První certifikační autorita, a.s.

Certification Policy

for Issuing Qualified Certificates

for Electronic Signatures

(RSA algorithm)

Version 1.11

CONTENT

Table 1 – Document Development

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 Certificate Program.
1.11	3 May 2018	CEO of První certifikační autorita, a.s.	More detailed description of filling up Subject field items, note for filling up KeyUsage extension. More detailed text in 8.4.

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.

Note: Any reference to technical and other standards or laws is always a reference to that technical standard or law or the replacing technical standard or law. If this CP is in conflict with any technical standard or law that replaces the current technical standard or law, a new version of the CP 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 rules 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 application, the revocation of the Certificate, the services related to the verification 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 spread 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 1.11
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 valid 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 entitled, for urgent operational or technical reasons, to suspend, in whole or in part, the performance of their activities.
- Are authorized to enter into contracts, on behalf of I.CA, on the provision of the Service.
- 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 entered into 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 valid legislation for trust services.

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 the valid 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
bit	from English *binary digit* – a binary system digit – the fundamental and the smallest unit of information in numeral technologies
contracting partner	provider of selected trust services contracted by I.CA for providing trust services or parts thereof – usually, it is the contracted RA
Directive	DIRECTIVE 1999/93/EC OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 13 December 1999 on a Community framework for electronic signatures
electronic seal	electronic seal or advanced electronic seal or recognized electronic seal or qualified electronic seal under valid trust services legislation
electronic sign	electronic sign under valid trust services legislation
electronic signature	electronic signature or advanced electronic signature or qualified electronic signature or recognized electronic signature under valid trust services legislation
electronic signature creation device	configured software or technical equipment to create electronic signatures
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)
issuing, subordinate CA	for this document, the CA issuing certificates to end users
key pair	a private key and the 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
private key	unique data to create electronic signature/sign/seal
public key	unique data to verify electronic signature/sign/seal
qualified electronic signature certificate	certificate defined by valid trust services legislation
qualified electronic signature creation device	electronic signature creation device that meets the requirements defined in Attachment 2 to eIDAS

relying party	party relying on a certificate in its operations
root CA	certification authority which issues certificates to subordinate certification authorities
supervisory body	body supervising compliance with trust services legislation
time stamp	electronic time stamp or qualified electronic time stamp as defined by valid trust services legislation
the Classified Information Protection Act	the Czech Republic's Act No. 412/2005 Coll., regulating classified information protection and security competence, as amended
trust services legislation	the Czech Republic's legislation related to electronic transaction trust services and the eIDAS Regulation
trust service / qualified trust service	electronic service / qualified trust service as defined in eIDAS
TWINS	I.CA's commercial product containing a pair of certificates: • qualified electronic signature certificate – issued in accordance with this CP; • commercial certificate – issued solely under a contract between I.CA and the end user
two-factor authentication	authentication employing two of three factors – I know something (the password), I have something (a chip card or a hardware token) or I am something (fingerprint, retina or iris reading)
written contract	text of an electronic or printed contract

Table 3 – Acronyms

Acronym	Explanation
BIH	Bureau International de l'Heure – The International Time Bureau
CA	certification authority
CEN	European Committee for Standardization, an association of national standardization bodies
CRL	Certificate Revocation List – the list of revoked certificates, which are not held as valid any longer
ČR	The Czech Republic
ČSN	designation of Czech technical standards
DER, PEM	methods of certificate encoding (certificate formats)
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
FAS	Fire Alarm System
ESI	Electronic Signatures and Infrastructures
ETSI	European Telecommunications Standards Institute, a European standardization institute for information and communication technologies
EU	European Union
IAS	Intrusion Alarm System
FIPS	Federal Information Processing Standard, standards for information technologies for U.S. non-military state organizations
html	Hypertext Markup Language, a markup language for creating hypertext documents
http	Hypertext Transfer Protocol, a protocol for exchanging html text documents
https	Hypertext Transfer Protocol, a protocol for secure exchanging of html text documents
I.CA	První certifikační autorita, a.s.
IEC	International Electrotechnical Commission, a global organization publishing standards for electrical and electronic engineering, communication technologies and related industries
IPS	Intrusion Prevention System
ISMS	Information Security Management System
ISO	International Organization for Standardization, an international organization of national standardization organizations; designation of standards
ITU	International Telecommunication Union
ITU-T	Telecommunication Standardization Sector of ITU
MPSV	Ministry of Labour and Social Affairs
OCSP	Online Certificate Status Protocol, the protocol to identify public key certificate status
OID	Object Identifier, numerical object identification
OSVČ	self-employed person
ARC	alarm receiving centre
PDCA	Plan-Do-Check-Act, Deming cycle, a method of continuous improvement
PDS	PKI Disclosure Statement, message for the user
PKCS	Public Key Cryptography Standards, designation for a group of standards for public key cryptography

PKI	Public Key Infrastructure
PUB	Publication, FIPS standard designation
QSCD	Qualified Electronic Signature/Seal Creation Device
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)
SHA	type of hash function
TS	Technical Specification, type of ETSI standard
UPS	Uninterruptible Power Supply/Source
URI	Uniform Resource Identifier, defined-structure text string for accurate specification of a source of information
UTC	Universal Coordinated Time, 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
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: info@ica.cz.

The aforesaid website provides information about:

- public certificates – the following information is published (and more information can be obtained from the certificate):
  - certificate number;
  - content of commonName;
  - valid from data (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):
  - data of CRL release;
  - CRL number;
  - link to where the CRL can be obtained in the specified format (DER, PEM, TXT);
- certification and other policies and implementing regulations, certificates issued or revoked 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 a certificate employed in issuing certificates to end users, a release of certificate revocation list, and the provision of certificate status information (also as Infrastructure Certificates) 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 every time a new Certificate is issued;
- certificate revocation list (CRL) – see 4.9.7;
- information about infrastructure certificate revocation with the date 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 applicable 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 verifiable names given in the field Subject and extension SubjectAlternativeName must carry a meaning. See chapter 7 for the items supported for this field and the extension.

3.1.3 Anonymity or pseudonymity of subscribers

The Certificates issued under this CP do 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 carried over in Subject or SubjectAlternativeName 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 verification 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 verify 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 methods of verifying the identity of individuals, i.e.:

- the individual applying for the Certificate (the Certificate subscriber);
- the individual representing the Organization applying for the Certificate for the subscriber, and the subscriber (employee).

The Certificate subscriber identity verification procedure requires two documents, a primary and a secondary document, 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 verified in this document:

- full civil name;
- data and place of birth or the birth identification 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 identification number or personal identity card number, matching it to the primary document and must show at least one of these items:

- data of birth (or birth identification 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, a certificate of employment 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 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 an officially authenticated power of attorney, signed by the Organization's authorized representative, for representing the Organization.

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 an entrepreneur and this is to be specified in the Certificate, the relevant requirements under 3.2.2 apply.

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 item of the SubjectAlternativeName extension, if this has been verified for the given application during the Certificate issuance procedure.

The attribute that the key pair was generated and stored at QSCD device may only be inserted in the Certificate if this has been verified 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 are effected 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 verification apply.

3.4 Identification and authentication for revocation request

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

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

The following methods of identification and authentication are permitted for **Certificate revocation applications 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 effected with the private key belonging to the Certificate to be revoked) and sending it to revoke@ica.cz;
- using the I.CA's data box (and using the Certificate revocation password);
- using a defined person assigned to represent the Organization in the contractual relation with I.CA.

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

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

Certificate revocation may also be requested, via the authorized person, by the entities permitted by law to do so.

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

4 CERTIFICATE LIFE CYCLE OPERATIONAL REQUIREMENTS

4.1 Certificate application

4.1.1 Who can submit a certificate applicatio

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

Effected only for the issuance of the primary Certificate, the subscriber initiates the registration procedure by appearing at an RA office and bringing all the required documents plus the Certificate application (if already existing); at the RA office, the data in the submitted documents are entered in 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 executing the Certificate issuance contract;
- conclude with the subscriber or the Organization, such a Certificate issuance contract that meets the requirements imposed by valid trust services legislation and technical and other standards;
- during the Certificate issuance process, check with RA all the verifiable data specified in the application against the documents submitted;
- require a proof of QSCD private key generation if the private key is QSCD-generated;
- 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 valid trust services legislation, this CP, the relevant CPS, the System Security Policy, 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.

Private key ownership verification, specific rights verification 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 on business days during business hours unless other agreement is stipulated in a contract:

- primary Certificate – issued within 15 minutes, or a longer time exceptionally;
- 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 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 and 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 with 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.

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 email provided during registration as mandatory data.

Subsequent Certificates are sent to the contact email 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 accept the Certificate. 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 the publication of which could be contrary to relevant legislation, such as the Personal Data Protection Act);
- required by the subscriber not to be published.

4.4.3 Notification of certificate issuance by the CA to other entities

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

4.5 Key pair and certificate usage

4.5.1 Subscriber private key and certificate usage

Certificate's subscribers must, among other things:

- observe all relevant provisions of the contract of the provision of this Service;
- use the private key and corresponding Certificate issued under this CP solely for the purposes defined in this CP and valid trust services legislation;
- 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 of the private key;
- inform immediately the Service provider of everything that leads to the Certificate's revocation, in particular of suspected abuse of the private key, apply for the Certificate's revocation and stop using the pertinent private key.

4.5.2 Relying party public key and certificate usage

Relying parties must, among other things:

- obtain, from a secure source, 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 valid 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 verified. The same requirements as those in the initial identity verification 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 items 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 verifying 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 a subsequent Certificate with a replaced public key must meet the following requirements:

- the items 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 other application items are the same as the original data in the documents submitted in the initial verification of natural person identity;
- the electronic subsequent Certificate application is verified 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

Changing Certificate data under this CP means the issuance of a new Certificate in which a minimum of one change made to the content of the items, concerning the Certificate's subscriber, under the Subject field or the SubjectAlternativeName extension or in which one field which requires content verification is deleted or added. The public key must be different from that in the Certificate which is 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 verifying 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

Applications for the issuance of a Certificate (the PKCS#10 structure) with changed data (a subsequent Certificate) must meet the following requirements:

- the items to be changed or added in the Subject field or the SubjectAlternativeName extension must be duly verified;
- the other application data are the same as the original data in the documents submitted in the initial verification of natural person identity;
- the public key must be different from that in the original Certificate;
- the electronic subsequent Certificate application is verified 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 applications 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 is in breach of the contract of providing the Service under this CP;
- in any event specified in valid 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 valid trust services legislation.

4.9.2 Who can request revocation

Certificate revocation request may be filed by:

- Certificate's subscriber;
- the entity explicitly specified therefore in the contract of providing the Service under this CP;
- 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 entitled to apply for the revocation of a Certificate issued by I.CA):
  - if the Certificate is issued on the basis of false data;
  - if CEO demonstrably establishes that the private key belonging to the public key specified in the Certificate has been compromised;
  - if CEO establishes that the Certificate is issued in spite of the failure to meet the requirements of valid trust services legislation;
  - if CEO demonstrably establishes that the Certificate was used contrary to the restrictions defined in 1.4.2;
  - if CEO 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 have ceased to be true;
  - 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 valid trust services legislation.

4.9.3 Procedure for revocation request

Any Certificate revocation application 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 natural person authorized to apply for the Certificate's revocation, and the Certificate revocation password. If the natural 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 application is legitimate, the RA employee revokes the Certificate, and the Certificate revocation date and time are the date and time the application is dealt with. If the Certificate revocation application cannot be accepted (wrong revocation password or no proof of identity of the natural person authorized to apply for Certificate revocation) the RA employee seeks to rectify these defects, and dismisses the application if the defects cannot be rectified for any reason. The RA employee always notifies the applicant of the result.

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

- Using the form on the information web page. The Certificate revocation date and time are the date and time a valid Certificate revocation application is dealt with in the CA's information system. The applicant receives a notice if the application 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 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 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 with 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 application 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 applicant receives a notice if the application is granted.

If Certificate revocation application is filed as a registered post letter, the application must contain follows (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 in the decimal or hexadecimal format (introduced by the string ‘0x’). If the application 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 application cannot be accepted (wrong revocation password), the Certificate revocation application will be rejected. How the application is handled is notified to the applicant in a registered post letter sent to the postal address given as the sender’s address.

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 application 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 application 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 always released within 24 hours of the release of the previous CRL.

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

The fact that the Authority provides Certificate status information as OCSP (the OCSP service) 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 (valid CRLs), plus the availability of the OCSP service.

4.10.3 Optional features

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

4.11 End of subscription

The obligations of I.CA out of the certificates issuance contract survive the expiration of that contract until the expiration of the last Certificate issued under that contract.

4.12 Key escrow and recovery

Not applicable to this document; the private key escrow 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, Certification Practice Statement, Business Continuity Plan and Recovery Plan as well as the more detailed internal documents. 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 centre (ARC) and, as may be the case, a special system to monitor movement of persons and vehicles.

5.1.3 Power and air conditioning

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

5.1.4 Water exposures

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

areas in which the trustworthy systems designed to support trust services are situated, and fire extinguishers are fitted in these areas.

5.1.6 Media storage

Storage 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 by valid trust services legislation to be kept are stored at 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 at a place designated by the Chief Executive Officer 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 documents.

No I.CA employee appointed to a trusted role may be in a conflict of interests that could compromise the impartiality of I.CA's operations.

5.2.2 Number of persons required per task

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

- initializing cryptographic module;
- generating key pair of any certification authority and the OCSP responder of the root certification authority;
- destroying the private keys of any certification authority and the OCSP responder of the root certification authority;
- making backups of the private keys of certification authorities (including the root certification authority), which issue qualified certificates to end users;
- recovering the private keys of all certification authorities and their OCSP responders;
- activating and deactivating the private keys of any certification authority and the OCSP responder of the root certification authority.

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

I.CA's trusted role employees are 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 I.CA's employees are:

- the employees themselves;
- any 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 the company's 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 I.CA's internal documentation provided for them, and the required normative documents. Contractual penalties are demanded 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 valid trust services legislation or the relevant technical and other standards to be logged, that is, for example, the life cycle events for the

Certificates, the certificates of the Authority and the root CA and their respective OCSP responders.

The Authority's key pair generation event is a special case of event logging; the following minimum standard is applied at all times:

- the generation takes place according to a pre-determined scenario in a physically secure environment;
- the event is video-recorded where possible.

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, theft and destruction (willful or accidental).

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

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

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

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

5.5.1 Types of stored records

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

- life cycle records for the Certificates issued, the Certificates issued and the certificates related thereto;
- video recordings, if any, of the generation of the Authority's paired data;
- 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 stored throughout the existence of I.CA. Other records are stored in accordance with 5.4.3.

The record storage procedures are regulated in the I.CA internal documentation.

5.5.3 Protection of archive

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

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

5.5.4 Archive backup procedures

The record backup procedures are regulated in the I.CA internal documentation.

5.5.5 Requirements for time-stamping of records

If time stamps are used, they are electronic time stamps issued by I.CA.

5.5.6 Archive collection system (internal or external)

Records are stored at a place designated by CEO of I.CA.

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

5.5.7 Procedures to obtain and verify archive information

Stored information and records are placed at sites designated therefore and are accessible to:

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

A written record is made of any such permitted access.

5.6 Key changeover

In standard situations (expiration of a certificate authority's 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 developments 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 certificate 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;
- 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 discontinuance of the Authority's operations must be notified in writing to the supervisory body, all subscribers of valid Certificates, and the parties having a contract with I.CA that directly concerns the provision of trust services;
- the termination of the Authority's operations must published on the web page pursuant to 2.2;
- if the Authority's certificate's expiration is part of the discontinuance 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 a 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

The generation of key pairs of certification authorities and the corresponding OCSP responders that is effected on secured reserved areas of operating sites, according to a pre-defined scenario, in accordance with 5.2 and 5.4.1, and is evidenced in a written report, is made in a cryptographic module assessed under FIPS PUB 140-2, level 3.

Key pairs of the employees taking part in the issuance of Certificates to end users are generated on chip cards that meet the QSCD requirements. The private keys of these key pair's data are saved on the chip card 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 on hardware and in software.

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 a cryptographic module under the sole control of I.CA.

The service of generating key pairs to end users is not provided.

6.1.3 Public key delivery to certificate issuer

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

6.1.4 CA public key delivery to relying parties

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

- handover from RA (visit in person);
- via I.CA's web Information Addresses;
- via the relevant supervisory body or its journal.

Obtaining other public keys by obtaining their certificates is described in 2.2.

6.1.5 Key sizes

The RSA asymmetric algorithm solely is used for the Service provided under this CP. The size of the key (or the given algorithm's parameters) of I.CA's root certification authority is 4096 bits; the minimum size of the keys (or the given algorithm's parameters) in the

certificates issued by that root 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 the public keys of certification authorities and their OCSP responders meet the requirements listed in valid trust services legislation and the technical and other standards referred to therein.

The parameters of the algorithms used in generating the public keys of end users must also meet these requirements.

I.CA checks the permitted key length and checks for any duplicate public key occurrence in the Certificates issued. If duplicate occurrence is detected, the pertinent Certificate is revoked immediately the Certificate's subscriber is suitably notified immediately and asked to generate new key pair.

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 are generated, and certificate authority private keys and their OCSP responders saved, in cryptographic modules which meet the requirements of the trust services legislation, that is, the FIPS PUB 140-2 standard, level 3.

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

If cryptographic module related operations require the presence of two I.CA management members, then each member only has knowledge of 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 module used for the administration of certification authorities and their OCSP responders' key pairs facilitates private key backup. Private keys are backed up using the native features of the cryptographic module in the encrypted form.

6.2.5 Private key archival

When certification authorities and their OCSP responders private keys expire, they and their backup copies are destroyed. Because storing these private keys is a security risk, it is prohibited at I.CA.

6.2.6 Private key transfer into or from a cryptographic module

The private keys of subordinate certification authorities which issue certificates to end users in accordance with the trust services legislation are transferred from/into the cryptographic module under direct personal participation of no fewer than two I.CA management members.

The private keys of other subordinate certification authorities and all OCSP responder are transferred from the cryptographic module under direct personal participation of one or more I.CA management members.

The private keys of other subordinate certification authorities and all OCSP responders are transferred into the cryptographic module under direct personal participation of no fewer than two I.CA management members.

Every actual transfer is documented in a written record.

6.2.7 Private key storage on cryptographic module

The private keys of certification authorities and their OCSP responders are saved in the cryptographic module which meets the requirements of valid trust services legislation, that is, the FIPS PUB 140-2 standard, level 3.

6.2.8 Method of activating private key

The private keys of certification authorities and the OCSP responders of the root certification authority saved in the cryptographic module are activated under direct personal participation of no fewer than two I.CA management members with the use of an activation chip card and pursuant to a strictly defined procedure described in internal documentation. Every actual activation is documented in a written record.

The private keys of OCSP responders of other certification authorities saved in the cryptographic module are activated under direct personal participation of a single I.CA management member with the use of an activation chip card and pursuant to a strictly defined procedure described in internal documentation. Every actual activation is documented in a written record.

6.2.9 Method of deactivating private key

The private keys of certification authorities and the OCSP responders of the root certification authority saved in the cryptographic module are deactivated under direct personal participation of no fewer than two I.CA management members with the use of an activation chip card and pursuant to a strictly defined procedure described in internal documentation. Every actual deactivation is documented in a written record.

The private keys of OCSP responders of other certification authorities saved in the cryptographic module are deactivated under direct personal participation of a single I.CA management member with the use of an activation chip card and pursuant to a strictly defined procedure described in internal documentation. Every actual deactivation is documented in a written record.

6.2.10 Method of destroying private key

The private keys of certification authorities and their OCSP responders saved in the cryptographic module are destroyed with the native features of that cryptographic module and under direct personal participation of no fewer than two I.CA management members pursuant to a strictly defined procedure described in internal documentation. Every actual destruction is documented in a written record.

Any external medium with a backup copy of those private keys is also destroyed. The destruction, consisting in physical destruction of those data media, is carried out under direct personal participation of no fewer than two I.CA management members pursuant to a strictly defined procedure described in internal documentation. Every actual destruction is documented in a written record.

6.2.11 Cryptographic module rating

The cryptographic modules in which paired data are generated and the private keys of certification authorities and their OCSP responders are saved meet the requirements of the trust services legislation, that is, the FIPS PUB 140-2 standard, level 3. The security of the modules is under monitoring as long as they are in use.

6.3 Other aspects of key pair management

6.3.1 Public key archival

The public keys of certification authorities and their OCSP responders are stored 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.

6.4 Activation data

6.4.1 Activation data generation and installation

The activation data of certification authorities and their OCSP responders are created during the generation of the corresponding key pair.

6.4.2 Activation data protection

The activation data of certification authorities and their OCSP responders are protected by a method described in internal documentation.

6.4.3 Other aspects of activation data

The activation data of the private keys of certification authorities and their OCSP responders for the provision of trust services must not be used for any other purpose and transferred or kept in an open form. All aspects are described in internal documentation.

6.5 Computer security controls

6.5.1 Specific computer security technical requirements

The security level of the components employed in providing trust services is defined by valid trust services legislation and the technical and other 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) – Policy and Security 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.
- ETSI TS 119 312 Electronic Signatures and Infrastructures (ESI); Cryptographic Suites.
- 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.

The Authority's operations are also governed by the following technical standards:

- FIPS PUB 140-2 Requirements for Cryptographic Modules.
- 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.
- 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 2: Certificate Profile for Certificates Issued to Legal Persons.
- 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: QC Statements.

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 in 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.
- ČSN ISO/IEC 27006 Information Technology – Security Techniques – Requirements for Bodies Providing Audit and Certification of Information Security Management Systems.

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

In the I.CA environment the trustworthy systems destined for supporting trust services and situated at I.CA's operating sites are not directly accessible from the Internet. These systems are protected with a firewall-type commercial product with an integrated intrusion prevention system (IPS). 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	sha256withRSAEncryption at minimum
Issuer	issuer of the Certificate (the Authority)
Validity	
notBefore	start of the Certificate's validity (UTC)
notAfter	end of the Certificate's validity (UTC)
Subject	see Table 5
SubjectPublicKeyInfo	
Algorithm	rsaEncryption
subjectPublicKey	2048 bits at minimum
Extensions	see Table 6
Signature	Authority's electronic sign/seal

Table 5 – Subject field items

All items[1] of the Subject field are taken over from the Certificate application except the items created by the Authority. The application must include the mandatory items.

Subject field item	Comments
countryName**	mandatory, country code (ISO 3166), single occurrence
givenName	mandatory if the pseudonym item is not specified; single occurrence
surName	mandatory if the pseudonym item is not specified; single occurrence
pseudonym	mandatory if the givenName and the surName items are not specified; single occurrence
serialNumber (1)	created by the Authority; unique identification of the Certificate's subscriber in the Authority's system (ICA – xxxxxxxx); also used in automated subsequent certificate issuance

[1] 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).

serialNumber (2)	optional; either of the following two options: • IDCss-nnnnnnnn; • PASss-nnnnnnnn; where ss is the country code (ISO 3166) of document 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 item must not be included in the primary Certificate
Name	this item must not be included in the primary Certificate
generationQualifier	optional; single occurrence
organizationName	employee of the Organization: mandatory; single occurrence individual-entrepreneur: optional; single occurrence individual non-entrepreneur: must not be specified
organizationIdentifier	optional and only if the organizationName attribute is specified; single occurrence – one of the following three options: • NTRss-id, (**N**ational **T**rade **R**egister, i.e. business/company identification number); • VATss-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 (must not be the 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 occurrence permitted
title	optional; multiple occurrence 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 item may also contain verified degrees of the Certificate's subscriber

** the items countryName, stateOrProvinceName, localityName, streetAddress and postalCode relate to the Certificate subscriber's primary document data

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[2]

Extension	Content	Comments
CertificatePolicies		non-critical; created by the Authority
.PolicyInformation (1)		
policyIdentifier	see 1.2	Certificate issued under this CP
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	either of the following two options: • OID (QCP-n): 0.4.0.194112.1.0	

[2] 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).

	(the private key is not generated and saved on QSCD); • OID (QCP-n-qscd): 0.4.0.194112.1.2 (the private key is generated and saved on QSCD)	
QCStatements		non-critical; created by the Authority
	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 saved 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
CRLDistributionPoints*	http://qcrldp1.ica.cz/2qcaRR_rsa.crl http://qcrldp2.ica.cz/2qcaRR_rsa.crl http://qcrldp3.ica.cz/2qcaRR_rsa.crl	non-critical; created by the Authority
authorityInformationAccess		non-critical; created by the Authority
id-ad-ocsp*	http://ocsp.ica.cz/2qcaRR_rsa	
id-ad-caIssuers*	http://q.ica.cz/2qcaRR_rsa.cer	
BasicConstraints		non-critical; created by the Authority
cA	False	
KeyUsage	one of the following three options, according to what is completed in Certificate application: • nonRepudiation; • digitalSignature, nonRepudiation; • digitalSignature, nonRepudiation and keyEncipherment***	critical, mandatory if this extension is missing from the application, the following will be added: digitalSignature, nonRepudiation
ExtendedKeyUsage	one of the following three options, according to what is completed in	non-critical, mandatory

	Certificate application: • id-kp-emailProtection; • ms-Document_Signing; • id-kp-emailProtection; • ms-Document_Signing	if this extension is missing from the application, the following will be added: id-kp-emailProtection
SubjectKeyIdentifier	hash of the public key (subjectPublicKey) in the Certificate	non-critical; created by the Authority
AuthorityKeyIdentifier		non-critical; created by the Authority
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	created by the Authority
otherName	MPSV_IK (1.3.6.1.4.1.11801.2.1): numerical identifier supplied by MPSV	optional; added by the Authority
rfc822Name	email address	optional; multiple occurrence permitted
nsComment	QSCD identification number	non-critical; optional – added by the Authority in the case of the verification of the generation and the saving of the private key on QSCD
I.CA_TWIN_ID: 1.3.6.1.4.1.23624.4.3	Certificate application number	non-critical; created by CA for internal use
I.CA_CERT_INTERCONNECTION: 1.3.6.1.4.1.23624.4.7	if multiple certificate types are issued to a single entity (entity's connection to the certificates issued)	non-critical; created by CA for internal use

* 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 item created by the Authority (see Table 5)

*** last option (containing setting keyEncipherment bit) for KeyUsage can not be used when the key is generated and stored on StarCos smartcard

7.1.3 Algorithm object identifiers

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

7.1.4 Name forms

Name forms included in the Authority-issued Certificates comply with RFC 5280. 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 saving of the private key and declaring that the Certificate is in compliance with eIDAS.

7.1.7 Usage of policy constrains 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[3]

Field	Content
Version	v2(0x1)
SignatureAlgorithm	sha256withRSAEncryption
Issuer	issuer of the CRL (the Authority)
thisUpdate	date and time the CRL is released (UTC)

[3] 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).

nextUpdate	date and expected time 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 item extensions – see Table 8
crlExtensions	CRL extensions – see Table 8
Signature	CRL issuer's (Authority's) electronic sign/seal

7.2.1 Version number(s)

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

7.2.2 CRL and CRL entry extensions

Table 8 – CRL Extension[4]

Extension	Content	Comments
crlEntryExtensions		
CRLReason	certificate revocation reason as the *certificateHold* reason is not admissible, I.CA does not use it	non-critical
crlExtensions		
AuthorityKeyIdentifier		
KeyIdentifier	hash of the CRL issuer's (Authority'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 are in accordance with RFC 6960 and RFC 5019.

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

See the relevant certification practice statement for more detail.

[4] 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).

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

8 CONFORMITY ASSESSMENTS AND OTHER ASSESSMENTS

8.1 Frequency or circumstances of assessment

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

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

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

8.2 Identity/qualifications of assessor

The identity (accredited conformity assessment entity) and the qualification of the assessor carrying out the assessment pursuant to the valid 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 Certificate 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 through property or organization.

8.4 Topics covered by assessment

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

The areas to be assessed in an assessment required for Microsoft Trusted Root Certificate 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 the trust services legislation and the relevant technical standards; the notification of Microsoft Trusted Root Certificate 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 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. for detailed information on the company's assets.

9.2.3 Insurance or warranty coverage for end-entities

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

9.3 Confidentiality of business information

9.3.1 Scope of confidential information

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

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

9.3.2 Information not within the Scope of confidential information

Public information is only the information designated as public and that published in the manner pursuant to 2.2.

9.3.3 Responsibility to protect confidential information

No I.CA employee who comes in contact with confidential information may disclose the same 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.

9.4.2 Information treated as private

Any personal data subject to protection under ZOOÚ are personal information.

I.CA employees or the entities defined by valid 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, that is, ZOOÚ, 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, that is, ZOOÚ.

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, that is, ZOOÚ.

9.4.7 Other Information disclosure circumstances

I.CA provides access to personal data strictly as regulated in relevant legislation, that is, ZOOÚ.

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's root certification authority), releasing certification 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 does not breach any obligation out of the contract of Services and this CP;
- the relying party does not breach any obligation out of 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 these Certificates and administering the same throughout their periods of validity.

The warranties include:

- checking the right to apply for the Certificate;
- verifying 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 the legislation in force;
- 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 the valid trust services legislation and this CP.

9.6.2 RA representations and warranties

The designated RA:

- assumes the obligation that the services the RA provides are correct;
- does not settle the application unless the RA verifies all the application items (except those not subject to verification), or the Certificate's subscriber provides the required data or is authorized to file 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 contract between I.CA and the Certificate's subscriber provides that the Certificate's subscriber is obligated to abide by this CP.

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. may not be held liable, in respect of this Service, for any damage suffered by relying parties where the relying party breaches its duty under the valid trust services legislation and this CP. První certifikační autorita, a.s. may also not be held liable 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 valid 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 the valid trust services legislation and must always take an electronic or printed form.

První certifikační autorita, a.s.:

- undertakes to discharge all the duties defined in valid legislation (including the 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;
- any other possible compensations are based on the relevant legislation and the amount of damages may be determined by court.

První certifikační autorita, a.s. **may not be held liable 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 contract of the Service, 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 made and delivered by:

- email to reklamace@ica.cz;
- message to I.CA's data box;
- 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 email, 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.

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 duties of I.CA out of this CP survive the expiration thereof until the expiration of the last Certificate issued under this CP.

9.11 Individual notices and communications with participants

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

Communication with I.CA may also be effected 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 document.

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

The policy's OID must be changed following any major change in how this Service is provided.

Any change to this document 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 statutory requirements of 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 illegal, the scope of that requirement will be so limited as to ensure the requirement is applicable and lawful.

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. may not be held liable for breaching its obligations if it is a result of force majeure, such as major natural disaster, major disaster caused by human activity, strike or civil unrest always followed by the declaration of a situation of emergency, or the declaration of a state threat to the 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 on 3 May 2018.