První certifikační autorita, a.s.




# Root Certification Authority for TLS Certificates

# Certificate Policy

(RSA Algorithm)

Root Certification Authority for TLS Certificates Certificate Policy (RSA Algorithm) is a public document, which is the property of První certifikační autorita, a.s., and has been prepared as integral part of comprehensive security documentation. No part of this document may be reproduced without the written consent of the copyright holder.

**Version 1.005**

**Copyright © První certifikační autorita, a.s.**

# TABLE OF CONTENTS

1 Introduction ..... 11
1.1 Overview ..... 11
1.2 Document name and identification ..... 12
1.3 PKI participants ..... 12
1.3.1 Certification authorities (also as 'CA') ..... 12
1.3.2 Registration authorities (also as 'RA') ..... 12
1.3.3 Subscribers ..... 12
1.3.4 Relying parties ..... 12
1.3.5 Other participants ..... 13
1.4 Certificate usage ..... 13
1.4.1 Appropriate certificate uses ..... 13
1.4.2 Prohibited certificate uses ..... 13
1.5 Policy administration ..... 13
1.5.1 Organization administering the document ..... 13
1.5.2 Contact person ..... 13
1.5.3 Person determining CPS suitability for the policy ..... 13
1.5.4 CPS approval procedures ..... 13
1.6 Definitions and acronyms ..... 13
2 Publication and repository responsibilities ..... 20
2.1 Repositories ..... 20
2.2 Publication of certification information ..... 20
2.3 Time or frequency of publication ..... 21
2.4 Access controls on repositories ..... 21
3 Identification and authentication ..... 22
3.1 Naming ..... 22
3.1.1 Types of names ..... 22
3.1.2 Need for names to be meaningful ..... 22
3.1.3 Anonymity or pseudonymity of subscribers ..... 22
3.1.4 Rules for interpreting various name forms ..... 22
3.1.5 Uniqueness of names ..... 22
3.1.6 Recognition, authentication, and role of trademarks ..... 22
3.2 Initial identity validation ..... 22
3.2.1 Method to prove possession of private key ..... 22
3.2.2 Authentication of organization identity ..... 23

3.2.3 Authentication of individual identity ..... 23
3.2.4 Non-verified subscriber information ..... 23
3.2.5 Validation of authority ..... 23
3.2.6 Criteria for interoperation ..... 23
3.3 Identification and authentication for re-key requests ..... 24
3.3.1 Identification and authentication for routine re-key ..... 24
3.3.2 Identification and authentication for re-key after revocation ..... 24
3.4 Identification and authentication for revocation request ..... 24
4 Certificate life-cycle operational requirements ..... 25
4.1 Certificate application ..... 25
4.1.1 Who can submit a certificate application ..... 25
4.1.2 Enrolment process and responsibilities ..... 25
4.2 Certificate application processing ..... 25
4.2.1 Performing identification and authentication functions ..... 25
4.2.2 Approval or rejection of certificate applications ..... 26
4.2.3 Time to process certificate applications ..... 26
4.3 Certificate issuance ..... 26
4.3.1 CA actions during certificate issuance ..... 26
4.3.2 Notification to subscriber by the CA of issuance of certificate ..... 26
4.4 Certificate acceptance ..... 27
4.4.1 Conduct constituting certificate acceptance ..... 27
4.4.2 Publication of the certificate by the CA ..... 27
4.4.3 Notification of certificate issuance by the CA to other entities ..... 27
4.5 Key pair and certificate usage ..... 27
4.5.1 Subscriber private key and certificate usage ..... 27
4.5.2 Relying party public key and certificate usage ..... 27
4.6 Certificate renewal ..... 28
4.6.1 Circumstance for certificate renewal ..... 28
4.6.2 Who may request renewal ..... 28
4.6.3 Processing certificate renewal requests ..... 28
4.6.4 Notification of new certificate issuance to subscriber ..... 28
4.6.5 Conduct constituting acceptance of a renewal certificate ..... 28
4.6.6 Publication of the renewal certificate by the CA ..... 28
4.6.7 Notification of certificate issuance by the CA to other entities ..... 28
4.7 Certificate re-key ..... 28
4.7.1 Circumstance for certificate re-key ..... 28

4.7.2 Who may request certification of a new public key....29
4.7.3 Processing certificate re-keying requests....29
4.7.4 Notification of new certificate issuance to subscriber....29
4.7.5 Conduct constituting acceptance of a re-keyed certificate....29
4.7.6 Publication of the re-keyed certificate by the CA....29
4.7.7 Notification of certificate issuance by the CA to other entities....29
4.8 Certificate modification....29
4.8.1 Circumstance for certificate modification....29
4.8.2 Who may request certificate modification....29
4.8.3 Processing certificate modification requests....29
4.8.4 Notification of new certificate issuance to subscriber....29
4.8.5 Conduct constituting acceptance of modified certificate....30
4.8.6 Publication of the modified certificate by the CA....30
4.8.7 Notification of certificate issuance by the CA to other entities....30
4.9 Certificate revocation and suspension....30
4.9.1 Circumstances for revocation....30
4.9.2 Who can request revocation....30
4.9.3 Procedure for revocation request....30
4.9.4 Revocation request grace period....31
4.9.5 Time within which CA must process the revocation request....31
4.9.6 Revocation checking requirement for relying parties....31
4.9.7 CRL issuance frequency....31
4.9.8 Maximum latency for CRLs....31
4.9.9 On-line revocation/status checking availability....31
4.9.10 On-line revocation checking requirements....31
4.9.11 Other forms of revocation advertisements available....31
4.9.12 Special requirements for key compromise....31
4.9.13 Circumstances for suspension....31
4.9.14 Who can request suspension....32
4.9.15 Procedure for suspension request....32
4.9.16 Limits on suspension period....32
4.10 Certificate status services....32
4.10.1 Operational characteristics....32
4.10.2 Service availability....32
4.10.3 Optional features....32
4.11 End of subscription....32

4.12 Key escrow and recovery ..... 32
4.12.1 Key escrow and recovery policy and practices ..... 33
4.12.2 Session key encapsulation and recovery policy and practices ..... 33
5 Facility, management, and operational controls ..... 34
5.1 Physical controls ..... 34
5.1.1 Site location and construction ..... 34
5.1.2 Physical access ..... 34
5.1.3 Power and air-conditioning ..... 34
5.1.4 Water exposures ..... 34
5.1.5 Fire prevention and protection ..... 35
5.1.6 Media storage ..... 35
5.1.7 Waste disposal ..... 35
5.1.8 Off-site backup ..... 35
5.2 Procedural controls ..... 35
5.2.1 Trusted roles ..... 35
5.2.2 Number of persons required per task ..... 35
5.2.3 Identification and authentication for each role ..... 36
5.2.4 Roles requiring separation of duties ..... 36
5.3 Personnel controls ..... 36
5.3.1 Qualification, experience, and clearance requirements ..... 36
5.3.2 Background check procedures ..... 36
5.3.3 Training requirements ..... 36
5.3.4 Retraining frequency and requirements ..... 37
5.3.5 Job rotation frequency and sequence ..... 37
5.3.6 Sanctions for unauthorized actions ..... 37
5.3.7 Independent contractor requirements ..... 37
5.3.8 Documentation supplied to personnel ..... 37
5.4 Audit logging procedures ..... 37
5.4.1 Types of events recorded ..... 37
5.4.2 Frequency of processing log ..... 38
5.4.3 Retention period for audit log ..... 38
5.4.4 Protection of audit log ..... 38
5.4.5 Audit log backup procedures ..... 38
5.4.6 Audit collection system (internal or external) ..... 38
5.4.7 Notification to event-causing subject ..... 38
5.4.8 Vulnerability assessments ..... 39

5.5 Records archival ....39
5.5.1 Types of records archived ....39
5.5.2 Retention period for archive ....39
5.5.3 Protection of archive ....39
5.5.4 Archive backup procedures ....39
5.5.5 Requirements for time-stamping of records ....39
5.5.6 Archive collection system (internal or external) ....40
5.5.7 Procedures to obtain and verify archive information ....40
5.6 Key changeover ....40
5.7 Compromise and disaster recovery ....40
5.7.1 Incident and compromise handling procedures ....40
5.7.2 Computing resources, software, and/or data are corrupted ....40
5.7.3 Entity private key compromise procedures ....40
5.7.4 Business continuity capabilities after a disaster ....41
5.8 CA or RA termination ....41
6 Technical security controls ....42
6.1 Key pair generation and installation ....42
6.1.1 Key pair generation ....42
6.1.2 Private key delivery to subscriber ....42
6.1.3 Public key delivery to certificate issuer ....42
6.1.4 CA public key delivery to relying parties ....42
6.1.5 Key sizes ....43
6.1.6 Public key parameters generation and quality checking ....43
6.1.7 Key usage purposes (as per X.509 v3 key usage field) ....43
6.2 Private key protection and cryptographic module engineering controls ....43
6.2.1 Cryptographic module standards and controls ....43
6.2.2 Private key (n out of m) multi-person control ....43
6.2.3 Private key escrow ....43
6.2.4 Private key backup ....43
6.2.5 Private key archival ....44
6.2.6 Private key transfer into or from a cryptographic module ....44
6.2.7 Private key storage on cryptographic module ....44
6.2.8 Method of activating private key ....44
6.2.9 Method of deactivating private key ....44
6.2.10 Method of destroying private key ....45
6.2.11 Cryptographic module rating ....45

6.3 Other aspects of key pair management ..... 45
6.3.1 Public key archival ..... 45
6.3.2 Certificate operational periods and key pair usage periods ..... 45
6.4 Activation data ..... 45
6.4.1 Activation data generation and installation ..... 45
6.4.2 Activation data protection ..... 45
6.4.3 Other aspects of activation data ..... 46
6.5 Computer security controls ..... 46
6.5.1 Specific computer security technical requirements ..... 46
6.5.2 Computer security rating ..... 46
6.6 Life cycle technical controls ..... 48
6.6.1 System development controls ..... 48
6.6.2 Security management controls ..... 48
6.6.3 Life cycle security controls ..... 49
6.7 Network security controls ..... 49
6.8 Time-stamping ..... 49
7 Certificate, CRL and OCSP profiles ..... 50
7.1 Certificate profile ..... 50
7.1.1 Version number(s) ..... 51
7.1.2 Certificate extensions ..... 52
7.1.3 Algorithm object identifiers ..... 53
7.1.4 Name forms ..... 53
7.1.5 Name constraints ..... 53
7.1.6 Certificate policy object identifier ..... 53
7.1.7 Usage of Policy Constraints extension ..... 53
7.1.8 Policy qualifiers syntax and semantics ..... 53
7.1.9 Processing semantics for the critical Certificate Policies extension ..... 53
7.2 CRL profile ..... 54
7.2.1 Version number(s) ..... 54
7.2.2 CRL and CRL entry extensions ..... 54
7.3 OCSP profile ..... 55
7.3.1 Version number(s) ..... 55
7.3.2 OCSP extensions ..... 55
8 Compliance audit and other assesments ..... 56
8.1 Frequency or circumstances of assessment ..... 56
8.2 Identity/qualifications of assessor ..... 56

8.3 Assessor's relationship to assessed entity ....56
8.4 Topics covered by assessment ....56
8.5 Actions taken as a result of deficiency....56
8.6 Communication of results....57
9 Other business and legal matters....58
9.1 Fees....58
9.1.1 Certificate issuance or renewal fees ....58
9.1.2 Certificate access fees....58
9.1.3 Revocation or status information access fees....58
9.1.4 Fees for other services ....58
9.1.5 Refund policy....58
9.2 Financial responsibility ....58
9.2.1 Insurance coverage ....58
9.2.2 Other assets ....58
9.2.3 Insurance or warranty coverage for end-entities ....59
9.3 Confidentiality of business information ....59
9.3.1 Scope of confidential information....59
9.3.2 Information not within the scope of confidential information ....59
9.3.3 Responsibility to protect confidential information ....59
9.4 Privacy of personal information ....59
9.4.1 Privacy plan....59
9.4.2 Information treated as private ....59
9.4.3 Information not deemed private ....59
9.4.4 Responsibility to protect private information....60
9.4.5 Notice and consent to use private information ....60
9.4.6 Disclosure pursuant to judicial or administrative process ....60
9.4.7 Other information disclosure circumstances ....60
9.5 Intellectual property rights ....60
9.6 Representations and warranties....60
9.6.1 CA representations and warranties....60
9.6.2 RA representations and warranties....60
9.6.3 Subscriber representations and warranties....60
9.6.4 Relying parties representations and warranties ....61
9.6.5 Representations and warranties of other participants ....61
9.7 Disclaimers of warranties ....61
9.8 Limitations of liability ....61

9.9 Indemnities....61
9.10 Term and termination....61
9.10.1 Term....61
9.10.2 Termination....61
9.10.3 Effect of termination and survival....61
9.11 Individual notices and communications with participants....61
9.12 Amendments....62
9.12.1 Procedure for amendment....62
9.12.2 Notification mechanism and period....62
9.12.3 Circumstances under which OID must be changed....62
9.13 Disputes resolution provisions....62
9.14 Governing law....62
9.15 Compliance with applicable law....62
9.16 Miscellaneous provisions....62
9.16.1 Entire agreement....62
9.16.2 Assignment....62
9.16.3 Severability....63
9.16.4 Enforcement (attorneys' fees and waiver of rights)....63
9.16.5 Force majeure....63
9.17 Other provisions....63
10 Final provisions....64

**Table 1 – Document History**

| Version | Date of Release | Approved by | Comments |
|---|---|---|---|
| 1.00 | 20 April 2022 | CEO of První certifikační autorita, a.s. | First release. |
| 1.001 | 20 April 2023 | CEO of První certifikační autorita, a.s. | Annual revision of text. |
| 1.002 | 20 April 2024 | CEO of První certifikační autorita, a.s. | Annual revision, clarification of the text. |
| 1.003 | 20 April 2025 | CEO of První certifikační autorita, a.s. | List of referenced standards updated.<br>Annual revision, clarification of the text. |
| 1.004 | 20 April 2026 | CEO of První certifikační autorita, a.s. | Annual revision, clarification of the text. |

| | | | |
|---|---|---|---|
| 1.005 | 12 September 2026 | CEO of První certifikační autorita, a.s. | Signing up for CCADB Policy Compliance.<br>Clarification of CA actions during certificate issuance.<br>New organizational chart taken into account. |

# 1 INTRODUCTION

This document determines the principles applied by První certifikační autorita, a.s. (also as the I.CA), a qualified provider of trust services, when issuing certificates for subordinate certification authorities by the root certification authority for TLS certificates (also as the Service or the Certificate). The RSA cryptographic algorithm (also as the RSA) is used for the Service provided under this certificate policy (also as the CP).

The legal requirements in respect of the Service are defined in:

- 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;
- Act of the Czech Republic No. 297/2016 Coll., on trust services for electronic transactions;
- Legislation concerning personal data protection in compliance with Regulation (EU) no 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).

Note: Any reference to technical standard, norm or legislation is always a reference to that technical standard, norm or legislation or the replacing technical standard, norm or legislation. If this document is in conflict with any technical standard, norm or legislation that replaces the current technical standard, norm or legislation, a new version will be released.

## 1.1 Overview

The document **Root Certification Authority for TLS Certificates Certificate Policy (RSA Algorithm)**, also as the CP, is prepared by I.CA and deals with the issues related to life cycle processes of the Certificates and strictly follows a structure matching the scheme of current RFC 3647 standard while taking account of current technical standards and norms of the European Union and the laws of the Czech Republic pertinent to this sphere (therefore, each chapter is preserved in this document even if it is irrelevant to this sphere). The document is divided into nine basic chapters, and these are briefly introduced in the following list:

- Chapter 1 identifies this document with the allocated unique identifier, generally describes the entities and individuals taking part in the provision of this Service, and defines the acceptable use of the Certificates available to be issued;
- Chapter 2 deals with the responsibility for the publication and information or documents;
- Chapter 3 describes the processes of identification and authentication of an applicant for the issuance or revocation of a Certificate, and defines the types and contents of the names used in Certificates;
- Chapter 4 defines life cycle processes of Certificates i.e., application, the issuance of the Certificate, certificate revocation request, the revocation of the Certificate, the services related to the check of Certificate status, termination of the provision of the Service, etc.;
- Chapter 5 covers physical, procedural and personal security, including the definition of the set of events subject to logging, the keeping of these records and responses to emergency and compromising situations;

- Chapter 6 focuses on the technical security of the type of generating public and private keys, protection of private keys, including the computer and network protection;
- Chapter 7 defines the profile of issued Certificates and CRL;
- Chapter 8 focuses on assessing the Service delivered;
- Chapter 9 deals with commercial and legal aspects.

More detail on the fulfilment of the attributes and extensions of the certificates issued under this policy and the administration thereof can be provided in the relevant certification practice statement (also as the CPS).

Note: This is English translation of CP. Czech version always takes precedence. I.CA attests that the translation is not materially different to the original.

## 1.2 Document name and identification

| | |
|---|---|
| Document's title: | Root Certification Authority for TLS Certificates Certificate Policy (the RSA Algorithm), version 1.005 |
| Policy OID: | 1.3.6.1.4.1.23624.10.1.11.1.0 |

## 1.3 PKI participants

### 1.3.1 Certification authorities (also as 'CA')

The root certification authority (also as the Authority) issues certificates for the certification authorities subordinate to the Authority in a two-tier certification authority structure, in accordance with current legislation and technical and other standards.

As the Authority is offline, it has no live connection to the external network at any time. The Authority's physical information system is comprised of dedicated computers.

### 1.3.2 Registration authorities (also as 'RA')

A special (non-public) registration authority owned by I.CA participates in the life cycle processes of the Authority-issued Certificates.

### 1.3.3 Subscribers

The subscriber of the Certificate to be issued is První certifikační autorita, a.s., which applied for the Certificate for itself and is identified in the Certificate as subject (holder of the private key connected with the public key specified in this Certificate).

### 1.3.4 Relying parties

Any entity relying in their operations on the Certificates issued under this CP is a relying party.

### 1.3.5 Other participants

Other participating parties are investigative, prosecuting and judging bodies, supervisory bodies and other bodies recognised as such by current legislation.

## 1.4 Certificate usage

### 1.4.1 Appropriate certificate uses

Any Certificate issued under this CP may solely be used for verifying electronic seals of issued Certificates and certificate revocation lists (CRLs).

### 1.4.2 Prohibited certificate uses

Certificates issued under this CP may not be used contrary to the acceptable use described in 1.4.1 or contrary to law.

## 1.5 Policy administration

### 1.5.1 Organization administering the document

This CP and its CPS are administered by První certifikační autorita, a.s.

### 1.5.2 Contact person

The contact person of První certifikační autorita, a.s., in respect of this CP and its CPS is CEO of I.CA. The contact information given in chapter 2.2 applies.

### 1.5.3 Person determining CPS suitability for the policy

CEO of První certifikační autorita, a.s., is the sole person responsible for making decisions about compliance of the procedures of První certifikační autorita, a.s., as set out in CPS with this CP.

### 1.5.4 CPS approval procedures

If it is necessary to make changes to a CPS to create a new version thereof, CEO of První certifikační autorita, a.s., appoints a person authorized to perform such changes. No new CPS version may take force unless it has been approved by CEO of První certifikační autorita, a.s.

## 1.6 Definitions and acronyms

**Table 2 – Definitions**

| Term | Explanation |
|---|---|
| CA/Browser Forum | organization, consensual association of certification authorities |

| | |
|---|---|
| Classified Information Protection Act | the Czech Republic's Act No. 412/2005 Coll., regulating classified information protection and security competence, as amended |
| contracting partner | provider of services contracted by I.CA for certification services or parts thereof – usually, it is a contracted RA |
| domain name | node name in domain name system |
| domain name registrant/ registrant | sometimes referred to as a domain name owner, but more accurately a person or entity registered by a domain registrar as having the right to oversee the use of a domain name, a natural or legal person listed as a "Registrant" by WHOIS or a domain registrar |
| domain name registrar/ registrar | person or entity that registers domain names by mandate or with consent:<br>▪ Internet Corporation for Assigning Names and Numbers (ICANN) - Administrator of DNS Root Space;<br>▪ TLD administrator (e.g. .com) or ccTLD (e.g. .CZ, national administrator) |
| domain name space | a set of all possible domain names that are subordinate to one node in the domain name system |
| electronic seal | advanced electronic seal or recognized electronic seal or qualified electronic seal under trust services legislation |
| electronic signature | advanced electronic signature or recognized electronic signature or qualified electronic signature under trust services legislation |
| GET method | standard preferred method for sending http requests to OCSP responder via http, the method allows caching (the second method is POST) |
| hash function | transformation which receives, as an input, a string of characters of arbitrary length, and the result is a string of characters of fixed length (hash) |
| key pair | private key and corresponding public key |
| Labour Code | the Czech Republic's Act No. 262/2006 Coll., Labour Code, as amended |
| OCSP responder | server using the OCSP protocol to provide data on public key certificate status |
| OCSP stapling | way of minimizing queries for OCSP Responder, RFC 4366 - TLS Extensions; allows the TLS server to return the once-received answer to the question about certificate status from the OCSP (during its validity) to all end users accessing the TLS server |
| phishing | in an electronic communication attempt to obtain sensitive information (usernames, passwords, and credit card details) for malicious reasons |
| private key | unique data to create electronic signature / seal |

| | |
|---|---|
| public key | unique data to verify electronic signature / seal |
| PSP registrar | authority responsible for approving or rejecting authorization of payment services providers in their state, usually National Bank, in ETSI TS 119 495 called NCA (National Competent Authority) |
| qualified certificate for electronic signature or for electronic seal or for website authentication | certificate defined by trust services legislation |
| qualified signature / seal creation device | device meeting the requirements of eIDAS, annex II, intended for electronic signature / seal creation |
| relying party | party relying on a certificate in its operations |
| root CA | certification authority which issues certificates to subordinate certification authorities |
| secure cryptographic device | device on which the private key is stored |
| softcard | software emulation of smartcard for access to private key stored in HSM |
| SSL certificate | certificate for identification and encryption within SSL/TLS protocol communication |
| subordinate CA | CA issuing certificates to end users |
| supervisory body | the body supervising qualified trust services providers |
| trust service / qualified trust service | trust service / qualified trust service defined by eIDAS |
| trust services legislation | current legislation on trust services |
| TWINS | commercial product of I.CA consisting of:<br>▪ qualified certificate for electronic signature;<br>▪ non-qualified certificate which issuance is based only on contractual relationship between I.CA and end-user |
| two-factor authentication | authentication employing two of three factors – I know something (the password), I have something (a smartcard or a hardware token) or I am something (fingerprint, retina or iris reading) |
| written contract | text of the contract in electronic or paper form |

**Table 3 – Acronyms**

| Acronym | Explanation |
|---|---|
| ARC | Alarm Receiving Centre |
| ASCII | American Standard Code for Information Interchange, table containing binary codes of English alphabets, numbers and other common symbols |
| BIH | Bureau International de l'Heure – The International Time Bureau |

| | |
|---|---|
| bit | from English *binary digit* – a binary system digit – the fundamental and the smallest unit of information in digital technologies |
| BRG | document "Baseline Requirements for the Issuance and Management of Publicly-Trusted TLS Server Certificates" published by CA/Browser Forum |
| CA | certification authority |
| CAA | DNS Resource Record - see RFC 6844 |
| CCADB | Repository of information about Certification Authorities whose root and intermediate certificates are included within the products and services of several Root Store Operators |
| ccTLD | country code TLD, national top-level domain, usually user for countries, sovereign states or dependent territories, ASCII ccTLD identifiers are two letters long |
| CEN | European Committee for Standardization, an association of national standardization bodies |
| CEO | Chief Executive Officer |
| COO | Chief Operating Officer |
| CP | certificate policy |
| CPS | certification practice statement |
| CR | Czech Republic |
| CRL | Certificate Revocation List – the list of revoked certificates, which are not held as valid any longer |
| CT | Certificate Transparency, the system to mitigate misissuance of certificate based on adding new certificate (or rather precertificate) to public logs making possible to detect the misissuance (especially fraudulent getting the certificate by other than authorized applicant) |
| ČSN | Czech Technical Norm |
| DER, PEM | methods of certificate encoding (certificate formats) |
| DV | Domain Validation, SSL certificate type |
| DNS | Domain Name System, a hierarchical decentralized naming system implemented by DNS servers which are exchanging information via DNS protocol to translate domain names to the numerical IP addresses |
| EBA | European Banking Association |
| EC | Elliptic Curve |
| ECC | Elliptic Curve Cryptography |
| eIDAS | REGULATION (EU) no 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 |
| EN | European Standard, a type of ETSI standard |
| ESI | Electronic Signatures and Infrastructures |

| | |
|---|---|
| ETSI | European Telecommunications Standards Institute, a European standardization institute for information and communication technologies |
| EU | European Union |
| EV | Extended Validation, type of SSL certificate or certificate intended for websites authentication |
| EVCG | document "Guidelines For The Issuance And Management Of Extended Validation Certificates" published by CA/Browser Forum |
| EVCP | Extended Validation Certificate Policy, type of certificate policy |
| FAS | Fire Alarm System |
| FIPS | Federal Information Processing Standard, standards for information technologies for U.S. non-military state organizations |
| FQDN | Fully Qualified Domain Name, domain name that specifies all domain levels in Internet domain name system |
| GDPR | General Data Protection Regulation, 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) |
| gTLD | generic TLD, top level domain (e.g. .org for non-profit organizations) |
| html | Hypertext Markup Language, markup language for creating hypertext documents |
| http | Hypertext Transfer Protocol, protocol for exchanging html documents |
| https | Hypertext Transfer Protocol, protocol for secure exchanging of html documents |
| I.CA | První certifikační autorita, a.s. |
| IAS | Intrusion Alarm System |
| ICA_OID | OID belonging to OID space allocated to I.CA |
| ICANN | Internet Corporation for Assigned Names and Numbers, organization which among others assigns and administrates domain names and IP addresses |
| IEC | International Electrotechnical Commission, the global organization publishing standards for electrical and electronic engineering, communication technologies and related industries |
| IP | Internet Protocol, principal communications protocol in the Internet protocol suite for relaying packets across network and routing used in the Internet |
| IPS | Intrusion Prevention System |
| ISMS | Information Security Management System |
| ISO | International Organization for Standardization, an international organization of national standardization organizations; designation of standards |

| | |
|---|---|
| IT | Information Technology |
| ITU | International Telecommunication Union |
| ITU-T | Telecommunication Standardization Sector of ITU |
| MPSV | Ministry of Labor and Social Affairs of the Czech Republic |
| NCA | National Competent Authority - authority responsible for approving or rejecting authorization of payment services providers and assigning PSP numbers to them in particular state; see also PSP registrar above |
| NCP | Normalized Certificate Policy, non-qualified certificates certificate policy, qualitatively the same as certificate policy for issuing qualified certificates |
| NCP+ | Extended Normalized Certificate Policy, NCP certificate policy requiring a secure cryptographic device |
| OCSP | Online Certificate Status Protocol, the protocol to identify public key certificate status |
| OID | Object Identifier |
| OSVČ | self-employed person |
| OV | Organization Validation, SSL certificate type |
| PDCA | Plan-Do-Check-Act, Deming cycle, management method for control and continuous improvement |
| PDS | PKI Disclosure Statement |
| PKCS | Public Key Cryptography Standards, designation for a group of standards for public key cryptography |
| PKI | Public Key Infrastructure |
| PSD | Payment Services Directive, DIRECTIVE 2007/64/EC OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL on payment services in the internal market |
| PSD2 | DIRECTIVE (EU) 2015/2366 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL, superseding PSD and coming into effect January 13th 2018 |
| PSP | Payment Service Provider |
| PSS | Probabilistic Signature Scheme, electronic signature schema developed by M. Bellar and P. Rogaway and standardized as part of PKCS#1 v2.1 |
| PTC | Publicly-Trusted Certificate |
| PUB | Publication, FIPS standard designation |
| QSCD | Qualified Electronic Signature/Seal Creation Device (defined by eIDAS) |
| QWAC | Qualified Website Authentication Certificate |
| RA | registration authority |
| RFC | Request for Comments, designation for a range of standards and other documents describing web protocols, systems, etc. |
| RSA | signing and encrypting public key cipher (acronym from the names of the original authors - Rivest, Shamir and Adleman) |

| | |
|---|---|
| RTS | COMMISSION DELEGATED REGULATION (EU) 2018/389 of 27 November 2017 supplementing Directive (EU) 2015/2366 of the European Parliament and of the Council with regard to regulatory technical standards for strong customer authentication and common and secure open standards of communication |
| SCT | Signed Certificate Timestamp, signed timestamp from relevant CT log which confirms adding the precertificate |
| sha, SHA | type of hash function |
| SSL | Secure Sockets Layer, communication protocol, layer inserted between transport layer and application layer, providing securing of communication via encryption and authentication of communicating parties |
| TLD | Top Level Domain, top-level Internet domain, in domain name the top-level domain is placed at the end |
| TLS | Transport Layer Security, communication protocol superseding SSL |
| TS | Technical Specification, type of ETSI standard |
| TSA | Time-Stamping Authority |
| TSS | Time-Stamp Server |
| TSU | Time-Stamp Unit |
| UPN | User Principal Name, username based on RFC 822 |
| UPS | Uninterruptible Power Supply/Source |
| URI | Uniform Resource Identifier, defined-structure text string for accurate specification of a source of information |
| UTC | Coordinated Universal Time, the standard adopted on 1 January 1972 for the global coordinated time – Bureau International de l'Heure (BIH) plays the role of the 'official keeper' of the atomic time for the whole world |
| WHOIS | database including domain name registrant technical, billing and administrative contact information |
| ZOOÚ | current personal data protection legislation |

# 2 PUBLICATION AND REPOSITORY RESPONSIBILITIES

## 2.1 Repositories

První certifikační autorita, a.s., sets up and operates repositories of both public and non-public information.

## 2.2 Publication of certification information

The basic addresses (also as the Information Addresses) for obtaining information about První certifikační autorita, a.s., and the links to find out more information are as follows:

- Registered office:

  První certifikační autorita, a.s.

  Podvinný mlýn 2178/6

  190 00 Praha 9

  Czech Republic
- Website: http://www.ica.cz;
- Registered offices of the registration authorities.

Electronic address for contact between general public and I.CA: info@ica.cz, data box of I.CA ID is a69fvfb.

The aforesaid website provides information about:

- Certificates of certification authorities and time-stamping authorities;
- Public certificates of end users – the following information is published (and more information can be obtained from the certificate):
  - Certificate number;
  - Content of commonName;
  - Valid from date (specifying the hour, minute and second);
  - Link to where the certificate can be obtained in the specified format (DER, PEM, TXT);
- Certificate revocation list (CRL) – the following information is published (and more information can be obtained from the CRL):
  - Date of CRL release;
  - CRL number;
  - Link to where the CRL can be obtained in the specified format (DER, PEM, TXT);
- Certification and other policies, practice statements and other public information.

The Certification Authority issuing the Certificates adheres the requirements of the current version of the CCADB policy listed at https://www.ccadb.org/policy.

The Certification Authority issuing the Certificates complies with the requirements of the current version of the CCADB policy listed at https://www.ccadb.org/policy.

Http and https are the permitted protocols for access to public information. I.CA may terminate or suspend access to some information without cause.

Any revocation of the Certificate because of suspected or actual compromise of a given private key will be announced by I.CA on its web Information Address and in Hospodářské noviny or Mladá fronta Dnes, daily newspapers with national distribution.

The Certification Authority issuing the Certificates adheres the requirements of the current version of the CCADB policy listed at https://www.ccadb.org/policy.

## 2.3 Time or frequency of publication

I.CA publishes information as follows:

- Certificate policy – after a new version is approved and issued;
- Certification practice statement – immediately;
- List of the certificates issued – updated every time a new certificate subject to publication is issued;
- Certificate revocation list (CRL) – see 4.9.7;
- Information about Certificate revocation with the reason of revocation – immediately;
- Other public information – no specific time limit, the general rule is that this information must correspond to the current state of the services provided.

## 2.4 Access controls on repositories

All public information is made available by I.CA free of charge without any restrictions.

Non-public information is available only to authorized employees of I.CA or the parties specified by the relevant legislation. Access to such information is governed by the rules defined in internal documentation.

# 3 IDENTIFICATION AND AUTHENTICATION

## 3.1 Naming

### 3.1.1 Types of names

All names are construed in accordance with current technical and other standards.

### 3.1.2 Need for names to be meaningful

For a Certificate to be issued, all names which can be validated given in the field subject must carry a meaning. See chapter 7 for the attributes supported for this field.

### 3.1.3 Anonymity or pseudonymity of subscribers

The Certificates issued under this CP do not support neither anonymity nor pseudonymity.

### 3.1.4 Rules for interpreting various name forms

The data specified in a Certificate application (format PKCS#10) are transferred to subject field attributes of the Certificate in the form they are specified in the application.

### 3.1.5 Uniqueness of names

The Authority guarantees the uniqueness of a Certificate's subject and issuer fields.

### 3.1.6 Recognition, authentication, and role of trademarks

Any Certificate issued under this CP may only contain trademarks which are property of První certifikační autorita, a.s.

## 3.2 Initial identity validation

The following chapters specify the rules for the authentication of I.CA when applying for a Certificate and the identity authentication of I.CA's representative.

### 3.2.1 Method to prove possession of private key

The ownership of the private key matching the public key in the certificate application must be proved by submitting the application in the PKCS#10 format. The application is provided with electronic seal using this private key whereby the private key holder provides evidence that he is the holder of the private key when the electronic seal is created.

### 3.2.2 Authentication of organization identity

This requires the submission of the original or certified copy of the entry in the Commercial Register or in another register specified by law, of a trade license, of a deed of incorporation, or of another document of the same legal force.

This document must contain full business name, identification number (if any), registered office, the name(s) of the person(s) authorized to act on behalf of the legal entity (authorized representatives).

### 3.2.3 Authentication of individual identity

This chapter describes the identity authentication procedure of the person representing I.CA applying for a Certificate.

The I.CA representing person's identity authentication procedure requires two documents, primary and secondary one, that show the data specified further in this chapter.

Valid personal identity card or passport must be used as the primary personal document for the citizens of the Czech Republic. Valid passport is the primary personal document for foreigners; citizens of EU member countries may use their valid personal identity card they use in their country as the proof of their identity.

The following data are authenticated in this document:

- Full civil name;
- Date and place of birth or the birth certification number if shown in the primary document;
- Number of the primary personal document;
- Permanent address (if shown in the primary document).

The secondary document must contain a unique identification, such as birth certification number or personal identity card number, matching it to the primary document and must show at least one of these attributes:

- Date of birth (or birth certification number if specified);
- Permanent address;
- Photograph of the face.

The secondary personal document data must be identical to those in the primary personal document.

### 3.2.4 Non-verified subscriber information

All information must be duly verified.

### 3.2.5 Validation of authority

Not applicable for this document.

### 3.2.6 Criteria for interoperation

Any collaboration between První certifikační autorita, a.s., and other trust service providers is always based on a contract in writing.

## 3.3 Identification and authentication for re-key requests

### 3.3.1 Identification and authentication for routine re-key

A new Certificate with a new public key needs to be issued. The same requirements as those in the initial identity validation apply.

### 3.3.2 Identification and authentication for re-key after revocation

I.CA does not support re-keying of revoked Certificates. The only way is to obtain a new Certificate with a new public key. The same requirements as those in the initial identity validation apply.

## 3.4 Identification and authentication for revocation request

The entities authorized to request for Certificate revocation are listed in 4.9.2.

Every certificate revocation request must be made in writing and signed by CEO of I.CA or by a member of the board authorized by him. His identity must be duly authenticated with their primary personal documents.

The data required for certificate revocation request are listed in 4.9.3.

# 4 CERTIFICATE LIFE-CYCLE OPERATIONAL REQUIREMENTS

## 4.1 Certificate application

### 4.1.1 Who can submit a certificate application

Issuance of the Certificate may be applied by CEO of I.CA or by a member of the board authorized by him.

### 4.1.2 Enrolment process and responsibilities

The written application for the Certificate is submitted to the management of První certifikační autorita, a.s., by Certificate applicant and must include the business name and OID of this certificate policy and the required CA name (commonName). The application must be signed by the applicant.

I.CA's representative applying for Certificate issuance is required to do the following, among others, things:

- Get acquainted with this CP and observe it;
- Provide true and complete information for the issuance of the Certificate;
- Check whether the data specified in the certificate application and the Certificate issued are correct and correspond to the required data;
- Choose a suitable Certificate revocation password (the minimum/maximum password length is 4/32 characters; permitted characters: 0..9, A..Z, a..z).

The Service provider is required to do the following, among other things:

- During the Certificate issuance process, check with RA all the data specified in the application against the documents submitted;
- Issue a Certificate that contains materially correct data on the basis of the information available to the Service provider as at the issuance of the Certificate;
- Publish public information in accordance with 2.2;
- Publish the Certificates issued;
- Provide any Service-related activity in accordance with trust services legislation, the relevant technical standards, this CP, the relevant CPS, the System Security Policy – Trustworthy Systems and the operational documentation.

## 4.2 Certificate application processing

### 4.2.1 Performing identification and authentication functions

Certificate issuance identification and authentication are performed pursuant to 3.2.2 and 3.2.3.

### 4.2.2 Approval or rejection of certificate applications

The management of První certifikační autorita, a.s., considers the application and approves or dismisses the issuance of the Certificate. The result is documented.

### 4.2.3 Time to process certificate applications

The written certificate application must be handled within five business days after the date the application is submitted to the company management.

I.CA must issue the Certificate when Certificate issuance is granted. The Certificate is issued within units of minutes.

## 4.3 Certificate issuance

### 4.3.1 CA actions during certificate issuance

When issuing the Certificate, the RA employees do the following:

- checks described in chapter 4.2.1;
- visual check as to conformity of the data in the Certificate application (the PKCS#10 structure);
- visual check as to the formal correctness of data.

Prove of private key ownership, checking the supported hash function in the certificate application (not weaker than sha-256), the competence check and the formal data correctness check are conducted both by the software on RA employees' workstations and that on the CA system core. If any of these checks gives a fail result, the Certificate issuance procedure is terminated.

After uploading and verifying the certificate application, the root CA operator issues a deliberate, direct command to sign the certificate by the root CA. Prior to this, another person or persons acting in a trusted role must activate the root CA's private key before the signature is generated (see also Section 6.2.2) and deactivate it again after the certificate has been issued.

Prior to this, another person or persons acting in a trusted role must activate the root CA's private key before the signature is generated (see also Section 6.2.2) and deactivate it again after the certificate has been issued.

Before issuing the command to perform the Certificate signing operation by root CA, the person (or persons) in the trusted role must activate the Root CA private key (see also Section 6.2.2).

After uploading and verifying the Certificate request, the root RA operator issues an explicit, direct command to sign the certificate by the Root CA.

After the Certificate is issued, the person (or persons) in the trusted role must deactivate the root CA's private key.

### 4.3.2 Notification to subscriber by the CA of issuance of certificate

During the Certificate issuance process, the subscriber, or the representative of I.CA applying for the Certificate, receives information from the RA employee and the Certificate is sent to the contact e-mail provided during enrolment as mandatory data.

## 4.4 Certificate acceptance

### 4.4.1 Conduct constituting certificate acceptance

If the Certificate issuance requirements are met, representative of I.CA must accept the Certificate. The only way to refuse to take over the Certificate is to request for the Certificate's revocation in accordance with this CP.

### 4.4.2 Publication of the certificate by the CA

Certificates issued under this CP are published in the manner pursuant to 2.2.

The root certification authority's certificate and the subordinate certification authorities' certificates related to trust services are handed over to the supervisory body.

### 4.4.3 Notification of certificate issuance by the CA to other entities

Chapter 4.4.2 applies.

## 4.5 Key pair and certificate usage

### 4.5.1 Subscriber private key and certificate usage

Subscriber must, among other things:

- Observe all relevant provisions of the contract of the provision of the Services;
- Use the private key and the corresponding Certificate issued under a specific CP solely for the purposes defined in this CP and trust services legislation;
- Handle the private key corresponding to the public key contained in the Certificate issued under a specific CP in a manner as to prevent any unauthorized use of the private key;
- Notify immediately the Service provider of everything that leads to the Certificate's revocation, in particular of:
  - Suspected abuse of the private key; and
  - Invalidity or inaccuracy of Certificate's attributes;

  in this case apply for the Certificate's revocation and stop using the pertinent private key.

### 4.5.2 Relying party public key and certificate usage

Relying parties must, among others:

- Obtain the Certificates of certification authorities from a secure source (www.ica.cz, RA, relevant trust list) and verify checksum and validity of these Certificates;
- Perform any action necessary for them to check that the Certificates have not been revoked.

## 4.6 Certificate renewal

Certificate renewal under this CP means the issuance of a new Certificate for still valid Certificate or for revoked Certificate, or for expired Certificate without changing the public key or any other information in the Certificate.

Certificate renewal is not provided.

### 4.6.1 Circumstance for certificate renewal

See 4.6.

### 4.6.2 Who may request renewal

See 4.6.

### 4.6.3 Processing certificate renewal requests

See 4.6.

### 4.6.4 Notification of new certificate issuance to subscriber

See 4.6.

### 4.6.5 Conduct constituting acceptance of a renewal certificate

See 4.6.

### 4.6.6 Publication of the renewal certificate by the CA

See 4.6.

### 4.6.7 Notification of certificate issuance by the CA to other entities

See 4.6.

## 4.7 Certificate re-key

Certificate re-key under this CP means the issuance of a new Certificate (subsequent Certificate) with a different public key but with identical content of the attributes under the subject field of the Certificate which is requested to be re-keyed.

Certificate re-key is not provided.

### 4.7.1 Circumstance for certificate re-key

See 4.7.

### 4.7.2 Who may request certification of a new public key

See 4.7.

### 4.7.3 Processing certificate re-keying requests

See 4.7.

### 4.7.4 Notification of new certificate issuance to subscriber

See 4.7.

### 4.7.5 Conduct constituting acceptance of a re-keyed certificate

See 4.7.

### 4.7.6 Publication of the re-keyed certificate by the CA

See 4.7.

### 4.7.7 Notification of certificate issuance by the CA to other entities

See 4.7.

## 4.8 Certificate modification

Certificate modification under this CP means the issuance of a new Certificate with the same public key but with at least one change of attributes in subject field concerning the subscriber or with removed field or with added field, content of which must be validated.

Certificate modification is not provided.

### 4.8.1 Circumstance for certificate modification

See 4.8.

### 4.8.2 Who may request certificate modification

See 4.8.

### 4.8.3 Processing certificate modification requests

See 4.8.

### 4.8.4 Notification of new certificate issuance to subscriber

See 4.8.

### 4.8.5 Conduct constituting acceptance of modified certificate

See 4.8.

### 4.8.6 Publication of the modified certificate by the CA

See 4.8.

### 4.8.7 Notification of certificate issuance by the CA to other entities

See 4.8.

## 4.9 Certificate revocation and suspension

Certificate suspension is not provided by I.CA.

### 4.9.1 Circumstances for revocation

Certificate must be revoked as a result of the following, among other things:

- If the private key corresponding to the Certificate's public key is compromised or reasonably suspected to have been compromised;
- A Certificate's technical content or format is a non-acceptable risk, such as the given cryptographic/signing algorithm or the key length;
- In any event specified in trust services legislation or the relevant technical and other standards, such as invalid Certificate data.

### 4.9.2 Who can request revocation

Certificate revocation request may be submitted by:

- Subscriber (authorized requestor is in this case CEO of I.CA or a member of the board authorized by him); or
- The supervisory body or other entities specified in trust services legislation, as may be the case.

### 4.9.3 Procedure for revocation request

Certificate is revoked under personal participation of CEO of I.CA or a member of the board authorized by him.

Any written certificate revocation request must include the Certificate's serial number in the decimal or hexadecimal format (introduced by the string '0x'), the name of the Authority which issued the Certificate, the full name of the person authorized to request for the Certificate's revocation, and the Certificate revocation password. If the person authorized to request for revocation does not know the Certificate revocation password, s/he must explicitly state this in the written application, along with the number of the primary personal document submitted in the certificate application procedure or the number of the new primary personal document if the original document has been replaced. The person must use this primary personal document to prove their identity.

### 4.9.4 Revocation request grace period

Certificate revocation request must be made immediately.

### 4.9.5 Time within which CA must process the revocation request

If the request meets the requirements, the employee in charge immediately revokes the Certificate in the CA's system, and the date and time the request is processed are the date and time of the Certificate's revocation. The CRL containing the serial number of the revoked Certificate must be issued immediately after that Certificate's revocation.

### 4.9.6 Revocation checking requirement for relying parties

Relying parties must take the course of action pursuant to 4.5.2.

### 4.9.7 CRL issuance frequency

The list of the revoked Certificates is issued after every Certificate revocation, and also in regular intervals no longer than one year after issuing previous CRL.

### 4.9.8 Maximum latency for CRLs

CRL is released immediately after the issuance, conditions described in chapters 4.9.5 are 4.9.7 always observed.

### 4.9.9 On-line revocation/status checking availability

On-line revocation/status checking using the OCSP protocol is a service available to the general public. Every subordinate certification authority certificate issued under this CP includes a link to the pertinent (authorized) OCSP responder.

OCSP responses comply with the RFC 6960 and RFC 5019 standards. The OCSP responder's certificate includes an id-pkix-ocsp-nocheck extension as defined in RFC 6960.

### 4.9.10 On-line revocation checking requirements

See 4.9.9.

### 4.9.11 Other forms of revocation advertisements available

Not applicable for this document; no other certificate revocation notification service is provided.

### 4.9.12 Special requirements for key compromise

The Certificate revocation procedure in the event of private key compromise is not different from the Certificate revocation procedure described above.

### 4.9.13 Circumstances for suspension

Not applicable for this document; Certificate suspension is not provided.

### 4.9.14 Who can request suspension

Not applicable for this document; Certificate suspension is not provided.

### 4.9.15 Procedure for suspension request

Not applicable for this document; Certificate suspension is not provided.

### 4.9.16 Limits on suspension period

Not applicable for this document; Certificate suspension is not provided.

## 4.10 Certificate status services

### 4.10.1 Operational characteristics

Lists of the public Certificates issued by the Authority are provided as published information; certificate revocation lists are provided as published information and by specifying the CRL distribution points in the certificates issued by the Authority.

The fact that the Authority provides Certificate status information as OCSP is specified in the Certificates issued by it.

### 4.10.2 Service availability

The Authority guarantees round-the-clock (24/7) availability and integrity of the list of the Certificates it has issued and the list of revoked certificates (CRLs), plus the availability of the OCSP service.

Response time to revocation request using CRL or OCSP is normally less than 10 seconds.

Revocation records on CRL or in OCSP response are kept at least to the end of Certificate's validity period.

### 4.10.3 Optional features

Not applicable for this document; no other Certificate status check characteristics are provided.

## 4.11 End of subscription

The certificate issuance contract expires when the last certificate issued under this contract expires.

## 4.12 Key escrow and recovery

Not applicable for this document; key escrow and recovery service is not provided.

### 4.12.1 Key escrow and recovery policy and practices

See 4.12.

### 4.12.2 Session key encapsulation and recovery policy and practices

See 4.12.

# 5 FACILITY, MANAGEMENT, AND OPERATIONAL CONTROLS

The management, control and operating procedures primarily deal with:

- Trustworthy systems supporting trust services;
- All processes supporting trust services.

The management, control and operating procedures are addressed in the fundamental documents Corporate Security Policy, System Security Policy – Trustworthy Systems, Certification Practice Statement, Business Continuity Plan and Recovery Plan as well as the more detailed internal documentation. These documents take account of the results of periodic risk analyses.

## 5.1 Physical controls

### 5.1.1 Site location and construction

The operating site buildings are situated in geographically different locations, which are also different from the site of the company headquarters, the business and development sites, the registration authority sites and the points of sale.

The trustworthy systems designated to support trust services are situated on reserved premises of operating sites. These premises are secured in a manner similar to that required by the Classified Information Protection Act for the 'Confidential' category secure areas.

### 5.1.2 Physical access

See the internal documentation for the respective requirements as to physical access to the reserved premises (protected with mechanical and electronic features) of operating sites. Buildings are protected with intrusion alarm system (IAS), alarm receiving centre (ARC) and as may be the case, a special system to monitor movement of persons and vehicles.

### 5.1.3 Power and air-conditioning

The premises housing the trustworthy systems supporting trust services have active air-conditioning of adequate capacity, which keeps the temperature at 20°C ± 5°C all year round. The supply of electricity is backed up with a UPS (Uninterruptible Power Supply) and a diesel unit.

### 5.1.4 Water exposures

The trustworthy systems supporting trust services are so located as to ensure they cannot be flooded by a 100-year flood. Where it is relevant operating sites have water ingress sensors to detect heating water leakage or rainfall leakage through the roof (as a result of heavy rains).

### 5.1.5 Fire prevention and protection

The buildings of the operating sites and the information storage sites have electronic fire alarm system (FAS). Fireproof insulation is installed in the entrance doors to the restricted areas in which the trustworthy systems supporting trust services are situated, and fire extinguishers are fitted in these areas.

### 5.1.6 Media storage

Archive media containing operational backups and electronic records are stored in metal boxes or safes. Copies are kept at a site geographically different from the site of the operating office where the records originated.

Any paper media required to be kept are stored in a site geographically different from the site of the operating office where the records originated.

### 5.1.7 Waste disposal

Any paper office waste is shredded before it leaves I.CA operating sites.

### 5.1.8 Off-site backup

The copies of operating and working backups are stored in a place designated by COO of I.CA and described in internal documentation.

## 5.2 Procedural controls

### 5.2.1 Trusted roles

Trusted roles are defined for selected activities carried out at I.CA. The trusted role employee appointment procedure, the trusted roles operation and their responsibilities are defined in internal documentation.

I.CA employee appointed to a trusted role may not be in a conflict of interests that could compromise the impartiality of operations of I.CA.

### 5.2.2 Number of persons required per task

Jobs are defined for the processes related to the key pairs of certification authorities and these jobs must be performed with more than one single person attending. These jobs include:

- Initialization of cryptographic module;
- Generating key pairs of all certification authorities;
- Destroying private keys of all certification authorities;
- Backup and restore of private keys of all certification authorities;
- Activation and deactivation of private keys of all certification authorities.

The number of attending persons is not defined for other jobs, but all persons must be authorized persons.

### 5.2.3 Identification and authentication for each role

Each role's employees are assigned identification (name and certificate) and authentication (password and private key) data for those components which are necessary for their jobs.

Selected jobs require two-factor authentication by trusted role employees.

### 5.2.4 Roles requiring separation of duties

The roles requiring separation of duties (and the roles' job descriptions) are described in internal documentation.

## 5.3 Personnel controls

### 5.3.1 Qualification, experience, and clearance requirements

I.CA's trusted role employees are selected accepted using the following criteria:

- Clean criminal record – statement of criminal conviction records or affirmation is required;
- Bachelor's or master's degree in an accredited university program and ICT job experience of three years or longer, or secondary education and ICT job experience of five years or longer, of which at least one-year job experience in the provision of trust services;
- Knowledge in public key infrastructure and information security.

Any other I.CA employee taking part in providing trust services is accepted using the following criteria:

- Bachelor's or master's degree in an accredited university program, or secondary education;
- Basic orientation in public key infrastructure and information security.

Managers must have job experience or technical training in respect of the trustworthiness of trust services, the knowledge of security procedures with security responsibility, and experience in information security and risk assessment.

### 5.3.2 Background check procedures

The sources of information about all employees of I.CA are:

- The employees themselves;
- Persons familiar with a particular employee;
- Public sources of information.

Initial information is provided by employees at job interviews, and this information is updated at periodic appraisal interviews with the manager during employment.

### 5.3.3 Training requirements

I.CA employees receive technical training in the use of specific software and specialised devices. The training takes the form of self-study combined with guidance from a trained

employee. The training covers information security, personal protection data and other relevant topics.

### 5.3.4 Retraining frequency and requirements

I.CA employees are provided with the current developments in their spheres of interest two times every 12 months.

Training in the processes related to RA operations is held for RA employees at least once in every three years.

### 5.3.5 Job rotation frequency and sequence

I.CA employees are encouraged to acquire knowledge necessary for working in other roles at I.CA, in order to ensure substitutability for cases of emergency.

### 5.3.6 Sanctions for unauthorized actions

If an employee is detected to have been performing unauthorized activity, the employee is subject to the procedure described in internal documentation and governed by the Labour Code (this process does not prevent criminal prosecution if the unauthorized activity exhibits that degree of gravity).

### 5.3.7 Independent contractor requirements

I.CA may or must procure some activities from independent contractors but remains fully responsible for their operation. These business relations are regulated by bilateral business contracts with parties such as contracted registration authorities, application software developers, hardware suppliers, system software suppliers and other parties. These parties are required to observe the pertinent certificate policies, the relevant parts of internal documentation provided for them, and the required normative documents. Contractual penalties are applied for a breach of the obligations or duties specified in the said documents, or the contract with the contractor in breach is terminated immediately.

### 5.3.8 Documentation supplied to personnel

In addition to the certificate policy, the certification practice statement and the security and operational documentation, I.CA employees have available any other relevant standard, policy, manual and guidance they may need for their job.

## 5.4 Audit logging procedures

### 5.4.1 Types of events recorded

Subject to logging are all the events required by trust services legislation or the relevant technical and other standards to be logged, that is, for example, the life cycle events of Certificates.

The certification authorities' key pair generating is a special case of event logging. All this process complies with trust services legislation and the relevant technical and other standards.

Generating is carried out according to a pre-determined scenario in a physically secure environment and under the control of more I.CA employees in trusted roles. Protocol on key pair generating with data required by technical standards is signed by present employees in trusted roles. When the key pair of subordinate certification authority issuing SSL type certificates for end users is generated then the process is also video recorded.

When the key pair of root certification authority is generated, an auditor qualified in accordance with current technical standards personally attends the process, signs also the created protocol to confirm that the generating followed the pre-determined scenario and the measures to ensure integrity and confidentiality were in place.

All audit records are made, kept and processed to the extent as necessary, while preserving the proof of origin and maintaining integrity, availability, confidentiality and time authenticity.

The auditing system is designed and run in a manner ensuring audit data integrity, sufficient space for audit data, automatic non-rewriting of the audit file, user-friendly presentation of audit records, and audit file access limited to the defined users only.

### 5.4.2 Frequency of processing log

Audit records are checked and assessed at the intervals defined in internal documentation, or immediately when a security incident occurs.

### 5.4.3 Retention period for audit log

Unless the relevant legislation provides otherwise, audit records are kept for a minimum of ten years of the day they are made.

### 5.4.4 Protection of audit log

Both electronic and printed audit records are stored in a manner ensuring they are protected against change, theft and destruction (wilful or accidental).

Electronic audit records are stored in two copies. Printed audit records are kept outside the operating premises of I.CA.

The protection of the previously mentioned types of audit records is described in internal documentation.

### 5.4.5 Audit log backup procedures

Electronic audit records are backed up similarly to how other electronic information is backed up. No backup of printed audit records takes place.

### 5.4.6 Audit collection system (internal or external)

The audit record collection system is an internal one relative to the CA information systems.

### 5.4.7 Notification to event-causing subject

Parties are not notified of that an event is registered in an audit record.

### 5.4.8 Vulnerability assessments

První certifikační autorita, a.s., carries out periodic vulnerability assessments as part of risk assessments. Vulnerability monitoring of the hardware and software related to trust services is described in internal documentation.

## 5.5 Records archival

The storage of records i.e., information and documentation, at První certifikační autorita, a.s., is regulated by internal documentation.

### 5.5.1 Types of records archived

I.CA archives the following electronic or printed records pertaining to the trust services provided, such as:

- Reports / protocols on the generating of the certification authority's key pair;
- For subordinate CAs issuing SSL type certificates to end users:
  - Video recording of the key pair generating process;
- Records related to the life cycle of certificates (especially the documents relating to validation of certificate issuance applications and certificate revocation requests);
- Information handling records, such as takeover, handover, saving, check, conversion from printed to electronic form, etc.;
- Operational and security documentation.

### 5.5.2 Retention period for archive

Records relating to the certificates of all I.CA certification authorities and corresponding OCSP responders, excluding appropriate private keys, are kept throughout the existence of I.CA. Other records are kept in accordance with chapter 5.4.3.

The record storage procedures are regulated by internal documentation.

### 5.5.3 Protection of archive

The premises where records are stored are secured in a manner based on risk analysis results and the Classified Information Protection Act.

The procedures to protect the stored records are regulated by internal documentation.

### 5.5.4 Archive backup procedures

The record backup procedures are regulated by internal documentation.

### 5.5.5 Requirements for time-stamping of records

If time-stamp tokens are used, they are qualified electronic time-stamp tokens issued by I.CA.

### 5.5.6 Archive collection system (internal or external)

Records are stored in a place designated by COO of I.CA.

Internal documentation regulates how both electronic and printed records are prepared for archival and stored. Records are kept of collecting the records subject to storage.

### 5.5.7 Procedures to obtain and verify archive information

Archived information and records are stored at sites designated therefore and are accessible to:

- I.CA employees if they need to have such access for their job;
- Authorized inspection entities, the investigative, prosecuting and adjudicating bodies and courts of justice if required by legislation.

A written record is made of any such permitted access.

## 5.6 Key changeover

In standard situations (expiration of a certification authority's certificate), the key pair is replaced by issuing a new certificate a good time in advance (no later than one year prior to the expiration).

In non-standard situations (for instance such progress in cryptanalytic methods that could compromise the security of certificate issuance e.g., changes to cryptographic algorithms or key lengths) the key pair is replaced as soon as possible.

In both standard and non-standard situations, the replacement of the public key in Certificates is suitably notified to the public a good time in advance (if practicable).

## 5.7 Compromise and disaster recovery

### 5.7.1 Incident and compromise handling procedures

In the event of incident or compromise, I.CA takes a course of action in accordance with its internal business continuity plan and recovery plan, plus any other relevant internal documentation.

### 5.7.2 Computing resources, software, and/or data are corrupted

See 5.7.1.

### 5.7.3 Entity private key compromise procedures

In the case of reasonable concern that a private key of certification authority has been compromised, I.CA does the following:

- Stops using the private key;
- Revokes immediately and permanently the pertinent Certificate and destroys the corresponding private key;

- Revokes all valid certificates issued by specific certification authority;
- Immediately informs about this fact, including the reason of revocation, in accordance with Chapter 2.2; the list of revoked certificates is also used to make this information available;
- Notifies the supervisory body of that the pertinent certificate has been revoked and why it has been revoked.

A similar procedure will be applied in the event that cryptanalytic methods develop to such an extent (e.g., changes in cryptographic algorithms, key lengths, etc.) that the security of trust services could be immediately threatened.

### 5.7.4 Business continuity capabilities after a disaster

In the event of accident, I.CA takes a course of action in accordance with its internal business continuity plan and recovery plan, plus any other relevant internal documentation.

## 5.8 CA or RA termination

The following rules apply to the termination of the Authority's operations:

- The termination of the Authority's operations must be notified in writing to the supervisory body and the parties having a contract with I.CA that directly concerns the provision of services;
- The termination of the Authority's operations must be published on the web page pursuant to 2.2;
- If the Authority's certificate's expiration is part of the termination of operations, this information plus the reason for expiration must be included in that notice;
- The termination of operations is a controlled process following a pre-defined plan, which includes the description of the procedure to preserve and disclose information for judicial or administrative proceedings discovery and for arranging the continuity of services;
- The Authority or its successor must be able to revoke Certificates and publish CRLs as long as any certificate issued by the Authority is valid;
- After that the Authority must demonstrably destroy its private key, make a record of this destruction and keep this record in accordance with this CP; particular RA (see 1.3.2) corresponding with Authority will also be terminated.

Termination of subsequent CAs and corresponding RAs is described in CPs under which the certificates are issued.

In the event of withdrawal of the qualified Service provider status:

- The information must be notified in writing or electronically to all parties having a contract with I.CA that directly concerns the provision of the relevant services;
- The information must be published in accordance with 2.2. at all offices of registration authorities and must also communicate that certification authorities' certificates cannot be used in accordance with the purpose of their issuance any longer;
- The subsequent course of action will be decided by CEO of I.CA while taking account of the decision of the supervisory body.

# 6 TECHNICAL SECURITY CONTROLS

## 6.1 Key pair generation and installation

### 6.1.1 Key pair generation

Generating of certification authorities' and their corresponding OCSP responders' key pairs which is done in reserved areas of the operating site in compliance with the requirements of chapters 5.2 and 5.4.1 is carried out in cryptographic modules meeting the requirements of trust services legislation, which is ETSI and CEN standards.

All the requirements on the generating of these key pairs are described in internal documentation.

Key pairs of the employees taking part in the issuance of Certificates to end users are generated on chip cards that meet the QSCD requirements. The private keys of these key pairs data are stored on the smartcard in non-exportable form and PIN needs to be entered to use the keys.

### 6.1.2 Private key delivery to subscriber

Not applicable for this document; the private keys of certification authorities and their corresponding OCSP responders are stored in the cryptographic modules which are under sole control of I.CA.

The service of generating key pairs to employees taking part in issuing Certificates is not provided.

### 6.1.3 Public key delivery to certificate issuer

The public key is delivered to Certificate issuer in the Certificate application (the PKCS#10 format).

### 6.1.4 CA public key delivery to relying parties

The following are the options guaranteed for obtaining Authority's public key contained in its certificate:

- Receiving the key at RA;
- From the trust list of the Czech Republic;
- Receiving the key via the web information addresses of I.CA and the relevant supervisory body, or through the supervisory body's journal;
- Each certificate applicant receives Authority's certificate when obtaining the applicant's primary certificate.

### 6.1.5 Key sizes

The size of the key of I.CA root certification authority using RSA algorithm is 4096 bits, the size of the keys in certificates of subordinate certification authorities issued by this root certification authority is 4096, the size of the keys of OCSP responders is 2048 bits at minimum.

### 6.1.6 Public key parameters generation and quality checking

Parameters of the algorithms used for creating public keys of certification authorities and their corresponding OCSP responders comply with requirements stated in trust services legislation and in the technical and other standards referred to therein. These keys are generated and checked by relevant hardware and software.

The parameters of the algorithms used in generating public keys of other subscribers must also meet these requirements and are checked in the same way.

### 6.1.7 Key usage purposes (as per X.509 v3 key usage field)

The key usage options are specified in the Certificate's extension.

## 6.2 Private key protection and cryptographic module engineering controls

### 6.2.1 Cryptographic module standards and controls

The key pairs of certification authorities and their corresponding OCSP responders are generated, and the corresponding private keys are stored on cryptographic modules which meet the requirements of trust services legislation, which is ETSI and CEN standards and are used in accordance with their certification.

Employees taking part in issuing certificates use the smartcard meeting the QSCD requirements.

### 6.2.2 Private key (n out of m) multi-person control

If cryptographic module related operations require the presence of more persons, then each of them knows only part of the code required for these operations.

### 6.2.3 Private key escrow

Not applicable for this document; private key escrow service is not provided.

### 6.2.4 Private key backup

Private keys of certification authorities and their corresponding OCSP responders protected by cryptographic modules are backed up in encrypted form, which provides the same level of protection as the cryptographic module.

Not applicable for private keys of employees taking part in issuing certificates, these private keys are generated on smartcards as non-exportable.

### 6.2.5 Private key archival

When certification authorities' and their corresponding OCSP responders' private keys expire, they are not archived but destroyed including their backup copies.

Archiving period of private keys of employees taking part in issuing certificates is limited by the memory capacity of the smartcard.

### 6.2.6 Private key transfer into or from a cryptographic module

Private keys of certification authorities and their corresponding OCSP responders are generated in cryptographic modules (as not exportable) and cannot be exported out of these modules (operated in certified mode) in any form[1]. Import of the private key into the cryptographic module is not performed.

Not applicable for private keys of employees taking part in issuing certificates, these private keys are generated on smartcards as non-exportable.

### 6.2.7 Private key storage on cryptographic module

Private keys of certification authorities and their corresponding OCSP responders are stored on cryptographic modules meeting the requirements of trust services legislation, which is ETSI and CEN standards. Cryptographic modules are operated in compliance with their certification.

Private keys of employees taking part in issuing certificates are stored on smartcards meeting the QSCD requirements.

### 6.2.8 Method of activating private key

Activation of certification authorities' and their corresponding OCSP responders' private keys (allowing the use of these private keys) is done:

- In case of smartcard activation by inserting the smartcard into card reader and entering the password;
- In case of softcard activation by entering the softcard and password.
- Private keys of employees taking part in issuing certificates are activated by inserting the smartcard into and entering PIN.

### 6.2.9 Method of deactivating private key

Deactivation of certification authorities' and their corresponding OCSP responders' private keys is done by removing the smartcard from card reader or by terminating the specific application.

Private keys of employees taking part in issuing certificates are deactivated by removing the smartcard from card reader.

[1] There is one exception – encrypted backup, which can be used only in cryptographic module (or in HA/LB modules) where the key pair was generated.

### 6.2.10 Method of destroying private key

After expiration of specific certification authority's private key and based on subsequent decision of CEO of I.CA this private key is destroyed according to specific procedure including all backups of this key. Destroying is documented in a written record.

Private keys of OCSP responders are destroyed on the decision of I.CA representative when issuing OCSP responder's certificate. Destroying is documented in a written record.

Destroying private keys of employees taking part in issuing certificates is fully within the competence of these employees, it is not ordered. It is necessary only when the smartcard memory is full.

### 6.2.11 Cryptographic module rating

Cryptographic modules used for generating of key pairs and storing corresponding private keys of certification authorities and their corresponding OCSP responders meet the requirements of trust services legislation, which is ETSI and CEN standards and are used in accordance with their certification.

Smartcards used for generating of key pairs and storing corresponding private keys of employees taking part in issuing certificates meet QSCD requirements.

## 6.3 Other aspects of key pair management

### 6.3.1 Public key archival

All public keys as part of Certificates are archived throughout the existence of I.CA.

### 6.3.2 Certificate operational periods and key pair usage periods

The maximum period of validity of each Certificate issued is specified in the body of that Certificate and is the same as key pair usage period.

## 6.4 Activation data

### 6.4.1 Activation data generation and installation

Activation data of certification authorities' and their corresponding OCSP responders' private keys (smartcards or softcards) are created before or during the generating of the corresponding key pair.

Activation data of employees' taking part in issuing certificates private keys is PIN, which is under sole control of these employees.

### 6.4.2 Activation data protection

Activation data of certification authorities' and their corresponding OCSP responders' private keys (smartcards or softcards) are protected by passwords.

Activation data of employees taking part in issuing certificates private keys protection is fully within the competence of these employees.

### 6.4.3 Other aspects of activation data

Not applicable for this document.

## 6.5 Computer security controls

### 6.5.1 Specific computer security technical requirements

The level of security of the components used in providing trust services is, including the scope of necessary evaluations and assessments and also trustworthy systems configuration checks, and their periodicity, defined for qualified services in trust services legislation and the technical standards referred to therein, otherwise in the relevant technical standards.

### 6.5.2 Computer security rating

The assessment of I.CA computer security is based on the requirements set out in the specified technical standards and norms, in particular:

- CEN/TS 419261 Security Requirements for Trustworthy Systems Managing Certificates and Time-stamps;
- ČSN ETSI EN 319 401 Electronic Signatures and Infrastructures (ESI) – General Policy Requirements for Trust Service Providers;
- ETSI EN 319 401 Electronic Signatures and Infrastructures (ESI); General Policy Requirements for Trust Service Providers;
- ČSN ETSI EN 319 403-1 Electronic Signatures and Infrastructures (ESI); Trust Service Provider Conformity Assessment; Part 1: Requirements for conformity assessment bodies assessing Trust Service Providers;
- ETSI EN 319 403-1 Electronic Signatures and Infrastructures (ESI); Trust Service Provider Conformity Assessment; Part 1: Requirements for conformity assessment bodies assessing Trust Service Providers;
- ČSN 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 319 411-1 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 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 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;

- ČSN ETSI EN 319 412-1 Electronic Signatures and Infrastructures (ESI); Certificate Profiles; Part 1: Overview and Common Data Structures;
- ETSI EN 319 412-1 Electronic Signatures and Infrastructures (ESI); Certificate Profiles; Part 1: Overview and Common Data Structures;
- ČSN ETSI EN 319 412-2 Electronic Signatures and Infrastructures (ESI); Certificate Profiles; Part 2: Certificate Profile for Certificates Issued to Natural Persons;
- ETSI EN 319 412-2 Electronic Signatures and Infrastructures (ESI); Certificate Profiles; Part 2: Certificate Profile for Certificates Issued to Natural Persons;
- ČSN ETSI EN 319 412-3 Electronic Signatures and Infrastructures (ESI); Certificate Profiles; Part 3: Certificate Profile for Certificates Issued to Legal Persons;
- ETSI EN 319 412-3 Electronic Signatures and Infrastructures (ESI); Certificate Profiles; Part 3: Certificate Profile for Certificates Issued to Legal Persons;
- ČSN ETSI EN 319 412-4 Elektronické podpisy a infrastruktury (ESI) - Profily certifikátu – Část 4: Profil certifikátu pro certifikáty webových stránek;
- ETSI EN 319 412-4 Electronic Signatures and Infrastructures (ESI); Certificate Profiles; Part 4: Certificate profile for web site certificates;
- ČSN ETSI EN 319 412-5 Electronic Signatures and Infrastructures (ESI); Certificate Profiles; Part 5: QC Statements;
- ETSI EN 319 412-5 Electronic Signatures and Infrastructures (ESI); Certificate Profiles; Part 5: QCStatements;
- ČSN EN 419 221-5 Protection profiles for TSP Cryptographic modules - Part 5 Cryptographic Module for Trust Services;
- EN 419 221-5 Protection profiles for TSP Cryptographic modules - Part 5 Cryptographic Module for Trust Services;
- FIPS PUB 140-2 Requirements for Cryptographic Modules;
- ČSN ISO/IEC 15408-1 Information security, cybersecurity and privacy protection - Evaluation criteria for IT security - Part 1: Introduction and general model;
- ISO/IEC 15408-1:2022 Information security, cybersecurity and privacy protection - Evaluation criteria for IT security - Part 1: Introduction and general model;
- ČSN ISO/IEC 15408-2 Information security, cybersecurity and privacy protection - Evaluation criteria for IT security - Part 2: Security functional components;
- ISO/IEC 15408-2:2022 Information security, cybersecurity and privacy protection - Evaluation criteria for IT security - Part 2: Security functional components;
- ČSN ISO/IEC 15408-3 Information security, cybersecurity and privacy protection - Evaluation criteria for IT security - Part 3: Security assurance components;
- ISO/IEC 15408-3:2022 Information security, cybersecurity and privacy protection - Evaluation criteria for IT security - Part 3: Security assurance components;
- ETSI TS 119 312 Electronic Signatures and Infrastructures (ESI); Cryptographic Suites;
- European Cybersecurity Certification Group Sub-group on Cryptography - Agreed Cryptographic Mechanisms;
- ČSN EN ISO/IEC 27006 Information Technology – Security Techniques – Requirements for Bodies Providing Audit and Certification of Information Security Management Systems.

- ISO/IEC 17021 Conformity Assessment -- Requirements for Bodies Providing Audit and Certification of Management Systems;
- ISO/IEC 17065 Conformity Assessment -- Requirements for Bodies Certifying Products, Processes and Services.
- ISO 3166-1 Codes for the Representation of Names of Countries and Their Subdivisions – Part 1: Country Codes;
- ITU-T - X.501 Information Technology – Open Systems Interconnection – The Directory: Models;
- ITU-T - X.509 Information Technology – Open Systems Interconnection – The Directory: Public-key and Attribute Certificate Frameworks;
- ITU-T - X.520 Information Technology – Open Systems Interconnection – The Directory: Selected Attribute Types;
- RSA Laboratories - PKCS#10: Certification Request Syntax Standard;
- RFC 6960 X.509 Internet Public Key Infrastructure Online Certificate Status Protocol – OCSP;
- RFC 3647 Internet X.509 Public Key Infrastructure Certificate Policy and Certification Practices Framework;
- RFC 5019 The Lightweight Online Certificate Status Protocol (OCSP) Profile for High-Volume Environments;
- RFC 5280 Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile;
- EN 301 549 Accessibility requirements for ICT products and services.

## 6.6 Life cycle technical controls

### 6.6.1 System development controls

System development is carried out in accordance with internal documentation.

### 6.6.2 Security management controls

Information security management and compliance with technical standards are inspected as part of the periodic trust services audits and conformity assessments and also in information security management system (ISMS) audits.

Information security at I.CA is managed by the following standards:

- ČSN EN ISO/IEC 27000 Information Technology – Security Techniques – Information Security Management Systems – Overview and Vocabulary;
- ČSN EN ISO/IEC 27001 Information security, cybersecurity and privacy protection - Information security management systems – Requirements;
- ČSN EN ISO/IEC 27002 Information security, cybersecurity and privacy protection - Information security controls.

### 6.6.3 Life cycle security controls

I.CA takes the Plan-Do-Check-Act (PDCA) procedural approach to life cycle security management; the PDCA approach consists of the following consecutive processes:

- Establishing – defining the scope and the boundaries for information security management, determining a security policy and plans, and choosing security controls depending on the risks identified, all this in accordance with the corporate security policy;
- Implementing and operating – effective and systematic enforcement of the selected security controls;
- Monitoring and reviewing – providing feedback, regular monitoring and evaluation of the successful and the poor aspects of information security management, providing the knowledge gained for the company management for assessment;
- Maintenance and improvement – implementing corrective and improvement measures as decided by the company management.

## 6.7 Network security controls

Network infrastructure of the operating site is protected with a firewall-type commercial product with an integrated intrusion prevention system. The detailed network security management solution is described in internal documentation.

## 6.8 Time-stamping

See 5.5.5 for the time-stamping solution.

# 7 CERTIFICATE, CRL AND OCSP PROFILES

## 7.1 Certificate profile

**Table 4 – Authority's certificate**

| Field | Content | Comments |
|---|---|---|
| version | v3 (0x2) | |
| serialNumber | unique serial number of the certificate to be issued | |
| signatureAlgorithm | sha512WithRSAEncryption | |
| issuer | | |
| commonName | I.CA TLS Root CA/RSA *MM*/*RRRR* | *MM*/*YYYY*: the month and the year when the root CA's certificate is issued |
| organizationName | První certifikační autorita, a.s. | |
| country | CZ | |
| organizationIdentifier | NTRCZ-26439395 | attribute included in the certificate issued after the effective date of policy version 1.10 |
| validity | | |
| notBefore | start of Certificate's validity | UTC |
| notAfter | notBefore + 25 years | UTC |
| subject | | |
| commonName | I.CA TLS Root CA/RSA *MM*/*RRRR* | *MM*/*YYYY*: the month and the year when the root CA's certificate is issued |
| organizationName | První certifikační autorita, a.s. | |
| country | CZ | |
| organizationIdentifier | NTRCZ-26439395 | |
| subjectPublicKeyInfo | | |
| algorithm | rsaEncryption | |
| subjectPublicKey | public key (4096 bits) | |

| | | |
|---|---|---|
| extensions | certificate extensions | see Table 6 |
| signature | advanced electronic seal of Certificate's issuer | |

**Table 5 – Subordinate certification authority's certificate**

| Field | Content | Comments |
|---|---|---|
| version | v3 (0x2) | |
| serialNumber | unique serial number of the certificate to be issued | |
| signatureAlgorithm | sha256WithRSAEncryption at minimum | |
| issuer | certificate issuer | see Table 4 |
| validity | | |
| notBefore | start of Certificate's validity | UTC |
| notAfter | notBefore + 10 years | UTC |
| subject | | |
| commonName | name of the subordinate certification authority | includes the string *MM/YYYY*: the month and the year when the subordinate certification authority's certificate is issued |
| organizationName | První certifikační autorita, a.s. | |
| country | CZ | |
| organizationIdentifier | NTRCZ-26439395 | |
| subjectPublicKeyInfo | | |
| algorithm | rsaEncryption | |
| subjectPublicKey | public key (2048 bits at minimum) | |
| extensions | certificate extensions | see Table 7 |
| signature | advanced electronic seal of the Certificate's issuer | |

### 7.1.1 Version number(s)

Any certificate issued complies with standard X.509, version 3.

### 7.1.2 Certificate extensions

**Table 6 – Authority's certificate extensions**

| Extension | Content | Comments |
|---|---|---|
| certificatePolicies | | non-critical |
| policyIdentifier | 2.5.29.32.0 (anyPolicy) | |
| basicConstraints | | critical |
| cA | True | |
| keyUsage | keyCertSign, cRLSign | critical |
| subjectKeyIdentifier | | non-critical |
| keyIdentifier | hash of the Authority's public key | |

**Table 7 – Subordinate certification authority's certificate extensions**

| Extension | Content | Comments |
|---|---|---|
| certificatePolicies | | non-critical |
| policyIdentifier | 2.5.29.32.0 (anyPolicy) | |
| basicConstraints | | critical |
| cA | True | |
| pathLenConstraint | 0 | |
| keyUsage | keyCertSign, cRLSign | critical |
| extendedKeyUsage | according to the content of subordinate certification authority certificate application | non-critical<br>in compliance with BRG and Mozilla requirements to limit the types of certificates issued by specific subordinate certification authority |
| subjectKeyIdentifier | | non-critical |
| keyIdentifier | hash of this subordinate certification authority's public key | |
| authorityKeyIdentifier | | non-critical |
| keyIdentifier | hash of the Authority's public key | |
| CRLDistributionPoints* | http://qcrldp1.ica.cz/rcatls*RR*_rsa.crl<br>http://qcrldp2.ica.cz/rcatls*RR*_rsa.crl<br>http://qcrldp3.ica.cz/rcatls*RR*_rsa.crl | non-critical |

| | | |
|---|---|---|
| authorityInformationAccess | | non-critical |
| id-ad-ocsp* | http://ocsp.ica.cz/rcatls*RR*_rsa | URI (http) to root CA's OCSP responder |
| id-ad-caIssuers* | http://r.ica.cz/rca*RR*_rsatls.cer | URI (http) to root CA's certificate |

* *RR* – last two digits of the year when the Authority's certificate is issued.

For extensions containing URLs (where relevant), an additional URL can be added to obtain the object.

### 7.1.3 Algorithm object identifiers

The algorithms used in providing trust services are in compliance with the relevant technical standards.

### 7.1.4 Name forms

Name forms in issued Certificates comply with RFC 5280 standard. The provisions of 3.1 also apply.

### 7.1.5 Name constraints

Not applicable for the certificates issued under this CP.

### 7.1.6 Certificate policy object identifier

This document's/policy's OID is specified in 1.2. Certification authorities' certificates include a special anyPolicy policy identification, the OID of which is 2.5.29.32.0.

### 7.1.7 Usage of Policy Constraints extension

Not applicable for Certificates issued under this CP.

### 7.1.8 Policy qualifiers syntax and semantics

See Certificate extensions in 7.1.2 above.

### 7.1.9 Processing semantics for the critical Certificate Policies extension

Not applicable for this document – not classified as critical.

## 7.2 CRL profile

**Table 8 – CRL profile**[2]

| Attribute | Content |
|---|---|
| version | v2(0x1) |
| signatureAlgorithm | sha512WithRSAEncryption |
| issuer | CRL issuer |
| thisUpdate | date and time of issue (UTC) |
| nextUpdate | thisUpdate + maximum 365 days (UTC) |
| revokedCertificates | list of revoked certificates |
| **crlEntries** | |
| userCertificate | revoked certificate's serial number |
| revocationDate | certificate revocation date and time |
| crlEntryExtensions | list attribute extension – see Table 9 |
| | |
| crlExtensions | CRL extensions – see Table 9 |
| signature | advanced electronic seal of CRL's issuer |

### 7.2.1 Version number(s)

Certificate revocation lists are issued pursuant to X509, version 2.

### 7.2.2 CRL and CRL entry extensions

**Table 9 – CRL extensions**[3]

| Attribute | Content | Comments |
|---|---|---|
| **crlExtensions** | | |
| authorityKeyIdentifier | | |
| keyIdentifier | hash of the CRL issuer's (Authority's) public key | non-critical |
| CRLNumber | unique number of the CRL | non-critical |
| **crlEntryExtensions** | | |
| CRLReason | certificate's revocation reason:<br>• the certificateHold reason is not admissible as it is out of use; | non-critical, optional |

[2] I.CA reserves the right to modify the set and the content of the CRL fields as may be required by updated ETSI standards or third parties (Microsoft, for example).

[3] I.CA reserves the right to modify the set and the content of the CRL extensions as may be required by updated ETSI standards or third parties (Microsoft, for example).

| | | |
|---|---|---|
| | • another reason than unspecified (0) is given when subordinate CA's certificate is revoked | |

## 7.3 OCSP profile

Both the OCSP request profile and the OCSP response profile comply with RFC 6960 and RFC 5019.

OCSP responses are of the BasicOCSPResponse type and contain all mandatory fields. An optional revocationReason field is included for revoked certificates. When subordinate certification authority's certificate is revoked, another reason than unspecified (0) is given.

The unAuthorized response is given for any certificate not issued by the relevant CA. Http only is used as the transmission protocol.

See the relevant certification practice statement for more detail.

### 7.3.1 Version number(s)

Version 1 is specified in a certificate status request and response using the OCSP protocol.

### 7.3.2 OCSP extensions

The specific extensions for OCSP protocol certificate status requests and responses are given in the relevant certification practice statement.

# 8 COMPLIANCE AUDIT AND OTHER ASSESMENTS

## 8.1 Frequency or circumstances of assessment

The assessment interval and circumstances are defined in trust services legislation and the technical standards referred to therein regulating the assessment procedure.

The Microsoft Trusted Root Program assessment interval and circumstances are strictly defined by Microsoft, and the audit period is not longer than one year.

The intervals for other assessments are specified in the relevant technical standards.

## 8.2 Identity/qualifications of assessor

The identity (accredited conformity assessment entity) and the qualification of the assessor carrying out the assessment pursuant to trust services legislation are defined in this legislation and the technical standards referred to therein.

The identity (accredited conformity assessment entity) and the qualification of the assessor carrying out assessment defined by Microsoft Trusted Root Program are described in ETSI EN 319 403-1.

The identity of the assessor carrying out other assessments is specified in the relevant technical standards.

## 8.3 Assessor's relationship to assessed entity

Internal assessor is not subordinate to the organisational unit which provides the operation of trust services.

External assessor is an assessor without any property or personal relation to I.CA.

## 8.4 Topics covered by assessment

The areas to be assessed in an assessment required under trust services legislation are those as specified in that legislation.

The areas to be assessed in an assessment required for Microsoft Trusted Root Program are strictly given by requirements of Microsoft Company.

The areas to be assessed in any other assessment are specified in the technical standards under which the assessment is made.

## 8.5 Actions taken as a result of deficiency

The findings in any type of assessment are communicated to the I.CA security manager, who makes sure that any defect identified is remedied. If defects are identified that critically prevent the provision of a specific trust service, I.CA must suspend that service until the defects are remedied.

## 8.6 Communication of results

Assessment result notification is subject to the requirements of trust services legislation and the relevant technical standards; the notification of Microsoft Trusted Root Program assessment results is subject to Microsoft requirements.

Assessments results are notified as a written report handed over by the assessor to CEO and the security manager of I.CA.

The I.CA security manager calls a security committee meeting as soon as possible and communicates the final report at the meeting; company management members must attend the meeting.

# 9 OTHER BUSINESS AND LEGAL MATTERS

## 9.1 Fees

### 9.1.1 Certificate issuance or renewal fees

První certifikační autorita, a.s., is the operator of all the certification authorities the Certificates of which have been issued under this CP. No fee is charged for the issuance of certificates by the root certification authority.

### 9.1.2 Certificate access fees

No fee is charged by I.CA for electronic access to the certificates issued under this CP.

### 9.1.3 Revocation or status information access fees

No fee is charged by I.CA for electronic access to revocation information (CRL) and status information (OCSP) about the certificates issued under this CP.

### 9.1.4 Fees for other services

Not applicable for this document.

### 9.1.5 Refund policy

Not applicable for this document.

## 9.2 Financial responsibility

### 9.2.1 Insurance coverage

První certifikační autorita, a.s., represents it holds the valid business risk insurance policy that covers financial damage.

První certifikační autorita, a.s., has drawn an employee liability insurance policy for each employee, with a scope of coverage as determined by the company's board of directors.

### 9.2.2 Other assets

První certifikační autorita, a.s., represents it has available financial resources and other financial assurances sufficient for providing trust services given the risk of a liability-for-damage claim.

See the Annual Report of První certifikační autorita, a.s., published in Commercial Register for detailed information on the company's assets.

### 9.2.3 Insurance or warranty coverage for end-entities

Not applicable for this document.

## 9.3 Confidentiality of business information

### 9.3.1 Scope of confidential information

I.CA's confidential information covers any information other than public information and other than that published in the manner pursuant to 2.2, including:

- All private keys, which are employed in providing trust services;
- I.CA's business information;
- Any internal information and documentation;
- Any personal data.

### 9.3.2 Information not within the scope of confidential information

Public information is marked as public or published in the manner pursuant to 2.2.

### 9.3.3 Responsibility to protect confidential information

I.CA employee who comes in contact with confidential information may not disclose this information to a third party without consent of CEO of I.CA.

## 9.4 Privacy of personal information

### 9.4.1 Privacy plan

I.CA protects personal data and other non-public information in accordance with the relevant legislation, which means ZOOU and GDPR in particular.

### 9.4.2 Information treated as private

Any personal data subject to protection under relevant legislation are treated as private.

I.CA employees or the entities defined by current legislation that come into contact with personal data must maintain confidentiality of these data and the security controls, the disclosure of which would put the security of these data at risk. The confidentiality duty survives the termination of employment or other similar relationship, or the completion of pertinent work.

### 9.4.3 Information not deemed private

Any information outside the scope of relevant legislation is not considered personal data.

### 9.4.4 Responsibility to protect private information

CEO of I.CA is responsible for the protection of personal data.

### 9.4.5 Notice and consent to use private information

I.CA deals with the notifying of personal data use and consents to personal data processing in accordance with the relevant legislation.

### 9.4.6 Disclosure pursuant to judicial or administrative process

I.CA discloses personal data for judicial or administrative purpose in accordance with the relevant legislation.

### 9.4.7 Other information disclosure circumstances

I.CA provides access to personal strictly as regulated by relevant legislation.

## 9.5 Intellectual property rights

This CP, all related documents, the website content and the procedures facilitating the operation of trustworthy systems supporting trust services are copyrighted by První certifikační autorita, a.s., and are important know-how thereof.

## 9.6 Representations and warranties

### 9.6.1 CA representations and warranties

I.CA warrants that:

- It will only use the private keys pertinent to the Authority's certificates for creating the electronic seal of the Certificates issued by it, of the lists of revoked certificates issued by it, of the certificates of its OCSP responder and of its certificates for infrastructure purposes;
- The Authority-issued Certificates meets the requirements of the relevant technical standards and trust services legislation;
- It will revoke the Authority-issued Certificates if the revocation request is submitted in the manner defined in this CP.

### 9.6.2 RA representations and warranties

Not applicable for this document; see 1.3.2.

### 9.6.3 Subscriber representations and warranties

The subscriber acts in accordance with the relevant technical standards and trust services legislation and warrants that the information given by him are correct throughout the life cycle of the usage of trusted services.

### 9.6.4 Relying parties representations and warranties

Relying parties observe this CP.

### 9.6.5 Representations and warranties of other participants

Not applicable for this document.

## 9.7 Disclaimers of warranties

První certifikační autorita, a.s., only provides those warranties as given in 9.6.

## 9.8 Limitations of liability

První certifikační autorita, a.s., is not responsible for any damage suffered by relying parties where the relying party fails to meet the obligations required under the certificate policy under which the pertinent certificate is issued. První certifikační autorita, a.s., is also not responsible for any damage resulting from breach of obligations of I.CA as a result of force majeure.

## 9.9 Indemnities

Not applicable for this document; see policies of the authorities which issue certificates to end users.

## 9.10 Term and termination

### 9.10.1 Term

This CP takes effect on the date specified in chapter 10 and remains in effect no shorter than the expiration of the last Certificate issued under this CP.

### 9.10.2 Termination

CEO of První certifikační autorita, a.s., is the sole person authorized to approve the termination of this CP.

### 9.10.3 Effect of termination and survival

The obligations of I.CA arising from this CP survive the expiration thereof until the expiration of the last Certificate issued under this CP.

## 9.11 Individual notices and communications with participants

All the participating parties are organisational parts of I.CA and their mutual communication is governed by internal rules of I.CA.

## 9.12 Amendments

### 9.12.1 Procedure for amendment

This procedure is a controlled process described in internal documentation.

### 9.12.2 Notification mechanism and period

The release of a new CP version is always notified as published information.

### 9.12.3 Circumstances under which OID must be changed

CP's OID must be changed when the changes of the CP will materially reduce the assurance that the Certificate is trusted and will have a significant effect on the acceptability of the Certificate in compliance with trust services legislation.

Any change to this CP results in a new version of the document.

## 9.13 Disputes resolution provisions

All the participating parties are organisational components of I.CA and the resolution of their disputes is governed by internal rules of I.CA.

## 9.14 Governing law

The business of První certifikační autorita, a.s., is governed by the legal order of the Czech Republic.

## 9.15 Compliance with applicable law

The system of providing trust services is in compliance with the statutory requirements of EU and the Czech Republic and with all relevant international standards.

## 9.16 Miscellaneous provisions

### 9.16.1 Entire agreement

Not applicable for this document.

### 9.16.2 Assignment

Not applicable for this document.

### 9.16.3 Severability

If a court or a public authority with jurisdiction over the activities covered by this CP establishes that the implementation of a mandatory requirement is unlawful, the scope of that requirement will be so limited as to ensure the requirement is lawful and complies with relevant legislation.

### 9.16.4 Enforcement (attorneys' fees and waiver of rights)

Not applicable for this document.

### 9.16.5 Force majeure

První certifikační autorita, a.s., is not responsible for breaching its obligations stipulated in client contract if it is a result of force majeure, such as major natural disaster, major disaster caused by human activity, strike or civil unrest always followed by the declaration of a situation of emergency, or the declaration of a threat to the state or a state of war, or communication failure.

## 9.17 Other provisions

Not applicable for this document.

# 10 FINAL PROVISIONS

This certificate policy issued by První certifikační autorita, a.s., takes force and effect on the date mentioned above in Table 1.