První certifikační autorita, a.s.

Certification Policy

for Issuing Qualified Certificates

for Electronic Signatures

(RSA Algorithm)

Version 1.16

CONTENT

Table 1 – Document history

Version	Date of Release	Approved by	Comments
1.00	29 March 2016	CEO of První certifikační autorita, a.s.	First release.
1.10	3 March 2017	CEO of První certifikační autorita, a.s.	Modified to match statutory requirements for trust services. Modified to match the requirements of Microsoft Trusted Root Program.
1.11	3 May 2018	CEO of První certifikační autorita, a.s.	More detailed description of filling up subject field attributes, note for filling up KeyUsage extension. More detailed text in 8.4.
1.12	30 April 2019	CEO of První certifikační autorita, a.s.	Annual revision, formal errors correction.

1.13	10 December 2019	CEO of První certifikační autorita, a.s.	Support of RSA-PSS (pkcs#1 2v1) algorithm when creating advanced electronic seal of issuer of the certificate.
1.14	28 November 2020	CEO of První certifikační autorita, a.s.	Classification of document marked, change of CA actions during certificate issuance, revision, more accurate text.
1.15	6 April 2022	CEO of První certifikační autorita, a.s.	Remote natural person identity authentication via ZealiD TRA Service added. Revision of text.
1.16	11 June 2022	CEO of První certifikační autorita, a.s.	Cryptographic module evaluation updated.

1 INTRODUCTION

This document determines the principles applied by První certifikační autorita, a.s. (also as the I.CA), a qualified provider of trust services, in providing qualified trust service of issuing qualified certificates for electronic signatures (also as the Service or the Certificate) to natural persons. The RSA algorithm is used for the Service provided under this certification policy (also as the CP).

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

- Regulation (EU) no 910/2014 of the European Parliament and of the Council on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC;
- Act of the Czech Republic No. 297/2016 Coll., on trust services for electronic transactions;
- Legislation concerning personal data protection in compliance with Regulation (EU) no 2016/679 of the European Parliament and of the Council on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation).

Note: Any reference to technical standard, norm or legislation is always a reference to that technical standard, norm or legislation or 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.

The Service is provided to all end users on the basis of a 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.

1.1 Overview

The document **Certification Policy for Issuing Qualified Certificates for Electronic Signature (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 valid RFC 3647 standard while taking account of valid technical and other standards and norms of the European Union and the laws of the Czech Republic pertinent to this sphere (therefore, each chapter is preserved in his document even if it is irrelevant to this sphere). The document is divided into nine basic chapters and these are briefly introduced in the following list:

- Chapter 1 identifies this document with the allocated unique identifier, generally describes the entities and individuals taking part in the provision of this Service, and defines the acceptable use of the Certificates available to be issued;
- Chapter 2 deals with the responsibility for the publication and information or documents;
- Chapter 3 describes the processes of identification and authentication of an applicant for the issuance or revocation of a Certificate, and defines the types and contents of the names used in Certificates;
- Chapter 4 defines life cycle processes of Certificates, i.e., Certificate issuance application, the issuance of the Certificate, Certificate revocation request, the

revocation of the Certificate, the services related to checking of Certification status, termination of the provision of the Service, etc.;

- Chapter 5 covers physical, procedural and personal security, including the definition of the set of events subject to logging, the keeping of these records and responses to emergency and compromising situations;
- Chapter 6 focuses on the technical security of the type of generating public and private keys, protection of private keys, including the computer and network protection;
- Chapter 7 defines the profile of issued Certificates and CRL;
- Chapter 8 focuses on assessing the Service delivered;
- Chapter 9 deals with commercial and legal aspects.

More detail on the fulfillment of fields and extensions of Certificates issued under this CP and on Certificate administration may be included in the relevant certification practice statement (also as the CPS).

Note: This is English translation of CP; Czech version always takes precedence.

1.2 Document name and identification

Document's title:	Certification Policy for Issuing Qualified Certificates for Electronic Signatures (RSA Algorithm), version 1.16
Policy OID:	1.3.6.1.4.1.23624.10.1.30.1.1

1.3 PKI Participants

1.3.1 Certification authorities

The root certification authority of První certifikační autorita, a.s., issued a certificate to a subordinate certification authority (also as the Authority) operated by I.CA, in a two-tier certification authority structure, in accordance with relevant legislation and technical and other standards. This Authority issues Certificates under this CP and certificates for its own OCSP responder.

1.3.2 Registration authorities

The services of První certifikační autorita, a.s., are provided through registration authorities (stationary or mobile), which are either public (providing services for the general public) or client (providing services for their customers). These registration authorities:

- Accept applications for the services listed in this CP (Certificate issuance applications, in particular), arrange the handover of Certificates and certificate revocation lists, provide required information, handle complaints, etc.;
- Are authorized, for urgent operational or technical reasons, to suspend, in whole or in part, the performance of their activities;
- Are authorized to conclude Service contracts on behalf of I.CA;

- Are authorized to charge for the I.CA services provided through RA unless otherwise agreed in a contract;
- If contracted RA, exercise similar duties and responsibilities on behalf of I.CA as the RA proper, under a written contract concluded between I.CA and the operator of the contracted RA.

1.3.3 Subscribers

Subscriber of a Certificate may be a natural person identified in the Certificate as the owner of the private key connected with the public key specified in the Certificate.

1.3.4 Relying parties

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

1.3.5 Other participants

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

1.4 Certificate usage

1.4.1 Appropriate certificate uses

Certificates issued under this CP may only be used in electronic signature verification processes in accordance with trust services legislation.

1.4.2 Prohibited certificate uses

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

1.5 Policy administration

1.5.1 Organization administering the document

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

1.5.2 Contact person

The contact person of První certifikační autorita, a.s., in respect of this CP and its CPS is 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 CPS with this CP.

1.5.4 CPS approval procedures

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

1.6 Definitions and acronyms

Table 2 – Definitions

Term	Explanation
CA/Browser Forum	organization, consensual association of certification authorities
Classified Information Protection Act	the Czech Republic's Act No. 412/2005 Coll., regulating classified information protection and security competence, as amended
contracting partner	provider of services contracted by I.CA for certification services or parts thereof – usually, it is a contracted RA
domain name	node name in domain name system
domain name registrant/ registrant	sometimes referred to as a domain name owner, but more accurately a person or entity registered by a domain registrar as having the right to oversee the use of a domain name, a natural or legal person listed as a "Registrant" by WHOIS or a domain registrar
domain name registrar/ registrar	person or entity that registers domain names by mandate or with consent: ▪ Internet Corporation for Assigning Names and Numbers (ICANN) - Administrator of DNS Root Space; ▪ 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
OCSP responder	server using the OCSP protocol to provide data on public key certificate status
OCSP stapling	way of minimizing queries for OCSP Responder, RFC 4366 - TLS Extensions; allows the TLS server to return the once-received answer to the question about certificate status from the OCSP (during its validity) to all end users accessing the TLS server
phishing	in an electronic communication attempt to obtain sensitive information (usernames, passwords, and credit card details) for malicious reasons
private key	unique data to create electronic signature / seal
public key	unique data to verify electronic signature / seal
PSP registrar	authority responsible for approving or rejecting authorization of payment services providers in their state, usually National Bank, in ETSI TS 119 495 called NCA (National Competent Authority)
qualified certificate for electronic signature or for electronic seal or for website authentication	certificate defined by trust services legislation
qualified signature / seal creation device	device meeting the requirements of eIDAS, annex II, intended for electronic signature / seal creation
relying party	party relying on a certificate in its operations
root CA	certification authority which issues certificates to subordinate certification authorities
secure cryptographic device	device on which the private key is stored
softcard	software emulation of smartcard for access to private key stored in HSM
SSL certificate	certificate for identification and encryption within SSL/TLS protocol communication
subordinate CA	CA issuing certificates to end users
supervisory body	the body supervising qualified trust services providers
trust service / qualified trust service	trust service / qualified trust service defined by eIDAS
trust services legislation	current legislation on trust services
TWINS	commercial product of I.CA consisting of:

	▪ qualified certificate for electronic signature; ▪ non-qualified certificate which issuance is based only on contractual relationship between I.CA and end-user
two-factor authentication	authentication employing two of three factors – I know something (the password), I have something (a smartcard or a hardware token) or I am something (fingerprint, retina or iris reading)
written contract	text of the contract in electronic or paper form

Table 3 – Acronyms

Acronym	Explanation
ARC	Alarm Receiving Centre
ASCII	American Standard Code for Information Interchange, table containing binary codes of English alphabets, numbers and other common symbols
BIH	Bureau International de l'Heure – The International Time Bureau
bit	from English *binary digit* – a binary system digit – the fundamental and the smallest unit of information in digital technologies
BRG	document "Baseline Requirements for the Issuance and Management of Publicly-Trusted 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)

DV	Domain Validation, SSL certificate type
DNS	Domain Name System, a hierarchical decentralized naming system implemented by DNS servers which are exchanging information via DNS protocol to translate domain names to the numerical IP addresses
EBA	European Banking Association
EC	Elliptic Curve
ECC	Elliptic Curve Cryptography
eIDAS	REGULATION (EU) no 910/2014 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 23 July 2014 on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC
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
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
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 RESPONSIBILITIES

2.1 Repositories

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

2.2 Publication of certification information

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

- Registered office:

  První certifikační autorita, a.s.

  Podvinný mlýn 2178/6

  190 00 Praha 9

  The 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;
  - Link to where the CRL can be obtained in the specified format (DER, PEM, TXT);
- Certification and other policies, practice statements and other public information.

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, daily newspapers with national distribution.

2.3 Time or frequency of publication

I.CA publishes information as follows:

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

2.4 Access controls on repositories

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

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

3 IDENTIFICATION AND AUTHENTICATION

3.1 Naming

3.1.1 Types of names

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

3.1.2 Need for names to be meaningful

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

3.1.3 Anonymity or pseudonymity of subscribers

The Certificates issued under this CP support pseudonyms but do not support anonymity.

3.1.4 Rules for interpreting various name forms

The data specified in a Certificate application (format PKCS#10) are transferred to subject attribute or subjectAlternativeName extension of the Certificate in the form they are specified in the application.

3.1.5 Uniqueness of names

The Authority guarantees that the subject field in a Certificate of specific subscriber is unique.

3.1.6 Recognition, authentication, and role of trademarks

Any Certificate issued under this CP may only contain a trademark with evidenced ownership or license. The Certificate's subscriber bears any consequence resulting from unauthorized use of a trademark.

3.2 Initial identity validation

The entities authorized to apply for a Certificate are listed in 4.1.1. The following chapters specify the rules for the initial validation of the identity of these entities.

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 whereby the subscriber provides evidence that he is the owner of the private key when the electronic signature is created.

3.2.2 Authentication of organization identity

The following must be submitted to authenticate the identity of a legal entity or a government authority (also as the Organization):

- Original or certified copy of the entry in the Commercial Register or in another register specified by law, of a trade license, of a deed of incorporation, or of another document of the same legal force; or
- Printed extract from public registers to be submitted by the applicant or prepared by the RA operator.

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

3.2.3 Authentication of individual identity

This chapter describes the identity authentication procedure of the person applying for the Certificate (the Certificate subscriber). Identity authentication can take place in the following ways:

- In person / on-site (the individual applicant arrives at the RA with the required documents); or
- Remotely, i.e., on-line without the physical presence of the individual applicant at the RA.

In case of **on-site** identity authentication procedure, the individual applicant is required to submit two personal documents, a primary and a secondary one, that show the data specified further in this chapter.

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

The following data are validated in this document:

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

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

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

The secondary personal document data uniquely identifying the Certificate subscriber must be identical to those in the primary personal document.

If neither the primary nor the secondary personal document shows permanent address, no permanent address may be specified in the Certificate application and the Certificate issued.

For employees an employment certificate with the Organization is also required. This certificate is to be submitted by the Certificate subscriber to RA, but may be provided in the manner defined in the contract concluded between I.CA and the Organization. The person authorized to act for the Organization must prove their identity through the primary personal document – see above, or the signature on the certificate of the Certificate subscriber's employment must be officially authenticated. If this person is not defined by law as a person authorized to represent the Organization, this person must also submit his/her officially authenticated power of attorney, signed by the Organization's authorized representative, for representing the Organization.

Employment certificate can be also submitted electronically. Must be .PDF format electronically signed by the person authorized to act for the Organization. Advanced (at least) electronic signature must be based on qualified certificate.

If an agent represents the Certificate subscriber vis-à-vis RA, officially authenticated authorization to act as agent is required.

If the individual who applies for a Certificate for themselves is OSVČ and this is to be specified in the Certificate, the relevant requirements under 3.2.2 apply.

In case of **on-line** identity authentication procedure, the usage of certified ZealiD TRA Service (certified by TÜV Informationstechnik GmbH) using ZealiD application installed on the applicant's mobile phone or tablet is required for remote verification of the identity of the natural person applying for the Certificate (Certificate subscriber).

For this method of identity authentication, a primary personal document is required, which must be a valid personal identity card or passport for the citizens of the Czech Republics. Valid passport is the primary personal identity document for foreigners; citizens of EU member countries may use their valid personal identity card they use in their country as the proof of their identity. At the I.CA website - see chapter 2.2 - the guide with detailed instructions is can be found. The guide informs the applicant (Certificate subscriber) about the process of issuing the Certificate, including information for users that issuing the Certificate in this way is possible only with explicit consent to the described procedure expressed by clicking on the appropriate button.

The actual process of authenticating the applicant's identity and issuing the Certificate takes consists of several successive steps and includes:

- Installation of the ZealiD application on the applicant's mobile device (supported platforms are Apple and Android);
- Verification of the applicant's identity towards the bank - the current list of banks against which ZealiD supports verification can be found at: https://www.zealid.com/en/coverage;
- Biometric facial analysis - for the required functionality, it is necessary to allow access to the camera when installing the ZealiD application;
- Verification of the personal document - its scanning and further biometric comparison of the photograph from the document with the applicant's face is performed;
- Generating Certificate application;
- Signing of the contact on the issuance and use of the Certificate.

If any of the inspections does not end with a positive result, e.g., if the verification of the form does not take place in required quality, the process is terminated and the Certificate is not issued. The condition for the exposure of the Certificate on the list of issued certificates is the signing of the agreement on the issuance and use of the certificate, otherwise the Certificate is revoked.

Restrictions for usage of the online identity authentication procedure of the identity of a natural person:

- The applicant cannot be represented by an agent;
- If the Certificate is to state that it is an employee of the Organization, the contractual relationship between I.CA and the Organization is required and the contract must state how the confirmation of employment with the Organization is performed.

3.2.4 Non-verified subscriber information

The information not subject to verification is:

- Pseudonym;
- GenerationQualifier.

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, if this has been validated for the given application during the Certificate issuance procedure.

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

3.2.6 Criteria for interoperation

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

3.3 Identification and authentication for re-key requests

3.3.1 Identification and authentication for routine re-key

The identification and authentication in routine re-key request (subsequent Certificate issuance) are as follows - the application for the issuance of subsequent Certificate in the PKCS#10 structure must also have an electronic signature with the use of a private key matching the public key contained in the valid Certificate which is to be re-keyed.

3.3.2 Identification and authentication for re-key after revocation

This is irrelevant to this document as the service of re-keying after Certificate revocation is not supported. A new Certificate with a new public key needs to be issued. The same requirements as those in the initial identity validation apply.

3.4 Identification and authentication for revocation request

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

If the **Certificate revocation request is submitted to RA by hand**, it must be in writing and signed by a person whose identity must be duly authenticated through the primary personal document (see 3.2.3).

The following methods of identification and authentication are permitted for **Certificate revocation request submitted electronically**:

- Using the form on the company's website (and using the Certificate revocation password);
- Using an unsigned electronic message containing the Certificate revocation password and sent to revoke@ica.cz;
- Using a signed electronic message (the electronic signature must be created with the private key belonging to the Certificate to be revoked) and sending it to revoke@ica.cz;
- Using the data box of I.CA (and using the Certificate revocation password);
- Using a defined person assigned to represent the Organization in the contractual relationship with I.CA.

If the **Certificate revocation request is sent as a letter** (using the Certificate revocation password), the letter must be sent by registered post to registered office of I.CA.

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

I.CA reserves the right to accept also other Certificate revocation identification and authentication procedures, which, however, must not be contrary to trust services legislation.

4 CERTIFICATE LIFE CYCLE OPERATIONAL REQUIREMENTS

4.1 Certificate application

4.1.1 Who can submit a certificate application

Individuals may apply for a Certificate for themselves and Organizations may apply for a Certificate for their employee.

4.1.2 Enrollment process and responsibilities

Process is performed only when the primary Certificate is issued. In case of **on-site** identity authentication, the subscriber (or his agent) initiates the registration process by appearing at an RA office and bringing all the required documents plus the Certificate application (if already existing). In case of **on-line** identity authentication, the process is initiated by running Zealid application on the mobile device of the subscriber and connecting this way to the ZealiD TRA Service. When the authentication is finished, the data contained in the submitted documents are entered into the Authority's information system and the Certificate application is processed.

The Certificate's subscriber is required to do the following, among other things:

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

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

- Inform the Certificate subscriber or the Organization about the terms and conditions prior to concluding the Certificate issuance contract;
- Conclude with the subscriber or the Organization, such a Certificate issuance contract that meets the requirements imposed by trust services legislation and technical and other standards;
- During the Certificate issuance process, check with RA all the data which can be validated specified in the application against the documents submitted;
- Require the proof of fact that private key was generated and stored on QSCD;
- Issue a Certificate that contains materially correct data on the basis of the information available to the Service provider as at the issuance of the Certificate;
- Publish public information in accordance with 2.2;
- Publish the Authority's certificates and the root CA's certificates;
- Provide any Service-related activity in accordance with trust services legislation, this CP, the relevant CPS, the System Security Policy - Trustworthy Systems and the operating documentation.

4.2 Certificate application processing

4.2.1 Performing identification and authentication functions

The identification and authentication procedure for the **primary Certificate** follows the rules given in 3.2.3, or 3.2.2 where applicable, and the procedure for **subsequent Certificates** follows the rules given in 3.3.1.

4.2.2 Approval or rejection of certificate applications

RA employees (also as the Employees) do the following in the procedure leading to the decision accepting or dismissing the issuance of the **primary Certificate**:

- Make a visual check as to conformity of the data in the Certificate application (the PKCS#10 structure) with the data in the documents submitted;
- Make a visual check as to the formal correctness of data.

The private key ownership verification, competence check and formal data correctness check are also carried out using the RA system software.

If any of these checks gives a fail result, the Certificate issuance procedure is terminated; otherwise, the procedure continues in accordance with 4.3.

See 4.3 for the procedure for the issuance of **subsequent Certificates**.

4.2.3 Time to process certificate applications

I.CA must issue the Certificate 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, exceptionally it can take longer;
- Subsequent Certificates – within units of minutes.

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 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.

4.3.2 Notification to subscriber by the CA of issuance of certificate

During the **primary Certificate** issuance process, the Certificate subscriber receives information from the RA employee and the Certificate is sent to the contact e-mail provided during registration as mandatory data.

Subsequent Certificates are sent to the contact e-mail provided during registration as mandatory data.

4.4 Certificate acceptance

4.4.1 Conduct constituting certificate acceptance

If the Certificate issuance requirements are met, the Certificate's subscriber must take the Certificate over. The only way to refuse to take over the Certificate is applying for the Certificate's revocation in accordance with this CP.

I.CA may agree with the Organization a procedure different from this provision of CP. However, that must not be contrary to the relevant provisions of the trust services legislation.

4.4.2 Publication of the certificate by the CA

I.CA publishes every Certificate it issues, except any Certificate:

- Containing data 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;
- 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) certification authority certificates linked with the Certificate issued under this CP, and verify those certificates' fingerprint values and validity;
- Carry out any operation necessary for them to verify that the Certificate is valid;
- Observe all and any provisions of this CP and trust services legislation which relate to the relying party's duties.

4.6 Certificate renewal

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

Certificate renewal is not provided.

In respect of this CP, it is always the issuance of a new Certificate with a new public key, with all the information having to be duly validated. 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

Certificate public key replacement under this CP means the issuance of a new Certificate with a different public key but identical content of the attributes under the subject field or the subjectAlternativeName extension of the Certificate the public key of which is requested to be replaced.

If the whole new Certificate issuance procedure is handled solely electronically without requiring any natural person to be present at an RA office, it is the issuance of a subsequent Certificate. See 4.7.1 for the requirements in respect of validating electronic applications for subsequent Certificates; if these requirements are not met, it is the primary Certificate issuance procedure, which starts with the registration procedure.

4.7.1 Circumstance for certificate re-key

Applications for the subsequent Certificate (the PKCS#10 structure) with a replaced public key must meet the following requirements:

- The attributes under the subject field or the subjectAlternativeName extension must be identical to those in the Certificate which is to be replaced;
- The public key must be different from that in the Certificate which is to be replaced;
- The electronic subsequent Certificate application is validated in accordance with 3.3.1.

4.7.2 Who may request certification of a new public key

Replacement of the public key in a Certificate may be requested by the Certificate's subscriber.

4.7.3 Processing certificate re-keying requests

If the public key replacement requirements are met, the procedure continues in accordance with 4.2 and 4.3.1, otherwise the Certificate issuance procedure is terminated.

4.7.4 Notification of new certificate issuance to subscriber

See 4.3.2.

4.7.5 Conduct constituting acceptance of a re-keyed certificate

See 4.4.1.

4.7.6 Publication of the re-keyed certificate by the CA

See 4.4.2.

4.7.7 Notification of certificate issuance by the CA to other entities

See 4.4.3.

4.8 Certificate modification

Modifying Certificate data under this CP means the issuance of a new Certificate in which a minimum of one modification made to the content of the attributes, concerning the Certificate's subscriber, under the subject field or the subjectAlternativeName extension or in which one field which requires content validation is deleted or added. The public key must be different from that in the Certificate which is to be modified.

If the whole new Certificate issuance procedure is handled solely electronically without requiring any natural person to be present at an RA office, it is the issuance of a subsequent Certificate. See 4.8.1 for the requirements in respect of validating electronic applications for subsequent Certificates; if these requirements are not met, it is the primary Certificate issuance procedure, which starts with the registration procedure.

4.8.1 Circumstance for certificate modification

Application for the subsequent Certificate (the PKCS#10 structure) with modified data must meet the following requirements:

- The attributes to be modified or added in the subject field or the subjectAlternativeName extension must be duly validated;
- The public key must be different from that in the original Certificate;
- The electronic subsequent Certificate application is validated in accordance with 3.3.1.

4.8.2 Who may request certificate modification

Change to the data in a Certificate may be requested by the Certificate's subscriber.

4.8.3 Processing certificate modification requests

If the certificate data change requirements are met, the procedure continues in accordance with 4.2 and 4.3.1, otherwise the Certificate issuance procedure is terminated.

4.8.4 Notification of new certificate issuance to subscriber

See 4.3.2.

4.8.5 Conduct constituting acceptance of modified certificate

See 4.4.1.

4.8.6 Publication of the modified certificate by the CA

See 4.4.2.

4.8.7 Notification of certificate issuance by the CA to other entities

See 4.4.3.

4.9 Certificate revocation and suspension

Certificate revocation requests are accepted irrespective of the time of the day if submitted electronically or by post. Submission in person to an RA is only possible during the particular RA's business hours.

I.CA does not provide certificate suspension.

4.9.1 Circumstances for revocation

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

- If the private key corresponding to the Certificate's public key is compromised or reasonably suspected to have been compromised;
- If the Certificate's subscriber or the Organization violated Service (under this CP) contract;
- In any event specified in trust services legislation or the relevant technical and other standards, such as invalid Certificate data;
- 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 Certificate revocation situations, which, however, must not be contrary to trust services legislation.

4.9.2 Who can request revocation

Certificate revocation request may be submitted by:

- Certificate's subscriber;
- Subject explicitly specified therefore in the Service (under this CP) contract;
- Any person who is beneficiary in Certificate's subscriber probate proceedings;
- Any person authorized to act for the legal successor to the original entity (the Organization) to which the Certificate was issued for that entity's employee;
- Provider of this Service (CEO of I.CA is the person authorized to request for the revocation of a Certificate issued by I.CA):
  - If the Certificate is issued on the basis of false data;

- □ If demonstrably establishes that the private key belonging to the public key specified in the Certificate has been compromised;
- □ If establishes that the Certificate was issued in spite of nonconformance with the requirements of trust services legislation;
- □ If demonstrably establishes that the Certificate was used contrary to the restrictions defined in 1.4.2;
- □ If demonstrably establishes that the Certificate's subscriber has died or been limited in legal capacity by court or the data by which the Certificate was issued are no longer valid;
- □ If the public key in the Certificate application is the same as the public key in a certificate already issued;

■ Supervisory body and other entities as may be specified in trust services legislation.

4.9.3 Procedure for revocation request

Any Certificate revocation request delivered to RA in person must include the Certificate's serial number in the decimal or hexadecimal format (introduced by the string '0x'), the full name of the person authorized to request for the Certificate's revocation, and the Certificate revocation password. If the person authorized to request for revocation does not know the Certificate revocation password, s/he must explicitly state this in the written application, along with the number of the primary personal document submitted in the Certificate application procedure or the number of the new primary personal document if the original document has been replaced. The person must use this primary personal document to prove their identity with the RA employee. If the request is legitimate, the RA employee revokes the Certificate, and the Certificate revocation date and time are the date and time when the request is processed by CA's information system. If the Certificate revocation application cannot be accepted (wrong revocation password or no proof of identity of the person authorized to request for Certificate revocation) the RA employee seeks to rectify these defects, and dismisses the request if the defects cannot be rectified for any reason. The RA employee always notifies the requestor of the result.

The following options are available for electronic submission of Certificate revocation request:

- Using the form on the information web page. The Certificate revocation date and time are the date and time a valid Certificate revocation request is dealt with in the CA's information system. The request receives a notice if the request is granted;
- Message signed electronically – the body text must contain (in Czech or Slovak with or without diacritics, or in English):

  Zadam o zneplatneni certifikatu cislo = xxxxxxx. [I request revocation of certificate number = xxxxxxx.],

  where '*xxxxxxx*' is the Certificate's serial number and must be given either in the decimal or hexadecimal format (introduced by the string '0x').

  The message must be electronically signed with the private key corresponding to the public key in the Certificate to be revoked;
- Electronic message not signed electronically – the body text must contain (in Czech or Slovak with or without diacritics, or in English):

  Zadam o zneplatneni certifikatu cislo = xxxxxxx. [I request revocation of certificate number = xxxxxxx.]

Heslo pro zneplatneni = yyyyyy. [Revocation password = yyyyyy.],

where '*xxxxxxx*' is the Certificate's serial number and '*yyyyyy*' the revocation password. The Certificate's serial number must be given either in the decimal or hexadecimal format (introduced by the string '0x');

- Message signed electronically, or not signed electronically in special cases, and sent by a defined person authorized to represent the Organization in the contractual relation ship1with I.CA:

  Zadam o zneplatneni certifikatu cislo = xxxxxxx. [I request revocation of certificate number = xxxxxxx.],

  where '*xxxxxxx*' is the Certificate's serial number. The Certificate's serial number must be given in the decimal or hexadecimal format (introduced by the string '0x').

Note: If the request meets the requirements of the three options listed above, the employee in charge immediately revokes the Certificate in the CA's system, and the date and time the request is processed by the CA's information system are the date and time of the Certificate's revocation. The requestor receives a notice if the request was accepted.

If Certificate revocation request is submitted as a registered post letter, the request must contain following text (in Czech or Slovak with or without diacritics, or in English):

Zadam o zneplatneni certifikatu cislo = xxxxxxx. [I request revocation of certificate number = xxxxxxx.]

Heslo pro zneplatneni = yyyyyy. [Revocation password = yyyyyy.],

where '*xxxxxxx*' is the Certificate's serial number and '*yyyyyy*' the revocation password. The serial number is to be given either in the decimal or hexadecimal format (introduced by the string '0x'). If the request meets these requirements, the I.CA employee in charge immediately revokes the Certificate in the CA's system, and the date and time the request is processed by the CA's information system are the date and time of the Certificate's revocation. If the request cannot be accepted (wrong revocation password), the Certificate revocation request will be rejected. Requestor is informed by a registered letter sent to postal address of request sender how the request was handled.

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.

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 certificate revocation list is released immediately after a Certificate revocation request is handled affirmatively. If a Certificate is not revoked, the new CRL is usually released within 8 but no more than 24 hours after the previous CRL is released.

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 using the OCSP protocol is a service available to the general public. Every certificate issued under this CP includes a 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.

4.9.11 Other forms of revocation advertisements available

Not applicable to this document.

4.9.12 Special requirements re 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; Certificate suspension is not provided.

4.9.14 Who can request suspension

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

4.9.15 Procedure for suspension request

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

4.9.16 Limits on suspension period

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

4.10 Certificate status services

4.10.1 Operational characteristics

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

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

4.10.2 Service availability

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

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

4.10.3 Optional features

Not applicable to this document; no other certificate status check characteristics are provided.

4.11 End of subscription

The contract can be terminated by written agreement of both parties or by the expiration of the last Certificate issued under this 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

Facility, management, and operational controls primarily deal with:

- Trustworthy systems designed to support trust services;
- All processes supporting the provision of the services specified above.

The facility, management, and operational controls 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 in the more detailed internal documentation. These documents take account of the results of periodic risk analyses.

5.1 Physical controls

5.1.1 Site location and construction

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

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

5.1.2 Physical access

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

5.1.3 Power and air conditioning

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

5.1.4 Water exposures

The trustworthy systems supporting trust services are so located as to ensure they cannot be flooded 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 electronic fire alarm system (FAS). Fireproof insulation is installed in the entrance doors to the restricted areas in which the trustworthy systems designed to support trust 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.

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

5.2.2 Number of persons required per task

Jobs are defined for the processes related to the key pairs of certification authorities and 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 their 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.

5.2.3 Identification and authentication for each role

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

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

5.2.4 Roles requiring separation of duties

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

5.3 Personnel controls

5.3.1 Qualification, experience, and clearance requirements

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 trust services is accepted using the following criteria:

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

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

5.3.2 Background check procedures

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

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

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

5.3.3 Training requirements

I.CA employees receive technical training in the use of specific software and 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.

5.3.4 Retraining frequency and requirements

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

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

5.3.5 Job rotation frequency and sequence

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

5.3.6 Sanctions for unauthorized actions

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

5.3.7 Independent contractor requirements

I.CA may or must procure some activities from independent contractors, and is fully liable 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 pertinent 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 certificate 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

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.

5.4.2 Frequency of processing log

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

5.4.3 Retention period for audit log

Unless the relevant legislation provides otherwise, audit records are kept for a minimum of 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 archived 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.

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 vs. external)

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

5.4.7 Notification to event-causing subject

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

5.4.8 Vulnerability assessments

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

5.5 Records archival

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

5.5.1 Types of records archived

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

- 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 archived are secured in a manner based on risk analysis results and the Classified Information Protection Act.

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

5.5.4 Archive backup procedures

The record backup procedures are regulated in internal documentation.

5.5.5 Requirements for time-stamping of records

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

5.5.6 Archive collection system (internal or external)

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

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

5.5.7 Procedures to obtain and verify archive information

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

- I.CA employees if they need to have such 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 authority certificates is suitably notified to the public a good time in advance (if practicable).

5.7 Compromise and disaster recovery

5.7.1 Incident and compromise handling procedures

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

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

See. 5.7.1.

5.7.3 Entity private key compromise procedures

In the case of reasonable concern that a private key of certification 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 list of revoked certificates is used for disclosing this information;
- Notifies the supervisory body of that the pertinent certificate has been revoked and why it has been revoked.

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 trust 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 its internal business continuity plan and recovery plan, plus any other relevant internal documentation.

5.8 CA or RA termination

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

- The termination of the Authority's operations must be notified in writing to the supervisory body, all subscribers of valid Certificates, and the parties having contract with I.CA that directly concerns the provision of trust services;
- The termination of the Authority's operations must be published on the web page pursuant to 2.2;
- If the Authority's certificate's expiration is part of the termination of operations, this information plus the reason for expiration must be included in that notice;
- The termination of operations is a controlled process following a pre-defined plan, which includes the description of the procedure to preserve and disclose information for

judicial or administrative proceedings discovery and for arranging the continuity of services;

- The Authority or its successor must be able to revoke Certificates and publish CRLs as long as any Certificate issued by the Authority is valid;
- After that the Authority must demonstrably destroy its private key, make a record of this destruction and keep this record in accordance with this CP.

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

- The information must be notified in writing or electronically to all subscribers of valid Certificates, and the parties having contract with I.CA 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 certification authorities' certificates cannot be used in accordance with the purpose of their issuance any longer;
- The subsequent course of action will be decided by CEO of I.CA while taking account of the decision of the supervisory body.

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

6 TECHNICAL SECURITY CONTROLS

6.1 Key pair generation and installation

6.1.1 Key pair generation

Key pairs of certification authorities and their corresponding OCSP responders 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 fulfilling requirements of trust service legislation, i.e., ETSI and CEN standards.

Key pairs of the employees taking part in the issuing Certificates 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 Certificates issued under this CP are generated on devices which are under sole control of the respective subscribers. These key pairs may be stored in hardware or in software.

All requirements concerning generating of key pairs mentioned above are described both in internal and external documentation.

6.1.2 Private key delivery to subscriber

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

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

6.1.3 Public key delivery to certificate issuer

Not applicable to the private keys of certification authorities and their corresponding OCSP responders – public keys as parts of key pairs are generated in a cryptographic module under the sole control of I.CA.

Other public keys are delivered to the certification authority in the certificate application (PKCS#10 format).

6.1.4 CA public key delivery to relying parties

Following options for obtaining the certification authority's public key contained in this certification authority’s certificate 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 RSA asymmetric algorithm is solely used for the Service provided under this CP. The size of the key of I.CA root certification authority is 4096 bits; the minimum size of the keys in the certificates issued by this root certification authority is 2048 bits. The minimum size of the keys in the Certificates issued under this CP is 2048 bits.

6.1.6 Public key parameters generation and quality checking

The parameters of the algorithms used in generating public keys of certification authorities and their corresponding OCSP responders meet the requirements listed in trust services legislation and the technical and other standards referred to therein. These keys are checked by relevant hardware and software.

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

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

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

6.2 Private key protection and cryptographic module engineering controls

6.2.1 Cryptographic module standards and controls

Key pairs of certification authorities and their corresponding OCSP responders are generated and private keys are stored in cryptographic modules which meet the requirements of trust services legislation, that is ETSI and CEN standards.

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

Using cryptographic modules by 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' key pairs 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.

Backup of private keys of 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 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 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 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 cryptographic module is not performed.

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

Transferring private keys of 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 and their corresponding OCSP responders are stored in the cryptographic modules which meets the requirements of trust services legislation, i.e., ETSI and CEN standards.

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

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

[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.

6.2.9 Method of deactivating private key

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

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

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

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

6.2.11 Cryptographic module rating

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

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 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 (smartcard or softcard) of are created before or during the generating of the corresponding key pair.

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

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

6.4.2 Activation data protection

Activation data of certification authorities' and their corresponding OCSP responders' private keys are protected by passwords.

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

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 Electronic Signatures and Infrastructures (ESI) – General Policy Requirements for Trust Service Providers;
- ETSI EN 319 401 Electronic Signatures and Infrastructures (ESI); General Policy Requirements for Trust Service Providers;

- ČSN ETSI EN 319 403 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 Elektronické podpisy a infrastruktury (ESI) - Profily certifikátu – Část 4: Profil certifikátu pro certifikáty webových stránek;
- ETSI EN 319 412-4 Electronic Signatures and Infrastructures (ESI); Certificate Profiles; Part 4: Certificate profile for web site certificates;
- ČSN ETSI EN 319 412-5 Electronic Signatures and Infrastructures (ESI); Certificate Profiles; Part 5: QC Statements;
- ETSI EN 319 412-5 Electronic Signatures and Infrastructures (ESI); Certificate Profiles; Part 5: QCStatements;
- ČSN EN 419 221-5 Protection profiles for TSP Cryptographic modules - Part 5 Cryptographic Module for Trust Services;
- EN 419 221-5 Protection profiles for TSP Cryptographic modules - Part 5 Cryptographic Module for Trust Services;
- FIPS PUB 140-2 Requirements for Cryptographic Modules;

- ISO/IEC 15408-1:2009 Information technology — Security techniques — Evaluation criteria for IT security — Part 1: Introduction and general model;
- ČSN EN ISO/IEC 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/IEC 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;
- ETSI TS 119 312 Electronic Signatures and Infrastructures (ESI); Cryptographic Suites;
- 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.

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.

6.6.3 Life cycle security controls

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

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

6.7 Network security controls

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

6.8 Time-stamping

See 5.5.5 for the time-stamping solution.

7 CERTIFICATE, CRL AND OCSP PROFILES

7.1 Certificate profile

Table 4 – Basic certificate fields

Field	Content
version	v3 (0x2)
serialNumber	unique serial number of the Certificate
signatureAlgorithm	on the basis of application (depending on signature algorithm of the certificate) one of following options: ▪ ***sha256withRSAEncryption*** (with parameters = NULL, pkcs#1 1v5) at minimum; or ▪ ***rsassaPss*** (pkcs#1 2v1) with parameters: – hashAlgorithm: sha256 at minimum; – maskGenAlgorithm: mgf with the same hash function as v hashAlgorithm; – saltLength: depending on used hash function; – trailerField: 0xBC (default)
issuer	issuer of the Certificate
validity	
notBefore	start of the Certificate's validity (UTC)
notAfter	notBefore + at maximum 365 days, or 366 days in case of leap year (UTC)
subject	see Table 5
subjectPublicKeyInfo	
Algorithm	rsaEncryption
subjectPublicKey	2048 bits at minimum
extensions	see Table 6
signature	electronic sign or advanced electronic seal of Certificate's issuer (Authority)

Table 5 – Subject field attributes

All attributes[2] of the subject field are taken over from the Certificate application except the attributes created by the Authority. The application must include the mandatory attributes.

Subject field attributes	Comments
countryName**	mandatory, country code (ISO 3166), single occurrence
givenName	mandatory if the pseudonym attribute is not specified; single occurrence
surName	mandatory if the pseudonym attribute is not specified; single occurrence
pseudonym	mandatory if the givenName and the surName attributes are not specified; single occurrence
serialNumber (1)	unique identification of the Certificate's subscriber in the Authority's system (ICA - xxxxxxxx); also used in automated subsequent certificate issuance
serialNumber (2)	optional; one of following options: • IDC*ss-nnnnnnnn*; • PASss-*nnnnnnnn*; where *ss* is the country code (ISO 3166) of document's issuer, and *nnnnnnnn* is the document number
commonName*	mandatory; single occurrence: • if givenName and surName are specified, these must be included in commonName; • if pseudonym is specified, the string ' - PSEUDONYM' is added to the content
initials	optional; single occurrence
emailAddress	this attribute must not be included in the primary Certificate
name	this attribute must not be included in the primary Certificate
generationQualifier	optional; single occurrence
organizationName	• employee of the Organization: mandatory; single occurrence; • OSVČ: optional; single occurrence; • other physical persons: must not be specified
organizationIdentifier	optional and only if the organizationName attribute is specified; single occurrence – one of following options: • NTR*ss-id*, (**N**ational **T**rade **R**egister, i.e.,

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

	business/company identification number); • VAT*ss-id*, (**V**alue **A**dded **T**ax, i.e., tax identification number); • XX:*ss-id*; where: • *ss* is the country code (ISO 3166) of the state where the employer of OSVČ is registered (does not have to be same as countryName); • *id* is the organization's identification number in the relevant register, • XX is two characters defined by the given country's authority and followed by ':' (colon) – type of national register other than VAT and NTR
organizationalUnitName	optional; multiple occurrences permitted
title	optional; multiple occurrences permitted
stateOrProvinceName**	optional; single occurrence
localityName**	optional; single occurrence primary Certificate: if specified, streetAddress and postalCode must also be specified
streetAddress**	optional; single occurrence primary Certificate: if specified, localityName and postalCode must also be specified
postalCode**	optional; single occurrence primary Certificate: if specified, localityName and streetAddress must also be specified

* The name under which the Certificate subscriber (private key holder) normally appears, the attribute may also contain validates degrees of the Certificate's subscriber.

** The attributes countryName, stateOrProvinceName, localityName, streetAddress and postalCode relate to data validated during initial identity validation.

7.1.1 Version number(s)

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

7.1.2 Certificate extensions

Table 6 – Certificate Extensions[3]

Extension	Content	Comments
certificatePolicies		non-critical
.policyInformation (1)		
policyIdentifier	see 1.2	
policyQualifiers		
cPSuri	http://www.ica.cz	
userNotice	Tento kvalifikovany certifikat pro elektronicky podpis byl vydan v souladu s narizenim EU c. 910/2014. This is a qualified certificate for electronic signature according to Regulation (EU) No 910/2014.	
.policyInformation (2)		
policyIdentifier	one of following options: • OID (QCP-n): 0.4.0.194112.1.0 (the private key is not generated and stored on QSCD); • OID (QCP-n-qscd): 0.4.0.194112.1.2 (the private key is generated and stored on QSCD)	
QCStatements		non-critical
	0.4.0.1862.1.1	Id-etsi-qcs-QcCompliance
	0.4.0.1862.1.4	Id-etsi-qcs-QcSSCD; specified if the private key is generated and stored on QSCD
	0.4.0.1862.1.5	id-etsi-qcs-QcPDS; link (URI, https) to user notice (PDS)
	0.4.0.1862.1.6 = 0.4.0.1862.1.6.1	id-etsi-qcs-QcType = id-etsi-qct-esign

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

CRLDistributionPoints*	http://qcrldp1.ica.cz/2qca*YY*_rsa.crl http://qcrldp2.ica.cz/2qca*YY*_rsa.crl http://qcrldp3.ica.cz/2qca*YY*_rsa.crl	non-critical
authorityInformationAccess		non-critical
id-ad-ocsp*	http://ocsp.ica.cz/2qca*YY*_rsa	
id-ad-caIssuers*	http://q.ica.cz/2qca*YY*_rsa.cer	
basicConstraints		non-critical
cA	False	
keyUsage	▪ TWINS (created by the Authority): – digitalSignature, nonRepudiation ▪ other cases: depending on the content of Certificate application - one of following options: – nonRepudiation; – digitalSignature, nonRepudiation; – digitalSignature, nonRepudiation and keyEncipherment***	critical, mandatory if this extension is missing in the application, the following will be added: digitalSignature, nonRepudiation
extendedKeyUsage	depending on the content of Certificate application - one of following options: • id-kp-emailProtection; • ms-Document_Signing; • id-kp-emailProtection, ms-Document_Signing	non-critical, mandatory if this extension is missing in the application, the following will be added: id-kp-emailProtection
subjectKeyIdentifier	hash of the public key (subjectPublicKey) in the Certificate	non-critical
authorityKeyIdentifier		non-critical
keyIdentifier	hash of the Authority's public key	
subjectAlternativeName		non-critical
otherName**	I.CA_User_ID(1.3.6.1.4.1.23624.4.6) : xxxxxxxx	
otherName	MPSV_IK (1.3.6.1.4.1.11801.2.1): numerical identifier supplied by MPSV	optional

rfc822Name	e-mail address	optional; multiple occurrences permitted
nsComment	QSCD identification number	non-critical; optional – creates Authority when generating and storing of the private key on QSCD (smartcard Starcos type) was verified
I.CA_TWIN_ID: 1.3.6.1.4.1.23624.4.3	Certificate application number	non-critical
I.CA_CERT_INTERCONNECTION: 1.3.6.1.4.1.23624.4.7	if more certificate types are issued to a single entity (entity's connection to the certificates issued)	non-critical

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

** It is a selected sub-string from the subject field's serialNumber attribute created by the Authority (see Table 5).

*** Last option (containing setting keyEncipherment bit) for keyUsage cannot be used when the key is generated and stored on Starcos 3.5 (or higher) smartcard.

7.1.3 Algorithm object identifiers

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

7.1.4 Name forms

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

7.1.5 Name constraints

Not applicable to Certificates issued to end users.

7.1.6 Certificate policy object identifier

První certifikační autorita, a.s., inserts in the Certificates issued the following certification policy object identifiers:

- OID of the I.CA certification policy under which the Certificate is issued;
- OID of the relevant certification policy defined by ETSI EN 319 411-2, or ČSN ETSI EN 319 411-2 as applicable, for a certificate issued to an individual with regard to the storing of the private key and declaring that the Certificate is in compliance with eIDAS.

7.1.7 Usage of Policy Constraints extension

Not applicable to Certificates issued to end users.

7.1.8 Policy qualifier syntax and semantics

See Certificate extensions in 7.1.2 above.

7.1.9 Processing semantics for the critical certificate policies extension

Not applicable to this document – not classified as critical.

7.2 CRL profile

Table 7 – CRL profile[4]

Field	Content
version	v2(0x1)
signatureAlgorithm	sha256withRSAEncryption at minimum
issuer	issuer of the CRL
thisUpdate	date and time when the CRL were released (UTC)
nextUpdate*	date and expected time when the next CRL will be released (UTC)
revokedCertificates	list of revoked certificates
userCertificate	revoked certificate's serial number
revocationDate	certificate revocation date and time
crlEntryExtensions	list attribute extensions – see Table 8
crlExtensions	CRL extensions – see Table 8
signature	electronic sign or advanced electronic seal of CRL's issuer

* In case of root CA 365 days at maximum, in case of subordinate CA 24 hours at maximum.

7.2.1 Version number(s)

Certificate revocation lists are issued pursuant to X.509, version 2.

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

7.2.2 CRL and CRL entry extensions

Table 8 – CRL Extension[5]

Extension	Content	Comments
crlEntryExtensions		
CRLReason	certificate revocation reason as the *certificateHold* reason is not admissible, it is not used another reason than unspecified (0) is given when subordinate CA's certificate is revoked	non-critical; optional
crlExtensions		
authorityKeyIdentifier		
keyIdentifier	hash of the CRL issuer's public key	non-critical
CRLNumber	unique number of the CRL to be released	non-critical

7.3 OCSP profile

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

OCSP responses are of the BasicOCSPResponse type and contain all mandatory fields. An optional revocationReason field is included for revoked certificates. The unAuthorized response is given for any certificate not issued by the relevant CA.

Http only is used as the transmission protocol.

See the relevant certification practice statement for more detail.

7.3.1 Version number(s)

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

7.3.2 OCSP extensions

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

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

8 CONFORMITY ASSESSMENTS AND OTHER ASSESSMENTS

8.1 Frequency or circumstances of assessment

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

The Microsoft Trusted Root Program assessment interval and circumstances are strictly defined by Microsoft, and the audit period is no longer than one year.

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

8.2 Identity/qualifications of assessor

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

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

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

8.3 Assessor's relationship to assessed entity

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

External assessor is an assessor without any ties to I.CA both through property and person.

8.4 Topics covered by assessment

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

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

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

8.5 Actions taken as a result of deficiency

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

8.6 Communication of results

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

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

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

9 OTHER BUSINESS AND LEGAL MATTERS

9.1 Fees

9.1.1 Certificate issuance or renewal fees

The fees for Certificate issuance 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. Certificate renewal is not provided.

9.1.2 Certificate access fees

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

9.1.3 Revocation or status information access fees

No fee is charged by I.CA for electronic access to revocation information (CRL) and status information about the Certificates issued by the Authority.

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 a valid business risk insurance policy that covers financial damage.

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

9.2.2 Other assets

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

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

9.2.3 Insurance or warranty coverage for end-entities

Not applicable to this document.

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 trust 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 the relevant legislation, that is ZOOÚ and GDPR in particular.

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 the relevant legislation.

9.4.6 Disclosure pursuant to judicial or administrative process

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

9.4.7 Other Information disclosure circumstances

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

9.5 Intellectual property rights

This CP, 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 I.CA root certification authority), 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;
- Certificates issued to end users meet the statutory trust services requirements and those of the relevant technical standards;
- It will revoke any issued Certificate if the revocation request is filed in the manner defined in this CP.

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

- The Certificate's subscriber did not violate any obligation arising from Service contract and this CP;
- The relying party did not violate any obligation arising from this CP.

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

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

The warranties include:

- Checking the right to apply for the 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 Certificate issuance contract meets the requirements of relevant legislation;
- Ensuring that certificate status information repository is maintained 24 hours a day and 7 days a week;
- Ensuring that the Certificate may be revoked for reasons specified in trust services legislation and this 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 Certificate's subscriber provides the required data or is authorized to submit the application;
- Is responsible for passing a hand-delivered Certificate revocation application to an Authority office in due time for the office to handle the application;
- 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 observe this CP.

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 and particular 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 the current legislation regulating provider–consumer relations and the warranties agreed between První certifikační autorita, a.s., and the applicant for the Service. 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 in relevant legislation (including trust services legislation) and those in the relevant policies;
- Gives the aforesaid warranties throughout the term of the contract of trust services;
- 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 Certificate 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 CP, and for any defect due to force majeure, including a temporary telecommunication connection failure;
- Any damage resulting from using the Certificate after filing the application for that certificate's revocation if První certifikační autorita, a.s., meets the defined time limit for publishing the revoked Certificate on the list of revoked certificates (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 (subscriber of the Certificate 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 30 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;
- The Authority finds out, in the Certificate application acceptance procedure, that a different Certificate with a duplicate public key exists.

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

9.10 Term and termination

9.10.1 Term

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

9.10.2 Termination

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

9.10.3 Effect of termination and survival

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

9.11 Individual notices and communications with participants

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.

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

9.12 Amendments

9.12.1 Amending procedure

This procedure is a controlled process described in an internal documentation.

9.12.2 Notification mechanism and period

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

9.12.3 Circumstances under which OID must be changed

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

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

9.13 Disputes resolution provisions

If the Certificate's subscriber or the relying party disagrees with the proposed way of resolving the dispute, 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

9.16.1 Entire agreement

Not applicable to this document.

9.16.2 Assignment

Not applicable to this document.

9.16.3 Severability

If a court or a public authority with jurisdiction over the activities covered by this CP establishes that the implementation of a mandatory requirement is unlawful, the scope of that

requirement will be so limited as to ensure the requirement is lawful and complies with relevant legislation.

9.16.4 Enforcement (attorneys' fees and waiver of rights)

Not applicable to this document.

9.16.5 Force Majeure

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

9.17 Other provisions

Not applicable to this document.

10 FINAL PROVISIONS

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