První certifikační autorita, s.r.o.

PKI Disclosure Statement

Version 1.3

CONTENTS

1 INTRODUCTION

This document provides a basic overview of the two-level topology of certification authorities operated by První certifikační autorita, a.s., (hereinafter as I.CA), within this topology are also operated certification authorities of První certifikační autorita, s.r.o., (hereinafter as I.CA SK), and the obligations and rights of subscribers and the relying parties.

Note: This is English translation of PKI Disclosure Statement; Czech version always takes precedence.

1.1 Document history

Table 1 – Document history

Version	Date of release	Note
1.0	28 March 2023	First release.
1.1	23 November 2023	List of passed audits updated.
1.2	23 April 2024	List of passed audits updated.
1.3	28 August 2024	Requirements of ETSI TS 119 411-6 taken into account.

1.2 Audits and inspections of I.CA and I.CA SK

Table 2 – Audits and other inspections

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	COMPLIANCE

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 b) NCP+: Normalized Certificate Policy requiring a secure cryptographic device Audit Statement Report dated 21 May 2024 Certificate valid from 19 May 2024 to 18 May 2025	
Audit (full) required by eIDAS/SR for: a) Qualified trust service - creation and verification of qualified certificates for electronic signatures b) Qualified trust service - creation and verification of qualified certificates for electronic seals Report dated 9 December 2022 Certificate valid from 9 December 2022 to 8 December 2024	COMPLIANCE
Audit (surveillance) required by eIDAS/SR for: a) Qualified trust service - creation and verification of qualified certificates for electronic signatures b) Qualified trust service - creation and verification of qualified certificates for electronic seals Report dated 12 December 2023	COMPLIANCE

2 CONTACT INFORMATION

2.1 Head office

The address of the company's head office:

První certifikační autorita, s.r.o.

Galvaniho 19045/19

821 04 Bratislava – mestská časť Ružinov

Slovak Republic

Contact to the company head office:

Phone: +420 284 081 940

Fax.: +420 284 081 965

E-mail: info@ica.cz

2.2 Disclosure

All public information can be found on the Internet at: http://www.ica.cz.

2.3 Communication with the public

Communication with the public may be conducted as follows:

- General contact: info@ica.cz,
- Registration authorities: see http://www.ica.cz,
- Technical support:
  - Phone: +420 284 081 930-33,
  - E-mail: support@ica.cz,
- Claims: reklamace@ica.cz,
- Sales department: sales@ica.cz.

3 CERTIFICATE TYPES, VERIFICATION PROCEDURES AND USE

3.1 Compliance with standards

I.CA SK issues certificates (for individuals and organizations), profile of which is conform to standard X.509 version 3 in compliance with norms and standards:

- 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 Types of certificates

3.2.1 Root certification authority I.CA Root CA/RSA 05/2022

The root certification authority **I.CA Root CA/RSA 05/2022** (RSA key 4096 bits, signature algorithm sha512WithRSAEncryption) of I.CA issues, in accordance with the requirements of technical standards and current legislation, certificates solely to subordinate CAs (RSA key 4096 bits, signature algorithm sha256WithRSAEncryption) and to its OCSP responder (with RSA key 2048 bits, signature algorithm sha256WithRSAEncryption). These subordinate CAs (see chapter 3.2.2) issue certificates to end users and to their OCSP responders.

3.2.2 Subordinate certification authorities

The certification authority **I.CA EU Qualified CA-SK/RSA 10/2022** (RSA key 4096 bits, signature algorithm sha256WithRSAEncryption) owned by I.CA SK company is intended for issuing qualified certificates for electronic signature and electronic seal and certificates for its OCSP responder (with RSA keys at least 2048 bits, signature algorithm at least sha256WithRSAEncryption).

3.3 Verification procedures

Always when the primary certificate is issued, so called registration process is performed i.e.:

- Identity of Individual i.e., subscriber or his/her agent, or the representative of subscriber, is verified on the basis of his/her identity papers;
- In case of the certificate for an organization, the certificate applicant's relationship with the organization is verified;
- E-mail address validation is performed in two ways, by checking whether the address belongs to a registered DNS domain (validating authority over mailbox via domain) or by validation the holder of the e-mail address using the content of the sent e-mail (validating control over mailbox via email), when the use of the appropriate validation method depends on the type of contractual relationship with the client.

S/MIME certificates, namely "Individual-validated" and "Organization-validated" type certificates, are issued in accordance with the document Baseline Requirements for the Issuance and Management of Publicly-Trusted S/MIME Certificates. Currently, the "Individual-validated" and "Organization-validated" policy OIDs are not listed in the certificates.

Identity authentication of the subscriber or his/her agent in case of the certificate for natural person may be performed on-site i.e., he arrives at the RA with the required documents, or remotely (on-line) using certified ZealiD TRA Service – this cannot be used by subscriber’s agent.

If the relevant certificate policy allows for the issuance of a “subsequent certificate” (a certificate that will comply with the agreement on the provision of relevant services, concluded between the applicant and I.CA SK, issued to the applicant on the basis of a new application for a certificate during the validity period of the certificate for which this subsequent certificate is issued), then the physical presence of the applicant for a certificate at the registration authority office is not required. A detailed description of registration procedures is provided in the relevant certificate policies.

4 USE OF CERTIFICATES

Qualified certificates may be used solely for verifying electronic signatures and electronic seals in compliance with Regulation (EU) no 910/2014 of the European Parliament and of the Council on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC, as amended.

When using certificates, it is always necessary to proceed in accordance with the applicable certificate policy.

Unless the relevant legislative standard specifies otherwise, audit records and records generated during the registration process are kept for at least 10 years from their inception.

I.CA SK retains issued certificates and lists of revoked certificates for the entire period of its existence.

5 OBLIGATIONS OF APPLICANTS AND SUBSCRIBERS

Subscriber is the applicant for a certificate to whom/which this certificate was issued. From the ICA SK's point of view this is the entity (natural or legal person) who entered into subscriber agreement with I.CA SK. The basic obligations of the applicant for this certificate, and subsequently the subscriber, include:

- To provide truthful and complete information when registering the application for issuance of the certificate;
- To immediately inform the service provider of changes in data contained in the issued certificate, respectively in the agreement;
- To familiarize himself/herself with the certificate policy under which the certificate was issued;
- To check whether the information given in the application for the certificate and in the certificate, itself are correct and match the required data;
- To use the devices and the private key corresponding to the public key in the issued certificate in such a way so as to prevent its unauthorized use;
- To use the private key and the corresponding issued certificate in accordance with the relevant certificate policy and solely for the purposes set out in this certificate policy;
- To immediately request revocation of the certificate and terminate the use of the relevant private key, especially in the case of private key compromise or suspicion that the private key has been abused.

6 OBLIGATIONS OF RELYING PARTIES

Relying parties are entities who, in their work, rely on the certificate issued by I.CA SK. The basic obligations of these entities include:

- To obtain, from a secure source, relevant certificates of certification authorities as referred to in Chapters 3.2 or 3.3, and to verify the checksum of these certificates;
- Before using the end-user certificate, to verify the validity of CA certificates relating to the certificate of the end user;

- To make sure that the end-user certificate is suitable for intended use;
- To comply with all relevant provisions of the certificate policy under which the end-user certificate was issued;
- When verifying the validity of EU qualified certificates (qualified certificates for electronic signature and qualified certificates for electronic seal issued in compliance with eIDAS) the trust anchor is issuer's certificate published in EU trusted list.

7 LIMITATIONS OF WARRANTY AND RESPONSIBILITY

I.CA SK:

- Undertakes to fulfill all of the obligations as defined both by applicable laws and regulations, and by relevant certificate policies;
- Shall provide guarantees presented in relevant certificate policy for the duration of the agreement on the provision of services or trust services; if a breach of obligations on the part of the subscriber or the relying party having a connection with the alleged damage is determined, the warranty claims shall not be provided – this must be reported to the subscriber or to the relying party and recorded;
- Agrees that the suppliers of application software, who have a valid contract for the distribution of the root certificate, shall not assume any obligations or potential liability, except in cases where the damage or loss was directly caused by this software of this supplier;
- Does not provide any guarantees other than those presented in relevant certificate policy;
- Other possible damages based on the provisions of relevant laws, and their amounts, may be decided upon by the court.

I.CA SK is not liable:

- For faults of provided services incurred due to improper or unauthorized use of services, particularly for operating in violation of the conditions specified in the certificate policy, as well as for faults caused by force majeure, including temporary loss of telecommunication connection, etc.;
- For damages resulting from the use of the certificate in the period after requesting its revocation, if I.CA SK complies with the defined deadline for publishing the revoked certificate on the certificate revocation list (CRL).

8 AGREEMENT AND CERTIFICATE POLICY

The relationship between the subscriber and the certification service provider (I.CA SK) apart from the relevant provisions of relevant legislation, is governed by the agreement and by the relevant provisions of applicable certificate policies.

The relationship between the relying party and the services or trust services provider (I.CA SK) is governed by the relevant provisions of the applicable certificate policies. The relationship between I.CA SK and the relying parties is not governed by contract.

All public information can be obtained from the contact addresses listed in Chapter 2 of this document.

9 PERSONAL DATA PROTECTION

The protection of personal data at I.CA SK is resolved in compliance with applicable legislation concerning personal data i.e., Slovak Republic Act No. 18/2018 Coll. on the personal data protection and on changes and amendments of certain laws and REGULATION (EU) 2016/679 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation).

10 REFUND POLICY AND CLAIMS

A claim may be submitted as follows:

- By e-mail to reklamace@ica.cz;
- By registered mail to the address of the I.CA SK head office;
- In person at the I.CA SK head office.

The claiming person (subscriber) must provide:

- Description of the faults and their manifestations, as accurately as possible;
- Serial number of the claimed product;
- Suggestion how the claim/complaint should be resolved.

I.CA SK will decide upon the claim/complaint within three working days from receipt of the complaint and will notify the claimant (by e-mail or registered mail), unless the parties agree otherwise.

The claim/complaint, including the fault, will be processed without undue delay and not later than thirty days from the date of claim, unless the parties agree otherwise.

The subscriber shall be provided with a new certificate free of charge in the following cases:

- If there is reasonable suspicion that the private key of the certification authority was compromised;
- Based on the decision of the members of I.CA management or the managing director of I.CA SK taking into account the specific circumstances;
- If the specific certification authority, after receiving application for a certificate, discovers, that there exists a different certificate with a duplicate public key.

11 LEGAL ENVIRONMENT

Providing trust services by I.CA SK is in compliance with the statutory requirements of EU and the Czech Republic, in particular:

- REGULATION (EU) 910/2014 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 23 July 2014 on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC, as amended;
- Act of the Slovak Republic No. 272/2016 Coll., on trust services for electronic transactions in the internal market and on amendment and supplementing of certain acts;
- REGULATION (EU) 2016/679 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation);
- Act of the Slovak Republic No. 18/2018 Coll., on personal data protection and on changes and amendments of certain laws.

12 QUALIFICATION, AUDITS, INSPECTIONS

I.CA SK is the qualified trust services provider and due to this it is regularly audited and inspected in compliance with requirements of legislation mentioned in chapter 11 above.

I.CA is a member of Microsoft Trusted Root Program (its root certificate is included into the list of trusted certification authorities.) due to this provided services are regularly audited according to requirements of Microsoft Company.

On behalf of První certifikační autorita, s.r.o.

Ing. Ctirad Fischer