První certifikační autorita, s.r.o.

Zpráva pro uživatele

Verze 1.3

OBSAH

1 Úvod 3
1.1 Vývoj dokumentu 3
1.2 Audity a kontroly I.CA, resp. I.CA SK 3
2 Kontaktní informace 4
2.1 Sídlo společnosti 4
2.2 Zveřejňování informací 4
2.3 Komunikace s veřejností 5
3 Typy certifikátů, ověřovací procedury a použití 5
3.1 Soulad se standardy 5
3.2 Typy certifikátů 6
3.2.1 Kořenová certifikační autorita I.CA Root CA/RSA 05/2022 6
3.2.2 Podřízené certifikační autority 6
3.3 Ověřovací procedury 6
4 Užití certifikátů 7
5 Povinnosti žadatelů nebo držitelů certifikátu 7
6 Povinnosti spoléhajících se stran 7
7 Omezení záruky a odpovědnosti 8
8 Smlouvy a certifikační politika 8
9 Ochrana osobních údajů 9
10 Politika náhrad a reklamace 9
11 Právní prostředí 9
12 Kvalifikace, audity a kontroly 10

1 ÚVOD

Tento dokument poskytuje základní přehled o dvouúrovňové topologii certifikačních autorit, provozovaných společností První certifikační autorita, a.s., (I.CA), v rámci které jsou provozovány také certifikační autority společnosti První certifikační autorita, s.r.o., (I.CA SK) a dále o povinnostech a právech držitelů certifikátů a spoléhajících se stran.

1.1 Vývoj dokumentu

Tabulka 1 - Vývoj dokumentu

Verze	Datum vydání	Poznámka
1.0	28.03.2023	První vydání.
1.1	23.11.2023	Aktualizace údajů o provedených auditech.
1.2	23.04.2024	Aktualizace údajů o provedených auditech.
1.3	28.08.2024	Zohlednění požadavků ETSI TS 119 411-6.

1.2 Audity a kontroly I.CA, resp. I.CA SK

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 05/2022: **ETSI EN 319 411-2 V2.4.1 (2021-11)** 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 V1.3.1 (2021-05)** 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	COMPLIANCE

b) NCP+: Normalized Certificate Policy requiring a secure cryptographic device Auditní závěrečná zpráva z 21.05.2024 Platnost certifikátu: 19.05.2024 - 18.05.2025	
Audit (plný) požadovaný eIDAS/SR pro služby: a) Kvalifikovaná dôveryhodná služba vyhotovovania a overovania kvalifikovaných certifikátov pre elektronický podpis b) Kvalifikovaná dôveryhodná služba vyhotovovania a overovania kvalifikovaných certifikátov pre elektronickú pečať Auditní závěrečná zpráva z 09.12.2022 Platnost certifikátu: 09.12.2022 – 08.12.2024	SHODA
Audit (dohledový) požadovaný eIDAS/SR pro služby: a) Kvalifikovaná dôveryhodná služba vyhotovovania a overovania kvalifikovaných certifikátov pre elektronický podpis b) Kvalifikovaná dôveryhodná služba vyhotovovania a overovania kvalifikovaných certifikátov pre elektronickú pečať Auditní závěrečná zpráva z 12.12.2023	SHODA

2 KONTAKTNÍ INFORMACE

2.1 Sídlo společnosti

Adresa sídla společnosti je:

První certifikační autorita, s.r.o.

Galvaniho 19045/19

821 04 Bratislava – mestská časť Ružinov

Slovenská republika

Spojení 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.

3 TYPY CERTIFIKÁTŮ, OVĚŘOVACÍ PROCEDURY A POUŽITÍ

3.1 Soulad se standardy

Společnost I.CA SK vydává certifikáty (určené fyzickým a právnickým osobám), jejichž profil vyhovuje standardu X.509 verze 3 v souladu s normami a standardy:

- STN ETSI EN 319 411-1 Elektronické podpisy a infraštruktúry (ESI). Požiadavky politiky a bezpečnosti na poskytovateľov dôveryhodných služieb vydávajúcich certifikáty. Časť 1: Obecné požiadavky.
- ETSI EN 319 411-1 Electronic Signatures and Infrastructures (ESI); Policy and security requirements for Trust Service Providers issuing certificates; Part 1: General requirements.
- STN ETSI EN 319 411-2 Elektronické podpisy a infraštruktúry (ESI). Požiadavky politiky a bezpečnosti na poskytovateľov dôveryhodných služieb vydávajúcich certifikáty. Časť 2: Požiadavky na poskytovateľov dôveryhodných služieb vydávajúcich kvalifikované certifikáty.
- ETSI EN 319 411-2 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.
- ETSI TS 119 411-6 Electronic Signatures and Infrastructures (ESI); Policy and security requirements for Trust Service Providers issuing certificates; Part 6: Requirements for Trust Service Providers issuing publicly trusted S/MIME certificates.
- CA/Browser Forum – Baseline Requirements for the Issuance and Management of Publicly-Trusted S/MIME Certificates.

3.2 Typy certifikátů

3.2.1 Kořenová certifikační autorita I.CA Root CA/RSA 05/2022

Kořenová certifikační autorita **I.CA Root CA/RSA 05/2022** (klíč RSA 4096 bitů, algoritmus podpisu sha512WithRSAEncryption) společnosti I.CA vydává v souladu s požadavky technických standardů a platné právní úpravy certifikáty výhradně podřízeným certifikačním autoritám (klíč RSA 4096 bitů, algoritmus podpisu sha256WithRSAEncryption) a svému OCSP respondéru (s klíčem RSA 2048 bitů, algoritmus podpisu sha256WithRSAEncryption). Tyto podřízené certifikační autority (viz kapitola 3.2.2) vydávají certifikáty koncovým uživatelům a svým OCSP respondérům.

3.2.2 Podřízené certifikační autority

Certifikační autorita **I.CA EU Qualified CA-SK/RSA 10/2022** (klíč RSA 4096 bitů, algoritmus podpisu sha256WithRSAEncryption) společnosti I.CA SK je určena k vydávání kvalifikovaných certifikátů pro elektronický podpis a elektronickou pečeť a svému OCSP respondéru (s klíči RSA minimálně 2048 bitů, algoritmus podpisu minimálně sha256WithRSAEncryption).

3.3 Ověřovací procedury

Při vydávání prvotního certifikátu je vždy prováděn tzv. registrační proces, tedy:

- je ověřována totožnost fyzické osoby, tj. žadatele nebo jeho zmocněnce, resp. zástupce žadatele, na základě osobních dokladů,
- v případě certifikátu pro organizaci je ověřována i vazba žadatele o certifikát na tuto organizaci,
- ověření e-mailové adresy je prováděno dvěma způsoby, a to kontrolou příslušnosti adresy k registrované DNS doméně (validating authority over mailbox via domain) nebo ověřením držitele e-mailové adresy pomocí obsahu zasílaného e-mailu (validating control over mailbox via email), kdy užití příslušné ověřovací metody odvisí od typu smluvního vztahu s klientem.

V případě vydávání S/MIME certifikátů jsou v souladu s dokumentem Baseline Requirements for the Issuance and Management of Publicly-Trusted S/MIME Certificates vydávány certifikáty typu „Individual-validated“ a „Organization-validated“. V současné době nejsou OID těchto politik v certifikátech uváděny.

Ověřování totožnosti žadatele nebo jeho zmocněnce v případě certifikátu pro fyzickou osobu může probíhat buď prezenčně, tedy za osobní přítomnosti žadatele, nebo jeho zmocněnce, na RA, nebo distančně s využitím certifikované služby ZealiD TRA Service – to není možné v případě zmocněnce.

Pokud příslušná certifikační politika umožňuje vydání tzv. následného certifikátu (jedná se o certifikát, který bude v souladu se smlouvou o poskytování příslušné služby, uzavřenou mezi žadatelem a I.CA SK, vydán žadateli na základě nové žádosti o certifikát v období platnosti certifikátu, ke kterému je tento následný certifikát vydáván), není fyzická přítomnost žadatele o certifikát na pracovišti registrační autority vyžadována. Podrobný popis registračních postupů je uveden v příslušných certifikačních politikách.

4 UŽITÍ CERTIFIKÁTŮ

Kvalifikované certifikáty lze použít k ověřování elektronických podpisů a elektronických pečetí v souladu s nařízením Evropského parlamentu a Rady č. 910/2014 o elektronické identifikaci a službách vytvářejících důvěru pro elektronické transakce na vnitřním trhu a o zrušení směrnice 1999/93/ES v platném znění.

Při využívání certifikátů je vždy nutno postupovat v souladu s příslušnou certifikační politikou.

Nestanoví-li relevantní právní předpis jinak, jsou auditní záznamy a záznamy vzniklé v průběhu registračního procesu uchovávány po dobu nejméně 10 let od jejich vzniku.

Společnost I.CA SK uchovává vydané certifikáty a seznamy zneplatněných certifikátů po celou dobu své existence.

5 POVINNOSTI ŽADATELŮ NEBO DRŽITELŮ CERTIFIKÁTU

Držitelem certifikátu je žadatel o certifikát, kterému byl tento certifikát vydán. Z pohledu společnosti I.CA SK se jedná o osobu (fyzickou, nebo organizaci), která uzavřela se společností I.CA SK smlouvu o vydání certifikátu. Mezi základní povinnosti žadatele o certifikát a následně držitele tohoto certifikátu patří zejména:

- poskytovat pravdivé a úplné informace při registraci žádosti o vydání certifikátu,
- neprodleně uvědomit poskytovatele služeb o změně údajů, uvedených ve vydaném certifikátu, popř. ve smlouvě,
- seznámit se s certifikační politikou, podle které bude certifikát vydán,
- překontrolovat, zda údaje uvedené v žádosti o certifikát a certifikátu jsou správné a odpovídají požadovaným údajům,
- nakládat s prostředkem a se soukromým klíčem, který odpovídá veřejnému klíči ve vydaném certifikátu takovým způsobem, aby nemohlo dojít k jeho neoprávněnému použití,
- užívat soukromý klíč a odpovídající certifikát vydaný podle příslušné certifikační politiky pouze pro účely stanovené touto certifikační politikou,
- neprodleně požádat o zneplatnění certifikátu a ukončit používání příslušného soukromého klíče zejména v případech kompromitace soukromého klíče, případně podezření, že soukromý klíč byl zneužit.

6 POVINNOSTI SPOLÉHAJÍCÍCH SE STRAN

Spoléhající se stranou jsou subjekty spoléhající se při své činnosti na certifikát vydaný společností I.CA SK. Mezi základní povinnosti těchto subjektů patří zejména:

- získat z bezpečného zdroje relevantní certifikáty certifikačních autorit uvedených v kapitole 3.2 a ověřit kontrolní součet těchto certifikátů,
- před použitím certifikátu koncového uživatele ověřit platnost certifikátů certifikačních autorit souvisejících s certifikátem tohoto koncového uživatele,

- ujistit se, zda certifikát koncového uživatele je vhodný pro předpokládané využití,
- dodržovat veškerá relevantní ustanovení certifikační politiky, dle které byl certifikát koncového uživatele vydán,
- při ověřování platnosti kvalifikovaných EU certifikátů (kvalifikované certifikáty pro elektronické podpisy a kvalifikované certifikáty pro elektronické pečetě vydané v souladu s eIDAS) je důvěryhodnou kotvou certifikát vydavatele uvedený v důvěryhodném seznamu SR (tj. certifikát vydávající certifikační autority).

7 OMEZENÍ ZÁRUKY A ODPOVĚDNOSTI

Společnost I.CA SK:

- se zavazuje, že splní veškeré povinnosti definované jak příslušnými právními předpisy, tak příslušnými certifikačními politikami,
- poskytuje záruky uvedené v příslušné certifikační politice po celou dobu platnosti smlouvy o poskytování služeb, resp. služeb vytvářejících důvěru; pokud bylo zjištěno porušení povinností držitele certifikátu nebo spoléhající se strany, mající souvislost s uváděnou škodou, záruční plnění se neposkytne – tato skutečnost musí být držiteli certifikátu nebo spoléhající se straně oznámena a zaprotokolována,
- souhlasí s tím, že dodavatelé aplikačního programového vybavení, kteří mají platnou smlouvu na distribuci kořenového certifikátu, nepřebírají žádné závazky nebo potenciální odpovědnost s výjimkou případů, kde poškození či ztráta byly přímo způsobeny programovým vybavením tohoto dodavatele,
- jiné záruky než uvedené v příslušné certifikační politice, neposkytuje,
- další možné náhrady škody vycházejí z ustanovení příslušných právních předpisů a o jejich výši může rozhodnout soud.

Společnost I.CA SK neodpovídá:

- za vady poskytnutých služeb vzniklé z důvodu nesprávného nebo neoprávněného využívání služeb, zejména za provozování v rozporu s podmínkami uvedenými v certifikační politice, jakož i za vady vzniklé z důvodu vyšší moci, včetně dočasného výpadku telekomunikačního spojení aj.,
- za škodu vyplývající z použití certifikátu v období po podání žádosti o jeho zneplatnění, pokud společnost I.CA SK dodrží definovanou lhůtu pro zveřejnění zneplatněného certifikátu na seznamu zneplatněných certifikátů (CRL).

8 SMLOUVY A CERTIFIKAČNÍ POLITIKA

Vztah mezi držitelem certifikátu a poskytovatelem služeb, resp. služeb vytvářejících důvěru – společností I.CA SK je (kromě příslušných ustanovení příslušných právních předpisů) upraven smlouvou a příslušnými ustanoveními platných certifikačních politik.

Vztah mezi spoléhající se stranou a poskytovatelem služeb, resp. služeb vytvářejících důvěru – společností I.CA SK je upraven příslušnými ustanoveními platných certifikačních politik. Vztah společnosti I.CA SK a spoléhajících se stran smlouvou upraven není.

Veškeré veřejné informace je možné získat na kontaktních adresách uvedených v kapitole 2 tohoto dokumentu.

9 OCHRANA OSOBNÍCH ÚDAJŮ

Ochrana osobních údajů je ve společnosti I.CA SK řešena v souladu s požadavky aktuální právní úpravy týkající se ochrany osobních údajů, tj. zákona Slovenské republiky č. 18/2018 Z.z. o ochrane osobných údajov a o zmene a doplnení niektorých zákonov, 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 SK,
- osobně v sídle společnosti I.CA SK.

Reklamující osoba (držitel certifikátu) je povinna uvést:

- co nejvýstižnější popis závad a jejich projevů,
- sériové číslo reklamovaného produktu,
- požadovaný způsob vyřízení reklamace.

O reklamaci rozhodne I.CA SK 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 30 dnů ode dne uplatnění reklamace, pokud se strany nedohodnou jinak.

Nový certifikát bude držiteli poskytnut zdarma v následujících případech:

- existuje-li důvodné podezření, že došlo ke kompromitaci soukromého klíče certifikační autority,
- na základě rozhodnutí členů vedení I.CA, resp. jednatele společnosti I.CA SK s přihlédnutím ke konkrétním okolnostem,
- v případě, že příslušná certifikační autorita při příjmu žádosti o vydání certifikátu zjistí, že existuje jiný certifikát s duplicitním veřejným klíčem.

11 PRÁVNÍ PROSTŘEDÍ

Společnost I.CA SK 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 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),
- 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).
- zákonem Slovenské republiky č.18/2018 Z.z. o ochrane osobných údajov a o zmene a doplnení niektorých zákonov.

12 KVALIFIKACE, AUDITY A KONTROLY

Společnost I.CA SK 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 I.CA 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 vyžadovaných touto společností.

Za společnost První certifikační autorita, s.r.o.

Ing. Ctirad Fischer v.r.