První certifikační autorita, a.s.

Certification Practice Statement

(RSA Algorithm)

Version 1.63

TABLE OF CONTENTS

Table 1 – Document history

Version	Date of Release	Approved by	Comments
1.0	15 July 2015	CEO of První certifikační autorita, a.s.	First release.
1.1	2 November 2015	CEO of První certifikační autorita, a.s.	Updated OIDs of certification policies (TSA, OCSP).

1.2	29 March 2016	CEO of První certifikační autorita, a.s.	Updated OID of SSL certification policy.
1.3	6 April 2016	CEO of První certifikační autorita, a.s.	Adding supported certification policies.
1.4	15 March 2017	CEO of První certifikační autorita, a.s.	Updated policy OIDs. Modified to match statutory requirements for trust services and technical standard requirements. Modified to match the requirements of Microsoft Trusted Root Certificate Program.
1.5	3 April 2017	CEO of První certifikační autorita, a.s.	Updated policy OIDs.
1.6	20 November 2017	CEO of První certifikační autorita, a.s.	New policies added. Changed method to record policy OIDs.
1.61	30 April 2018	CEO of První certifikační autorita, a.s.	Change of versioning the document. Adding the description of QSCD list checking. Adding the description of CAA records checking.
1.62	13 September 2018	CEO of První certifikační autorita, a.s.	New policies added.
1.63	30 April 2019	CEO of První certifikační autorita, a.s.	Annual revision, formal errors correction.

1 INTRODUCTION

This document details and clarifies the principles specified in specific certification policies (CPs) which První certifikační autorita, a.s. (also as I.CA), a qualified trust service provider, applies in providing qualified trust services and non-qualified trust services and issuing other certificate types (also as the Services). The RSA algorithm is used for the Services provided under this certification practice statement (also as CPS) and the relevant certification policies.

Where applicable, the Services are provided for 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.

Note: Any reference to standards or laws is always a reference to that standard or law or the replacing standard or law. If this CPS or the relevant certification policy is in conflict with any standard or law that replaces the current standard or law, a new version will be released.

1.1 Overview

The document **Certification Practice Statement (RSA Algorithm)** is prepared by První certifikační autorita, a.s., deals with the issues related to life cycle processes of certificates and follows a structure matching the scheme of effective RFC 3647 standard while taking account of effective EU standards and the laws of the Czech Republic pertinent to this sphere (therefore, each chapter is preserved in this document even if it is irrelevant to this sphere). This applies to the certification policies listed in 1.2.

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

- Chapter 1 identifies this document, generally describes the entities and individuals taking part in the provision of the Services, and defines the acceptable usage of the certificates available to be issued;
- Chapter 2 deals with the responsibility for the publication and information or documents;
- Chapter 3 describes the processes of identification and authentication of an applicant for the issuance or revocation of a certificate, and defines the types and contents of the names used in certificates;
- Chapter 4 defines life cycle processes of certificates, i.e. certificate issuance application, the issuance of the certificate, certificate revocation request, the revocation of the certificate, the services related to the verification of certification status, termination of the provision of the Services, etc;
- Chapter 5 covers physical, procedural and personal security, including the definition of the set of recorded events, the keeping of these records and responses to emergency and compromising situations;
- Chapter 6 focuses on the technical security of the type of generating public and private keys, protection of private keys, including the computer and network protection,
- Chapter 7 refers to certificate profiles and CRL profiles in specific CPs and specifies the types and the length of the attributes in the subject field and the subjectAlternativeName extension;

- Chapter 8 focuses on Service assessment;
- Chapter 9 deals with commercial and legal aspects.

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

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

1.2 Document name and identification

This document's title: Certification Practice Statement (RSA Algorithm), version 1.63

Document OID: No OID assigned.

This CPS applies to the following certification policies:

OID	CP
1.3.6.1.4.1.23624.10.1.10.*x.y*	Root Qualified Certification Authority's Certification Policy (RSA Algorithm)
1.3.6.1.4.1.23624.10.1.30.*x.y*	Certification Policy for the Issuance of Qualified Electronic Signature Certificates (RSA Algorithm)
1.3.6.1.4.1.23624.10.1.31.*x.y*	Certification Policy for the Issuance of Qualified Electronic Seal Certificates (RSA Algorithm)
1.3.6.1.4.1.23624.10.1.32.*x.y*	Certification Policy for the Issuance of TSA System Certificates (RSA Algorithm)
1.3.6.1.4.1.23624.10.1.32.*x.y*	Certification Policy for the Issuance of Qualified Certificates for TSA2 System Electronic Seal (RSA Algorithm)
1.3.6.1.4.1.23624.10.1.33.*x.y*	Certification Policy for the Issuance of System Certificates (RSA Algorithm)
1.3.6.1.4.1.23624.10.1.34.*x.y*	Certification Policy for the Issuance of Qualified PSD2 Electronic Seal Certificates (RSA Algorithm)
1.3.6.1.4.1.23624.10.1.35.*x.y*	Certification Policy for the Issuance of Qualified Website Authentication Certificates for Legal Entities (RSA Algorithm)
1.3.6.1.4.1.23624.10.1.40.*x.y*	Certification Policy for the Issuance of Qualified Website Authentication Certificates for Legal Entities PSD2 (RSA Algorithm)
1.3.6.1.4.1.23624.10.1.70.*x.y*	Certification Policy for the Issuance of Commercial Certificates (RSA Algorithm)
1.3.6.1.4.1.23624.10.1.71.*x.y*	Certification Policy for the Issuance of Commercial Technology Certificates (RSA Algorithm)
1.3.6.1.4.1.23624.10.1.72.*x.y*	Certification Policy for the Issuance of SSL Certificates (RSA Algorithm)

1.3.6.1.4.1.23624.10.1.80.*x.y*	Certification Policy for the Issuance of OCSP Responder Certificates (RSA Algorithm)
1.3.6.1.4.1.23624.10.1.90.*x.y*	Certification Policy for the Issuance of Qualified SK Certificates for Electronic Signatures (RSA Algorithm)
1.3.6.1.4.1.23624.10.1.91.*x.y*	Certification Policy for the Issuance of Qualified Electronic SK Signature Certificates (RSA Algorithm)

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

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

1.3 PKI participants

1.3.1 Certification authorities (also as 'CA')

1.3.1.1 Root certification authority

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

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

1.3.1.2 Issuing Certification Authorities

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

1.3.2 Registration authorities (also as 'RA')

The registration authorities employed in the life cycle processes of the certificates issued to end users. These RAs can be stationary or mobile.

1.3.3 Subscribers

1.3.3.1 Certificates of the provider (I.CA)

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

1.3.3.2 End user certificates

The certificates are issued to end users who use the certification service of I.CA.

1.3.4 Relying parties

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

1.3.5 Other participants

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

1.4 Certificate usage

1.4.1 Appropriate certificate uses

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

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

The certificates of the time servers of time stamp authorities may only be used for verifying the time stamps issued by these time servers.

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

1.4.2 Prohibited certificate uses

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

1.5 Policy administration

1.5.1 Organization administering the document

This CP and the certification policies corresponding thereto are administered by První certifikační autorita, a.s.

1.5.2 Contact person

The contact person of První certifikační autorita, a.s. in respect of this CPS and the corresponding certification policies is specified on a web page – see 2.2.

1.5.3 Person determining CPS suitability for the policy

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

1.5.4 CPS approval procedures

If it is necessary to make changes to a CPS to create a new version thereof, the 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
Classified Information Protection Act	the Czech Republic's Act No. 412/2005 Coll., regulating classified information protection and security competence, as amended
contracting partner	provider of selected certification services contracted by I.CA for certification services or parts thereof – usually, it is a 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 effective trust services legislation
electronic mark	electronic mark under effective trust services legislation
electronic signature	electronic signature or advanced electronic signature or qualified electronic signature or recognized electronic signature under effective trust services legislation
electronic signature creation device	configured software or hardware 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/mark/seal

public key	unique data to verify electronic signature/mark/seal
qualified electronic signature certificate	certificate defined by effective 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
secure cryptographic device	device on which the private key is saved
supervisory body	body supervising compliance with trust services legislation
time stamp	electronic time stamp or qualified electronic time stamp as defined by effective trust services legislation
trust service / qualified trust service	electronic service / qualified trust service as defined in eIDAS
trust services legislation	the Czech Republic's or the Slovak Republic legislation related to electronic transaction trust services and the eIDAS Regulation
TWINS	I.CA's commercial product containing a pair of certificates: ▪ qualified electronic signature certificate – issued in accordance with the corresponding 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 smart 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
ARC	Alarm Receiving Centre
bit	from English *binary digit* – a binary system digit – the fundamental and the smallest unit of information in digital technologies
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

CR	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
ESI	Electronic Signatures and Infrastructures
ETSI	European Telecommunications Standards Institute, a European standardization institute for information and communication technologies
EU	European Union
FAS	Fire 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.
IAS	Intrusion Alarm System
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
PDCA	Plan-Do-Check-Act, Deming cycle, a method of continuous improvement
PDS	PKI Disclosure Statement
PKCS	Public Key Cryptography Standards, designation for a group of standards for public key cryptography
PKI	Public Key Infrastructure
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
TSA	Time Stamping Authority – comprised of multiple servers which issue time stamps, with each server having a unique private key and, therefore, a unique qualified system certificate
TSS	Time Stamp Server
UPS	Uninterruptible Power Supply/Source
URI	Uniform Resource Identifier, defined-structure text string for accurate specification of a source of information
UTC	Coordinated Universal Time, the standard adopted on 1 January 1972 for the global coordinated time – Bureau International de l'Heure (BIH) plays the role of the 'official keeper' of the atomic time for the whole world
ZOOÚ	current personal data protection legislation

2 PUBLICATION AND REPOSITORY RESPONSIBILITY

2.1 Repositories

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

2.2 Publication of certification information

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

- Registered office:

  První certifikační autorita, a.s.

  Podvinný mlýn 2178/6

  190 00 Praha 9

  Czech Republic
- Website: http://www.ica.czů
- 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 date (specifying the hour, minute and second);
  - Link to where the certificate can be obtained in the specified format (DER, PEM, TXT);
- Certificate revocation list (CRL) – the following information is published (and more information can be obtained from the CRL):
  - Date of CRL release;
  - CRL number;
  - Links to where the CRL can be obtained in the specified formats (DER, PEM, TXT);
- Certification and other policies 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 a daily newspaper with national distribution – Hospodářské noviny or Mladá fronta Dnes (in the Czech Republic) and Hospodárské noviny or Sme (in Slovakia).

2.3 Time or frequency of publication

See 2.3 of a specific CP.

2.4 Access controls on repositories

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

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

- 'CA Operator';
- 'I.CA Registration Authority Employees Guidelines';
- 'Information Security Management';
- 'Administration Guidance';
- 'Security Incidents';
- 'HSM/Private Server';
- 'TSS Administration';
- 'Certification Services Documents';
- 'Certification Services Partial Document Management and Destruction Rules';
- 'Certification Services Partial Document Management and Destruction Plan'.

3 IDENTIFICATION AND AUTHENTICATION

3.1 Naming

3.1.1 Types of names

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

3.1.2 Need for names to be meaningful

For a certificate to be issued, all verifiable names given in the subject field and the subjectAlternativeName extension must carry a meaning. Refer to a specific CP for the attributes supported for this field and this extension.

3.1.3 Anonymity or pseudonymity of subscribers

See 3.1.3 of a specific CP.

3.1.4 Rules for interpreting various name forms

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

3.1.5 Uniqueness of names

See 3.1.5 of the specific certification policy.

3.1.6 Recognition, authentication, and role of trademarks

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

3.2 Initial identity validation

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

- 'I.CA Registration Authority Employees Guidelines'.

3.2.1 Method to prove possession of private key

The ownership of the private key matching the public key in the Certificate application must be proved by submitting the application in the PKCS#10 format. The application is electronically signed with this private key, and/or provided with electronic mark/seal as

applicable, whereby the private key holder provides evidence that he is the holder of the private key when the electronic signature, or the electronic mark/seal, is created.

3.2.2 Authentication of organization identity

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

- 'I.CA Registration Authority Employees Guidelines'.

3.2.3 Authentication of individual identity

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

- 'I.CA Registration Authority Employees Guidelines'.

3.2.4 Non-verified subscriber information

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

3.2.5 Validation of authority

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

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

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

3.2.6 Criteria for interoperation

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

3.3 Identification and authentication for re-key requests

3.3.1 Identification and authentication for routine re-key

A new certificate with a new public key always needs to be issued. Refer to 3.3.1 of a specific CP for requirements.

3.3.1.1 Certificates of the provider (I.CA)

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

3.3.1.2 End user certificates

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

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

3.3.2 Identification and authentication for re-key after revocation

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

3.4 Identification and authentication for revocation request

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

3.4.1 Certificates of the provider (I.CA)

The person authorized to apply for the revocation of a certificate of:

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

is CEO of I.CA.

The head of the authority which granted První certifikační autorita, a.s. the qualified trust service provider status may also be the requestor requesting the revocation of the root certification authority's certificate or a certificate related to qualified certification services. The authority must submit its request in writing or as a message delivered in I.CA's data box. CEO of I.CA must always attend in person the process of revoking such a certificate.

3.4.2 End user certificates

These are the available methods of identification and authentication:

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

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

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

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

4 CERTIFICATE LIFE-CYCLE REQUIREMENTS

4.1 Certificate application

4.1.1 Who can submit a certificate application

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

4.1.2 Enrollment process and responsibilities

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

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

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

The Service provider is particularly required to provide the Services in accordance with effective legislation, the specific CP and this CPS, the System Security Policy of CA and TSA and the operating documentation.

4.2 Certificate application processing

The handling of certificate applications is described in internal documentation:

- 'I.CA Registration Authority Employees Guidelines';
- 'CA Operator'.

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

- 'Procedures of validation the application for QC-web/EV SSL certificate'.

4.2.1 Performing identification and authentication functions

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

4.2.2 Approval or rejection of certificate applications

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

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

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

- 'I.CA Registration Authority Employees Guidelines'.

4.2.3 Time to process certificate applications

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

Any end user certificate must be issued by I.CA immediately after certificate issuance is granted. The following list gives tentative times for issuing certificates on business days during business hours unless other agreement is stipulated in a contract:

- First certificate – issued within 15 minutes, or a longer time exceptionally;
- Subsequent Certificates – within units of minutes.

SSL certificates and website authentication certificates are exceptions – usually, certificate applications are handled within five business days (because of verifying the application data).

4.3 Certificate issuance

4.3.1 CA actions during certificate issuance

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

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

The verification of private key ownership, the supported hash function in the Certificate application (no weaker than sha-256), the competence check and the formal data correctness check are carried out 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.

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

- 'I.CA Registration Authority Employees Guidelines';
- 'CA Operator'.

4.3.2 Notification to subscriber by the CA of issuance of certificate

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

These procedures are described in detail in internal documentation:

- 'I.CA Registration Authority Employees Guidelines';
- 'CA Operator'.

4.4 Certificate acceptance

4.4.1 Conduct constituting certificate acceptance

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

Process details are described in internal documentation:

- 'I.CA Registration Authority Employees Guidelines';
- 'CA Operator'.

4.4.2 Publication of the certificate by the CA

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

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

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

4.4.3 Notification of certificate issuance by the CA to other entities

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

4.5 Key pair and certificate usage

4.5.1 Subscriber private key and certificate usage

Subscriber must, among other things:

- Observe all relevant provisions of the contract of the provision of the Services;
- Use the private key and the corresponding certificate issued under a specific CP solely for the purposes defined in this CP and effective trust services legislation;
- Handle the private key corresponding to the public key contained in the certificate issued under a specific CP in a manner as to prevent any unauthorized use of the private key;
- 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, the certification authority certificates related to the end user certificate issued under a specific CP, and verify those certificates' fingerprint values and validity;

- Carry out any operation necessary for them to verify that the certificate is valid, i.e.:
  - Check certificate validity pursuant to RFC5280, chapter 6 (including the full certification path and certificate validity revocation);
  - Check whether the issuer of the qualified certificate is qualified (is on the trust services list with the pertinent attributes);
- Observe all and any provisions of the pertinent CP and effective trust services legislation which relate to the relying party's duties.

4.6 Certificate renewal

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

The certificate renewal service is not provided.

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

4.6.1 Circumstance for certificate renewal

See 4.6.

4.6.2 Who may request renewal

See 4.6.

4.6.3 Processing certificate renewal requests

See 4.6.

4.6.4 Notification of new certificate issuance to subscriber

See 4.6.

4.6.5 Conduct constituting acceptance of a renewal certificate

See 4.6.

4.6.6 Publication of the renewal certificate by the CA

See 4.6.

4.6.7 Notification of certificate issuance by the CA to other entities

See 4.6.

4.7 Certificate re-key

See 4.7 of a specific certification policy.

4.7.1 Circumstance for certificate re-key

See 4.7.

4.7.2 Who may request certification of a new public key

See 4.7.

4.7.3 Processing certificate re-keying requests

See to 4.7.

4.7.4 Notification of new certificate issuance to subscriber

See 4.7.

4.7.5 Conduct constituting acceptance of a re-keyed certificate

See 4.7.

4.7.6 Publication of the re-keyed certificate by the CA

See 4.7.

4.7.7 Notification of certificate issuance by the CA to other entities

See 4.7.

4.8 Certificate modification

See 4.8 of a specific certification policy.

4.8.1 Circumstance for certificate modification

See 4.8.

4.8.2 Who may request certificate modification

See 4.8.

4.8.3 Processing certificate modification requests

See 4.8.

4.8.4 Notification of new certificate issuance to subscriber

See 4.8.

4.8.5 Conduct constituting acceptance of modified certificate

See 4.8.

4.8.6 Publication of the modified certificate by the CA

See 4.8.

4.8.7 Notification of certificate issuance by the CA to other entities

See 4.8.

4.9 Certificate revocation and suspension

4.9.1 Circumstances for revocation

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

4.9.1.1 Certificates of the provider (I.CA)

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

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

4.9.1.2 End user certificates

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

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

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

4.9.2 Who can request revocation

4.9.2.1 Certificates of the provider (I.CA)

Revocation request may be submitted by:

- CEO of I.CA; and
- Other entities as may be specified in effective trust services legislation.

4.9.2.2 End user certificates

Revocation request may be submitted by:

- Subscriber;
- The entity explicitly specified therefore in the contract for providing the pertinent Service;
- Any person who is beneficiary in subscriber probate proceedings;
- Provider of the 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 demonstrably establishes that the certificate was used contrary to the restrictions defined in 1.4.2;
  - If CEO demonstrably establishes that the 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;
  - If CEO establishes that the Certificate is issued in spite of the failure to meet the requirements of effective trust services legislation;
- Supervisory body, and other entities specified in effective trust services legislation.

4.9.3 Procedure for revocation request

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

The identification and authentication requirements are listed in 3.4.

4.9.4 Revocation request grace period

Certificate revocation request must be made immediately.

4.9.5 Time within which CA must process the revocation request

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

Detailed procedures are described in internal documentation:

- 'CA Operator'.

4.9.6 Revocation checking requirement for relying parties

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

4.9.7 CRL issuance frequency

The interval for releasing revocation certificate lists is specified in 4.9.7 of the specific CP.

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

- 'CA Operator'.

4.9.8 Maximum latency for CRLs

The CRL is always released within 24 hours of the release of the previous CRL.

4.9.9 On-line revocation/status checking availability

Checking certificate status online using the OCSP protocol is a service available to the general public. Every certificate 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 for key compromise

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

4.9.13 Circumstances for suspension

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

4.9.14 Who can request suspension

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

4.9.15 Procedure for suspension request

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

4.9.16 Limits on suspension period

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

4.10 Certificate status services

4.10.1 Operational characteristics

Lists of public certificates are provided as published information; revocation certificate lists are provided as published information and the list of CRL distribution points in the certificates issued by specific certification authority.

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

4.10.2 Service availability

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

The procedure is specified in internal documentation including:

- ‘Administration Guidance’;
- ‘Operating Site Component Recovery’;
- ‘Operating Site Relocation’.

4.10.3 Optional features

I.CA also includes expired certificates in the certificate revocation list, for three days after a certificate’s expiration. Expired certificates are included in CRLs for a limited period in order to keep CRLs to a reasonable length.

If I.CA makes a decision to terminate the certificate status service (CRLs), I.CA releases and publishes the last CRL with the ‘99991231235959Z’ value in the ‘nextUpdate’ attribute.

As part of the certificate status service (OCSP) I.CA includes, in OCSP responses, also the expired certificate status information for certificates which expired no more than three days ago (in accordance with the CRL and with regard to the consistency of the information in the CRL and that in OCSP).

If the certificate of the issuing CA is nearing expiration, I.CA specifies the ‘99991231235959Z’ value in the ‘nextUpdate’ attribute in the last OCSP response for each issued certificate.

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 storage service is not provided.

4.12.1 Key escrow and recovery policy and practices

See 4.12.

4.12.2 Session key encapsulation and recovery policy and practices

See 4.12.

5 FACILITY, MANAGEMENT, AND OPERATIONAL CONTROLS

The management, control and operating procedures primarily deal with:

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

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

5.1 Physical controls

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

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

5.1.1 Site location and construction

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

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

5.1.2 Physical access

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

5.1.3 Power and air-conditioning

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

5.1.4 Water exposures

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

5.1.5 Fire prevention and protection

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

5.1.6 Media storage

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 effective 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 documentation in general and the following documents in particular:

- ‘System Security Policy of CA and TSA’;
- ‘Information Security Management’;
- ‘Administration Guidance’.

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 pair 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.

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

- 'Administration Guidance';
- 'Hierarchical Structure – Procedures to Generate CA Keys and Certificates';
- 'HSM/Private Server'.

5.2.3 Identification and authentication for each role

Each role's employees are assigned identification (name and certificate) and authentication (password and private key) data for those components which are necessary for their jobs. These topics are regulated in internal documentation in general and these documents in particular:

- 'I.CA Registration Authority Employees Guidelines';
- 'CA Operator';
- 'Administration Guidance'.

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

5.2.4 Roles requiring separation of duties

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

- 'System Security Policy of CA and TSA'.

5.3 Personnel controls

5.3.1 Qualification, experience, and clearance requirements

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

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

Any other I.CA employee taking part in providing the Services is hired subject to the following criteria:

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

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

These topics are described in detail in internal documentation:

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

5.3.2 Background check procedures

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

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

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

5.3.3 Training requirements

I.CA employees receive technical training in the use of specific software and specialized devices. The training takes the form of self-study combined with guidance from a trained employee. The training covers information security, personal protection data and other relevant topics.

These topics are described in detail in the internal documentation:

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

5.3.4 Retraining frequency and requirements

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

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

These topics are described in detail in internal documentation:

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

5.3.5 Job rotation frequency and sequence

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

5.3.6 Sanctions for unauthorized actions

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

These topics are described in detail in internal documentation:

- 'Employment Rules'.

5.3.7 Independent contractor requirements

I.CA may or must procure some activities from independent contractors, and is fully liable for the job they deliver. These business relations are regulated in bilateral business contracts with parties such as contracted registration authorities, application software developers, hardware suppliers, system software suppliers, external auditors and other parties. These parties are required to observe the pertinent certification policies, the relevant parts of internal documentation provided for them, and the required normative documents. Contractual penalties are 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 certification practice statement and the security and operating documentation, I.CA employees have available any other relevant standard, policy, manual and guidance they may need for their job.

5.4 Audit logging procedures

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

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

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

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

- 'Administration Guidance';
- 'Gathering Data to Be Stored';
- 'Application Systems Data Backup';
- 'Certification Services Documents';
- 'Certification Services Partial Document Management and Destruction Rules';
- 'Certification Services Partial Document Management and Destruction Plan'.

5.4.1 Types of events recorded

The generation of the root certification authority's key pair and a subordinate certification authority's key pair are special cases of event logging. All the process for the root certification authority are carried out in accordance with effective trust services legislation and the relevant technical standards, and the following minimum requirements are complied with at all times:

- The process is organized according to a pre-determined scenario in a physically secure environment; and
  - The process is attended in person by an auditor qualified in accordance with effective technical standards; or
  - A video recording is made and, where practicable, the generation is attended by a notary, who takes down a certification report to document the course of the event;
- Relying on his personal attendance, or on the video recording and the certificate if any, the auditor, qualified in accordance with effective technical standards, makes a report to document that the root certification authority followed the pre-determined scenario in key pair generation and to document the measures to ensure integrity and confidentiality.

The following minimum requirements are complied with in generating a certification authority's key pair:

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

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

- System-relevant events in environment and key management;
- Audit function start and audit function end;
- Changes to audit parameters;

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

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

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

5.4.2 Frequency of processing log

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

- ‘Administration Guidance’.

or immediately when a security incident occurs.

5.4.3 Retention period for audit log

Unless 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 – see 5.4.

5.4.5 Audit log backup procedures

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

5.4.6 Audit collection system (internal or external)

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

5.4.7 Notification to event-causing subject

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

5.4.8 Vulnerability assessments

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

- ‘Administration Guidance’.

5.5 Records archival

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

- ‘I.CA Rooms Physical Access Control ’;
- ‘Gathering Data to Be Stored’;
- ‘Application Systems Data Backup’;
- ‘Administration Guidance’;
- ‘Certification Services Documents’;
- ‘Certification Services Partial Document Management and Destruction Rules’;
- ‘Certification Services Partial Document Management and Destruction Plan’.

5.5.1 Types of records archived

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

- Video recording of the generation of the root certification authority's key pair;
- Notary's certificate of the generation of the root certification authority's key pair, if any;
- Auditor's report on the generation of the root certification authority's key pair;
- Life cycle records for the certificates issued, the certificates issued and the certificates related thereto;
- Video recording, if any, of the generation of the certification authority's key pair;
- 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

The records pertaining to the certificates issued by the root certification authority, except the pertinent private keys of the provider, 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 internal documentation – see 5.5.

5.5.3 Protection of archive

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

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

5.5.4 Archive backup procedures

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

5.5.5 Requirements for time-stamping of records

If time 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 – refer to 5.5. Records are kept of collecting records.

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 documentation:

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

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

See 5.7.1.

5.7.3 Entity private key compromise procedures

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

- Stops using the private key;
- Revokes immediately and permanently the pertinent certificate and destroys the corresponding private key;
- Revokes all valid certificates issued by this authority;
- Notifies this and the reason immediately on its web Information Address, and also the list of revoked certificates is used for disclosing this information;

- For qualified certificates, notifies the supervisory body of the revocation of a certificate and the reason therefore.

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

5.7.4 Business continuity capabilities after a disaster

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

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

5.8 CA or RA termination

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

- Such termination must be notified in writing to all subscribers of valid certificates, the entities having a contract directly pertaining to the provision of the certification Services, and the supervisory body if qualified certificates are concerned;
- The termination of the CA's operations must published on the web page pursuant to 2.2;
- If the CA certificate's expiration is part of the termination of operations, this information plus the reason for expiration must be included in that notice;
- The termination of operations is a controlled process following a pre-defined plan, which includes the description of the procedure to preserve and disclose information for judicial or administrative proceedings discovery and for arranging the continuity of the Services;
- The certification authority must arrange no less than certificate revocation and CRL release as long as any certificate issued by the certification authority is valid;
- After that the CA must demonstrably destroy its private key, make a record of this destruction and keep this record in accordance with this CPS and the specific CP.

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

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

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

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

- ‘Termination of I.CA’s Services’.

6 TECHNICAL SECURITY CONTROLS

6.1 Key pair generation and installation

6.1.1 Key pair generation

The generation of key pair 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 evidenced in a written report is made in a cryptographic module assessed under FIPS PUB 140-, level 3.

All the requirements on the generation of CA key pair are described in internal documentation:

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

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

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

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

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

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

Public keys (the PKCS#10 format) are delivered as part of the certificate application.

6.1.4 CA public key delivery to relying parties

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

- Handover by hand 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 size of the key (and the algorithm's parameters) of a root certification authority using the RSA algorithm is 4096 bits. The size of the key (and the algorithm's parameters) of other certificates issued is always specified in the specific CP.

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 electronic signature legislation and the technical 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 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 field)

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

6.2 Private key protection and cryptographic module engineering controls

The specific procedures to protect certification authority private keys are described in internal documentation:

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

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 of the code required for these operations.

6.2.3 Private key escrow

Not applicable to this document; the private key storage 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 or 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 responder 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 smart card and pursuant to a strictly defined procedure described in internal documentation. 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 smart card and pursuant to a strictly defined procedure described in internal documentation:

- 'HSM/Private Server'.

The private key of the time server of the time stamping authority is activated through a procedure described in internal documentation:

- 'TSS Administration'.

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 smart 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 smart card and pursuant to a strictly defined procedure described in internal documentation.

The procedure is regulated in internal documentation:

- 'HSM/Private Server'.

Every actual deactivation is documented in a written record.

The private key of the time server of the time stamping authority is activated through a procedure described in internal documentation:

- 'TSS Administration'.

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:

- 'HSM/Private Server'.

The private key of the time server of the time stamping authority is destroyed through a procedure described in internal documentation:

- 'TSS Administration'.

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. Destruction is documented in a written record.

6.2.11 Cryptographic module rating

The cryptographic modules in which key pairs 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, their OCSP responders and their time servers are created during the generation of the corresponding key pair. The specific procedure is described in internal documentation:

- 'HSM/Private Server';
- 'TSS Administration'.

6.4.2 Activation data protection

The activation data of certification authorities, their OCSP responders and their times servers are protected by a method described in internal documentation:

- 'HSM/Private Server';
- 'TSS Administration'.

6.4.3 Other aspects of activation data

The activation data of the private keys of certification authorities, their OCSP responders and their time servers must not be transferred or kept in a clear form. All aspects are described in internal documentation:

- 'HSM/Private Server';
- 'TSS Administration'.

6.5 Computer security controls

6.5.1 Specific computer security technical requirements

The level of the security of the components used in the provision of the Services is defined, for qualified service certificates, in the effective trust services legislation and the technical standards referred to therein, otherwise the security level is defined in the relevant technical standards. The solution is described in detail in internal documentation, in particular in:

- 'System Security Policy of CA and TSA';
- 'Business Continuity Plan and Recovery Plan';
- 'Operating Site Component Recovery';
- 'Operating Site Relocation';
- 'Application Systems Data Backup';
- 'Gathering Data to Be Stored';
- 'Administration Guidance';
- 'I.CA Rooms Physical Access Control ';
- 'HSM/Private Server';
- 'TSS Administration'.

6.5.2 Computer security rating

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

- CEN/TS 419261 Security Requirements for Trustworthy Systems Managing Certificates and Time-stamps;
- ČSN ETSI EN 319 401 Electronic Signatures and Infrastructures (ESI) – General Policy Requirements for Trust Service Providers;
- ETSI EN 319 401 Electronic Signatures and Infrastructures (ESI); General Policy Requirements for Trust Service Providers;
- ČSN ETSI EN 319 403 Electronic Signatures and Infrastructures (ESI) – Trust Service Provider Conformity Assessment – Requirements for Conformity Assessment Bodies Assessing Trust Service Providers;
- ETSI EN 319 403 Electronic Signatures and Infrastructures (ESI); Trust Service Provider Conformity Assessment – Requirements for Conformity Assessment Bodies Assessing Trust Service Providers;

- ČSN ETSI EN 319 411-1 Electronic Signatures and Infrastructures (ESI) – Policy and Security Requirements for Trust Service Providers Issuing Certificates – Part 1: General Requirements;
- ETSI EN 319 411-1 Electronic Signatures and Infrastructures (ESI); Policy and Security Requirements for Trust Service Providers Issuing Certificates; Part 1: General Requirements;
- ČSN ETSI EN 319 411-2 Electronic Signatures and Infrastructures (ESI) – Policy and Security Requirements for Trust Service Providers Issuing Certificates – Part 2: Requirements for Trust Service Providers Issuing EU Qualified Certificates;
- ETSI EN 319 411-2 Electronic Signatures and Infrastructures (ESI); Policy and Security Requirements for Trust Service Providers Issuing Certificates; Part 2: Requirements for Trust Service Providers Issuing EU Qualified Certificates;
- ETSI TS 119 312 Electronic Signatures and Infrastructures (ESI); Cryptographic Suites;
- ČSN ISO/IEC 27006 Information Technology – Security Techniques – Requirements for Bodies Providing Audit and Certification of Information Security Management Systems.
- ISO/IEC 17021 Conformity Assessment -- Requirements for Bodies Providing Audit and Certification Of Management Systems;
- ISO/IEC 17065 Conformity Assessment -- Requirements for Bodies Certifying Products, Processes and Services.

The operations of certification authorities 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;
- RFC 6844 DNS Certification Authority Authorization (CAA) Resource Record;
- RFC 6962 Certificate Transparency;

- EBA draft document: Regulatory Technical Standards on Strong Customer Authentication and Common and Secure Communication under Article 98 of Directive 2015/2366 (PSD2);
- REGULATION (EU) 2018/389 of 27 November 2017 supplementing Directive (EU) 2015/2366 of the European Parliament and of the Council with regard to regulatory technical standards for strong customer authentication and common and secure open standards of communication.
- ETSI TS 119 495 Electronic Signatures and Infrastructures (ESI); Sector Specific Requirements; Qualified Certificate Profiles and TSP Policy Requirements under the payment services Directive (EU) 2015/2366.
- EN 301 549 Accessibility requirements for ICT products and services.
- ČSN ETSI EN 319 412-1 Electronic Signatures and Infrastructures (ESI); Certificate Profiles; Part 1: Overview and Common Data Structures;
- ETSI EN 319 412-1 Electronic Signatures and Infrastructures (ESI); Certificate Profiles; Part 1: Overview and Common Data Structures;
- ČSN ETSI EN 319 412-2 Electronic Signatures and Infrastructures (ESI); Certificate Profiles; Part 2: Certificate Profile for Certificates Issued to Natural Persons;
- ETSI EN 319 412-2 Electronic Signatures and Infrastructures (ESI); Certificate Profiles; Part 2: Certificate Profile for Certificates Issued to Natural Persons;
- ČSN ETSI EN 319 412-3 Electronic Signatures and Infrastructures (ESI); Certificate Profiles; Part 3: Certificate Profile for Certificates Issued to Legal Persons;
- ETSI EN 319 412-3 Electronic Signatures and Infrastructures (ESI); Certificate Profiles; Part 3: Certificate Profile for Certificates Issued to Legal Persons;
- ČSN ETSI EN 319 412-5 Electronic Signatures and Infrastructures (ESI); Certificate Profiles; Part 5: QCStatements;
- ETSI EN 319 412-5 Electronic Signatures and Infrastructures (ESI); Certificate Profiles; Part 5: QC Statements.

6.6 Life cycle technical controls

6.6.1 System development controls

System development is carried out in accordance with internal documentation:

- ‘Change Control’;
- ‘Development Methodology’.

6.6.2 Security management controls

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

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

- ČSN ISO/IEC 27000 Information Technology – Security Techniques – Information Security Management Systems – Overview and Vocabulary;

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

These topics are described in internal documentation:

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

6.6.3 Life cycle security controls

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

- Establishing – defining the scope and the boundaries for information security management, determining a security policy and plans, and choosing security controls depending on the risks identified, all this in accordance with the corporate security policy, as is described in internal documentation:
  - 'Corporate Security Policy';
  - 'Information Security Policy - Trustworthy Systems';
  - 'Approaches to Assess and Address Information Security Risks - Trustworthy Systems';
  - 'ISMS Scope - Trustworthy Systems';
  - 'Risk Analysis - Trustworthy Systems, Final Report';
  - 'Statement of Applicability - Trustworthy Systems';
  - 'Risk Handling/Management Plan- Trustworthy Systems';
  - 'Residual Risks – Summary for Management - Trustworthy Systems';
- Implementing and operating – effective and systematic enforcement of the selected security controls, as is described in internal documentation:
  - 'I.CA Rooms Physical Access Control ';
  - 'Fire Safety';
  - 'HSM/Private Server';
  - 'Information Security Management';
  - 'Application Systems Data Backup';
  - 'Administration Guidance';
  - 'Firewall – Operating Site';
  - 'Inspection Activity, Clean Criminal Record and Competence';
  - 'Change Control';
  - 'Security Incidents';
  - 'Operating Site Component Recovery';
  - 'Operating Site Relocation';
  - 'Firewall – Operating Site';
  - 'Electronic Mail Policy';

- □ ‘CCTV – Operating Site’;
- □ ‘Crisis Scenarios’;
- □ physical security projects of particular operating sites;
- □ in other documentation maintained at the operating site (see ‘Administration Guidance’);

- Monitoring and reviewing – providing feedback, regular monitoring and evaluation of the successful and the poor aspects of information security management, providing the knowledge gained for the company management for assessment, as is described in the documents:
  - □ Internal inspection reports;
  - □ External inspection reports and external audit reports;
- Maintenance and improvement – implementing corrective and improvement measures as decided by the company management.

6.7 Network security controls

The root certification authority’s information system runs off line, so it connects to no external network. The other trustworthy systems destined for supporting the 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. All communication between RA and the operating sites is encrypted. The detailed network security management solution is described in internal documentation:

- ‘System Security Policy of CA and TSA’;
- ‘Administration Guidance’;
- ‘Firewall – Operating Site’;
- ‘Business Continuity Plan and Recovery Plan’;
- ‘Operating Site Component Recovery’;
- ‘Operating Site Relocation’.

6.8 Time-stamping

See 5.5.5 for the time-stamping solution.

7 CERTIFICATE, CRL AND OCSP PROFILES

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

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

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

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

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

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

dNSName	IA5String (1..255) check: correct DNS name format	not permitted
description	UnboundDirectoryString (1..1024)	
DN Qualifier	PrintableString (1..64)	
DMDName	UnboundDirectoryString (1..64)	

7.1 Certificate profile

See chapter 7.

7.1.1 Version number(s)

See chapter 7.

7.1.2 Certificate extensions

See chapter 7.

7.1.3 Algorithm object identifiers

See chapter 7.

7.1.4 Name forms

See chapter 7.

7.1.5 Name constraints

See chapter 7.

7.1.6 Certificate policy object identifier

See chapter 7.

7.1.7 Usage of Policy Constrains extension

See chapter 7.

7.1.8 Policy qualifiers syntax and semantics

See chapter 7.

7.1.9 Processing semantics for the critical Certificate Policies extension

See chapter 7.

7.2 CRL profile

See chapter 7.

7.2.1 Version number(s)

See chapter 7.

7.2.2 CRL and CRL entry extensions

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

7.3 OCSP profile

Both the OCSP request profile and the OCSP response profile are in accordance with RFC 6960 and RFC 5019.

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

Table 5 – OCSP request profile

Request attributes	Notes
OCSPRequest ::= SEQUENCE {	
tbsRequest TBSRequest	
TBSRequest ::= SEQUENCE {	
version [0] EXPLICIT Version DEFAULT v1,	
requestorName [1] EXPLICIT GeneralName OPTIONAL	
requestList SEQUENCE OF Request,	The OCSP responder only responds to the first request in the list in the OCSP request and ignores any other request. (RFC5019)
Request ::= SEQUENCE {	
reqCert CertID,	mandatory attribute (unless the attribute is included, malformedRequest will be the response)
CertID ::= SEQUENCE {	
hashAlgorithm AlgorithmIdentifier,	OID of the hash algorithm for the following two attributes – the identification of the requested certificate's issuer specified by the client, OCSP responder imposes no limit (and processes requests with

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

Table 6 – OCSP response profile

Response attributes	**Notes**
OCSPResponse ::= SEQUENCE {	
responseStatus OCSPResponseStatus	
OCSPResponseStatus ::= ENUMERATED	*(0) successful* – successful response to OCSPrequest *(1) malformedRequest* – returned after OCSPrequest syntax error; *(2) internalError* – OCSP responder internal error *(3) tryLater* – not in use *(5) sigRequired* – never returned as request signature is not required *(6) unauthorized* – if OCSP responder does not recognise the issuer = foreign certificate

	(client is not authorized to make a query to this server – RFC2560, or the server is unable to make an authoritative response, for instance it may not have authoritative information about certificate revocation – RFC5019)
responseBytes [0] EXPLICIT ResponseBytes OPTIONAL }	only if OCSPResponseStatus=*successful*
ResponseBytes ::= SEQUENCE {	
responseType OBJECT IDENTIFIER	always *Basic OCSP Response*
response OCTET STRING	
BasicOCSPResponse ::= SEQUENCE {	
tbsResponseData ResponseData,	
ResponseData ::= SEQUENCE {	
version [0] EXPLICIT Version DEFAULT v1,	v1
responderID ResponderID,	
ResponderID ::= CHOICE { byName [1] Name, byKey [2] KeyHash }	returns byName=issuer's DN
producetAt GeneralizedTime,	time the responder signs the response
responses SEQUENCE OF SingleResponse,	returns only a single response to the first certificate in the request list
SingleResponse ::= SEQUENCE {	
certID CertID,	

CertID ::= SEQUENCE {
hashAlgorithm AlgorithmIdentifier,
issuerNameHash OCTET STRING,
issuerKeyHash OCTET STRING,
serialNumber CertificateSerialNumber
}
	identical to the content of the attribute *CertID* specified in the request

certStatus CertStatus,	certificate revocation status one of the options listed below
CertStatus ::= CHOICE {	
good [0] IMPLICIT NULL,	certificate has not been revoked (in the validity interval) or the time the OCSP response is created is outside the certificate validity interval
revoked [1] IMPLICIT RevokedInfo,	certificate has been revoked (in the validity interval)
RevokedInfo ::= SEQUENCE {	
revocationTime GeneralizedTime	certificate revocation time
revocationReason [0] EXPLICIT CRLReason OPTIONAL }	reason included in the response
CRLReason ::= ENUMERATED	may contain: *unspecified* (0), *keyCompromise* (1), *cACompromise* (2), *affiliationChanged* (3), *superseded* (4),

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

7.3.1 Version number(s)

See 7.3.

7.3.2 OCSP extensions

See tables in 7.3.

The OCSP response returning the ‘good’ certificate status may contain a positive statement as the CertHash attribute of singleExtentions.

8 COMPLIANCE AUDIT AND OTHER ASSESMENTS

Assessment information is provided in specific certification policies.

8.1 Frequency or circumstances of assessment

See chapter 8.

8.2 Identity/qualifications of assessor

See chapter 8.

8.3 Assessor's relationship to assessed entity

See chapter 8.

8.4 Topics covered by assessment

See chapter 8.

8.5 Actions taken as a result of deficiency

See chapter 8.

8.6 Communication of results

See chapter 8.

9 OTHER BUSINESS AND LEGAL MATTERS

9.1 Fees

9.1.1 Certificate issuance or renewal fees

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

The certificate renewal service is not provided.

9.1.2 Certificate access fees

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

9.1.3 Revocation or status information access fees

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

9.1.4 Fees for other services

Not applicable to this document.

9.1.5 Refund policy

Not applicable to this document.

9.2 Financial responsibility

9.2.1 Insurance coverage

První certifikační autorita, a.s. represents it holds 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 the Services given the risk of a liability-for-damage claim.

Please refer to 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 the 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. These requirements are regulated in detail in internal documentation:

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

9.4.2 Information treated as private

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

I.CA employees or the entities defined by effective 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 strictly as regulated in relevant legislation, that is, ZOOÚ.

9.5 Intellectual property rights

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

9.6 Representations and warranties

9.6.1 CA representations and warranties

I.CA warrants that:

- It will use the certification authorities' private keys solely for issuing certificates to end users (except 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;
- The qualified certificates, and the non-qualified certificates, issued to end users meet the statutory trust services requirements and the requirements of the relevant technical standards, and the requirements of the relevant technical standards, respectively;

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

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

- The subscriber does not breach any obligation out of the contract of Services, this CPS and the specific CP;
- The relying party does not breach any obligation out of this CPS and the specific CP.

The subscriber of a certificate issued under this CPS or a specific 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 subscribers and relying parties, that I.CA will observe this CPS and the specific CPs in issuing these certificates and administering the same throughout their periods of validity.

The warranties include:

- Checking the right to apply for a 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 storage place is maintained 24 hours a day and 7 days a week;
- Ensuring that a certificate may be revoked for reasons specified in the effective trust services legislation and this CPS or the specific CP.

9.6.2 RA representations and warranties

The designated RA:

- Assumes the obligation that the services the RA provides are correct;
- Does not accept the application unless the RA validates all the application items (except those not subject to validation) or the subscriber provides the required data or is authorized to submit the application;
- Is responsible for passing a hand-delivered certificate revocation application to a CA office in due time for the CA 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 subscriber always provides that the subscriber is obligated to abide by the CP under which is the certificate is issued.

9.6.4 Relying parties representations and warranties

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

9.6.5 Representations and warranties of other participants

Not applicable to this document.

9.7 Disclaimers of warranties

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

9.8 Limitations of liability

První certifikační autorita, a.s. 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 effective trust services legislation and this CPS or the specific 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 effective legislation regulating provider–consumer relations and the warranties agreed between První certifikační autorita, a.s. and the applicant for the Services. The contract must not be in conflict with the effective legislation and must always take an electronic or printed form.

První certifikační autorita, a.s.:

- Undertakes to discharge all the duties defined in effective legislation (including the trust services legislation in the case of qualified certificates) and those in the relevant policies;
- Gives the aforesaid warranties throughout the term of the contract of 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 damages 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 subscriber's incorrect or unauthorized use of the services rendered under the contract of Services, particularly for any use contrary to the terms and conditions specified in this CPS and/or the specific CP, and for any defect due to force majeure, including a temporary telecommunication connection failure;
- Any damage resulting from using the certificate after submitting the request for 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:

- E-mail 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 (the subscriber or the relying party) must provide:

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

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

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

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

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

9.10 Term and termination

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

9.10.1 Term

Certification policies – see 9.10.

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

9.10.2 Termination

Certification policies – see 9.10.

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

9.10.3 Effect of termination and survival

Certification policies – see 9.10.

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

9.11 Individual notices and communications with participants

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

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

Communication with I.CA may also be effected through the channels specified on the web Information Address.

9.12 Amendments

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

9.12.1 Procedure for amendment

Certification policies – see 9.12.

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

9.12.2 Notification mechanism and period

Certification policies – see 9.12.

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

9.12.3 Circumstances under which OID must be changed

Certification policies – refer to 9.12.

No OID assigned to this CPS.

9.13 Disputes resolution provisions

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

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

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

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

9.14 Governing law

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

9.15 Compliance with applicable law

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

9.16 Miscellaneous provisions

Any miscellaneous provision is always described in the specific certification policy.

9.16.1 Entire agreement

See 9.16.

9.16.2 Assignment

See 9.16.

9.16.3 Severability

See 9.16.

9.16.4 Enforcement (attorneys' fees and waiver of rights)

See 9.16.

9.16.5 Force majeure

See 9.16.

9.17 Other provisions

Not applicable to this document.

10 FINAL PROVISIONS

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