První certifikační autorita, a.s.

TSA PKI Disclosure Statement

Version 4.5

OBSAH

1 INTRODUCTION

This document - TSA PKI Disclosure Statement - released by První certifikační autorita, a.s. (hereinafter as I.CA), provides a basic overview of provided service of issuing qualified electronic time-stamp tokens (hereinafter as time-stamp tokens) including rights and obligations of time-stamp tokens requestors.

This document is only simplified selection of pieces of information contained in service policy, in relevant practice statement and in contract document. It is intended to simplify the guidance of the time-stamp tokens users.

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	25 January 2006	First release.
1.1	14 October 2006	Decree amendment, security compliance inspection carried out, accreditation in the Slovak Republic.
2.0	01 November 2007	ISMS audit, clearing up matters of warranties, obligations, refunds and claims, dedicated servers for issuing qualified electronic time-stamp tokens.
2.1	21 October 2009	• ISMS audit in accordance with the Czech Republic legislation on trust services' providers requirements. • Audit of state of security of provided certification services. in accordance with the Slovak Republic legislation carried out.
3.0	01 March 2010	Issuing certificates with parameters meeting requirements of relevant legislation concerning hash functions (family SHA-2) and minimum length of RSA cryptographic key 1(2048 bits at least).
3.1	15 September 2011	List of passed inspections updated.
3.2	14 May 2012	Audit of state of security of provided certification services. in accordance with the Slovak Republic legislation carried out.
3.3	10 September 2012	Security compliance inspection added.
3.4	11 June 2013	• ISMS audit in accordance with the Czech Republic legislation on trust services' providers requirements. • Audit of state of security of provided certification services. in accordance with the Slovak Republic legislation carried out.
3.5	10 September 2013	Security compliance inspection added, revision of the document.

3.6	19 November 2014	• Audit of state of security of provided certification services. in accordance with the Slovak Republic legislation carried out. • Security compliance inspection carried out. • Inspection carried out by MV ČR in accordance with § 4 of act no. 255/2012 Coll, on Inspection (Inspection Code) and in accordance with § 9 article 2 (b) and articles 3 and 4 of act no. 227/2000 Coll., on electronic signatures.
3.7	21 December 2015	• Audit of state of security of provided certification services. in accordance with the Slovak Republic legislation carried out. • ISMS audit in accordance with the Czech Republic legislation on trust services' providers requirements carried out. • Security compliance inspection carried out.1
3.8	18 April 2017	Update caused by trust services legislation.
3.9	16 November 2017	List of certification authorities' types and list of passed audits updated.
4.0	08 August 2018	List of passed audits updated.
4.1	27 June 2019	List of passed audits updated.
4.2	14 July 2020	Revision of document, list of passed audits updated.
4.3	17 June 2021	List of passed audits updated.
4.4	02 December 2022	List of passed audits and inspections limited to only the most recent passed.
4.5	28 November 2023	List of passed audits updated.

1.2 I.CA audits and inspections

Table 2 – Passed audits and other inspections

Type	Inspector's/Auditor's Statement
Audit required by Microsoft Trusted Root Program - AUDIT STATEMENT REPORT – I.CA Root CA/RSA: **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	COMPLIANCE

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) QEVCP-w: Policy for EU qualified certificates for website authentication **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 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 2023 Certificate valid since 19 May 2023 till 18 May 2024	
Audit required by Microsoft Trusted Root Program - AUDIT STATEMENT REPORT – I.CA Root CA/RSA 05/2022: **ETSI EN 319 411-2 V2.4.1 (2021-11)** Electronic Signatures and Infrastructures (ESI); Policy and security requirements for Trust Service Providers issuing certificates; Part 2: Requirements for trust service providers issuing EU qualified certificates: a) QCP-n Policy for EU qualified certificate issued to a natural person (for electronic signatures) b) QCP-n-qscd Policy for EU qualified certificate issued to a natural person where the private key and the related certificate reside on a QSCD (for qualified electronic signatures) c) QCP-l Policy for EU qualified certificate issued to a legal person (for electronic seals) d) QCP-l-qscd Policy for EU qualified certificate issued to a legal person where the private key and the related certificate reside on a QSCD (for qualified electronic seals) **ETSI EN 319 411-1 V1.3.1 (2021-05)** Electronic Signatures and Infrastructures (ESI); Policy and security requirements for Trust Service Providers issuing certificates; Part 1: General requirements, policies:	

a) NCP: Normalized Certificate Policy NCP+: Normalized Certificate Policy requiring a secure cryptographic device Audit Statement Report dated 18 May 2023 Certificate valid since 19 May 2023 till 18 May 2024	
Audit required by eIDAS: a) Creation of qualified electronic time-stamp tokens Audit Statement Report dated 25 May 2023 Certificate valid since 26 May 2023 till 25 May 2025	COMPLIANCE

2 CONTACT INFORMATION

2.1 Head office

The address of the company 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;
- TSA support: tsa@ica.cz.

3 ELECTRONIC TIME-STAMP TYPES AND USAGE

3.1 Types of issued time-stamp tokens

I.CA issues time-stamp tokens in compliance with current trust services legislation.

Time-stamp tokens are issued by I.CA under its own policy OID= 1.3.6.1.4.1.23624.10.1.50.x.y (x.y is version.subversion of the policy), which includes all requirements of BTSP policy (Best practices Time-Stamp Policy) specified in ETSI EN 319 421 Electronic Signatures and Infrastructures (ESI); Policy and Security Requirements for Trust Service Providers issuing Time-Stamps.

Expected life time of time-stamp token depends on validity of TSU (server issuing time-stamp tokens) certificate, which is set with respect to used cryptographic algorithms following recommendations of ETSI TS 119 312 Electronic Signatures and Infrastructures (ESI); Cryptographic Suites valid at the time of time-stamp token issuance. Because of potential progression in cryptoanalysis in the period of expected time-stamp token life time, the real time stamp token life time cannot be guaranteed.

3.2 Verification procedures

Issuing time-stamp tokens by I.CA is a commercially offered service, contract of which is concluded in a manner ordinary in course of trade.

With regard to commercial base and above-standard services the requestor is identified and authenticated using one of the following ways:

- Non-qualified certificate issued by I.CA; or
- Name and password; or
- Static IP address.

I.CA reserves the right to use other ways of identification and authentication of time-stamp tokens requestors.

3.3 Time-stamping request

After successful identification and authentication requestor creates, in accordance with relevant policy, time-stamping request (normalized according to RFC 3161), This request is sent to TSA system which passes it to one of servers issuing time-stamp tokens. Time-stamping request supports SHA-256 and SHA-512 algorithms.

3.4 Time-stamp token issuance

TSA system checks formal correctness of time-stamping request and based on the result of this check the time-stamping response is created by particular TSU. If the result of the check was positive the time-stamping response contains the time-stamp token (see RFC 3161). Accuracy of time information (UTC) inserted into the time-stamp token is 1 second or less, usually 500 milliseconds or less (stated in accuracy item of time-stamp token), time information is synchronized with trustworthy time source.

Time-stamp token is sealed (advanced electronic seal) using the private key of TSU which issued the time-stamp token.

Every time-stamping response is sent by TSA system back to the requestor and also stored in TSA system repository.

Certificates if servers issuing time-stamp tokens may be obtained on web pages of První certifikační autorita, a.s., on web pages of Digital and Information Agency or in relevant TSL (Trust Service List).

3.5 Time-stamp token verification

Time-stamp token requestors are, after receiving time-stamping response, obliged to check the status of the response. In case of an error time-stamp token is not included in the response and the requestor is obliged to check up corresponding error message. In an opposite case the requestor is obliged in particular:

- To verify validity of electronic seal of issued time-stamp token and also validity of all certificates related to TSU which created this time-stamp token;
- To check whether the hash in issued time-stamp token is the same as in time-stamping request;
- To check, if items “nonce” or “reqPolicy” have been included in time-stamping request, that the values of this items in issued time-stamp token are the same.

4 RELIANCE LIMITS

There are no reliance limits concerning usability of time-stamp token issued under policy mentioned above in chapter 3.1. In general time-stamp token is a data message binding in a trustworthy manner electronic data with time information and ensuring that this data existed before this time.

5 OBLIGATIONS OF CLIENTS

Clients (requestors) are obliged to request for time-stamp tokens in accordance with relevant policy. Obligations when verifying validity of time-stamp token are mentioned in chapter 3.5.

6 OBLIGATIONS OF RELYING PARTIES

Relying party is obliged in particular to:

- Obtain relevant certificates concerning time-stamp token from secure source and verify their hashes;
- Verify validity of electronic seal of issued time-stamp token and also validity of all certificates related to TSU which created this time-stamp token;
- Verify the content of issued time-stamp token - especially the hash of time-stamped data and whether the policy under which the time-stamp token is issued meets its needs or needs of operated applications.

7 LIMITATIONS OF WARRANTY AND REPONSIBILITY

První certifikační autorita, a.s.:

- Undertakes to discharge all the obligations defined in policies and valid legislation;
- Warranties mentioned in policy for issuing qualified electronic time-stamp tokens identified in chapter 3.1 are provided all the time when client's contract is valid. If client's breach of the obligations related to referred damage has been found the claim compensation is not granted. Client must be notified about this fact and the fact must be recorded. Any other possible compensation is based on the relevant legislation and the amount of compensation may be determined by court.
- May not be held liable for any fault in the services rendered which is caused by the use of these services contrary to the terms and conditions specified in relevant service policy or if it is the result of force majeure including temporary communication failure etc.

8 APPLICABLE AGREEMENTS AND SERVICE POLICY

Relationship between client and První certifikační autorita, a.s., is (besides relevant provisions of mandatory legislation) regulated by the contract and by relevant provisions of relevant service policy.

Relationship between relying party and První certifikační autorita, a.s., is regulated by relevant provisions of relevant service policy.

To get all published information see contact address mentioned above in chapter 2.2 and other addresses in chapter 2.3.

To get additional and more detailed information concerning time-stamp tokens issuance see relevant practice statement (its public part).

9 PERSONAL DATA PROTECTION

Personal data protection in První certifikační autorita, a.s., is in compliance with the relevant legislation concerning personal data protection i.e., Act of the Czech Republic No. 110/2019 Coll., on personal data processing 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

Claims and complaints may be submitted as follows:

- By e-mail to reklamace@ica.cz;
- By registered letter to the address of I.CA head office;
- By sending a message to databox od I.CA;
- In person at the I.CA head office.

The party making the claim or complaint (time-stamp token owner or the relying party) must provide:

- Description of the fault that is as accurate as possible;
- Serial number of the product complained about;
- Suggestion how the claim/complaint should be resolved.

I.CA will decide the claim/complaint within three business days of receiving it. The decision will be communicated to the party making the claim/complaint by e-mail, data box message or registered post letter unless the parties agree to a different method.

The claim/complaint, including the fault, will be dealt with without undue delay, within thirty days of the date of the claim/complaint unless the parties agree otherwise.

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) 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;
- Act of the Czech Republic No. 297/2016 Coll., on trust services for electronic transactions;
- Act of the Slovak Republic No. 272/2016 Coll. on trust services for electronic transactions in the internal market and on amendments to certain laws (trust services act);
- 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, v.r.