První certifikační autorita, a.s.


# Certification Practice Statement

(RSA Algorithm)



**Version 1.69**

# TABLE OF CONTENTS

**Table 1 – Document history**

| Version | Date of Release | Approved by | Comments |
|---|---|---|---|
| 1.0 | 15 July 2015 | CEO of První certifikační autorita, a.s. | First release. |
| 1.1 | 2 November 2015 | CEO of První certifikační autorita, a.s. | Updated OIDs of certification policies (TSA, OCSP). |
| 1.2 | 29 March 2016 | CEO of První certifikační autorita, a.s. | Updated OID of SSL certification policy. |
| 1.3 | 6 April 2016 | CEO of První certifikační autorita, a.s. | Adding supported certification policies. |
| 1.4 | 15 March 2017 | CEO of První certifikační | Updated policy OIDs. |

| | | | |
|---|---|---|---|
| | | autorita, a.s. | Modified to match statutory requirements for trust services and technical standard requirements.<br>Modified to match the requirements of Microsoft Trusted Root Certificate Program. |
| 1.5 | 3 April 2017 | CEO of První certifikační autorita, a.s. | Updated policy OIDs. |
| 1.6 | 20 November 2017 | CEO of První certifikační autorita, a.s. | New policies added.<br>Changed method to record policy OIDs. |
| 1.61 | 30 April 2018 | CEO of První certifikační autorita, a.s. | Change of versioning the document.<br>Adding the description of QSCD list checking.<br>Adding the description of CAA records checking. |
| 1.62 | 13 September 2018 | CEO of První certifikační autorita, a.s. | New policies added. |
| 1.63 | 30 April 2019 | CEO of První certifikační autorita, a.s. | Annual revision, formal errors correction. |
| 1.64 | 25 October 2019 | CEO of První certifikační autorita, a.s. | New policy added and job titles in compliance with Internal Governance Code. |
| 1.65 | 7 March 2020 | CEO of První certifikační autorita, a.s. | New policy added, formal errors correction. |
| 1.66 | 29 April 2020 | CEO of První certifikační autorita, a.s. | Revision, more accurate text. |
| 1.67 | 28 November 2020 | CEO of První certifikační autorita, a.s. | Classification of document marked, change of CA actions during subsequent certificate issuance, revision, more accurate text. |
| 1.68 | 5 January 2022 | CEO of První certifikační autorita, a.s. | New certification policy (for the issuance of qualified electronic signature certificates through NKČR) and new guideline (for DRA NKČR) added. |
| 1.69 | 20 April 2022 | CEO of První certifikační autorita, a.s. | Remote natural person identity authentication via ZealiD TRA Service added.<br>Cryptographic module evaluation updated.<br>Revision of text. |

# 1 INTRODUCTION

This document makes more specific the principles stated in specific certification policies (CPs) and applied by První certifikační autorita, a.s. (also as the I.CA), a qualified provider of trust services, when providing qualified trust services and when issuing other types of certificates (also as the Services) in compliance with:

- Regulation (EU) no 910/2014 of the European Parliament and of the Council on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC;
- Act of the Czech Republic No. 297/2016 Coll., on trust services for electronic transactions;
- Act of the Slovak Republic No. 272/2016 Coll., on trust services for electronic transactions in the internal market and on amendments to certain laws (trust services act);
- 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).

For Services provided in compliance with this certification practice statement (also as CPS) the RSA algorithm is used.

Where applicable, the Services are provided for all end users on the basis of the contract. I.CA imposes no restrictions on potential end users, and the provision of the service is non-discriminatory and the service is also available to the disabled.

For all certificates issued by I.CA the terms Certificate or Certificates are used hereinafter.

Note: Any reference to technical standard, norm or legislation is always a reference to that technical standard, norm or legislation or to 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 **Certification Practice Statement (RSA Algorithm)** is prepared by První certifikační autorita, a.s., deals with the issues related to life cycle processes of certificates and follows a structure matching the scheme of current RFC 3647 standard while taking account of current EU standards 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). This applies to the certification policies listed in 1.2.

The document is divided into nine basic chapters and these are briefly introduced in the following list:

- Chapter 1 identifies this document, generally describes the entities and individuals taking part in the provision of the Services, and defines the acceptable usage 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., certificate issuance application, the issuance of the certificate, certificate revocation request, the revocation of the certificate, the services related to the verification of certification status, termination of the provision of the Services, etc.;
- Chapter 5 covers physical, procedural and personal security, including the definition of the set of recorded events, 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 refers to certificate profiles and CRL profiles in specific CPs and specifies the types and the length of the attributes in the subject field and the subjectAlternativeName extension;
- Chapter 8 focuses on Service assessment;
- Chapter 9 deals with commercial and legal aspects.

This document may also be used by independent institutions, such as auditing companies, as the basis for a confirmation that the certification services pertinent to certificate issuance and provided by První certifikační autorita, a.s., can be considered trustworthy.

Note: This document is English translation of CPS, the Czech version always takes the precedence.

## 1.2 Document name and identification

This document's title: Certification Practice Statement (RSA Algorithm), version 1.69

Document OID: No OID assigned

This CPS applies to the following certification policies:

| OID | CP |
|---|---|
| 1.3.6.1.4.1.23624.10.1.10.*x.y* | Root Qualified Certification Authority Certification Policy (RSA Algorithm) |
| 1.3.6.1.4.1.23624.10.1.11.*x.y* | Root Certification Authority for TLS Certificates Certification Policy (RSA Algorithm) |
| 1.3.6.1.4.1.23624.10.1.30.*x.y* | Certification Policy for the Issuance of Qualified Electronic Signature Certificates (RSA Algorithm) |
| 1.3.6.1.4.1.23624.10.1.31.*x.y* | Certification Policy for the Issuance of Qualified Electronic Seal Certificates (RSA Algorithm) |
| 1.3.6.1.4.1.23624.10.1.32.*1.y* | Certification Policy for the Issuance of TSA System Certificates (RSA Algorithm) |
| 1.3.6.1.4.1.23624.10.1.32.*2.y* | Certification Policy for the Issuance of Qualified Certificates for TSA2 System Electronic Seal (RSA Algorithm) |

| | |
|---|---|
| 1.3.6.1.4.1.23624.10.1.33.*x.y* | Certification Policy for the Issuance of System Certificates (RSA Algorithm) |
| 1.3.6.1.4.1.23624.10.1.34.*x.y* | Certification Policy for the Issuance of Qualified PSD2 Electronic Seal Certificates (RSA Algorithm) |
| 1.3.6.1.4.1.23624.10.1.35.*x.y* | Certification Policy for the Issuance of Qualified Website Authentication Certificates for Legal Entities (RSA Algorithm) |
| 1.3.6.1.4.1.23624.10.1.37.*x.y* | Certification Policy for the Issuance of Qualified Remote Electronic Signature Certificates (RSA Algorithm) |
| 1.3.6.1.4.1.23624.10.1.38.*x.y* | Certification Policy for the Issuance of Qualified Remote Electronic Seal Certificates (RSA Algorithm) |
| 1.3.6.1.4.1.23624.10.1.40.*x.y* | Certification Policy for the Issuance of Qualified Website Authentication Certificates for Legal Entities PSD2 (RSA Algorithm) |
| 1.3.6.1.4.1.23624.10.1.41.*x.y* | Certification Policy for the Issuance of Qualified Electronic Signature Certificates through NKČR (RSA Algorithm) |
| 1.3.6.1.4.1.23624.10.1.70.*x.y* | Certification Policy for the Issuance of Commercial Certificates (RSA Algorithm) |
| 1.3.6.1.4.1.23624.10.1.71.*x.y* | Certification Policy for the Issuance of Commercial Technology Certificates (RSA Algorithm) |
| 1.3.6.1.4.1.23624.10.1.72.*x.y* | Certification Policy for the Issuance of SSL Certificates (RSA Algorithm) |
| 1.3.6.1.4.1.23624.10.1.74.*x.y* | Certification Policy for the Issuance of Electronic Identification System Certificates (RSA Algorithm) |
| 1.3.6.1.4.1.23624.10.1.80.*x.y* | Certification Policy for the Issuance of OCSP Responder Certificates (RSA Algorithm) |
| 1.3.6.1.4.1.23624.10.1.90.*x.y* | Certification Policy for the Issuance of Qualified SK Certificates for Electronic Signatures (RSA Algorithm) |
| 1.3.6.1.4.1.23624.10.1.91.*x.y* | Certification Policy for the Issuance of Qualified Electronic SK Signature Certificates (RSA Algorithm) |

* It is always the current policy version in the *x.yz* format as posted on http://www.ica.cz, where *x* and *y* are part of the policy OID.

The service of issuing qualified certificates is, in compliance with the eIDAS Regulation, on the trustworthy list maintained by the supervisory body.

## 1.3 PKI participants

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

#### 1.3.1.1 Root certification authority

The root certification authority of První certifikační autorita, a.s., issued Certificates to subordinate certification authorities operated by I.CA and to its OCSP responder, in a two-tier certification authority structure, in accordance with relevant legislation and technical and other standards. These authorities issue Certificates to end users and for the authorities' own OCSP responders.

As the root certification authority is off line, it has no live connection to the external network at any time. Only the authority's OCSP responder is online. The authority's physical information system is comprised of dedicated computers; the HSM module containing the private key connects to this information system via a dedicated secured interface.

#### 1.3.1.2 Issuing Certification Authorities

Public certification authorities, operated by První certifikační autorita, a.s., provide the Services for end users and the TSA system.

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

The registration authorities employed in the life cycle processes of issued Certificates. These RAs can be stationary or mobile.

### 1.3.3 Subscribers

#### 1.3.3.1 Certificates of the provider (I.CA)

The Certificates are solely issued for the certification authorities, their OCSP responders and the time servers of time-stamping authorities, all operated by I.CA. I.CA as a legal entity is the eligible applicant and the subscriber.

#### 1.3.3.2 End user certificates

The Certificates are issued to end users who use the Services.

### 1.3.4 Relying parties

Any entity relying in their operations on the Certificates issued as part of the Services is a relying party.

### 1.3.5 Other participants

Other participating parties are investigative, prosecuting and adjudicating bodies, supervisory bodies and other bodies recognized as such by relevant legislation.

## 1.4 Certificate usage

### 1.4.1 Appropriate certificate uses

The root CA's Certificates may be solely used for verification the Certificates issued by the root CA, the lists of the Certificates revoked by the root CA (CRLs and ARLs), and the OCSP responses released by the root CA's OCSP responder.

The Certificates of the issuing certification authorities may only be used for verification the Certificates issued, and the CRL released, by these issuing certification authorities, and the OCSP responses released by the OCSP responders (if implemented) of these issuing certification authorities.

The Certificates of the time-stamp servers of time-stamping authorities may only be used for verification of the time-stamp tokens issued by these time-stamp servers.

End user Certificates may generally be used in PKI processes, that is, for the verification of electronic signatures/marks/seals, identification, authentication and encryption.

### 1.4.2 Prohibited certificate uses

Certificates issued in accordance with a specific CP may not be used contrary to the usage described in specific CP or contrary to law.

## 1.5 Policy administration

### 1.5.1 Organization administering the document

This CPS and the certification policies corresponding thereto 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 CPS and the corresponding certification policies is specified on a web page – see 2.2.

### 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 this CPS with a specific CP.

### 1.5.4 CPS approval procedures

If it is necessary to make changes to a CPS to create a new version thereof, the 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 |
|---|---|
| authorization domain name | FQDN used to obtain authorization for a given FQDN to be included in a Certificate; CA may use the FQDN returned from a DNS CNAME lookup as the FQDN for the purposes of domain validation |
| base domain name | part of FQDN, which is first node of domain name left from:<br>▪ the one (name) checked by register; or<br>▪ public extension plus the name checked by register public extension |
| 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 label | ordered list of zero or more octets that makes up a portion of a domain name (see also RFC 8499); using graph theory, a label identifies one node in a portion of the graph of all possible domain names |
| 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,<br>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 sign | electronic sign 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 |
| LDH label | type of domain label in DNS - a string consisting of ASCII letters, digits, and the hyphen with the further restriction that the hyphen cannot appear at the beginning or end of the string, and its total length must not exceed 63 octets (see also RFC 5890)<br>note: abbreviation LDH means Letters, Digits, Hyphen |
| 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 |
| P-label | XN-Label that contains valid output of the Punycode algorithm (see RFC 3492, Section 6.3) |
| phishing | in an electronic communication attempt to obtain sensitive information (usernames, passwords, and credit card details) for malicious reasons |
| POST method | method of communication between client and http server by sending data from client to server (e.g., sending request to OCSP responder via http protocol) |
| private key | unique data to create 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) |
| public key | unique data to verify electronic signature / seal |
| 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) |
| wildcard certificate | certificate containing at least one Wildcard Domain Name within the subjectAlternativeName extensions in the Certificate |
| written contract | text of the contract in electronic or paper form |
| XN-label | class of LDH labels prefixed by "xn--" (from RFC 5890) |

**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 Certificates" published by CA/Browser Forum |
| CA | certification authority |
| CAA | DNS Resource Record - see RFC 6844 |
| 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 | certification 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) |
| DRA | distanced registration authority |
| 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 |
| DV | Domain Validation, SSL certificate type |
| EAL | Evaluation Assurance Level |
| 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 |
| 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 certification 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 certification policy, qualitatively the same as certification policy for issuing qualified certificates |
| NCP+ | Extended Normalized Certificate Policy, NCP certification policy requiring a secure cryptographic device |

| | |
|---|---|
| NKČR | Notářská komora České republiky, Notarial Chamber of the Czech Republic |
| 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 |
| SSCD | Secure Signature Creation Device (defined by directive 1999/93/ES) |

| | |
|---|---|
| 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 |
| TSP | Trust Service Provider |
| TSS | Time-Stamp Server |
| TSU | Time-Stamp Unit |
| UPN | User Principal Name, user name 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 RESPONSIBILITY

## 2.1 Repositories

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

## 2.2 Publication of certification information

The basic addresses (also as the Information Addresses) for obtaining information about První certifikační autorita, a.s., 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 is 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 – 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;
  - Links to where the CRL can be obtained in the specified formats (DER, PEM, TXT);
- Certification and other policies, practice statements and other public information.

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 certification authority's 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 (in the Czech Republic) and Hospodárske noviny or Sme (in the Slovak Republic), daily newspapers with national distribution.

## 2.3 Time or frequency of publication

See 2.3 of specific CP.

## 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, contracting partners or the parties specified by relevant legislation. Access to such information is governed by the rules defined in internal documentation, such as:

- "CA Operator";
- "I.CA Registration Authority Employees Guidelines";
- "NKČR Registration Authority (DRA NKČR) Employees Guidelines";
- "Information Security Management";
- "Administration Guidance";
- "Security Incidents";
- "HSM/Private Server";
- "HSM/nShield XC“;
- "TSS Administration";
- "TSMC Administration";
- "Certification Services Documents";
- "Certification Services Partial Document Management and Shredding Rules";
- "Certification Services Partial Document Management and Shredding Plan".

# 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 verifiable names given in the subject field and the subjectAlternativeName extension must carry a meaning. Refer to a specific CP for the attributes supported for this field and this extension.

### 3.1.3 Anonymity or pseudonymity of subscribers

See 3.1.3 of the specific certification policy.

### 3.1.4 Rules for interpreting various name forms

The data specified in a certificate application (format PKCS#10) are carried over in subject field or subjectAlternativeName extension of the Certificate in the form they are specified in the application.

### 3.1.5 Uniqueness of names

See 3.1.5 of the specific certification policy.

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

Any Certificate issued under this CPS and the relevant CPs may only contain a trademark with evidenced ownership or license. The subscriber bears any consequence resulting from unauthorized use of a trademark.

## 3.2 Initial identity validation

The identity validation procedure is given in 3.2 of specific CP and detailed in internal documentation:

- "I.CA Registration Authority Employees Guidelines";
- "NKČR Registration Authority (DRA NKČR) Employees Guidelines".

### 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

electronically signed with this private key, and/or provided with electronic sign/seal as applicable, whereby the private key holder provides evidence that he is the holder of the private key when the electronic signature, or the electronic sign/seal, is created.

### 3.2.2 Authentication of organization identity

The procedure is described in 3.2.2 of specific CP and in internal documentation:

- "I.CA Registration Authority Employees Guidelines";
- "NKČR Registration Authority (DRA NKČR) Employees Guidelines".

### 3.2.3 Authentication of individual identity

The procedure is described in 3.2.3 of a specific CP and in internal documentation:

- "I.CA Registration Authority Employees Guidelines";
- "NKČR Registration Authority (DRA NKČR) Employees Guidelines";
- "Issuing Qualified Certificates Using ZealiD Identification“.

### 3.2.4 Non-verified subscriber information

The information not subject to verification is always specified in 3.2.4 of a specific CP.

### 3.2.5 Validation of authority

Electronic mail address may be placed in the Certificate extension, that is, in the rfc822Name attribute of the subjectAlternativeName extension, only if this has been verified for the given application during the Certificate issuance procedure.

The attribute that the key pair was generated on a QSCD device may only be inserted in the Certificate if this has been verified for the given application during the Certificate issuance procedure.

The procedure to validate other specific rights is described in 3.2.5 of a specific CP.

### 3.2.6 Criteria for interoperation

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

## 3.3 Identification and authentication for re-key requests

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

Refer to 3.3.1 of a specific CP for requirements.

#### 3.3.1.1 Certificates of the provider (I.CA)

This concerns the issuance of the first Certificate, when the same requirements as those in the initial identity validation apply.

#### 3.3.1.2 End user certificates

For SSL, EV SSL and website authentication certificates, it is always the issuance of the first certificate, when the same requirements as those in the initial identity validation apply.

A subsequent Certificate may be issued for other Certificate types – the submitted standard application for a Certificate (with a new public key) is electronically signed or provided with an electronic sign/seal created with the private key matching the public key in the valid Certificate to which this subsequent Certificate is issued. In this case the applicant is not required to appear at RA in person; the Certificate applicant confirms with this electronic signature/sign/seal that no change is made to the data about the entity.

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

I.CA does not support the replacement of key pair of revoked Certificates. The only way to obtain a new Certificate is to obtain a new Certificate with a new public key.

## 3.4 Identification and authentication for revocation request

Refer to 3.4 of specific CP for specific identification and authentication methods in processing certificate revocation requests.

### 3.4.1 Certificates of the provider (I.CA)

The person authorized to request for the revocation of provider's certificate, i.e.:

- The root certification authority and the OCSP responder’s certificate issued by that root certification authority;
- The subsequent certification authority and the OCSP responder’s certificate issued by that certification authority;
- The time server of the time-stamping authority;

is CEO of I.CA.

The representative of the supervisory body may also be the requestor requesting the revocation of the root certification authority’s certificate or a certificate related to qualified certification services. The supervisory body must submit its request in writing or as a message delivered in data box of I.CA.

### 3.4.2 End user certificates

These are the available methods of identification and authentication:

- In person at RA;
- Using the form on the company’s website (and using the Certificate revocation password);
- Using an unsigned electronic message (containing the Certificate revocation password);
- Using an electronic message electronically signed/marked or having electronic seal (using the private key pertinent to the Certificate in question, which is to be revoked, or the signature Certificate’s private key);

- Using data box (and using the Certificate revocation password);
- As registered post letter sent to registered office address of I.CA (and using the Certificate revocation password).

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

I.CA reserves the right to accept also other identification and authentication procedures in processing certificate revocation requests.

# 4 CERTIFICATE LIFE-CYCLE REQUIREMENTS

## 4.1 Certificate application

### 4.1.1 Who can submit a certificate application

Certificate application may be submitted by natural person, by legal person or by government authority (also as Organization). The entities authorized to apply for a Certificate are listed in chapter 4.1.1 of specific CP.

### 4.1.2 Enrollment process and responsibilities

The processes carried out in the enrollment procedure are listed in specific CP.

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

- Provide true and complete information in application enrollment;
- Get acquainted with the CP, under which the Certificate will be issued.

The Service provider is particularly required to provide the Services in accordance with relevant legislation, the specific CP and this CPS, the System Security Policy – Trustworthy Systems and the operating documentation.

## 4.2 Certificate application processing

The handling of certificate applications is described in internal documentation:

- "I.CA Registration Authority Employees Guidelines";
- "NKČR Registration Authority (DRA NKČR) Employees Guidelines";
- "Issuing Qualified Certificates Using ZealiD Identification“;
- "CA Operator".

Checking CAA records, where relevant, is performed according to internal documentation:

- "Procedures of validation (for SSL OV/DV certificate)";
- "Procedures of validation the application for QC-web/EV SSL certificate".

### 4.2.1 Performing identification and authentication functions

The applicant for a Certificate must identify and authenticate himself in the manner defined in 3.2.2 and 3.2.3.

### 4.2.2 Approval or rejection of certificate applications

In the case of issuing Certificates of the Service provider, the management of První certifikační autorita, a.s., considers the written certificate application and may dismiss it. The result is documented.

If any of these validations done by an RA employee gives a fail result, the Certificate issuance procedure is terminated. The RA employee carries out the issuance of the Certificate if no fail result is obtained.

The procedures to accept or dismiss certificate applications are listed in 4.2.2 of specific CP and in internal documentation.

- "I.CA Registration Authority Employees Guidelines";
- "NKČR Registration Authority (DRA NKČR) Employees Guidelines".

### 4.2.3 Time to process certificate applications

In the case of issuing provider Certificates, the written certificate application must be handled within five business days of the date the application is submitted to the company management.

Any end user Certificate must be issued by I.CA immediately after Certificate issuance is granted. The following list gives tentative times for issuing Certificates unless other agreement is stipulated in the contract:

- Primary Certificate – is usually (only on business days and during business hours) issued within 15 minutes, only exceptionally it can take longer;
- Subsequent Certificates – within units of minutes.

SSL Certificates and website authentication Certificates are exceptions, Certificate applications are handled within five business days (because of validating the application data).

## 4.3 Certificate issuance

### 4.3.1 CA actions during certificate issuance

CA operators (also as the Operators) carry out the following in the **primary Certificate** issuance procedure:

- Make a visual check as to conformity of the data in the Certificate application (the PKCS#10 structure) and the data entered by an RA employee;
- Make a visual check as to the formal correctness of data.

The verification of private key ownership, the supported hash function in the Certificate application (no weaker than sha-256), the competence check and the formal data correctness check are carried out by both the software on CA operators' work stations and that on the CA system core. If any of these checks gives a fail result, the Certificate issuance procedure is terminated.

**Subsequent Certificate** issuance procedure, where applicable, is automatic without Operators' intervention. The verification of private key ownership, the supported hash function in the Certificate application (no weaker than sha-256) and the competence check are carried out by software on the CA system core. If any of these checks gives a fail result, the Certificate issuance procedure is terminated.

The procedures are described chapter in 4.3.1 of a specific CP and detailed in internal documentation:

- "I.CA Registration Authority Employees Guidelines";

- "NKČR Registration Authority (DRA NKČR) Employees Guidelines";
- "CA Operator".

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

If the certificate applicant is present at the process of Certificate issuance, the applicant receives the Certificate issuance notice from the RA employee. Issued end user certificate is always sent to the applicant's contact e-mail.

These procedures are described in detail in internal documentation:

- "I.CA Registration Authority Employees Guidelines";
- "NKČR Registration Authority (DRA NKČR) Employees Guidelines";
- "CA Operator".

## 4.4 Certificate acceptance

### 4.4.1 Conduct constituting certificate acceptance

The Certificate takeover related operations are described in 4.4.1 of specific CP.

Process details are described in internal documentation:

- "I.CA Registration Authority Employees Guidelines";
- "NKČR Registration Authority (DRA NKČR) Employees Guidelines";
- "CA Operator".

### 4.4.2 Publication of the certificate by the CA

Provider Certificates are published on I.CA website, and the Certificates related to qualified trust services are also submitted to the supervisory body.

For end user Certificates I.CA must arrange for the publication of the Certificate it issued, except any Certificate:

- Containing data, the publication of which could be contrary to relevant legislation, such as the Personal Data Protection Act;
- Required by the subscriber not to be published.

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

Chapter 4.4.2 and the requirements set out in trust services legislation apply.

## 4.5 Key pair and certificate usage

### 4.5.1 Subscriber private key and certificate usage

Subscribers must, among other things:

- Observe all relevant provisions of the Service contract (if electronic then qualified electronic signature of the contract is required);
- Use the private key and corresponding Certificate solely for the purposes defined in this CP;
- Handle the private key corresponding to the public key contained in the Certificate issued under this CP in a manner as to prevent any unauthorized use;
- Inform immediately the Service provider of everything that leads to the Certificate's revocation, in particular of:
  - Suspected abuse of the private key; and
  - Invalid or inaccurate attributes of Certificate;

  In this case request 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 other things:

- Obtain from a secure source (e.g., www.ica.cz, supervisory body web pages, RA workplace, relevant trusted list) the certification authority Certificates related to the end user Certificate issued under specific CP, and verify those Certificates' fingerprint values and validity;
- Carry out any operation necessary for them to verify that the Certificate is valid, i.e.:
  - Check Certificate validity pursuant to RFC5280, chapter 6 (including the full certification path and Certificate revocation);
  - Check whether the issuer of the qualified Certificate is qualified (is on the trust services list with the pertinent attributes);
- Observe all and any provisions of the pertinent CP and trust services legislation which relate to the relying party's duties.

## 4.6 Certificate renewal

The certificate renewal service means the issuance of a subsequent certificate for a still valid certificate without changing the public key or changing other information in the certificate, or for a revoked certificate, or for an expired certificate.

The certificate renewal service is not provided.

It is always the issuance of a new Certificate with a new public key, with all the information having to be duly verified. The same requirements as those in the initial identity validation apply – see 3.2.

### 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

See 4.7 of specific CP.

### 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 to 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

See 4.8 of specific CP.

### 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

### 4.9.1 Circumstances for revocation

In addition to the conditions specified in the following sections, I.CA reserves the right to accept also other Certificate revocation situations.

#### 4.9.1.1 Certificates of the provider (I.CA)

A Certificate must be revoked as a result of the following situations:

- The private key corresponding to the Certificate's public key is compromised or reasonably suspected to have been compromised;
- CEO of I.CA requests so;
- In any event specified in trust services legislation or technical standards.

#### 4.9.1.2 End user certificates

A Certificate must be revoked as a result of the following situations:

- The private key corresponding to the Certificate's public key is compromised or reasonably suspected to have been compromised;
- The subscriber violated the Service contract (under specific CP);
- In any event specified in trust services legislation or the relevant technical standards, such as Certificate data being or having become invalid;
- If the public key in the certificate application is the same as the public key in a Certificate already issued.

I.CA reserves the right to accept also other end user Certificate revocation situations, which, however, must not be contrary to trust services legislation.

### 4.9.2 Who can request revocation

In case of provider's (I.CA) certificates:

- CEO of I.CA or the person authorized by him; and
- Other entities as may be specified in trust services legislation.

In case of end user certificates see 4.9.2 of the specific certification policy.

### 4.9.3 Procedure for revocation request

The procedure for submitting end user certificate revocation request is always described in 4.9.3 of specific CP.

The identification and authentication requirements are listed in 3.4.

### 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

The maximum time allowed between accepting a certificate revocation request and the Certificate's revocation is 24 hours.

Procedures are described in internal documentation:

- "I.CA Registration Authority Employees Guidelines";
- "NKČR Registration Authority (DRA NKČR) Employees Guidelines";
- "CA Operator".

### 4.9.6 Revocation checking requirement for relying parties

Relying parties must carry out all the operations specified in 4.5.2.

### 4.9.7 CRL issuance frequency

The interval for releasing CRLs is specified in 4.9.7 of specific CP.

The operations of CA operators in creating and releasing CRLs are described in internal documentation:

- "CA Operator'.

### 4.9.8 Maximum latency for CRLs

The CRL is published immediately after issuing, conditions described in 4.9.5 and 4.9.7 are always met.

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

Checking certificate status online using the OCSP protocol is a service available to the general public. Every certificate excluding root certification authorities' certificates and OCSP responders' certificates contains the link to the pertinent OCSP responder.

OCSP responses satisfy the RFC 2560 and RFC 5019 standards. The OCSP responder's certificate includes an id-pkix-ocsp-nocheck extension as defined in RFC 2560.

### 4.9.10 On-line revocation checking requirements

See 4.9.9.

If on-line Certificate status information is different from the one from CRL then it is necessary to repeat on-line status information checking after at least ten seconds.

### 4.9.11 Other forms of revocation advertisements available

Not applicable to this document.

### 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 to this document; the certificate suspension service is not provided.

### 4.9.14 Who can request suspension

Not applicable to this document; the certificate suspension service is not provided.

### 4.9.15 Procedure for suspension request

Not applicable to this document; the certificate suspension service is not provided.

### 4.9.16 Limits on suspension period

Not applicable to this document; the certificate suspension service is not provided.

## 4.10 Certificate status services

### 4.10.1 Operational characteristics

Lists of public Certificates are provided as published information; CRLs are provided as published information and CRL distribution points are contained in certificates excluding root certification authorities' certificates and OCSP responders' certificates.

The fact that certification authorities provide certificate status information as OCSP is specified in the certificates issued by these authorities.

### 4.10.2 Service availability

I.CA guarantees round-the-clock (24/7) availability and integrity of the list of the I.CA-issued certificates and the certificate revocation lists (CRLs), plus the availability of the OCSP service.

The procedure is specified in internal documentation including:

- "Administration Guidance";
- "Operating Site Component Recovery";
- "Operating Site Relocation".

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

I.CA publishes, in compliance with relevant standards requirements, CRLs containing qualified certificates which expired no more than three days ago (CRL contains extension ExpiredCertsOnCRL). The period is limited in order to keep CRLs to a reasonable length.

I.CA in compliance with relevant standards requirements ensures consistency of certificate status information between CRL and OCSP response. OCSP responses concerning qualified certificates contain ArchiveCutOff extension to support these requirements.

## 4.11 End of subscription

Contract can be terminated by written agreement of the parties or after the expiration of the last Certificate issued under that contract.

## 4.12 Key escrow and recovery

Not applicable to this document; the 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 designed to support the Services;
- All processes supporting the provision of the Services specified above.

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 more detailed internal documentation. These documents take account of the results of periodic risk analyses.

## 5.1 Physical controls

Physical security is addressed in detail in internal documentation in general and these documents in particular:

- "I.CA Rooms Physical Access Control";
- "Fire Safety";
- "Inspection Activity, Clean Criminal Record and Competence";
- "Security Incidents";
- "Operating Site Component Recovery";
- "Operating Site Relocation";
- "CCTV – Operating Site";
- physical security projects of particular operating sites.

### 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 designed to support the 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

Refer to 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 the 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 the Services are so located as to ensure they cannot be flooded with a 100-year flood. Where 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 archiving sites have fire alarm system (FAS). Fireproof insulation is installed in the entrance doors to the restricted areas in which the trustworthy systems destined to support the Services are situated, and fire extinguishers are fitted in these areas.

### 5.1.6 Media storage

Archiving 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.

Any paper media required to be archived are stored in a site geographically different from the site of the operating office.

### 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 the 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 and their responsibilities are defined in internal documentation in general and the following documents in particular:

- "System Security Policy – Trustworthy Systems";
- "Information Security Management";
- "Administration Guidance".

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

### 5.2.2 Number of persons required per task

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

- Initialization of cryptographic module;
- Generating key pairs of certification authorities and their OCSP responders;
- Destroying private keys of certification authorities and their OCSP responders including the backups;
- Backup and restore of private keys of certification authorities and their OCSP responders;
- Activation and deactivation of private keys of certification authorities and their OCSP responders.

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

Detailed information is always specified in 5.2.2 of specific CP and in internal documentation:

- "Administration Guidance";
- "Hierarchical Structure – Procedures to Generate CA Keys and Certificates";
- "HSM nShield – Procedures to Generate CA and OCSP Keys and Certificates";
- "HSM/Private Server";
- „HSM/nShield XC“.

### 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. These topics are regulated in internal documentation in general and these documents in particular:

- "I.CA Registration Authority Employees Guidelines";
- "NKČR Registration Authority (DRA NKČR) Employees Guidelines";
- "CA Operator";
- "Administration Guidance".

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

### 5.2.4 Roles requiring separation of duties

The roles requiring distribution of responsibilities (and the roles' job descriptions) are described in internal documentation:

- "System Security Policy – Trustworthy Systems".

## 5.3 Personnel controls

### 5.3.1 Qualification, experience, and clearance requirements

Trusted roles employees are in I.CA selected and hired 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 the Services is hired subject to 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 or technical training experience in respect of the trustworthiness of the Services, the knowledge of security procedures with security responsibility, and experience in information security and risk assessment.

These topics are described in detail in internal documentation:

- "Inspection Activity, Clean Criminal Record and Competence".

### 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 specialized 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.

These topics are described in detail in the internal documentation:

- "Inspection Activity, Clean Criminal Record and Competence".

### 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.

These topics are described in detail in internal documentation:

- "Inspection Activity, Clean Criminal Record and Competence".

### 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).

These topics are described in detail in internal documentation:

- "Employment Rules".

### 5.3.7 Independent contractor requirements

I.CA may or must procure some activities from independent contractors and is fully responsible for the job they deliver. These business relations are regulated in bilateral business contracts with parties such as contracted registration authorities, application software developers, hardware suppliers, system software suppliers, external auditors and other parties. These parties are required to observe the specific certification 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 certification policy, the certification practice statement and the security and operating 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

For qualified Certificates, subject to logging are all events required by trust services legislation and the relevant technical standards referred to therein to be logged, otherwise it is the events required by the relevant technical standards to be logged, such as life cycle events of the Certificates issued, the handling of the provider’s private keys and other events (the termination of a certification authority’s operations, for example).

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 maintenance, sufficient space for audit data, automatic non-writing of the audit file, user-friendly presentation of audit records, and audit file access limited to the defined users only.

Creating, processing and keeping audit logs are addressed in detail in internal documentation and the following documents in particular:

- "Administration Guidance";
- "Gathering Data to Be Archived";
- "Application Systems Data Backup";
- "Certification Services Documents";
- "Certification Services Partial Document Management and Shredding Rules";
- "Certification Services Partial Document Management and Shredding Plan".

### 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 generating with data required by technical standards is created on key pair generating and is signed by present I.CA 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.

Given the requirements of relevant technical standards and trust services legislation, the following security-relevant operating events are electronically audit-logged in trustworthy systems of I.CA:

- System-relevant events in environment and key management;
- Audit function start and audit function end;
- Changes to audit parameters;
- Actions taken upon an audit record storage error;
- Any attempt to access the system;

- Any event pertaining to the life cycle of CA key pair and Certificates;
- Applicant registration record;
- Any attempted unauthorized applicant registration (with as much information about the unauthorized applicant as possible);
- Applicant registration cancellation record (applicant data are preserved);
- Anything about the life cycle of Certificate:
  - Record of RA certificate issuance application plus the result;
  - Record of unauthorized certificate issuance application plus result;
  - Record of subsequent certificate issuance application plus the result;
  - Record of unauthorized subsequent certificate issuance application plus the result;
  - Record of certificate revocation request plus requesting party data and the result;
  - Record of unauthorized certificate revocation request plus requesting party data and the result;
  - Record of the notification of possible compromise of the data for creating electronic signatures and/or marks by the signing/marking person;
  - Certificate revocation record;
  - Record of attempted unauthorized system access;
  - Record of Certificate publication plus the result;
  - Record of putting a revoked Certificate on the CRL;
  - CRL release record.

All the records in the audit log have the following parameters:

- Date (year, month, day) and time (hour, minute, second) of the event;
- Type of event;
- Identity of the entity responsible for the operation;
- Success/failure of the audited event.

### 5.4.2 Frequency of processing log

Audit records are checked and assessed at the intervals defined in internal documentation:

- "Administration Guidance".

or immediately when a security incident occurs.

### 5.4.3 Retention period for audit log

Unless relevant legislation provides otherwise, audit records are kept for a minimum of 10 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, stealing and destruction (willful or accidental).

Electronic audit records are archived in two copies, with each copy kept in a different room of the operating site. These audit records are saved on a medium each month or more frequently and this medium is kept outside the operating premises of I.CA.

Printed audit records are kept outside the operating premises of I.CA.

The protection of the aforesaid types of audit records is described in internal documentation – see 5.4.

### 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 the Services is described in internal documentation:

- "Approach to Assessment and Management of Information Security Risks - Trustworthy Systems";
- "Administration Guidance".

## 5.5 Records archival

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

- "I.CA Rooms Physical Access Control";
- "Gathering Data to Be Archived";
- "Application Systems Data Backup";
- "Administration Guidance";
- "Certification Services Documents";
- "Certification Services Partial Document Management and Shredding Rules";
- "Certification Services Partial Document Management and Shredding Plan".

### 5.5.1 Types of records archived

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

- Records / protocols on the course of certification authorities key pair generating;
- Life cycle records for the Certificates;
- Video recording of generating key pair of the subsequent certification authority issuing SSL type certificates to end users;
- Other records that may be necessary for issuing Certificates;
- Information handling records, such as takeover, handover, saving, check, conversion from printed to electronic, etc.;
- Application software, operating and security documentation.

### 5.5.2 Retention period for archive

All records pertaining to the certificates of all I.CA certification authorities and their respective OCSP responders, except for the pertinent private keys, are archived throughout the existence of I.CA. Other records are archived in accordance with 5.4.3.

The records archiving procedures are regulated in internal documentation.

### 5.5.3 Protection of archive

The premises where records are stored are secured with measures based on building and physical security and the Classified Information Protection Act.

The procedures to protect archived records are regulated in internal documentation – see 5.5.

### 5.5.4 Archive backup procedures

The record backup procedures are regulated in internal documentation – see 5.5.

### 5.5.5 Requirements for time-stamping of records

If time-stamp tokens are used, they will be 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 archiving and stored – refer to 5.5. Records are kept of collecting records.

### 5.5.7 Procedures to obtain and verify archive information

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

- I.CA employees if they need to have such an access for their job;
- Authorized supervising and inspection entities and law enforcement authorities 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 certificate), the key 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 cryptanalytic algorithms or key length), the key is replaced as soon as possible.

In both standard and non-standard situations, the replacement of the public key in certification authorities' 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 documentation:

- "Business Continuity Plan and Recovery Plan";
- "Operating Site Component Recovery";
- "Operating Site Relocation";
- "Security Incidents".

### 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 authorities 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 pertinent certification authority;
- Notifies this and the reason immediately on its web Information Address, and also the certificate revocation list (CRL) is used for disclosing this information;

- For qualified Certificates, notifies the supervisory body of the revocation of a Certificate and the reason therefore.

A similar course of action will be taken in the event of such developments in cryptanalytic methods, such as changes to cryptanalytic algorithms or key length that could immediately compromise the security of the Services.

### 5.7.4 Business continuity capabilities after a disaster

In the event of accident, I.CA takes a course of action in accordance with internal documentation:

- "Business Continuity Plan and Recovery Plan";
- "Operating Site Component Recovery";
- "Operating Site Relocation".

## 5.8 CA or RA termination

The following apply to the termination of the CA's operations:

- Such termination must be notified in writing to all subscribers of valid Certificates, the entities having a contract directly pertaining to the provision of the certification Services, and the supervisory body if qualified Certificates are concerned;
- The termination of the CA's operations must be published on the web page pursuant to 2.2;
- If the CA 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 the Services;
- The certification authority must arrange no less than certificate revocation and CRL release as long as any certificate issued by the certification authority is valid;
- After that the CA must demonstrably destroy its private key, make a record of this destruction and keep this record in accordance with this CPS and specific CP.

In the event of withdrawal of the qualified trust services provider status:

- The information must be notified in writing or electronically to all subscribers of valid Certificates, and the parties having a contract that directly concerns the provision of trust services;
- The information must be published in accordance with 2.2. at all offices of registration authorities and must also communicate that qualified system 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.

If a specific RA office closes down, this is published on http://www.ica.cz.

Planned termination of operations of I.CA in the position of qualified trust services provider is described in detail in internal documentation:

- "I.CA Services Termination".

Rules concerning to the termination of specific certification authorities and corresponding RAs are described in specific CPs.

# 6 TECHNICAL SECURITY CONTROLS

## 6.1 Key pair generation and installation

### 6.1.1 Key pair generation

Key pairs of certification authorities, their corresponding OCSP responders and TSUs of TSA2 system are generated in designated secured areas of operating sites, according to a pre-defined scenario, in accordance with 5.2 and 5.4.1. Generating is carried out in cryptographic modules evaluated according to the standard FIPS PUB 140-2 level 3 or to the standard ISO/IEC 15408 to assurance level at minimum EAL 4 with protection profile EN 419 221-5: Protection Profiles for TSP Cryptographic Modules - Part 5: Cryptographic Module. These cryptographic modules are under sole control of I.CA.

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

- "I.CA Rooms Physical Access Control";
- "HSM/Private Server";
- "HSM/nShied XC";
- "TSS Administration";
- "TSMC Administration";
- "Hierarchical Structure – Procedures to Generate CA Keys and Certificates";
- "HSM nShield – Procedures to Generate CA and OCSP Keys and Certificates".

The report documenting key pair generating must include no less than:

- List of the names of the employees who are present;
- Dates and times (to the minute) when key pair generating is started and ended;
- Place of generating;
- Description of the device on which generating is carried out – this description must uniquely identify the device;
- Date of the report;
- Own signatures of all the employees who carried out key pair generating.

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

Key pairs related to creation of remote electronic signatures and remote electronic seals of end users are generated in QSCD type cryptographic module which is under sole control of I.CA and is evaluated according to the standard ISO/IEC 15408 to assurance level at minimum EAL 4 with protection profile EN 419 221-5: Protection Profiles for TSP Cryptographic Modules - Part 5: Cryptographic Module. Both the presence of these devices in EU Trusted List and the device certification validity period are continuously checked according to internal documentation:

- "Administration Guidance'.

Key pairs related to the certificates issued to other end users are generated on devices which are under sole control of the respective private key holders. These key pairs may be stored on hardware and in software. In case of qualified certificates having the private key corresponding with public key contained in this certificate stored on QSCD, both the presence of these devices in EU Trusted List and the device certification validity period are continuously checked according to internal documentation:

- "QSCD Personalization".

### 6.1.2 Private key delivery to subscriber

Not applicable to private keys of certification authorities and their corresponding OCSP responders – private keys are stored in a cryptographic module under the sole control of I.CA.

Not applicable to private keys of TSUs of TSA2 system – private keys are stored in cryptographic modules which are parts of TSUs of TSA2 system and are under the sole control of I.CA.

Not applicable to the private keys related to the services of creation of remote electronic signatures and remote electronic seals - private keys are stored in a cryptographic module or in QSCD under the control of I.CA.

Generating key pairs for other end users and for the employees taking part in the issuance of Certificates to end users is not provided.

### 6.1.3 Public key delivery to certificate issuer

Not applicable to private keys of certification authorities, their OCSP responders, TSUs of TSA2 system and those related to services of creation of remote electronic signatures and remote electronic seals - private keys are stored in the cryptographic modules under the control of I.CA.

In other cases, public keys (the PKCS#10 format) are delivered as part of the certificate application.

### 6.1.4 CA public key delivery to relying parties

Certification authorities' public keys are included in these authorities' certificates, and the following options for obtaining the keys are guaranteed:

- Handover from RA;
- Via web information addresses of I.CA, relevant supervisory body or its journal;
- Every subscriber gets relevant certification authorities' certificates together with his 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 of other issued Certificates is stated in specific CP.

### 6.1.6 Public key parameters generation and quality checking

Parameters of the algorithms used in generating the public keys of certification authorities and their OCSP responders, public keys of TSUs of TSA2 system and private keys corresponding with certificates related to remote signing and remote sealing meet the requirements of trust services legislation i.e., in technical standards and norms referred by this legislation. These keys are generated and checked by relevant software.

Parameters of the algorithms used in generating the public keys of other subscribers must meet the same requirements and are check 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

The specific procedures how to protect private keys in cryptographic modules under control of I.CA are described in internal documentation:

- "I.CA Rooms Physical Access Control";
- "HSM/Private Server";
- "HSM/nShield XC";
- "Hierarchical Structure – Procedures to Generate CA Keys and Certificates";
- "HSM nShield – Procedures to Generate CA and OCSP Keys and Certificates";
- "TSS Administration";
- "TSMC Administration".

### 6.2.1 Cryptographic module standards and controls

Key pairs of certification authorities, their OCSP responders and TSUs of TSA2 system are generated and private keys are stored in cryptographic modules evaluated according to the standard FIPS PUB 140-2 level 3 or to the standard ISO/IEC 15408 to assurance level at minimum EAL 4 with protection profile EN 419 221-5: Protection Profiles for TSP Cryptographic Modules - Part 5: Cryptographic Module.

Key pairs corresponding with certificates related to services of creation of remote electronic signatures and remote electronic seals are generated and private keys are stored in QSCD type cryptographic module which is under sole control of I.CA and is evaluated according to the standard ISO/IEC 15408 to assurance level at minimum EAL 4.

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

Using cryptographic modules by other end users is fully within their competence.

### 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 some part of the code required for these operations.

### 6.2.3 Private key escrow

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

### 6.2.4 Private key backup

The cryptographic modules used for the administration of certification authorities' and their corresponding OCSP responders' private keys, private keys od TSUs of TSA2 system and private keys corresponding with certificates related to services of creation of remote electronic signatures and remote electronic seals facilitates private key backup. Encryption of these backups ensures the same level of protection as the cryptographic module does.

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

Backuping private keys of other end users is fully within the competence of these end users.

### 6.2.5 Private key archival

When certification authorities' and their corresponding OCSP responders' private keys, private keys of TSUs of TSA2 system and private keys corresponding with certificates related to services of creation of remote electronic signatures and remote electronic seals 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

Archiving private keys of other end users is fully within the competence of these end users.

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

Private keys of certification authorities and their corresponding OCSP responders, private keys of TSUs of TSA2 system and private keys corresponding with certificates related to services of creation of remote electronic signatures and remote electronic seals are generated (as non-exportable) in cryptographic modules (operated in certified mode) and there is no way to export them outside the cryptographic module[1]. Import of private keys into the specific cryptographic module complies with the certification of this module.

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

Transferring private keys of other end users is fully within the competence of these end users.

### 6.2.7 Private key storage on cryptographic module

Private keys of certification authorities, their OCSP responders and TSUs of TSA2 system are stored in the cryptographic module which meets the requirements of trust services legislation, that is FIPS PUB 140-2 level 3 standard or the standard ISO/IEC 15408 evaluated at minimum to assurance level EAL 4 with protection profile EN 419 221-5: Protection Profiles for TSP Cryptographic Modules - Part 5: Cryptographic Module for Trust

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

Services. When stored outside the cryptographic module the private keys are encrypted in compliance with the certification of the cryptographic module.

Private keys corresponding with certificates related to services of creation of remote electronic signatures are stored in QSCD type cryptographic modules under sole control of ICA, which fulfill the requirements of ISO/IEC 15408 standard to assurance level EAL4 at minimum.

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

Possible storing private keys of other end users in cryptographic modules is fully within the competence of these end users.

### 6.2.8 Method of activating private key

Activation of certification authorities' and their corresponding OCSP responders' private keys, private keys of TSUs of TSA2 system and private keys corresponding with certificates related to services of creation of remote electronic signatures and remote electronic seals (allowing the use of these private keys) is done:

- In case of smartcard activation by inserting the smartcard 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 and entering PIN.

Activation private keys of other end users is fully within the competence of these end users and depends on the way of storing these private keys.

### 6.2.9 Method of deactivating private key

Deactivation private keys of certification authorities' and their corresponding OCSP responders' is done by removing smartcard or by quitting specific application.

Deactivation private key of TSU of TSA2 system is done by selecting new profile.

Deactivation private keys corresponding with certificates related to services of creation of remote electronic signatures and remote electronic seals is done:

- When subsequent certificate is issued; or
- When quitting specific application.

Private keys of employees taking part in issuing certificates are deactivated by removing the smartcard,

Deactivation private keys of other end users is fully within the competence of these end users and depends on the way of storing these private keys.

### 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 TSUs of TSA2 system means secure deletion of securely and encrypted (certified method of encryption) directory structure and is done, including destroying backups, at the command od CEO of I.CA or the member of the board authorized by him. Destroying is documented in a written record.

Destroying private keys corresponding with certificates related to services of creation of remote electronic signatures and remote electronic seals, including backups, is done:

- When subsequent certificate is issued; or
- When the contract is terminated; or
- When the certificate expired or was revoked;

using native features of cryptographic module, or QSCD or QSealCD.

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.

Destroying private keys of other end users is fully within the competence of these end users.

### 6.2.11 Cryptographic module rating

Cryptographic modules in which key pairs of certification authorities, their OCSP responders and TSUs of TSA2 system of are generated and their private keys stored meet the requirements of trust service legislation i.e., standard FIPS PUB 140-2 level 3 or standard ISO/IEC 15408 with evaluation assurance level at minimum EAL 4; protection profile is EN 419 221-5 "Protection Profiles for TSP Cryptographic Modules - Part 5: Cryptographic Module for Trust Services". The security and listing on EU Trusted List of these modules are under monitoring as long as they are in use.

Cryptographic modules in which key pairs corresponding with certificates related to services of creation of remote electronic signatures and remote electronic seals are generated and the private keys are stored meet QSCD requirements. QSCD is under sole control of I.CA and is evaluated according to the standard ISO/IEC 15408 to assurance level at minimum EAL 4.

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

Possible usage of cryptographic modules by other end users (including evaluation these modules) is fully within the competence of these end users.

## 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, private keys of TSUs of TSA2 system and private keys corresponding with certificates related to services of creation of remote electronic signatures and remote electronic seals (smartcard or softcard) are created before or during the generating of the corresponding key pair.

Procedures are described in internal documentation:

- "HSM/Private Server";
- "HSM/nShield XC";
- "TSS Administration".

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

Possible usage of activation data by other end users is fully within the competence of these end users.

### 6.4.2 Activation data protection

Private keys of certification authorities, their OCSP responders, TSUs of TSA2 system and those corresponding with certificates related to services of creation of remote electronic signatures and remote electronic seals (smartcard or softcard) activation data are protected by passwords.

Procedures are described in internal documentation:

- "HSM/Private Server";
- "HSM/nShield XC";
- "TSS Administration".

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

Activation data of end users' private keys protection is fully within the competence of these employees.

### 6.4.3 Other aspects of activation data

Not applicable to this document.

## 6.5 Computer security controls

### 6.5.1 Specific computer security technical requirements

The security level 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, i.e., ETSI and CEN standards listed in 6.5.2. The solution is described in detail in internal documentation, in particular in:

- "System Security Policy – Trustworthy Systems";
- "Administration Guidance";
- "I.CA Rooms Physical Access Control";
- "HSM/Private Server";
- "HSM/nShield XC";
- "TSS Administration";
- "TSMC Administration".

### 6.5.2 Computer security rating

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

- CEN/TS 419261 Security requirements for trustworthy systems managing certificates and time-stamps.
- ČSN ETSI EN 319 401 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 Electronic Signatures and Infrastructures (ESI) – Trust Service Provider Conformity Assessment – Requirements for Conformity Assessment Bodies Assessing Trust Service Providers;
- ETSI EN 319 403 Electronic Signatures and Infrastructures (ESI); Trust Service Provider Conformity Assessment - 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 Electronic Signatures and Infrastructures (ESI); Certificate Profiles; Part 4: Certificate profile for web site certificates.
- 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: QCStatements.
- 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.
- ISO/IEC 15408-1:2009 Information technology — Security techniques — Evaluation criteria for IT security — Part 1: Introduction and general model.
- ČSN EN ISO/EC 15408-2 Information technology — Security techniques — Evaluation criteria for IT security — Part 2: Security functional components.
- ISO/IEC 15408-2:2008 Information technology — Security techniques — Evaluation criteria for IT security — Part 2: Security functional components.
- ČSN EN ISO/EC 15408-3 Information technology — Security techniques — Evaluation criteria for IT security — Part 3: Security assurance components.
- ISO/IEC 15408-3:2008 Information technology — Security techniques — Evaluation criteria for IT security — Part 3: Security assurance components.
- ČSN EN 419 241-1 – Trustworthy Systems Supporting Server Signing - Part 1: General System Security Requirements.
- EN 419 241-1 – Trustworthy Systems Supporting Server Signing - Part 1: General System Security Requirements.
- ČSN EN 419 241-2 – Trustworthy Systems Supporting Server Signing - Part 2: Protection profile for QSCD for Server Signing.
- EN 419 241-2 – Trustworthy Systems Supporting Server Signing - Part 2: Protection profile for QSCD for Server Signing.
- CA/Browser Forum - Baseline Requirements for the Issuance and Management of Publicly-Trusted Certificates (Baseline Requirements).
- CA/Browser Forum - Guidelines For The Issuance And Management Of Extended Validation Certificates.
- FIPS PUB 140-2 Requirements for Cryptographic Modules.

- ETSI TS 119 312 Electronic Signatures and Infrastructures (ESI); Cryptographic Suites.
- 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.
- ETSI TS 119 495 Electronic Signatures and Infrastructures (ESI); Sector Specific Requirements; Qualified Certificate Profiles and TSP Policy Requirements under the payment services Directive (EU) 2015/2366.
- ČSN 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 2560 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:

- "Change Control";
- "Development Methodology".

### 6.6.2 Security management controls

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

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

- ČSN ISO/IEC 27000 Information Technology – Security Techniques – Information Security Management Systems – Overview and Vocabulary;
- ČSN ISO/IEC 27001 Information Technology – Security Techniques – Information Security Management Systems – Requirements;
- ČSN ISO/IEC 27002 Information Technology – Security Techniques – Information Security Management Systems – Code of Practice for Information Security Controls.

These topics are described in internal documentation:

- "Inspection Activity, Clean Criminal Record and Competence".

### 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, as is described in internal documentation:
  - "Corporate Security Policy";
  - "Information Security Policy - Trustworthy Systems";
  - "Approaches to Assess and Address Information Security Risks - Trustworthy Systems";
  - "ISMS Scope - Trustworthy Systems";
  - "Risk Analysis - Trustworthy Systems, Final Report";
  - "Statement of Applicability - Trustworthy Systems";
  - "Risk Handling/Management Plan - Trustworthy Systems";
  - "Residual Risks – Summary for Management - Trustworthy Systems";
- Implementing and operating – effective and systematic enforcement of the selected security controls, as is described in internal documentation:
  - "I.CA Rooms Physical Access Control";
  - "Fire Safety";
  - "HSM/Private Server";
  - "HSM/nShield XC";
  - "Information Security Management";
  - ‘Application Systems Data Backup";
  - "Administration Guidance";
  - "Firewall – Operating Site";

- "Inspection Activity, Clean Criminal Record and Competence";
- "Change Control";
- "Security Incidents";
- "RemoteSign Activation Envelopes";
- "Operating Site Component Recovery";
- "Operating Site Relocation";
- "Firewall – Operating Site";
- "CCTV – Operating Site";
- "Crisis Scenarios";
- physical security projects of particular operating sites;
- in other documentation maintained at the operating site (see "Administration Guidance");

- 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, as is described in the documents:
  - Internal inspection reports;
  - External inspection reports and external audit reports;
- 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. All communication between RA and the operating sites is encrypted.

The detailed network security management solution is described in internal documentation:

- "System Security Policy – Trustworthy Systems";
- "Administration Guidance";
- "Firewall – Operating Site";
- "Business Continuity Plan and Recovery Plan";
- "Operating Site Component Recovery";
- "Operating Site Relocation".

## 6.8 Time-stamping

See 5.5.5 for the time-stamping solution.

# 7 CERTIFICATE, CRL AND OCSP PROFILES

The Certificate profile, the CRL profile and the OCSP profile are always given in specific CP. The following chapters only describe the changes, if any, the making of which is reserved by I.CA in specific CP.

Admitted attribute types and attribute length (in characters) for subject field and subjectAlternativeName extension if these are part of the Certificate:

- In qualified certificates for electronic signature, seal and website authentication and in system certificates, non-qualified (commercial) SSL Certificates (OVCP and DVCP), they are given in Table 4, column two;
- In other types of certificates, they are given in Table 4, column three.

**Table 4 – Attribute types and attribute length for subject field and subjectAlternativeName extension**

| **Field \| extension/attribute** | **Qualified certificates for electronic signature, seal and website authentication; system Certificates; non-qualified SSL Certificates (OVCP and DVCP)** | **Other types of certificates** |
|---|---|---|
| **subject** | | |
| countryName | PrintableString (2) | PrintableString (2) |
| givenName | UTF8String (1..64) | PrintableString,<br>UTF8String (1..64) |
| surName | UTF8String (1..64) | PrintableString,<br>UTF8String (1..64) |
| pseudonym | UTF8String (1..128) | PrintableString,<br>UTF8String (1..128) |
| serialNumber | PrintableString (1..64) | PrintableString (1..64) |
| commonName | UTF8String (1..64) | PrintableString,<br>UTF8String (1..64) |
| initials | UTF8String (1..64) | PrintableString,<br>UTF8String (1..64) |
| emailAddress | IA5String (1..64) | IA5String (1..64) |
| name | UTF8String (1..128) | PrintableString,<br>UTF8String (1..128) |
| generationQualifier | UTF8String (1..64) | PrintableString,<br>UTF8String (1..64) |
| organizationName | UTF8String (1..64) | PrintableString, |

| | | |
|---|---|---|
| | | UTF8String (1..64) |
| organizationalUnitName | UTF8String (1..64) | PrintableString,<br>UTF8String (1..64) |
| title | UTF8String (1..64) | PrintableString,<br>UTF8String (1..64) |
| stateOrProvinceName | UTF8String (1..128) | PrintableString,<br>UTF8String (1..128) |
| localityName | UTF8String (1..128) | PrintableString,<br>UTF8String (1..128) |
| streetAddress | UTF8String (1..128) | PrintableString,<br>UTF8String (1..128) |
| postalCode | UTF8String (1..40) | PrintableString,<br>UTF8String (1..40) |
| organizationIdentifier | UTF8String (1..128) | PrintableString,<br>UTF8String (1..128) |
| businessCategory | UnboundDirectoryString (1..64) | |
| jurisdictionCountryName | PrintableString (2) | |
| jurisdictionStateOrProvinceName | UTF8String (1..128) | |
| jurisdictionLocalityName | UTF8String (1..128) | |
| **subjectAlternativeName** | | |
| otherName.IKMPSV (1.3.6.1.4.1.11801.2.1) | UTF8String (1..10) | not permitted |
| otherName.ICA_SN (1.3.6.1.4.1.23624.4.6) | UTF8String (1..8)<br>check: only digits/characters ‘0’ to ‘9’ | UTF8String (1..7)<br>check: only digits/characters ‘0’ to ‘9’ |
| otherName.universalPrincipalName (1.3.6.1.4.1.311.20.2.3, Microsoft UPN) | not permitted | UTF8String (1..255) |
| rfc822Name | IA5String (1..320)<br>check: correct e-mail address format | IA5String (1..320)<br>check: correct e-mail address format |
| dNSName | IA5String (1..255) | not permitted |

| | | |
|---|---|---|
| | check: correct DNS name format | |
| description | UnboundDirectoryString (1..1024) | |
| DN Qualifier | PrintableString (1..64) | |
| DMDName | UnboundDirectoryString (1..64) | |

## 7.1 Certificate profile

See chapter 7.

### 7.1.1 Version number(s)

See chapter 7.

### 7.1.2 Certificate extensions

See chapter 7.

### 7.1.3 Algorithm object identifiers

See chapter 7.

### 7.1.4 Name forms

See chapter 7.

### 7.1.5 Name constraints

See chapter 7.

### 7.1.6 Certificate policy object identifier

See chapter 7.

### 7.1.7 Usage of Policy Constraints extension

See chapter 7.

### 7.1.8 Policy qualifiers syntax and semantics

See chapter 7.

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

See chapter 7.

## 7.2 CRL profile

See chapter 7.

### 7.2.1 Version number(s)

See chapter 7.

### 7.2.2 CRL and CRL entry extensions

For qualified Certificates, CRLs include an extension (expiredCertsOnCRL), which specifies that the CRL also contains expired Certificates for the defined period (see 4.10.3).

## 7.3 OCSP profile

Both the OCSP request profile and the OCSP response profile are in accordance 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. The unAuthorized response is given for any certificate not issued by the relevant CA. Http only is used as the transmission protocol.

**Table 5 – OCSP request profile**

| Request attributes | Notes |
|---|---|
| **OCSPRequest** ::= SEQUENCE { | |
| **tbsRequest** TBSRequest | |
| TBSRequest ::= SEQUENCE<br>{ | |
| version [0] EXPLICIT Version DEFAULT v1, | |
| requestorName [1] EXPLICIT GeneralName OPTIONAL | |
| **requestList** SEQUENCE OF Request, | OCSP responder only responds to the first request in the list in the OCSP request and ignores any other request.<br>(RFC5019) |
| **Request** ::= SEQUENCE<br>{ | |
| reqCert CertID, | mandatory attribute (if not included, *malformedRequest* will be the response) |
| CertID ::= SEQUENCE { | |
| hashAlgorithm AlgorithmIdentifier, | OID of the hash algorithm for the following two attributes - identification of the requested certificate's issuer specified by the client; OCSP responder imposes no limit (and processes requests with all the openssl-enabled hash algorithms) |

| | |
|---|---|
| issuerNameHash OCTET STRING, | hash field of the issuer of the certificate requested |
| issuerKeyHash OCTET STRING, | hash of the public key of the issuer of the certificate requested |
| serialNumber CertificateSerialNumber<br>} | serial number of the certificate requested |
| singleRequestExtensions [0]EXPLICIT Extensions OPTIONAL | it is not permitted under RFC5019, and if it is used in the request, it is ignored |
| Extensions ::= SEQUENCE SIZE (1..MAX) OF Extension | |
| Extension ::= SEQUENCE {<br>extnID OBJECT IDENTIFIER,<br>critical BOOLEAN DEFAULT FALSE,<br>extnValue OCTET STRING } | according to RFC6960, the following is permitted to occur here:<br>- *ServiceLocator* |
| } | |
| **requestExtensions** [2] EXPLICIT Extensions OPTIONAL | ignored |
| Extensions ::= SEQUENCE SIZE (1..MAX) OF Extension | all extensions ignored |
| Extension ::= SEQUENCE { | |
| extnID OBJECT IDENTIFIER,<br>critical BOOLEAN DEFAULT FALSE,<br>extnValue OCTET STRING } | according to RFC6960, the following is permitted to occur:<br>- *Nonce* - ignored according to RFC5019;<br>- *AcceptableResponses;*<br>- *PreferredSignatureAlgorithm*s |
| } | |
| **optionalSignature** [0] EXPLICIT Signature OPTIONAL | ignored (RFC5019) |
| Signature ::= SEQUENCE { | |
| signatureAlgorithm AlgorithmIdentifier, | |
| signature BIT STRING | |
| certs [0] EXPLICIT SEQUENCE OF Certificate OPTIONAL<br>} | |
| **}** | |

**Table 6 – OCSP response profile**

| **Response attributes** | **Notes** |
|---|---|
| **OCSPResponse** ::= SEQUENCE { | |
| **responseStatus** OCSPResponseStatus | |
| OCSPResponseStatus ::= ENUMERATED | *(0)* *successful* - successful response to OCSPRequest;<br>*(1)* *malformedRequest* - returned after OCSPRequest syntax error;<br>*(2)* *internalError* - OCSP responder internal error;<br>*(3)* *tryLater* - not used;<br>*(5)* *sigRequired* - never returned as request signature is not required;<br>*(6)* *unauthorized* - if OCSP responder does not recognize the issuer = foreign certificate |

| | |
|---|---|
| | (client is not authorized to make a query to this server – RFC2560, or the server is unable to make an authoritative response, for instance it may not have authoritative information about certificate revocation – RFC5019) |
| **responseBytes** [0] EXPLICIT ResponseBytes OPTIONAL } | only if OCSPResponseStatus=*successful* |
| ResponseBytes ::= SEQUENCE<br>{ | |
| responseType OBJECT IDENTIFIER | always "*Basic OCSP Response"* |
| response OCTET STRING | |
| BasicOCSPResponse ::= SEQUENCE<br>{ | |
| **tbsResponseData** ResponseData, | |
| ResponseData ::= SEQUENCE<br>{ | |
| version [0] EXPLICIT Version DEFAULT v1, | v1 |
| responderID ResponderID, | |
| ResponderID ::= CHOICE {<br>byName [1] Name,<br>byKey [2] KeyHash } | returns byName=issuer's DN |
| producetAt GeneralizedTime, | time the responder signs the response |
| responses SEQUENCE OF SingleResponse, | returns only a single response to the first certificate in the request list |
| SingleResponse ::= SEQUENCE<br>{ | |
| certID CertID, | |
| CertID ::= SEQUENCE {<br>hashAlgorithm AlgorithmIdentifier,<br>issuerNameHash OCTET STRING,<br>issuerKeyHash OCTET STRING,<br>serialNumber CertificateSerialNumber<br>} | identical to the content of the attribute *CertID* specified in the request |
| certStatus CertStatus, | certificate revocation status<br>one of options listed below |
| CertStatus ::= CHOICE<br>{ | |
| **good** [0] IMPLICIT NULL, | certificate has not been revoked (in the validity interval) or the time the OCSP response is created is outside the certificate validity interval |
| **revoked** [1] IMPLICIT RevokedInfo, | certificate has been revoked (in the validity interval) |
| RevokedInfo ::= SEQUENCE { | |
| revocationTime GeneralizedTime | certificate revocation time |
| revocationReason [0] EXPLICIT CRLReason OPTIONAL } | reason included in the response |
| CRLReason ::= ENUMERATED | can contain:<br>*(0) unspecified;*<br>*(1) keyCompromise;*<br>*(2) cACompromise;*<br>*(3) affiliationChanged;* |

| | |
|---|---|
| | *(4) superseded;*<br>*(5) cessationOfOperation;*<br>*(8) removeFromCRL;*<br>*(9) privilegeWithdrawn;*<br>*(10) aACompromise*<br><br>I.CA does not admit *certificateHold* (6) as the revocation reason; value (7) is not used |
| **unknown** [2] IMPLICIT UnknownInfo<br>UnknownInfo ::= NULL | I.CA does not use this (but does use OCSPResponseStatus = unauthorized under RFC5019)<br>(the provider is unable to respond, and 'knows nothing' about the certificate usually because it is a foreign certificate) |
| } | |
| thisUpdate GeneralizedTime, | time for which certificate status is known |
| nextUpdate [1] EXPLICIT GeneralizedTime OPTIONAL, | always specified (mandatory under RFC5019); the time this response expires and a new response will be available |
| singleExtensions [1] EXPLICIT Extensions | |
| Extensions::= SEQUENCE SIZE (1..MAX) OF Extension<br>Extension::= SEQUENCE {<br>extnID OBJECT IDENTIFIER,<br>critical BOOLEAN DEFAULT FALSE,<br>extnValue OCTET STRING } | the response may contain extension(s):<br>- ***id-commonpki-at-certHash*** - inserted at least in SK certificates (also referred to as positive statement); the algorithm according to the responder's certificate's signature (sha256) will be used for the hash from the requested certificate;<br>- ***id-pkix-ocsp-archive-cutoff*** – for qualified certificates, it specifies the time after certificate expiration the certificate status given in the OCSP response can be relied on |
| } | |
| responseExtensions [1] EXPLICIT Extensions OPTIONAL } | response contains no field responseExtensions |
| Extensions::= SEQUENCE SIZE (1..MAX) OF Extension<br>Extension::= SEQUENCE {<br>extnID OBJECT IDENTIFIER,<br>critical BOOLEAN DEFAULT FALSE,<br>extnValue OCTET STRING } | according to RFC6960, the following is permitted to be here:<br>- id-pkix-ocsp-nonce;<br>- id-pkix-ocsp-extended-revoke |
| } | |
| signatureAlgorithm AlgorithmIdentifier, | sha256WithRSAEncryption |
| signature BIT STRING, | |
| certs [0] EXPLICIT SEQUENCE OF Certificate OPTIONAL | specified:<br>- certificate of the issuing CA;<br>- certificate of the OCSP responder |
| } | |
| } | |
| } | |
| } | |

### 7.3.1 Version number(s)

See 7.3.

### 7.3.2 OCSP extensions

See tables in 7.3.

The OCSP response returning the "good" Certificate status may contain a positive statement as the CertHash attribute of singleExtentions.

# 8 COMPLIANCE AUDIT AND OTHER ASSESMENTS

Assessment information is provided in specific CP.

## 8.1 Frequency or circumstances of assessment

See chapter 8.

## 8.2 Identity/qualifications of assessor

See chapter 8.

## 8.3 Assessor's relationship to assessed entity

See chapter 8.

## 8.4 Topics covered by assessment

See chapter 8.

## 8.5 Actions taken as a result of deficiency

See chapter 8.

## 8.6 Communication of results

See chapter 8.

# 9 OTHER BUSINESS AND LEGAL MATTERS

## 9.1 Fees

### 9.1.1 Certificate issuance or renewal fees

The fees for issuing end user Certificates are given in the current price list, which is available on the web information address of I.CA or in the contract if there is a contract between I.CA and the Organization. No fee is charged for the Certificates held by I.CA.

The certificate renewal service is not provided.

### 9.1.2 Certificate access fees

I.CA charges no fee for electronic access to the public Certificates issued under specific CP – refer to 1.2.

### 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 certification policies.

### 9.1.4 Fees for other services

Not applicable to this document.

### 9.1.5 Refund policy

Not applicable to 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 the Services given the risk of a liability-for-damage claim.

Please refer to the Annual Report of První certifikační autorita, a.s., disclosed in business register for detailed information on the company's assets.

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

Not applicable to this document; the service is not provided.

## 9.3 Confidentiality of business information

### 9.3.1 Scope of confidential information

Confidential information of I.CA 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 the Services;
- Business information of I.CA;
- Any internal information and documentation;
- Any personal data.

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

Public information is only the information designated as public and that 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 relevant legislation, which means ZOOU and GDPR in particular. These requirements are regulated in detail in internal documentation:

- "Personal Data Protection at I.CA";
- "Information Security Management".

### 9.4.2 Information treated as private

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

I.CA employees or the entities defined by relevant 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 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 relevant legislation.

### 9.4.7 Other information disclosure circumstances

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

## 9.5 Intellectual property rights

This CPS, all related documents, the website content and the procedures facilitating the operation of the systems providing 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 use the certification authorities' private keys solely for issuing Certificates to end users (except root certification authority of I.CA), releasing certificate revocation lists and issuing OCSP responder Certificates;
- It will use the private keys of certification authorities' OCSP responders solely in the processes of providing responses to certificate status requests;
- The qualified Certificates issued to end users meet trust services legislation requirements and the requirements of the relevant technical standards and norms, the non-qualified Certificates issued to end users meet the requirements of the relevant technical standards and norms;

- It will revoke any Certificate issued if the revocation request is submitted in the manner defined in this CPS or specific CP, as applicable.

All warranties and the performance resulting therefrom may only be recognized on condition that:

- The subscriber did not violate any obligation arising from Service contract of Services or specific CP;
- The relying party did not violate any obligation arising from specific CP.

The subscriber of a Certificate issued under specific CP must always make his warranty claim with the RA which handled his application for this Certificate.

I.CA represents and warrants, vis-à-vis subscribers and relying parties, that I.CA will observe specific CPs in issuing Certificates and administering the same throughout their periods of validity.

The warranties include:

- Checking the right to apply for a Certificate;
- Validating the information given in the certificate application, checking due completion of the items in the certificate application (PKCS#10 format) and checking the identity;
- Ensuring that the Service contract meets the requirements of relevant legislation;
- Ensuring that Certificate status information storage place is maintained 24 hours a day and 7 days a week;
- Ensuring that a Certificate may be revoked for reasons specified in trust services legislation and specific CP.

### 9.6.2 RA representations and warranties

The designated RA:

- Assumes the obligation that the services which the RA provides are correct;
- Does not accept the application unless the RA validates all the application items (except those not subject to validation) or the subscriber provides the required data or is authorized to submit the application;
- Is responsible for passing a hand-delivered certificate revocation request to a CA office in due time for the CA office to handle the request;
- Is responsible for handling objections and complaints.

### 9.6.3 Subscriber representations and warranties

The subscriber representations and warranties are stated in the contract between I.CA and the Certificate's subscriber.

### 9.6.4 Relying parties representations and warranties

Relying parties follow the CP under which the Certificate is issued.

### 9.6.5 Representations and warranties of other participants

Not applicable to this document.

## 9.7 Disclaimers of warranties

První certifikační autorita, a.s., only provides the 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 breaches its obligations under trust services legislation or specific CP. 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

Applicable to the provision of trust services are the relevant provisions of current legislation regulating provider–consumer relations and the warranties agreed between První certifikační autorita, a.s., and the user of the Services. The contract must not be in conflict with current legislation and must always take an electronic or printed form.

První certifikační autorita, a.s.:

- Undertakes to discharge all the obligations defined by relevant legislation (including trust services legislation in the case of qualified Certificates) and those in the relevant policies;
- Gives the aforesaid warranties throughout the term of the Service contract;
- Agrees that the application software suppliers with a valid contract with První certifikační autorita, a.s., for the distribution of the root Certificate assume no obligation or liability, except for where damage or loss is directly attributable to the software of that supplier.

První certifikační autorita, a.s., **is not responsible for:**

- Any defect in the services rendered which is due to the subscriber's incorrect or unauthorized use of the services rendered under the Service contract, particularly for any use contrary to the terms and conditions specified in this CPS and/or specific CP, and for any defect due to force majeure, including a temporary telecommunication connection failure;
- Any damage resulting from using the Certificate after submitting the request for this Certificate's revocation if První certifikační autorita, a.s., meets the defined time limit for publishing the Certificate on certificate revocation list (CRL or OCSP).

Claims and complaints may be submitted by:

- E-mail to reklamace@ica.cz;
- Message to data box of I.CA;
- Registered post letter to the registered office of the company;
- Hand at the registered office of the company.

The party making the claim or complaint (the subscriber or the relying party) must provide:

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

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

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

The subscriber will be provided with a new Certificate free of charge if:

- There is reasonable suspicion that the certification authority's private key has been compromised;
- The management of I.CA decide so taking account of the circumstances of the case;
- CA finds out, in the certificate application acceptance procedure, that a different Certificate with a duplicate public key exists.

Any other possible damages are based on relevant legislation and the amount of damages may be determined by court.

## 9.10 Term and termination

The period when certification policies are in effect and the conditions for their expiry are always specified in specific CP.

### 9.10.1 Term

Certification policies – see 9.10.

This CPS takes force on the date specified in chapter 10 and is in force until replaced by a new version or until the expiration of the last Certificate issued under any of the certification policies – refer to 1.2.

### 9.10.2 Termination

Certification policies – see 9.10.

CEO of První certifikační autorita, a.s., is the sole person authorized to approve the termination of this CPS if this CPS is replaced by a new version or the certification service provider terminates its operations.

### 9.10.3 Effect of termination and survival

Certification policies – see 9.10.

This CPS is in effect for a period no shorter than the expiration of the last Certificate issued under any of the certification policies – refer to 1.2.

## 9.11 Individual notices and communications with participants

If the participating parties are organizational components of I.CA, the communication between them is governed by internal rules of I.CA.

For individual notices and communication with the participating parties, I.CA may use the e-mail and postal addresses and the phone numbers provided by the participating parties, personal meetings and other channels.

Communicate with I.CA is also possible through the channels specified on the web information address.

## 9.12 Amendments

The procedure for a certification policy is always described in that specific certification policy.

### 9.12.1 Procedure for amendment

Certification policies – see 9.12.

The procedure for this CPS is a controlled process described in internal documentation.

### 9.12.2 Notification mechanism and period

Certification policies – see 9.12.

The procedure for this CPS is a controlled process described in internal documentation.

### 9.12.3 Circumstances under which OID must be changed

Certification policies – refer to 9.12.

No OID assigned to this CPS.

## 9.13 Disputes resolution provisions

If all the parties are organizational components of I.CA, the resolution of disputes is governed by internal rules of I.CA.

If any party is not an organizational component of I.CA and the subscriber or the relying party disagrees with the suggested solution, they may use the following levels of appeal:

- RA employee in charge;
- I.CA employee in charge (electronic or written filing is required);
- CEO of I.CA (electronic or written filing is required).

This procedure provides the dissenting party with an opportunity to assert its opinion more swiftly than before a court.

## 9.14 Governing law

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

## 9.15 Compliance with applicable law

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

## 9.16 Miscellaneous provisions

Any miscellaneous provision is always described in specific CP.

### 9.16.1 Entire agreement

See 9.16.

### 9.16.2 Assignment

See 9.16.

### 9.16.3 Severability

See 9.16.

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

See 9.16.

### 9.16.5 Force majeure

See 9.16.

## 9.17 Other provisions

Not applicable to this document.

# 10 FINAL PROVISIONS

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