První certifikační autorita, a.s.

CA PKI Disclosure Statement

Version 1.9

CONTENTS

1 INTRODUCTION

This document provides a basic overview of the two-level topology of certification authorities operated by První certifikační autorita, a.s. (First Certification Authority, hereinafter as I.CA) 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	2 September 2015	First release.
1.1	7 April 2016	Extended to include other issuing CAs.
1.2	18 April 2017	Update concerning passed inspections and audits. Update required by the legislation for Trust Services.
1.3	18 November 2017	Update concerning types of issuing certification authorities and passed audits.
1.4	8 August 2018	Update concerning of passed audits.
1.5	27 June 2019	Update concerning of passed audits.
1.6	27 January 2020	Support elliptic curve cryptography (ECC, cryptography EC). Update concerning of passed audits.
1.7	14 July 2020	Revision of document, list of passed audits updated.
1.8	17 June 2021	List of passed audits updated.
1.9	12 May 2022	New issuing certification authority added. List of audits and inspections limited to the last performed. Notice for relying parties what trust anchor to use when verifying the validity of EU qualified certificate added to chapter 6.

1.2 I.CA audits and inspections

Table 2 – Security compliance inspections, audits and other inspections

Type	Inspector/Auditor statement
Audit required by Microsoft Trusted Root Program - AUDIT STATEMENT REPORT – I.CA Root CA/RSA: **ETSI EN 319 411-2 V2.2.2 (2018-04)** Electronic Signatures and Infrastructures (ESI); Policy and security requirements for Trust Service Providers issuing certificates; Part 2: Requirements for trust	COMPLIANCE

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) e) QCP-w: Policy for EU qualified certificates for website authentication **ETSI EN 319 411-1 V1.2.2 (2018-04)** 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 Audit Statement Report dated 18 May 2021	
Audit required by Microsoft Trusted Root Program - AUDIT STATEMENT REPORT – I.CA Root CA/ECC 12/2016: **ETSI EN 319 411-2 V2.2.2 (2018-04)** 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 V1.2.2 (2018-04)** Electronic Signatures and Infrastructures (ESI); Policy and	COMPLIANCE

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 18 May 2021	
Conformity assessment report (eIDAS/ČR) a) Creation of qualified certificates for electronic signatures b) Creation of qualified certificates for electronic seals c) Creation of qualified certificates for website authentication Audit Statement Report dated 11 June 2021 Certificate valid since 14 June 2021 till 13 June 2023	COMPLIANCE
Conformity assessment report (eIDAS/Slovak Republic): 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 Audit Statement Report dated 11 June 2021 Certificate valid since 14 June 2021 till 13 June 2023	COMPLIANCE

2 CONTACT INFORMATION

2.1 Head office

The address of the company's head office:

První certifikační autorita, a.s.
Podvinný mlýn 2178/6
190 00 Praha 9
Czech Republic

Contact to the company head office:

Phone: +420 284 081 940
Fax.: +420 284 081 965
E-mail: info@ica.cz
Databox ID: a69fvfb

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

The company První certifikační autorita, a.s., issues certificates (for individuals and organizations), profile of which is conform to standard X.509 version 3 in compliance with norms and standards:

- ETSI EN 319 411-1 Electronic Signatures and Infrastructures (ESI); Policy and security requirements for Trust Service Providers issuing certificates; Part 1: General requirements;
- 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;
- 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.
- 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 Types of certificates – algorithm RSA

The root certification authority **I.CA Root CA/RSA** (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 issue certificates to end users and to their OCSP responders.

The certification authority **I.CA Qualified CA/RSA 07/2015** (RSA key 4096 bits, signature algorithm sha512WithRSAEncryption) is intended for issuing certificates for qualified certificates for electronic signature and electronic seal to end users (Slovak Republic) and its OCSP responder (with RSA key at least 2048 bits, signature algorithm at least sha256WithRSAEncryption).

The certification authority **I.CA Qualified 2 CA/RSA 02/2016** (RSA key 4096 bits, signature algorithm sha256WithRSAEncryption) is intended for issuing qualified certificates for electronic signature and electronic seal (optionally with the extension required by the European Union Payment Services Directive No. 2015/2366) and system certificates to end users and its OCSP responder (with RSA keys at least 2048 bits, signature algorithm at least sha256WithRSAEncryption).

The certification authority **I.CA TSACA/RSA 04/2017** (RSA key 4096 bits, signature algorithm sha256WithRSAEncryption) is intended for issuing qualified certificates for

electronic seal for the TSA2 System and its OCSP responder (with RSA keys at least 2048 bits, signature algorithm at least sha256WithRSAEncryption).

The certification authority **I.CA TSA CA/RSA 03/2022** (RSA key 3072 bits, signature algorithm sha256WithRSAEncryption) is intended for issuing qualified certificates for electronic seal for the TSA2 System and its OCSP responder (with RSA keys at least 2048 bits, signature algorithm at least sha256WithRSAEncryption).

The certification authority **I.CA Public CA/RSA 07/2015** (RSA key 4096 bits, signature algorithm sha256WithRSAEncryption) is intended for issuing commercial certificates to end users and its OCSP responder (with RSA keys at least 2048 bits, signature algorithm at least sha256WithRSAEncryption).

The SSL certification authority **I.CA SSL CA/RSA 07/2015** (RSA key 4096 bits, signature algorithm sha256WithRSAEncryption) is reserved solely for issuing certificates for access to web services protected by TLS/SSL protocols (SSL certificates), specifically “domain validation" and "organization validation" and to its OCSP responder (with RSA keys at least 2048 bits, signature algorithm at least sha256WithRSAEncryption).

The EV SSL certification authority **I.CA SSL EV CA/RSA 10/2017** (RSA key 4096 bits, signature algorithm sha256WithRSAEncryption) is reserved solely for issuing qualified certificates for website authentication (EV SSL certificates) in accordance with eIDAS (optionally with the extension required by the European Union Payment Services Directive No. 2015/2366) and to its OCSP responder (with RSA keys at least 2048 bits, signature algorithm at least sha256WithRSAEncryption).

3.3 Types of certificates – ECC

The root certification authority I.CA Root CA/ EC 12/2016 (EC key P-521 bits, signature algorithm ecdsa-with-SHA512) of I.CA issues, in accordance with the requirements of technical standards and current legislation, certificates solely to subordinate CAs (EC keys P-521 bits, signature algorithm ecdsa-with-SHA512) and to its OCSP responder (with keys EC P-256 bits, signature algorithm ecdsa-with-SHA256). These subordinate CAs issue certificates to end users and to their OCSP responders.

The certification authority I.CA Qualified 2 CA/ECC 06/2019 (EC key P-521 bits, signature algorithm ecdsa-with-SHA512) is intended for issuing qualified certificates for electronic signature and electronic seal and its OCSP responder (with keys EC at least P-256 bits, signature algorithm at least ecdsa-with-SHA256).

The certification authority I.CA Public CA/ECC 12/2016 (EC key P-521 bits, signature algorithm ecdsa-with-SHA512) is intended for issuing commercial certificates to end users and its OCSP responder (with keys EC at least P-256 bits, signature algorithm at least ecdsa-with-SHA256).

3.4 Verification procedures

In the process of issuing the initial certificate, when the physical presence of the applicant, or his/her representative, is necessary at the registration authority office (with exceptions as indicated in the following paragraph), the identity of this individual is always verified on the basis of his/her personal papers. In the case of a certificate for an organization, the certificate applicant's relationship with the organization is verified.

The presence of the natural person in the event of issuing an SSL or EV SSL certificates at the registration authority office is not required, and the verification process may take place, if possible, with the use of publicly available registers.

If the relevant certification 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, 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 certification policies.

4 USE OF CERTIFICATES

Qualified certificates may be used solely for verifying electronic signatures, electronic seals, respectively for website authentication 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.

Other types of certificates may generally be used to verify electronic signatures, for identification, authentication, and for secure communication.

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

The company První certifikační autorita, a.s., retains issued certificates and lists of revoked certificates for the entire period of its existence.

5 OBLIGATIONS OF APPLICANTS AND SUBSCRIBERS

A subscriber is the applicant for a certificate to whom/which this certificate was issued. From the point of view of I.CA, this is the person natural or legal entity) who entered into subscriber agreement with I.CA. 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 certification 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 certification policy and solely for the purposes set out in this certification 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. 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 certification policy under which the end-user certificate was issued;
- When verifying the validity of EU qualified certificates (qualified certificates for electronic signature, qualified certificates for electronic seal and qualified certificates for website authentication) the trust anchor is issuer's certificate published in the Czech Republic trusted list (i.e., certificate of issuing certification authority).

7 LIMITATIONS OF WARRANTY AND RESPONSIBILITY

The company První certifikační autorita, a.s.:

- Undertakes to fulfill all of the obligations as defined both by applicable laws and regulations, and by relevant certification policies;
- Shall provide guarantees presented in relevant certification 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 certification policy;
- Other possible damages based on the provisions of relevant laws, and their amounts, may be decided upon by the court.

The company První certifikační autorita, a.s. 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

certification 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 complies with the defined deadline for publishing the revoked certificate on the certificate revocation list (CRL).

8 AGREEMENT AND CERTIFICATION POLICY

The relationship between the subscriber and the certification service provider (První certifikační autorita, a.s.) apart from the relevant provisions of relevant legislation, is governed by the agreement and by the relevant provisions of applicable certification policies.

The relationship between the relying party and the services or trust services provider (První certifikační autorita, a.s.) is governed by the relevant provisions of the applicable certification policies. The relationship between I.CA and the relying parties is not governed by agreement.

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 is resolved in compliance with applicable legislation concerning personal data, i.e. Czech Republic Act No. 110/2019 Coll., on the processing of personal data and the 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 head office;
- By sending a message to the databox of I.CA;
- In person at the I.CA 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 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, 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 První certifikační autorita, a.s., 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;
- Act of the Czech Republic No. 297/2016 Coll., on trust services for electronic transaction;
- 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 Czech Republic No. 110/2019 Coll., on the processing of personal data and the amendments of certain laws;
- Act of the Czech Republic No. 90/2012 Coll., on commercial companies and cooperatives (Business Corporations Act).

12 QUALIFICATION, AUDITS, INSPECTIONS

První certifikační autorita, a.s., 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.

První certifikační autorita, a.s., 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, a.s.
Ing. Petr Budiš, Ph.D., MBA