First Certification Authority

První certifikační autorita, a.s.

CA PKI Disclosure Statement

Qualified and Commercial Certification Services - Hierarchical Topology

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. (First Certification Authority, hereinafter as I.CA) and the obligations and rights of subscribers and the relying parties.

1.1 Document Evolution

Table 1 – Document evolution

Version	Date of release	Note
1.0	2 Sept 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 CAs and passed audits.

1.2 I.CA Audits and Inspections

Table 2 – Inspections executed for safety compliance, audits, and other inspections

Type	Inspector/Auditor statement
Inspection of security compliance – report dated 26 June 2006	PASSED
Security Audit of certification services provided – report dated 9 August 2006	PASSED
Audit of Information Security Management System (ISMS) – report dated 30 April 2007	PASSED
Inspection of security compliance – report dated 28 June 2007	PASSED
Audit of I.CA for compliance with policy requirements for certification authorities issuing certificates in accordance with ETSI TS 101 456 – 3 March 2008	PASSED
Inspection of security compliance – report dated 18 June 2008	PASSED
Audit of Information Security Management System of I.CA (accredited provider of qualified certification services) – Final Report dated 30 April 2009	PASSED
Audit of state of security of issued certification services – Final Report dated 30 April 2009	PASSED
Audit of I.CA for compliance with policy requirements for certification authorities issuing certificates in accordance with ETSI TS 101 456 – 3 April 2009	PASSED

Inspection of security compliance – report dated 18 June 2009	PASSED
Audit of I.CA for compliance with policy requirements for certification authorities issuing certificates in accordance with ETSI TS 101 456 – 28 April 2010	PASSED
Audit of state of security of issued certification services – Final Report dated 30 April 2010	PASSED
Inspection of security compliance – report dated 30 June 2010	PASSED
Audit of I.CA for compliance with policy requirements for certification authorities issuing certificates in accordance with ETSI TS 101 456 – 2 May 2011	PASSED
Audit of state of security of issued certification services – Final Report dated 2 May 2011	PASSED
Audit of Information Security Management System of I.CA (accredited provider of qualified certification services) – Final Report dated 2 May 2011	PASSED
Inspection of security compliance – report dated 1 Sept 2011	PASSED
Audit of I.CA for compliance with policy requirements for certification authorities issuing certificates in accordance with ETSI TS 101 456 – Final Report, May 2012	PASSED
Audit of state of security of issued certification services – Final Report, May 2012	PASSED
Inspection of security compliance (corporate) – report dated 31 August 2012	PASSED
Audit of Information Security Management System of I.CA (accredited provider of qualified certification services) – Final Report dated 14 May 2013	PASSED
Audit of state of security of issued certification services – Final Report dated 14 May 2013	PASSED
Audit of I.CA for compliance with policy requirements for certification authorities issuing certificates in accordance with ETSI TS 101 456 – Final Report, May 2013	PASSED
Inspection of security compliance (partial) – report dated 28 August 2013	PASSED
Audit of state of security of issued certification services – Final Report, May 2014 (dated 20 May 2014)	PASSED
Audit of I.CA for compliance with policy requirements for certification authorities issuing certificates in accordance with ETSI TS 101 456 – Final Report,	PASSED

May 2014 (dated 20 May 2014)	
Inspection of security compliance (partial) – report dated 27 August 2014	PASSED
Inspection of I.CA as an accredited provider of certification services by employees of the eGovernment department of the Czech Ministry of the Interior – the subject of inspection was compliance with § 6, Section 1, point d) and Sections 5 and 6	The inspection verified that I.CA as an accredited certification service provider complies with these provisions (see http://www.mvcr.cz/clanek/vysledky-probehle-kontroly-akreditovaneho-poskytovatele-certifikacnich-sluzeb-i-ca.aspx)
Audit of Information Security Management System of I.CA (accredited provider of qualified certification services) – Final Report dated 14 May 2015	PASSED
Audit of state of security of issued certification services – Final Report, May 2015 (dated 20 May 2015)	PASSED
Audit of I.CA for compliance with policy requirements for certification authorities issuing certificates in accordance with ETSI TS 101 456 – Final Report, May 2015	PASSED
Audit of I.CA for compliance with policy requirements for certification authorities issuing certificates in accordance with ETSI TS 102 042 (policies DVCP, OVCP, NCP) – Audit Statement Report, August 2015	PASSED
Inspection of security compliance (corporate) – report dated 27 August 2015	PASSED
AUDIT STATEMENT REPORT- Root CA/RSA: ETSI TS 101 456 V1.4.3 (2007-05): "Electronic Signatures and Infrastructures (ESI); Policy requirements for certification authorities issuing qualified certificates", policies QCP public + SSCD, QCP public and ETSI TS 102 042V2.4.1 (2013-02): "Electronic Signatures and Infrastructures (ESI); Policy requirements for certification authorities issuing public key certificates", policies NCP, NCP+, DVCP, OVCP Audit Statement Report dated 18 May 2016	PASSED
Audit of state of security of issued certification services – Final Report, May 2014 (dated 20 May 2016)	PASSED
Inspection of security compliance (partial) – report dated 27 August 2016	PASSED

Audit required by Microsoft Trusted Root Certificate Program - AUDIT STATEMENT REPORT – I.CA Root CA/RSA: **ETSI EN 319 411-2 V2.1.1 (2016-02)** 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 V1.1.1 (2016-02)** 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 Audit Statement Report dated 18 May 2016	PASSED
Conformity assessment report (eIDAS/Czech Republic): a) The creation, verification, and validation qualified certificates for electronic signatures b) The creation, verification, and validation qualified certificates for electronic seals Audit Statement Report dated 26 May 2017	PASSED
Conformity assessment report (eIDAS/Slovak Republic): a) The creation, verification, and validation qualified certificates	PASSED

for electronic signatures a) The creation, verification, and validation qualified certificates for electronic seals Audit Statement Report dated 13 June 2017	

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

Telephone and mail contact to the company's head office:

tel.: +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
- office of the registration authorities: http://www.ica.cz,
- technical support:
  - tel.: +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 Certificate Types

The company První certifikační autorita, a.s. issues qualified certificates (for individuals) qualified system certificates (for individuals, organizations, and devices), commercial certificates (for individuals), commercial server certificates (for individuals, organizations, and devices) and commercial certificates for access to protected web services (for organizations) whose profile is compliant with standard X.509 v3.

The root certification authority (I.CA Root CA/RSA, RSA key length 4096 bits, algorithm SHA512) of I.CA issues, in accordance with the requirements of technical standards and current legislation, certificates solely to subordinate CAs and to its OCSP responder. 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 length 4096 bits, algorithm SHA256) is intended for issuing certificates for the TSA System and qualified certificates for electronic signature and electronic seal to end users (Slovak Republic) and its OCSP responder (RSA key length 2048 bits, algorithm SHA256).

The certification authority I.CA Qualified 2 CA/RSA 02/2016 (RSA key length 4096 bits, algorithm SHA256) 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) to end users and its OCSP responder (RSA key length 2048 bits, algorithm SHA256).

The certification authority I.CA TSAA/RSA 04/2017 (RSA key length 4096 bits, algorithm SHA256) is intended for issuing qualified certificates for electronic seal for the TSA2 System and its OCSP responder (RSA key length 2048 bits, algorithm SHA256).

The certification authority I.CA Public CA/RSA 07/2015 (RSA key length 4096 bits, algorithm SHA256) is intended for issuing commercial certificates to end users and its OCSP responder (RSA key length 2048 bits, algorithm SHA256).

The SSL certification authority I.CA SSL CA/RSA 07/2015 (RSA key length 4096 bits, algorithm SHA256) 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 (RSA key length 2048 bits, algorithm SHA256).

The EV SSL certification authority I.CA SSL EV CA/RSA 10/2017 (RSA key length 4096 bits, algorithm SHA256) 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 (RSA key length 2048 bits, algorithm SHA256).

End user certificates are issued in compliance with standards (and Czech technical standards, if applicable):

- 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.

3.2 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.

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 certification 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 THE 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 Chapter 3.1, 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 its use;
- to comply with all relevant provisions of the certification policy under which the end-user certificate was issued.

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 the above guarantees for the duration of the agreement on the provision of certification 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 mentioned above;
- 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 defects 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 defects 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 mandatory legislation, is governed by the agreement and by the relevant provisions of applicable certification policies.

The relationship between the relying party and the certification service 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. 101/2000 Coll. on Personal Data Protection, as amended before 25 May 2018 and REGILATION (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) since 25 May 2018.

The applicant for a certificate consents to the processing of personal data to the extent necessary for the issuance and revocation of this certificate. In the case of a qualified certificate, respectively a qualified system certificate, the applicant gives I.CA written consent to the processing and storage of personal data within the requirements of applicable legislation related to the issue of electronic signatures.

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 I.CA data mailbox;
- in person at the I.CA head office.

The claiming person (subscriber) must provide:

- a description of the defects and their manifestations, as accurately as possible;
- the serial number of the claimed product.

I.CA will decide upon the 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.

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

The holder 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, when receiving the request for issuance of a certificate, discovers that there exists a different certificate with a duplicate public key.

11 LEGAL ENVIRONMENT

The activities of První certifikační autorita, a.s. are governed by the relevant current provisions of the legislation, in particular:

- by 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;
- by Czech Republic Act No. 297/2016 Coll., on trust services for electronic transaction;
- by Slovak Republic Act No. 272/2016 Coll., on trust services for electronic transactions in the internal market and on amendment and supplementing of certain acts;
- by Czech Republic Act No. 90/2012 Coll., on business corporations;
- by Czech Republic Act No. 101/2000 Coll., on the protection of personal data and the amendments of certain laws before 25 May 2018;
- by 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) since 25 May 2018.

12 QUALIFICATION, AUDITS, INSPECTIONS

První certifikační autorita, a.s. is an qualified provider of trust services. The provision of these services is regularly subjected to audits and inspections according to the legislation requirements mentioned above in the chapter 11.

První certifikační autorita, a.s. is the member of Microsoft Trusted Certification Program (root certificate of I.CA is on the list of trusted root certificate authorities of the Microsoft Company). Provided services are subjected to regular audits as required by this company.

On behalf of První certifikační autorita, a.s.

Ing. Petr Budiš, Ph.D., MBA v.r.