První certifikační autorita, a.s.

Zpráva pro uživatele CA

Verze 1.14

OBSAH

1 ÚVOD

Tento dokument poskytuje základní přehled o dvouúrovňové topologii certifikačních autorit, provozovaných společností První certifikační autorita, a.s., (I.CA), povinnostech a právech držitelů certifikátů a spoléhajících se stran.

1.1 Vývoj dokumentu

Tabulka 1 - Vývoj dokumentu

Verze	Datum vydání	Poznámka
1.0	02.09.2015	První vydání.
1.1	07.04.2016	Rozšíření o další vydávající CA.
1.2	18.04.2017	Aktualizace údajů o kontrolách a auditech. Aktualizace vyplývající z právní pro služby vytvářející důvěru.
1.3	16.11.2017	Aktualizace typů certifikačních autorit a údajů o provedených auditech.
1.4	08.08.2018	Aktualizace údajů o provedených auditech.
1.5	27.06.2019	Aktualizace údajů o provedených auditech.
1.6	27.01.2020	Podpora kryptografie eliptických křivek (ECC, kryptografie EC). Aktualizace údajů o provedených auditech.
1.7	14.07.2020	Revize textu, aktualizace údajů o provedených auditech.
1.8	17.06.2021	Aktualizace údajů o provedených auditech.
1.9	12.05.2022	Doplněna nová vydávající certifikační autorita. Seznam auditů a kontrol redukován jen na poslední provedené. Do kapitoly 6 doplněno upozornění pro spoléhající se strany, jakou důvěryhodnou kotvu použít při ověření platnosti certifikátu.
1.10	29.11.2022	Aktualizace údajů o provedených auditech.
1.11	9.10.2023	Aktualizace údajů o provedených auditech.
1.12	30.07.2024	Aktualizace údajů o provedených auditech.
1.13	28.08.2024	Zohlednění požadavků ETSI TS 119 411-6.
1.14	18.11.2024	Aktualizace údajů o provedených auditech.

1.2 Audity a kontroly I.CA

Tabulka 2 – Provedené kontroly bezpečnostní shody, audity, jiné kontroly

Typ	Výrok kontrolora/auditora
Audit required by Microsoft Trusted Root Program - AUDIT STATEMENT REPORT – I.CA Root CA/RSA:	COMPLIANCE

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, policies: 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 e) QEVCP-w: Policy for EU qualified website certificate issued to a legal person and linking the website to that person based on the EVCG **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 d) OVCP: Organizational Validation Certificate Policy 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, policies: 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	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 **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 Platnost certifikátu: 19.05.2024 - 18.05.2025	
Audit required by Microsoft Trusted Root Program - AUDIT STATEMENT REPORT – I.CA Root CA/ECC 12/2016: **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, policies: 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 V1.4.1 (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 Platnost certifikátu: 19.05.2024 - 18.05.2025	COMPLIANCE
Audit required by Microsoft Trusted Root Program - AUDIT STATEMENT REPORT – I.CA Root CA/ECC 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, policies: 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 V1.4.1 (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 Platnost certifikátu: 19.05.2024 - 18.05.2025	
Audit required by Microsoft Trusted Root Program - AUDIT STATEMENT REPORT – I.CA TLS 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, policies: 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 e) QEVCP-w: Policy for EU qualified website certificate issued to a legal person and linking the website to that person based on the EVCG **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 d) OVCP: Organizational Validation Certificate e) EVCP: Extended Validation Certificate Policy Auditní závěrečná zpráva z 21.05.2024 Platnost certifikátu: 19.05.2024 - 18.05.2025	
Audit požadovaný eIDAS/ČR pro služby: a) Vydávání kvalifikovaných certifikátů pro elektronické podpisy b) Vydávání kvalifikovaných certifikátů pro elektronické pečetě c) Vydávání kvalifikovaných certifikátů pro autentizaci internetových stránek Auditní závěrečná zpráva z 13.06.2024 Platnost certifikátu: 26.05.2023 - 25.05.2025	SHODA
Audit 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 13.06.2024 Platnost certifikátu: 14.06.2023 - 13.06.2025	SHODA
Audit required by Microsoft Trusted Root Program – S/MIME 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, as amended by **ETSI TS 119 411-6 V1.1.1 (2023-08)** 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, policies: 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	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 **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, as amended by **ETSI TS 119 411-6 V1.1.1 (2023-08)** 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, policies: a) NCP: Normalized Certificate Policy b) NCP+: Normalized Certificate Policy requiring a secure cryptographic device Auditní závěrečná zpráva z 19.09.2024	
Audit required by Microsoft Trusted Root Program – S/MIME AUDIT STATEMENT REPORT – I.CA Root CA/ECC 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, as amended by **ETSI TS 119 411-6 V1.1.1 (2023-08)** 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, policies: 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 V1.4.1 (2023-10)** Electronic Signatures and Infrastructures (ESI); Policy and security requirements for Trust Service Providers issuing certificates; Part 1: General requirements, as amended by **ETSI TS 119 411-6 V1.1.1 (2023-08)** Electronic Signatures and Infrastructures (ESI); Policy and security requirements for Trust Service Providers issuing certificates; Part 6: Requirements	COMPLIANCE

for Trust Service Providers issuing publicly trusted S/MIME certificates, policies: c) NCP: Normalized Certificate Policy d) NCP+: Normalized Certificate Policy requiring a secure cryptographic device Auditní závěrečná zpráva z 19.09.2024	

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.

3 TYPY CERTIFIKÁTŮ, OVĚŘOVACÍ PROCEDURY A POUŽITÍ

3.1 Soulad se standardy

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

- ČSN ETSI EN 319 411-1 Elektronické podpisy a infrastruktury (ESI) - Požadavky politiky a bezpečnosti na poskytovatele důvěryhodných služeb vydávající certifikáty – Část 1: Obecné požadavky.
- ETSI EN 319 411-1 Electronic Signatures and Infrastructures (ESI); Policy and security requirements for Trust Service Providers issuing certificates; Part 1: General requirements.
- ČSN ETSI EN 319 411-2 Elektronické podpisy a infrastruktury (ESI) - Požadavky politiky a bezpečnosti na poskytovatele důvěryhodných služeb vydávající certifikáty – Část 2: Požadavky na poskytovatele důvěryhodných služeb vydávající kvalifikované certifikáty EU.
- 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 Certificates.
- CA/Browser Forum – Guidelines for the Issuance and Management of Extended Validation Certificates.
- CA/Browser Forum – Baseline Requirements for the Issuance and Management of Publicly-Trusted S/MIME Certificates.
- ETSI TS 119 495 Electronic Signatures and Infrastructures (ESI); Sector Specific Requirements; Qualified Certificate Profiles and TSP Policy Requirements under the payment services Directive (EU) 2015/2366.
- ETSI EN 319 422 Electronic Signatures and Infrastructures (ESI); Time-stamping protocol and time-stamp token profiles.

3.2 Typy certifikátů – algoritmus RSA

3.2.1 Certifikační autority vytvořené do 04/2022

3.2.1.1 Kořenová certifikační autorita **I.CA Root CA/RSA**

Kořenová certifikační autorita **I.CA Root CA/RSA** (klíč RSA 4096 bitů, algoritmus podpisu sha512WithRSAEncryption) společnosti První certifikační autorita, a.s., vydává v souladu s požadavky technických standardů a platné právní úpravy certifikáty výhradně podřízeným

certifikačním autoritám (klíč RSA minimálně 3072 bitů, algoritmus podpisu sha256WithRSAEncryption) a svému OCSP respondéru (s klíčem RSA 2048 bitů, algoritmus podpisu sha256WithRSAEncryption). Tyto podřízené certifikační autority (viz kapitola 3.2.1.2) vydávají certifikáty koncovým uživatelům a svým OCSP respondérům.

3.2.1.2 Podřízené certifikační autority

Certifikační autorita **I.CA Qualified CA/RSA 07/2015** (klíč RSA 4096 bitů, algoritmus podpisu sha256WithRSAEncryption) je určena k vydávání kvalifikovaných certifikátů pro elektronický podpis a elektronickou pečeť (Slovenská republika) a svému OCSP respondéru (s klíči RSA minimálně 2048 bitů, algoritmus podpisu minimálně sha256WithRSAEncryption).

Certifikační autorita **I.CA Qualified 2 CA/RSA 02/2016** (klíč RSA 4096 bitů, algoritmus podpisu sha256WithRSAEncryption) je určena k vydávání kvalifikovaných certifikátů pro elektronický podpis a elektronickou pečeť (volitelně s rozšířením vyžadovaným směrnicí Evropské unie o platebních službách č. 2015/2366) a systémových certifikátů koncovým uživatelům a svému OCSP respondéru (s klíči RSA minimálně 2048 bitů, algoritmus podpisu minimálně sha256WithRSAEncryption).

Certifikační autorita **I.CA TSACA/RSA 04/2017** (klíč RSA 4096 bitů, algoritmus podpisu sha256WithRSAEncryption) je určena k vydávání kvalifikovaných certifikátů pro elektronickou pečeť pro systém TSA2 a svému OCSP respondéru (s klíči RSA minimálně 2048 bitů, algoritmus podpisu sha256WithRSAEncryption).

Certifikační autorita **I.CA TSACA/RSA 03/2022** (klíč RSA 3072 bitů, algoritmus podpisu sha256WithRSAEncryption) je určena k vydávání kvalifikovaných certifikátů pro elektronickou pečeť pro systém TSA2 a svému OCSP respondéru (s klíči RSA minimálně 2048 bitů, algoritmus podpisu sha256WithRSAEncryption).

Certifikační autorita **I.CA Public CA/RSA 07/2015** (klíč RSA 4096 bitů, algoritmus podpisu sha256WithRSAEncryption) je určena k vydávání komerčních certifikátů koncovým uživatelům a svému OCSP respondéru (s klíči RSA minimálně 2048 bitů, algoritmus podpisu minimálně sha256WithRSAEncryption).

Certifikační autorita **I.CA SSL CA/RSA 07/2015** (klíč RSA 4096 bitů, algoritmus podpisu sha256WithRSAEncryption) je vyhrazena pouze pro vydávání certifikátů pro přístup k webovým službám chráněným protokoly TLS/SSL (SSL certifikáty, „domain validation“ a „organization validation“) a svému OCSP respondéru (s klíči RSA minimálně 2048 bitů, algoritmus podpisu minimálně sha256WithRSAEncryption).

Certifikační autorita **I.CA SSL EV CA/RSA 10/2017** (klíč RSA 4096 bitů, algoritmus podpisu sha256WithRSAEncryption) je vyhrazena pouze pro vydávání kvalifikovaných certifikátů pro autentizaci internetových stránek („extended validation“ SSL certifikáty) v souladu s eIDAS (volitelně s rozšířením vyžadovaným směrnicí Evropské unie o platebních službách č. 2015/2366) a svému OCSP respondéru (s klíči RSA minimálně 2048 bitů, algoritmus podpisu minimálně sha256WithRSAEncryption).

3.2.2 Certifikační autority vytvořené od 05/2022

3.2.2.1 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 První certifikační autorita, a.s., 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 3.2.2.1.1) vydávají certifikáty koncovým uživatelům a svým OCSP respondérům.

3.2.2.1.1 Podřízené certifikační autority

Certifikační autorita **I.CA EU Qualified CA2/RSA 06/2022** (klíč RSA 4096 bitů, algoritmus podpisu sha256WithRSAEncryption) je určena k vydávání kvalifikovaných certifikátů pro elektronický podpis a elektronickou pečeť (volitelně s rozšířením vyžadovaným směrnicí Evropské unie o platebních službách č. 2015/2366) a systémových certifikátů koncovým uživatelům a svému OCSP respondéru (s klíči RSA minimálně 2048 bitů, algoritmus podpisu minimálně sha256WithRSAEncryption).

Certifikační autorita **I.CA TSA CA/RSA 06/2022** (klíč RSA 4096 bitů, algoritmus podpisu sha256WithRSAEncryption) je určena k vydávání kvalifikovaných certifikátů pro elektronickou pečeť pro systém TSA2 a svému OCSP respondéru (s klíči RSA minimálně 2048 bitů, algoritmus podpisu sha256WithRSAEncryption).

Certifikační autorita **I.CA Public CA/RSA 06/2022** (klíč RSA 4096 bitů, algoritmus podpisu sha256WithRSAEncryption) je určena k vydávání komerčních certifikátů koncovým uživatelům a svému OCSP respondéru (s klíči RSA minimálně 2048 bitů, algoritmus podpisu minimálně sha256WithRSAEncryption).

3.2.2.2 Kořenová certifikační autorita **I.CA TLS Root CA/RSA 05/2022**

Kořenová certifikační autorita **I.CA TLS Root CA/RSA 05/2022** (klíč RSA 4096 bitů, algoritmus podpisu sha512WithRSAEncryption) společnosti První certifikační autorita, a.s., 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 3.2.2.2.1) vydávají certifikáty koncovým uživatelům a svým OCSP respondérům.

3.2.2.2.1 Podřízené certifikační autority

Certifikační autorita **I.CA TLS EV CA/RSA 06/2022** (klíč RSA 4096 bitů, algoritmus podpisu sha256WithRSAEncryption) je vyhrazena pouze pro vydávání kvalifikovaných certifikátů pro autentizaci internetových stránek („extended validation“ SSL certifikáty) v souladu s eIDAS (volitelně s rozšířením vyžadovaným směrnicí Evropské unie o platebních službách č. 2015/2366) a svému OCSP respondéru (s klíči RSA minimálně 2048 bitů, algoritmus podpisu minimálně sha256WithRSAEncryption).

Certifikační autorita **I.CA TLS DV/OV CA/RSA 06/2022** (klíč RSA 4096 bitů, algoritmus podpisu sha256WithRSAEncryption) je vyhrazena pouze pro vydávání certifikátů pro přístup k webovým službám chráněným protokoly TLS/SSL (SSL certifikáty, „domain validation“ a „organization validation“) a svému OCSP respondéru (s klíči RSA minimálně 2048 bitů, algoritmus podpisu minimálně sha256WithRSAEncryption).

3.3 Typy certifikátů – ECC

3.3.1 Certifikační autority vytvořené do 04/2022

3.3.1.1 Kořenová certifikační autorita **I.CA Root CA/ECC 12/2016**

Kořenová certifikační autorita **I.CA Root CA/ECC 12/2016** (klíč EC P-521 bitů, algoritmus podpisu ecdsa-with-SHA512) společnosti První certifikační autorita, a.s., vydává v souladu s požadavky technických standardů a platné právní úpravy certifikáty výhradně podřízeným certifikačním autoritám (klíč EC P-521 bitů, algoritmus podpisu ecdsa-with-SHA512) a svému OCSP respondéru (s klíčem EC P-256 bitů, algoritmus podpisu ecdsa-with-SHA256). Tyto podřízené certifikační autority (viz kapitola 3.3.1.2) vydávají certifikáty koncovým uživatelům a svým OCSP respondérům.

3.3.1.2 Podřízené certifikační autority

Certifikační autorita **I.CA Qualified 2 CA/ECC 06/2019** (klíč EC P-521 bitů, algoritmus podpisu ecdsa-with-SHA512) je určena k vydávání kvalifikovaných certifikátů pro elektronický podpis a elektronickou pečeť a svému OCSP respondéru (s klíči EC minimálně P-256 bitů, algoritmus podpisu minimálně ecdsa-with-SHA256).

Certifikační autorita **I.CA Public CA/ECC 12/2016** (klíč EC P-521 bitů, algoritmus podpisu ecdsa-with-SHA512) je určena k vydávání komerčních certifikátů koncovým uživatelům a svému OCSP respondéru (s klíči EC minimálně P-256 bitů, algoritmus podpisu minimálně ecdsa-with-SHA256).

3.3.2 Certifikační autority vytvořené od 05/2022

3.3.2.1 Kořenová certifikační autorita **I.CA Root CA/ECC 05/2022**

Kořenová certifikační autorita **I.CA Root CA/ECC 05/2022** (klíč EC P-384 bitů, algoritmus podpisu ecdsa-with-SHA384) společnosti První certifikační autorita, a.s., vydává v souladu s požadavky technických standardů a platné právní úpravy certifikáty výhradně podřízeným certifikačním autoritám (klíč EC P-384 bitů, algoritmus podpisu ecdsa-with-SHA384) a svému OCSP respondéru (s klíčem EC P-256 bitů, algoritmus podpisu ecdsa-with-SHA256). Tyto podřízené certifikační autority (viz kapitola 3.3.2.1.1) vydávají certifikáty koncovým uživatelům a svým OCSP respondérům.

3.3.2.1.1 Podřízené certifikační autority

Certifikační autorita **I.CA EU Qualified CA2/ECC 06/2022** (klíč EC P-384 bitů, algoritmus podpisu ecdsa-with-SHA384) je určena k vydávání kvalifikovaných certifikátů pro elektronický podpis a elektronickou pečeť a svému OCSP respondéru (s klíči EC minimálně P-256 bitů, algoritmus podpisu minimálně ecdsa-with-SHA256).

Certifikační autorita **I.CA Public CA/ECC 06/2022** (klíč EC P-384 bitů, algoritmus podpisu ecdsa-with-SHA384) je určena k vydávání komerčních certifikátů koncovým uživatelům a svému OCSP respondéru (s klíči EC minimálně P-256 bitů, algoritmus podpisu minimálně ecdsa-with-SHA256).

3.4 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 (není možné v případě zmocněnce), s využitím certifikované služby ZealiD TRA Service nebo prostřednictvím Národní identitní autority (NIA) s využitím kteréhokoliv z prostředků pro elektronickou identifikaci nabízených při přihlašování prostřednictvím NIA, který splňuje úroveň záruky ZNAČNÁ nebo úroveň záruky VYSOKÁ, přičemž pokud se jedná úroveň záruky ZNAČNÁ a zároveň žadatel je samoplátce, je distanční ověřování identity fyzické osoby doplněno videohovorem jako bezpečnostní pojistkou.

Povinnost přítomnosti fyzické osoby v případě vydávání SSL, resp. EV SSL certifikátů není na pracovišti registrační autority vyžadována a proces ověření probíhá, je-li to možné, s využitím veřejně dostupných registrů.

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, 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, elektronických pečetí a autentizaci internetových stránek 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.

Ostatní typy certifikátů lze obecně použít k ověřování elektronických podpisů, identifikaci, autentizaci a k zabezpečené komunikaci.

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 První certifikační autorita, a.s., uchovává vydané certifikáty a seznamy zneplatněných certifikátů po celou dobu své existence.

5 POVINNOSTI ŽADATELŮ NEBO DRŽITELŮ CERTIFIKÁTU

Držitelem certifikátů je žadatel o certifikát, kterému byl tento certifikát vydán. Z pohledu společnosti První certifikační autorita, a.s., se jedná o osobu (fyzickou, nebo organizaci), která uzavřela se společností První certifikační autorita, a.s., 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 První certifikační autorita, a.s. Mezi základní povinnosti těchto subjektů patří zejména:

- získat z bezpečného zdroje relevantní certifikáty certifikačních autorit uvedených v kapitolách 3.2, resp. 3.3 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, kvalifikované certifikáty pro elektronické pečetě a kvalifikované certifikáty pro autentizaci webových stránek vydané v souladu s eIDAS) je důvěryhodnou kotvou certifikát vydavatele uvedený v důvěryhodném seznam ČR (tj. certifikát vydávající certifikační autority).

7 OMEZENÍ ZÁRUKY A ODPOVĚDNOSTI

Společnost První certifikační autorita, a.s.:

- 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 První certifikační autorita, a.s., 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 První certifikační autorita, a.s., 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 První certifikační autorita, a.s., 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 První certifikační autorita, a.s., je upraven příslušnými ustanoveními platných certifikačních politik. Vztah společnosti První certifikační autorita, a.s., 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 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 certifikátu) je povinna uvést:

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

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

- nařízení 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),

- 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 České republiky č. 110/2019 Sb., o zpracování osobních údajů a o změně některých zákonů,
- zákonem České republiky č. 90/2012 Sb., o obchodních společnostech a družstvech (zákon o obchodních korporacích).

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 vyžadovaných touto společností.

Za společnost První certifikační autorita, a.s.

Ing. Petr Budiš, Ph.D., MBA v.r.