvedeno v položce accuracy časového razítka), je synchronizován se zdrojem důvěryhodného času.

Časové razítko je opatřeno zaručenou 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 Digitální a informační agentury, 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, resp. zaručené elektronické pečetě časového razítka,
- platnost celé certifikační cesty certifikátu příslušného časového serveru včetně kontroly odvolání,
- v případě, že žádost obsahovala položku „nonce“ a/nebo „reqPolicy“ ověřit, že její hodnota v odpovědi je totožná.

4 OMEZENÍ POUŽITELNOSTI

Nejsou definována žádná omezení použitelnosti časového razítka vydaného v souladu s politikou vydávání časových razítek uvedenou v kapitole 3.1. 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 zaručené elektronické pečetě časového razítka a následně všech certifikátů, vztahujících se k časovému serveru, který tuto zaručenou elektronickou 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 právních předpisů.
- Poskytuje záruky uvedené v politice vydávání časových razítek dle kapitoly 3.1 po celou dobu platnosti smlouvy o poskytování služby, 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 právních předpisů 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.

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 kapitole 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 právní úpravy týkající se ochrany osobních údajů, tj. zákona České republiky č. 110/2019 Sb., o zpracování osobních údajů a o změně některých zákonů, 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).

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 právními 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) v platném znění,
- 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 společnostech a družstvech (zákon o obchodních korporacích),
- zákonem České republiky č. 110/2019 Sb., o zpracování osobních údajů a o změně některých zákonů,
- 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).

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 s právními požadavky vyjmenovanými v kapitole 11.

Společnost První certifikační autorita, a.s., je členem programu Microsoft Trusted Root 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.