První certifikační autorita, a.s.
(accredited provider of certification services)

CERTIFICATION POLICY

FOR THE ISSUANCE OF QUALIFIED SYSTEM CERTIFICATES

Classification: public document

Version 3.1

Table 1 - Document History

Version	Date of Release	Approved by	Comments
3.0	Oct 23, 2009	CEO of První certifikační autorita, a.s.	The issuance of certificates with parameters meeting the requirements of the applicable legislation concerning the matters of hash functions (use of SHA-2 family algorithms) and the minimum length of an encryption key for the RSA algorithm (2048 bits).
3.1	Apr 1, 2011	CEO of První certifikační autorita, a.s.	In the event of the first (initial) certificate acceptance of an electronic mail address only in the field SubjectAlternativeName.rfc822Name. More accurate description of supported fields key usage, extended key usage, entry check.

Contents

1 Introduction

This document has been prepared to meet the requirements of the applicable legislation concerning the matters of use of encryption algorithms in the process of creation of electronic signatures. In accordance with the recommendations of technical specification ETSI[1] TS 102 176-1, První certifikační autorita, a.s., issues qualified certificates with the use of the hash functions SHA-256 and SHA-512 in combination with the RSA algorithm of the key length of 2048 bits.

1.1 Overview

První certifikační autorita, a.s., (hereinafter also referred to as "I.CA") became:

- on March 18, 2002 – the first accredited provider of certification services in the Czech Republic for the field of issuance of qualified certificates under Act No. 227/2000 Coll. on electronic signatures and on the amendment to certain other acts (Electronic Signatures Act),
- on February 1, 2006 – an accredited provider of certification services in the Czech Republic for the field of issuance of qualified system certificates under Act No. 227/2000 Coll. on electronic signatures and on the amendment to certain other acts (Electronic Signatures Act),
- on February 1, 2006 – the first accredited provider of certification services in the Czech Republic for the field of issuance of qualified timestamps under Act 227/2000 Coll. on electronic signatures and on the amendment to certain other acts (Electronic Signatures Act),
- on September 21, 2006 – the first foreign qualified provider of certification services in the Slovak Republic, who has been given an accreditation for issuing of qualified certificates and timestamps under the current version of Act No. 215/2002 Coll. (the Slovak Republic) on electronic signature and related implementing regulations.

The document **Certification Policy for the Issuance of Qualified System Certificates** (hereinafter also referred to as the "CP"), prepared by První certifikační autorita, a.s., deals with the issues relating to the processes of the life cycle of qualified system certificates and is in accordance with:

- Directive 1999/93/EC of the European Parliament and of the Council of 13 December 1999 on a Community framework for electronic signatures,
- the current version of Act No. 227/2000 Coll. on electronic signatures and related rules and regulations,

and strictly follows the structure defined by Regulation No. 378/2006 Coll., which is based on the synopsis of the standard RFC 3647 – Internet X.509 Public Key Infrastructure Certificate Policy and Certification Practices Framework, with regard to the recommendations of the EU authorities and to the law order of the Czech Republic and the Slovak Republic in the field in question (individual chapters of this document are therefore maintained even where they are irrelevant thereto). The document is divided into nine chapters, a brief description of which is provided below:

- Chapter 1 identifies this document with the assigned unique identifier (OID of this certification policy), generally describes the entities and individuals taking part in the provision of this certification service, and defines the appropriate use of the issued qualified system certificates.
- Chapter 2 deals with the issues of responsibility for the publication and repositories of information or documents.
- Chapter 3 describes the processes of identification and authentication of an applicant for the issuance of a qualified system certificate or for the revocation of a qualified certificate, including the definition of the types and contents of names used in applications or in issued qualified system certificates.

[1] European Telecommunications Standards Institute

- Chapter 4 defines the processes of the life cycle of a qualified system certificate, i.e. application for the issuance of a qualified system certificate, revocation of a qualified system certificate, services related to the verification of the status of a qualified system certificate, termination of the provision of certification services, etc.
- Chapter 5 contains the issues of physical, procedural and personal security, including the definition and storage of the set of recorded events, and the issues of the handling of emergency and compromising situations.
- Chapter 6 focuses on the technical security, it means generating public and private keys, protection of private keys, including the computer and network protection.
- Chapter 7 defines the profile of issued qualified system certificates and qualified system certificate revocation lists.
- Chapter 8 focuses on the issues of assessment of the provided certification services.
- Chapter 9 deals with commercial and legal issues.

Since První certifikační autorita, a.s., issues several types of certificates under different policies, potential users of the certificates issued under this Certification Policy should familiarize themselves with this document and make sure that it corresponds to their requirements for the use of a qualified system certificate.

Among other things, this document may be used by independent institutions (such as audit firms) as a basis for the confirmation of the fact that it is possible to regard the certification services provided by První certifikační autorita, a.s., as trustworthy.

In the process of provision of certification services, První certifikační autorita, a.s., operates a single-level certification authority (root certification authority), which issued a “self-signed” I.CA signing certificate, the administration of which is controlled in První certifikační autorita, a.s., by special documents.

1.2 Document Name and Identification

Title of this document :		Certification Policy for the Issuance of Qualified System Certificates
OID	:	1.3.6.1.4.1.23624.1.1.40.3.1

1.3 PKI Participants

1.3.1 Certification Authorities (hereinafter referred to as “CA”)

První certifikační autorita, a.s., does not establish or support any subordinate certification authorities providing certification services.

1.3.2 Registration Authorities (hereinafter referred to as “RA”)

The provision of the services of První certifikační autorita, a.s., is carried out by registration authorities, which are either public (they provide services to the public) or client (they provide services to their customers). These registration authorities:

- accept applications for the services specified in this CP, in particular applications for certificates, arrange the handover of certificates and certificate revocation lists, provide required information, handle complaints, etc.,
- are entitled, for urgent operational or technical reasons, to suspend, in whole or in part, the performance of their activities – they must report any such measure immediately to the CEO of I.CA, who will either confirm, cancel or modify it,
- are authorized to enter into subscriber agreements on the provision of certification services on behalf of I.CA,

- are authorized to charge for the I.CA services, unless something different agreed in a subscriber agreement,
- contractual RA, under a written contract entered into between I.CA and the operator of the RA., are acting on behalf of I.CA in the same way as the RA owned by I.CA.

The registration authorities described above can be either stationary or mobile.

1.3.3 Subscribers

A subscriber is an individual, legal entity or a government authority, who/which applied for the issuance of a certificate for himself/herself/itself or for the signatory, and to whom/which a certificate was issued.

A marking person is an individual, legal entity or government authority that is the holder of a means for the creation of electronic marks and marks a data message with an electronic mark. An electronic mark may be created by a device representing the above persons (for example automatic replies of an e-registry to received e-mails).

1.3.4 Relying Parties

A relying party is a party that relies, in its activities, on a certificate issued by První certifikační autorita, a.s., and/or on an electronic marks verified by such a certificate.

1.3.5 Other Participants

Other participating parties are supervisory authorities defined by ESA, authorities engaged in criminal proceedings and other parties defined by law.

1.4 Certificate Usage

1.4.1 Appropriate Certificate Uses

Qualified system certificates issued under this Certification Policy by První certifikační autorita, a.s., may be used only in the processes of electronic mark verification in accordance with the applicable legislation (ESA, ESR).

1.4.2 Prohibited Certificate Uses

Qualified system certificates issued under this Certification Policy by První certifikační autorita, a.s., must not be used contrary to the purpose defined in this Certification Policy and in the applicable legislation (ESA, ESR and other enactments).

1.5 Policy Administration

1.5.1 Organization Administering the Document

This Certification Policy and the relevant Certification Practice Statement are administered by První certifikační autorita, a.s.

1.5.2 Contact Person

The Chief Executive Officer of První certifikační autorita, a.s., shall specify the person, whose contact data are available at the Internet address (see Chapter 2.2).

1.5.3 Person Responsible for Decisions on Compliance of the Provider's Procedures with the Procedures of Other Providers of Certification Services

The only person that is responsible for decisions on compliance of the procedures of První certifikační autorita, a.s., with the procedures of other providers of certification services is the Chief Executive Officer of První certifikační autorita, a.s.

1.5.4 Procedure for the Approval of Compliance under Section 1.5.3

If it is necessary to amend this Policy and or to create a new version thereof, the Chief Executive Officer of První certifikační autorita, a.s., shall appoint a person authorized to perform such changes. Any new version of the CP (specified in Chapter 10) must be, prior to its effective date, approved by the Chief Executive Officer of První certifikační autorita, a.s.

1.6 Definitions and Acronyms

The glossary of definitions and acronyms applies to this document. In the event of a definition, the right column may specify the source where the original definition appears. The acronyms are of an alternative nature, i.e. both the full text and its acronym may be used in the text, and both of them shall be deemed to convey the same information.

Table 2 – Definitions and Acronyms

Term	Explanation
bit	from English binary digit – a digit of the binary system is the fundamental and simultaneously the smallest unit of information used especially in digital and information technologies
CRL (Certification Revocation List)	a list identifying revoked certificates which is signed by a CA or CRL issuer and made freely available in a public repository
subscriber, certificate holder	an individual, legal entity or a government authority, who/which applied for the issuance of a certificate for himself/herself/itself or for the marking person, and to whom/which a certificate was issued
electronic signature or electronic mark	an electronic signature is data in an electronic form attached or logically associated with a data message and which serve as a method of unequivocal authentication of a signatory in relation to a data message electronic mark is data in electronic form which are attached to or logically associated with a data message and meet the following requirements: 1. they are unequivocally linked to the marking person and are capable of identifying that person by means of a qualified system certificate 2. they have been created and attached to a data message using an electronic mark creation device that the marking person can maintain under its sole control 3. they are linked to the data message to which they relate in such a manner that any subsequent change of the data is detectable
hash (fingerprint, …)	a transformation which receives, as an input, a string of characters of any length, and the result is a string of characters of fixed length
I.CA	První certifikační autorita, a.s.
qualified certificate, qualified system certificate	a certificate that meets the requirements defined by the applicable legislation
subsequent certificate	a certificate issued to an applicant that filed a new application for a qualified system certificate (PKCS#10 structure) during the term of the qualified system certificate with respect to which the subsequent qualified system certificate is issued, under a subscriber agreement on the provision of certification services entered into between the applicant and I.CA
marking person	an individual, legal person or government body that holds an electronic mark creation device and marks a data message by an electronic mark
key pair	unique data for the creation of an electronic signature or an electronic mark along with the corresponding data for the verification of an electronic signature or an electronic mark
signatory, subject	an individual who holds a signature creation device and acts either on his own behalf or on behalf of another natural or legal person

RA	registration authority
contractual partner	a provider of certification services that provides certification services or any part thereof on I.CA's behalf under a written contract – in most cases, it is a contractual RA
private key	unique data for the creation of an electronic signature or electronic mark
relying party	an individual or legal entity relying, in its activities, on a certificate issued by I.CA
public key	unique data for the verification of an electronic signature or an electronic mark
ESR	Regulation No. 378/2006 Coll. on procedures of qualified providers of certification services, on requirements for electronic signature tools, and on requirements for the protection of data used to create electronic marks (Regulation on Procedures of Qualified Certification Service Providers)
blocked	the state in which a certificate is after having been revoked by I.CA until I.CA publishes the CRL in which the certificate is listed for the first time
ESA	the current version of Act No. 227/2000 Coll. on electronic signatures and on the amendment to certain other acts (Electronic Signatures Act)

2 Publication and Repository Responsibilities

2.1 Repositories

With regard to the requirements of ESA, První certifikační autorita, a.s., establishes and operates repositories of information and documents, for which it is also responsible as a provider of certification services.

2.2 Publication of Certification Information

The primary addresses (hereinafter also referred to as "information addresses"), at which it is possible to find public information on První certifikační autorita, a.s., (certification policies, PKI disclosure statements, other information specified in ESA and ESR, other public and up-to-date information and documents, etc.) or links to other sources of information, are as follows:

a) the registered address of the company:

První certifikační autorita, a.s.
Podvinný mlýn 2178/6
190 00 Prague 9
Czech Republic

b) the website http://www.ica.cz,

c) the registered addresses of registration authorities.

The addresses, which are used for the contact between the general public and I.CA, are as follows:

a) the registered address of the registration authority which arranged the contractual relationship with I.CA,

b) the electronic mail address info@ica.cz.

I.CA publishes the above contact addresses at its website and in the offices of RAs. Employees of I.CA and its contractual partners are also obligated to provide such information upon request.

At the above website, it is possible to find information on:

- public certificates – the following information is published directly (other information can be seen on the certificate):
  - certificate number,
  - content of the field Common Name,
  - information on the beginning of the term of the certificate (including hours, minutes and seconds),
  - links to the locations where the certificate is available in the defined formats (DER, PEM, TXT),
- certificate revocation lists (CRL) – the following information is published directly (other information can be seen in the CRL):
  - date of issuance of the CRL,
  - CRL number,
  - links to the locations where the CRL is available in the designated formats (DER, PEM, TXT).

The supported protocols for the access to the public information are HTTP, HTTPS and FTP. No other protocols are allowed. I.CA may terminate or suspend the access via any of the above protocols without giving reasons – in doing so, I.CA must abide by the relevant provisions of ESA and ESR. I.CA shall

publish any such changes at its information addresses. Detailed information on the features and relevant specifications of the above protocols are published by I.CA at the same addresses.

In the event of termination of accreditation or in the event of a reasonable concern regarding the misuse of the data used for the creation of electronic marks of the issued certificates or of certificate revocation lists, I.CA shall announce this at its on-line information address and through the nationally distributed daily newspaper Hospodářské noviny or Mladá fronta Dnes.

2.3 Time or Frequency of Publication

I.CA shall publish information with the following frequency:

- certification policy – prior to the issuance of a first certificate under the relevant policy,
- list of issued certificates – updated upon each issuance of a new certificate intended for publication,
- certificate revocation lists (CRLs) – no later than 24 hours after the issuance of the previous CRL (usually every 8 hours),
- information required by ESA and ESR (in particular the granting or termination of accreditation, revocation of an I.CA signing certificate along with the reasons for revocation) – immediately,
- other public information – not specified in advance, but in general, such information must reflect the current state of the provided certification services.

2.4 Access Controls on Repositories

All public information (see Chapters 2.2 and 2.3) shall be made available by I.CA without any restrictions.

Non-public information is available only to authorized employees of I.CA, contractual partners or the parties specified by the applicable legislation. The access to such information is governed by the rules defined in internal regulations.

3 Identification and Authentication

3.1 Naming

3.1.1 Types of Names

The subchapters below define the requirements for the content of the fields of applications for a certificate, which will be included in the issued certificate after the necessary inspections (see Chapter 7.1).

3.1.1.1 countryName

This mandatory field (ex.: CZ) must contain the code of the country in which the applicant for a certificate has:

- in the event of a non-business individual – the address of a permanent residence, as indicated in a primary[2] personal identification document,
- in the event of a business individual, legal entity, government authority, employee, etc. – a registered address, as indicated in a copy of the entry in the Commercial Register, in the trade license, in the deed of incorporation, etc.),

In the process of inspection of an application for a first (initial) certificate, an RA employee shall check the correctness of all data against the above documents (if the code of the country of permanent residence is not explicitly indicated, the code of the country which issued the document will be entered), and if any discrepancy is discovered, the application shall be rejected. The country code must be in accordance with the ISO 3166 standard. The process of inspection of an application for a subsequent certificate is governed by Chapter 4, specifically by its relevant subchapters.

This field must appear in an application for a certificate and in the certificate issued with respect thereto exactly once.

3.1.1.2 commonName

This mandatory field may contain:

- the name of the system (example: Electronic Mail Inbox) or the domain name of the server (example www.firma.cz – in the event of the domain name of the server, credibly proven consent of the owner or an affirmation of the applicant for a certificate confirming the ownership of the domain name is required,
- the business name of a business individual, legal entity, government authority, etc. (example: Company, a.s.) – as indicated in a copy of the entry in the Commercial Register, in the deed of incorporation, etc.,
- full name of the applicant for a certificate including academic degrees, as indicated in his/her primary personal identification document (example: Ing. Jan Holoubek Ph.D.) or in other submitted documents. If an application mentions an academic degree that is not indicated in the submitted personal identification document or that is not the same as that indicated in the submitted personal identification document, the applicant for a certificate must prove the legitimacy of the use of the particular academic degree beyond a reasonable doubt[3].

In the process of inspection of an application for a first (initial) certificate, an RA employee shall check the correctness of all data against the above documents and if any discrepancy is discovered, the application shall be rejected. The process of inspection of an application for a subsequent certificate is governed by Chapter 4, specifically by its relevant subchapters. This field, which may contain characters with diacritics, must appear in an application for a first (initial)/subsequent certificate and in the certificate issued with respect thereto exactly once.

[2] Accepted primary or secondary documents are specified in the relevant subchapters of Chapter 3.2.
[3] For example by a diploma stating that the applicant has the right to use the academic degree.

3.1.1.3 stateorProvinceName

This optional field may contain only a designation of the local territorial community within which:

- a non-business individual has a permanent residence, as indicated in the primary identification document of the applicant for a certificate, i.e. the city, town or another community that is indicated in the primary identification document (example: Prague),
- a business individual, legal entity, government authority, employee, etc. has a registered address, as indicated in a copy of the entry in the Commercial Register, in the trade license, in the deed of incorporation, etc., i.e. the city, town or another community that is indicated in the document.

I.CA reserves the right to fill in or use this field in a different way, as agreed in a written subscriber agreement entered into with the applicant for a certificate.

In the process of inspection of an application for a first (initial) certificate, an RA employee shall check the correctness of this information, if provided, and if any discrepancy is discovered, the application shall be rejected. The process of inspection of an application for a subsequent certificate is governed by Chapter 4, specifically by its relevant subchapters.

This field, which may contain characters with diacritics, must not appear more than once in an application for a certificate and in the certificate issued with respect thereto.

3.1.1.4 localityName

This optional field may contain:

- for non-business individuals – the place of their permanent residence, as indicated in the primary personal identification document (example: Ovenecká 1047/17, 170 00 Prague 7) of the applicant for a certificate,
- for business individuals, legal entities, government authorities, employees, etc. – the place of their registered address, as indicated in a copy of the entry in the Commercial Register, in the trade license, in the deed of incorporation, etc.

I.CA reserves the right to fill in or use this field in a different way, as agreed in a written subscriber agreement entered into with the applicant for a certificate.

In the process of inspection of an application for a first (initial) certificate, an RA employee shall check the correctness of this information, if provided, and if any discrepancy is discovered, the application shall be rejected. The process of inspection of an application for a subsequent certificate is governed by Chapter 4, specifically by its relevant subchapters.

This field, which may contain characters with diacritics, must not appear more than once in an application for a certificate and in the certificate issued with respect thereto.

3.1.1.5 organizationName

This field (it is mandatory/optional depending on the type of certificate) may only contain the business name (example: Company, a.s.), as indicated in a copy of the entry in the Commercial Register or in another register specified by law, in the trade license, in the deed of incorporation, etc. – the applicant for a certificate must prove the legitimacy of the use of the content of the field beyond a reasonable doubt[4].

I.CA reserves the right to fill in this field in a different way (for example in order to meet the requirements of technical standards), as agreed in a written subscriber agreement entered into with the applicant for a certificate.

In the process of inspection of an application for a first (initial) certificate, an RA employee shall check the correctness of this information, if provided, and if any discrepancy is discovered, the application

[4] For example in the case of the business name of a sole proprietorship, by the relevant trade license, and in the case that person authorized to sign documents on behalf of the undertaking is the owner, member or employee thereof, by a copy of the entry in the Commercial Register.

shall be rejected. The process of inspection of an application for a subsequent certificate is governed by Chapter 4, specifically by its relevant subchapters.

This field, which may contain characters with diacritics, must not appear more than once in an application for a certificate and in the certificate issued with respect thereto.

3.1.1.6 organizationUnitName

This optional field may contain the name or identifier of an organizational unit.

In the process of inspection of an application for a first (initial) certificate, an RA employee shall check the correctness of this information, if provided and proven by a certificate of employment, and if any discrepancy is discovered, the application shall be rejected. The process of inspection of an application for a subsequent certificate is governed by Chapter 4, specifically by its relevant subchapters.

I.CA reserves the right to fill in and use this field in a different way, as agreed in a written subscriber agreement entered into with the applicant for a certificate.

This field, which may contain characters with diacritics, may appear multiple times in an application for a certificate and in the certificate issued with respect thereto.

3.1.1.7 email Address

This field must not appear in an application for a first (initial) certificate, and the process of inspection of an application for a subsequent certificate, as well as the certificate issued with respect thereto, is governed by Chapter 3.1.1.13 and Chapter 4, specifically by its relevant subchapters.

3.1.1.8 initials

This optional field may only contain the initials of the full name of the applicant for a certificate (example: PJH).

In the process of inspection of an application for a first (initial) certificate, an RA employee shall check the correctness of this information, if provided, and if any discrepancy is discovered compared to the primary document, the application shall be rejected. The process of inspection of an application for a subsequent certificate is governed by Chapter 4, specifically by its relevant subchapters.

This field, which may contain characters with diacritics, must not appear more than once in an application for a certificate and in the certificate issued with respect thereto.

3.1.1.9 name

This optional field (example: Ing. Petr Jan Holoubek, Ph.D.) may contain the full name of the applicant for a certificate including academic degrees, as indicated in his/her primary personal identification document or in other submitted documents. In the process of inspection of an application for a first (initial) certificate, an RA employee shall check the correctness of the data against the above documents, and if any discrepancy is discovered, the application shall be rejected. If an application mentions an academic degree that is not indicated in the submitted primary personal identification document or that is not the same as that indicated in the submitted primary personal identification document, the applicant for a certificate must prove the legitimacy of the use of the particular academic degree beyond a reasonable doubt. The process of inspection of an application for a subsequent certificate is governed by Chapter 4, specifically by its relevant subchapters. This field, which may contain characters with diacritics, must not appear in an application for a first (initial)/subsequent certificate and in the certificate issued with respect thereto more than once.

3.1.1.10 title

This optional field may contain, for example, the position of the applicant for a certificate in a specific (usually corporate) hierarchy, an identifier, or, in the event of communication between public authorities, the identification of relevant legal regulations. I.CA reserves the right to fill in and use this field in a different way, as agreed in a written subscriber agreement entered into with the applicant for a certificate.

In the process of inspection of an application for a first (initial) certificate, the content of this field shall be checked by an RA employee according to the information contained in it[5]. The process of inspection of an application for a subsequent certificate is governed by Chapter 4, specifically by its relevant subchapters.

This field, which may contain characters with diacritics, may appear multiple times in an application for a certificate and in the certificate issued with respect thereto.

3.1.1.11 serialNumber

The unique number of the subject, used to distinguish different clients of I.CA. It is generally filled in by I.CA in the form of "ICA –" followed by the identification number of the applicant for a certificate transformed to a string. In the event of a certificate issued under this CP, the field must not appear in an application for a first (initial) certificate, and it may appear only once in an application for a subsequent certificate and in the certificate issued with respect thereto.

3.1.1.12 generationQualifier

This optional field is used to identify the position in a family tree (example: Jr., Sr.).

In the process of inspection of an application for a first (initial) certificate, an RA employee shall not check the correctness of this information, if provided. However, vulgarisms and words promoting fascism or racial and class hatred are not allowed. The process of inspection of an application for a subsequent certificate is governed by Chapter 4, specifically by its relevant subchapters.

I.CA reserves the right to fill in this field in a different way, as agreed in a written subscriber agreement entered into with the applicant for a certificate.

This field, which may contain characters with diacritics, must not appear more than once in an application for a certificate and in the certificate issued with respect thereto.

3.1.1.13 Subject Alternative Name

If the applicant for a certificate has used an alternative name of the subject, it is necessary to verify the information contained in it (if such information require verification). An alternative name may include:

- **otherName**: Microsoft Universal Principal Name (UPN) – this field must not appear in an application for a first (initial) certificate. In the case of an application for a subsequent certificate and the certificate issued with respect thereto, the provisions of Chapter 4, specifically of its relevant subchapters, shall apply,
- **rfc822Name** (electronic address, example: *holy@quick.cz*), optional field:
    - first (initial) certificate: it may only contain an electronic mail address of the applicant for a certificate in the RFC 822 format,
    - subsequent certificates:
        - if this field has not been filled in, then if the emailAddress (see Chapter 3.1.1.7) has been filled in, I.CA shall fill the rfc822Name field with the content of the emailAddress field,
        - if this field has been filled in and at the same time the emailAddress has been filled in, and the contents of these two fields are different, I.CA shall fill the second row of the rfc882Name field with the content of the emailAddress field.
- **dNSName** (name of the domain server, example: www.server.cz): optional field,
- **uniformResourceIdentifier** (URI, example: http://www.moje.cz): optional field,
- **iPAddress** (IP address, example: 81.91.85.214): optional field.

[5] If the applicant wants the field to contain the text "Physician", it is possible to accept the application if the applicant has provided proof that he/she is a physician; if the applicant wants the field to contain the text "Linux guru", this cannot be verified and the application shall be rejected.

In the process of inspection of an application for a first (initial) certificate, either credible proof of ownership of the electronic mail address, domain name of the server, URI or IP address, or an affirmation[6] of the applicant in which such ownership is confirmed are required – if this condition has not been satisfied, an RA employee shall have the right to reject the application. The process of inspection of an application for a subsequent certificate is governed by Chapter 4, specifically by its relevant subchapters.

The above individual fields may appear once or multiple times in an alternative name, or they may not appear at all. I.CA may restrict or extend the above set of fields without giving reasons.

3.1.2 Need for Names to Be Meaningful

The significance and content of individual fields in specified in the subchapters of Chapter 3.1.1.

3.1.3 Anonymity or Pseudonymity of Subscribers

There matters are irrelevant for the application of the release of this document.

3.1.4 Rules for Interpretation of Various Name Forms

As regards names or other information indicated in a personal identification document of an individual or in other documents that are acceptable for the verification of identity or a relation of an individual to a legal entity, such names shall be entered in the same form as indicated in the relevant document. No different transcriptions are carried out for the purposes of the issuance of certificates. In the event of an application for a first (initial) certificate, the UTF8String type is strictly required to encode the fundamental fields,, with the exception of the countryName and serialNumber fields (PrintableString type), the rfc822Name, dNSName and uniformResourceIdentifier fields (IA5String type) and the iPAddress field (OctetString). The length of the content of individual fields is governed by the applicable technical standards. In the event of an application for a subsequent certificate, I.CA shall accept the appearance and encoding of the fields used in the in previous certificate, or alternatively it may change the encoding to the type indicated in the paragraph above.

3.1.5 Uniqueness of Names

The uniqueness of the name of the subject is guaranteed by the application of the above procedure for the creation of the SerialNumber field (see Chapter 3.1.1.11). Where the content of the SerialNumber field is determined by I.CA, the uniqueness is guaranteed. Where the content of the Serial Number field is determined by the applicant and there is a conflict with a previously entered unique name of another qualified system certificate, I.CA shall notify the applicant and request a change in the required data. If the applicant fails to do such a change, the qualified system certificate shall not be issued.

3.1.6 Recognition, Authentication, and Role of Trademarks

I.CA shall recognize only trademarks the ownership or lease of which has been proven by the applicant. I.CA shall not authenticate trademarks in any other way. Any and all consequences resulting from unauthorized use of a trademark shall be borne by the applicant for a certificate.

3.2 Initial Identity Validation

3.2.1 Method to Prove Possession of Private Key

Ownership of the data for the creation of electronic marks, consistent with the data for the verification of electronic marks that are contained in the relevant application for a certificate (PKCS#10 structure) and that will be contained in the issued certificate, is to be proven by the submission of the application for certificate to the verifying person, which may be an employee of a registration or certification authority. Since the application has been electronically marked with the data for the creation of electronic marks (private key), consistent with the data for the verification electronic marks (public key) contained in the application, the applicant for a certificate will prove in this way that at the time of the creation of the electronic mark the applicant owned a private key consistent with the public key specified in the application.

[6] The affirmation made for these purposes shall be in the form of confirmation of the truthfulness of the information contained in the subscriber agreement.

3.2.2 Authentication of Organization Identity

I.CA requires an original or certified copy of an entry in the Commercial Register or in another register specified by law, of a trade license, of a deed of incorporation, or of another document of the same legal force, which must contain the full business name, identification number (if allocated), registered address, names of the person(s) authorized to act on behalf of the legal entity (authorized representatives), and the method in which such authorized representatives act and sign documents on behalf of the legal entity.

3.2.3 Authentication of Individual Identity

I.CA requires an applicant for a certificate to provide the following information:

- full name,
- date of birth (or Birth Identification Number for citizens of the Czech Republic and the Slovak Republic),
- submitted primary personal identification document number,
- address of the permanent residence (if indicated in the primary document).

In the event of any change in the above information or information included in the certificate, occurring during the contractual relationship with I.CA, the subscriber or the signatory shall notify such a change to I.CA. The requirements applicable to the enrollment of an applicant for a first (initial) certificate are defined in Chapters 3.2.3.1 to 3.2.3.3.

3.2.3.1 Non-Business Individual

3.2.3.1.1 Documents Submitted to RA

If an **applicant appears at an RA in person**, the applicant shall submit the following types of documents:

- The original of the applicant's valid primary personal identification document and the original or another (secondary) personal identification document. For citizens of the Czech Republic, the primary personal identification document shall be a national identity card, passport or similar document of the same legal force. For foreign nationals, the primary personal identification document shall be a passport or a similar document of the same legal force. Citizens of the Slovak Republic may use their national identity cards as the personal identification document. The secondary personal identification document must be issued by a public authority or another organization the existence of which can be proven. The secondary personal identification document must contain the full name of the applicant for a certificate and at least one of the following data:
    - date of birth of the applicant (or the Birth Identification Number in the event of citizens of the Czech Republic or the Slovak Republic),
    - address of the applicant's permanent residence,
    - photograph of the applicant's face.

  The data required to be included in the secondary personal identification document must be identical to the same data included in the primary personal identification document. The consistency shall be determined by an RA employee. If the applicant fails to submit two personal identification documents of the above quality, the application shall not be accepted. Examples of an acceptable secondary personal identification document are passport, driver's license, employee identity card issued by government authorities, identity card of a Member of Parliament, identity card of a policeman, firearms certificate, military service card, health insurance card, mass transportation card, company card, student card, etc.

If an **applicant is represented by an agent at an RA**, the agent shall submit the following types of documents:

- The original of the agent's primary personal identification document and the original of the agent's secondary personal identification document (the quality of the primary and secondary documents is specified above).
- The original or certified copy of a primary personal identification document of the applicant for a certificate and the original or certified copy of a secondary personal identification document of the applicant for a certificate (the quality of the primary and secondary documents is specified above).
- A power of attorney (unless the Chief Executive Officer of I.CA decides otherwise) with an authenticated signature of the principal – if the power of attorney is executed in a foreign language (other than Slovak), it must be translated into Czech by a certified translator (verification of a signature performed in a foreign country[7] must be "legalized", i.e. certified by the representation of the Czech Republic in the country of origin of the power of attorney; in the event of documents certified in the countries listed at http://hcch.net/, legalization is not required[8]).
- If the applicant is the statutory representative[9] of the client, an official document proving this is required:
    - Parents and adoptive parents represent their minor children – since minors have a limited legal capacity, subscriber agreement with I.CA must be entered into on their behalf by their statutory representatives. The required proof is the birth certificate of the minor. Adoption is to be proven either by a copy of the entry in the register of births or by a judicial decision. In all the above cases, indication of the child in the national identity card shall suffice.
    - A guardian is appointed for persons without full capacity to contract, including adults, by a court. The required proof is the judicial decision.
        - A guardian of a child may also be an authority of social protection of children (usually a municipality or a public guardian appointed by a municipality). In such a case, it is a legal entity and in addition to the judicial decision, documents proving the facts relating to legal entities must be submitted as well.
        - A guardian may also be appointed for handicapped individuals who do not have limited legal capacity, but require assistance in the contractual procedures (for example visually impaired persons).

3.2.3.1.2 Documents Checked and Verified at RA

If an **applicant appears at an RA in person**, an RA employee shall check and verify:

- Whether the person indicated in the application for a certificate is identical to the applicant (against a valid primary document) and whether the data contained in the application are consistent with the data indicated in the submitted documents. Consistency is required for the following data:
    - surname, first name,
    - address (city),
    - area (street, if indicated).
- Full age of the applicant.
- Validity of the submitted documents.

[7] Pursuant to the Slovak legislation, only a notary may perform the certification of documents to be used in a foreign country – Section 2 of Act of the NATIONAL COUNCIL OF THE SLOVAKL REPUBLIC of 22 December 1992.

[8] In such a case, it is necessary to proceed on an individual basis in cooperation with the applicant for a certificate or in cooperation of RA employee with I.CA.

[9] For the purposes of the ESA, a foster parent is not deemed to be a statutory representative of a child.

- If the applicant has submitted a passport to prove his/her identity, the consistency of the address shall not be checked.
- A foreign national must at least meet all the requirements for legal capacity imposed by Czech laws – if he/she fails to do so, it is necessary to check whether he/she meets the requirements imposed by the laws of the country of which he/she is a national. In such a case, it is necessary to proceed on an individual basis in cooperation with the applicant and I.CA.

If an applicant is represented by an agent at an RA, the following shall be checked as well:

- consistency of the applicant's data contained in the application for the service with the data indicated in a power of attorney (unless another contractual document has been made with respect to this) or in a document proving statutory representation,
- validity and correctness of the submitted documents of the agent against the data indicated in a power of attorney (unless another contractual document has been made with respect to this) or in a document proving statutory representation and the right to apply for the requested service.

3.2.3.2 Business Individual (Self-Employed) or Employee

3.2.3.2.1 Documents Submitted to RA

An applicant for a certificate shall submit the following types of documents:

- The documents specified in Chapter 3.2.3.1.1.
- The document specified in Chapter 3.2.2. If the document is executed in a foreign language, the rules defined in Chapter 3.2.3.1 shall apply to the verification.
- In the event of an employee – a certificate of employment with the particular employer, unless a general agreement has been entered into with I.CA. The certificate of employment must be signed by a person authorized to act on behalf of the employer. If that person is not the person authorized to act on behalf of the employer, i.e. is not an authorized representative (is not indicated in a copy of the entry in the Commercial Register or in another register specified by law, in the trade license, in the deed of incorporation, etc. as a person authorized to act), it is further required to submit a certified document (power of attorney, authorization, proof of statutory representation) signed by the authorized representative of the employer proving the right of the person to act on behalf of the employer.

3.2.3.2.2 Documents Checked and Verified at RA

An RA employee shall check and verify:

- whether the data contained in the application for a certificate are consistent with the data indicated in the documents submitted by the applicant or by the agent – the RA employee shall proceed in the same manner as in the case of a non-business individual,
- the certificate of employment with the particular employer,
- whether the person signing the certificate of employment, indicated in an certified document (power of attorney, authorization, proof of statutory representation), is authorized to act on behalf of the employer – the RA employee shall verify whether such a person has the right to sign such certificate of employment or whether the power of attorney is granted to an authorized person in accordance with the above documents[10] (in the event of an individual/legal entity, it is a copy of the entry in the Commercial Register or in another register specified by law, trade certificate, deed of incorporation, provision of law, etc., and in the event of a government /public authority, it is a special provision of law).

[10] If the copy of the entry in the Commercial Register states, for example, that "the person authorized to sign documents on behalf of the company is the Chairman of the Board of Directors acting jointly with another member of the Board of Directors", this means that a power of attorney may be granted only by the Chairman of the Board of Directors acting jointly with another member of the Board of Directors (the power of attorney must therefore bear authenticated signatures of these two persons).

3.2.3.3 Government Authority (such as Electronic Registry – Public Authority) and Other Legal Entities

Where the representative of a government authority or a legal entity as an applicant for a qualified system certificate is an employee thereof, the provisions of Chapter 3.2.3.1.2 shall apply.

Where a government authority or a legal entity has authorized a third party to represent it under a contractual relationship, the relevant requirements defined in the previous chapters shall apply.

3.2.4 Non-Verified Subscriber Information

In the event of information that cannot be verified, the relevant subchapters of Chapter 3.1.2 shall apply.

3.2.5 Validation of Authority

See Chapter 3.1.1.2, paragraph *the name of the system*.

3.2.6 Criteria for Interoperation

Any cooperation of První certifikační autorita, a.s., with other providers of certification services is always based on written contracts entered into with such providers.

3.3 Identification and Authentication for Re-Key Requests

3.3.1 Identification and Authentication for Routine Re-Key

The identification and authentication of an applicant for the issuance of a subsequent certificate (PKCS#10 structure) is carried out by verifying the electronic mark of the application for the issuance of a subsequent qualified system certificate. In the process of verification of the electronic mark of the application for a subsequent certificate either the valid qualified system certificate issued under the Certification Policy for the Issuance of Qualified System Certificates version 3.0 and higher, to which the subsequent certificate is issued, must be used, or it's necessary to use the valid qualified certificate intended for signing, which is optionally issued in the process of issuing qualified system certificate, issued under the Certification Policy for the Issuance of Qualified Certificates – version 3.0 and higher.

3.3.2 Identification and Authentication Requirements for Re-Key after Certificate Revocation

I.CA does not support the replacement of key pair of a previously revoked certificate. The only way is to obtain a first (initial) certificate.

3.4 Identification and Authentication for Revocation Requests

In the event of **handover of an application for certificate revocation in person at an RA**, the applicant for certificate revocation must prove to be the subscriber of the relevant certificate. If the applicant is represented by an agent, the provisions of Chapter 3.2.3.1 shall apply. The application for certificate revocation must be in writing and signed by the applicant.

In the event of **handover of an application for certificate revocation in an electronic way**, the following options are acceptable:

- an electronically marked or signed electronic message – (revoke@ica.cz), the electronic mark must be performed with the data for the creation of an electronic mark that are relevant for the particular certificate which is to be revoked or the electronic signature must be performed with the data for the creation of an electronic signature that are included in the issued qualified certificate intended for signing relevant to the qualified system certificate, which is to be revoked,
- an electronically unsigned electronic message containing the password for the certificate revocation – (revoke@ica.cz),
- via the form available at the on-line information address (http://www.ica.cz),

- via a data box.

In the event of the **use of an item of correspondence for the handover of an application for certificate revocation**, the item of correspondence must be mailed in the form of a registered letter to the company's registered address (see Chapter 2.2).

I.CA reserves the right to accept other forms of procedures for the identification and authentication in the processing of requests for certificate revocation as well. Such other forms, however, must not be contrary to the applicable legislation (ESA, ESR).

4 Certificate Life-Cycle Operational Requirements

4.1 Certificate Application

4.1.1 Who Can Submit a Certificate Application

The issuance of I.CA certificates is a commercial service offered to all parties that have contractually undertaken to act in accordance with this CP.

I.CA requires the minimum age of 18 years for the person applying for a certificate. Applicants for a certificate between 15 and 18 years of age must apply through their statutory representatives.

In the event that an applicant is represented by an agent, the agent must have been authorized by the applicant to represent.

4.1.2 Enrollment Process and Responsibilities

The enrollment process and the responsibilities of both the provider of the certification service and the applicant for the service are specified in the following chapters.

4.2 Certificate Application Processing

4.2.1 Identification and Authentication

The supported hash functions used in the creation of the electronic mark of an application for a certificate and the hash functions used in the process of issuing that certificate: SHA-256 application-> issued SHA-256 certificate, SHA-512 application -> issued SHA-512 certificate.

In the event that an application for a certificate uses a hash function other than the above, the certificate shall not be issued.

An applicant for a **first (initial) certificate** shall create an application for the issuance of a certificate (PKCS#10 structure) and after having stored it on a storage medium, the applicant or an agent of the applicant shall appear at an RA with the application and the required documents. The subsequent process of identification and authentication by an RA employee includes the following stages:

1. Verification of ownership of the data for the creation of electronic marks (see Chapter 3.2.1) – the RA employee shall check this via special application software in such a manner so as to use the data for the verification of electronic marks contained in the application for a certificate to verify the validity of the electronic mark of the application. If the verification of the validity of the electronic mark is negative, the RA shall not accept the application and it shall terminate the certificate issuance procedure.
2. Verification of the originals of personal identification documents submitted by the applicant for a certificate or by the applicant's agent (see Chapter 3.2.3.1). In the event of doubt concerning the authenticity of the primary personal identification document submitted by the applicant for a certificate or by the applicant's agent, the RA shall terminate the certificate issuance procedure. In the event of doubt concerning the authenticity of the secondary personal identification document submitted by the applicant for a certificate or by the applicant's agent, or in the event of inconsistency of the required data with the primary personal identification document, the applicant for a certificate or the applicant's agent shall be requested to submit another secondary personal identification document. If the applicant for a certificate or the applicant's agent fails to submit a secondary personal identification document of the required quality, an RA employee shall not accept the application and shall terminate the certificate issuance procedure.
3. Verification of other documents follows, depending on the type of the issued certificate – see the relevant subchapters of Chapter 3.2.

4. Verification of the data contained in the application for a certificate against the data indicated in the documents submitted by the applicant for a certificate. In the event of discrepancy, the RA employee shall reject the application and terminate the certificate issuance procedure.
5. Verification of the existence of a password for certificate revocation (this may be carried out both during the process of creation of an application for a certificate and by an RA employee during the process of formal inspections of an application for a certificate) and its quality (required specifications – the minimum/maximum length of the password is 4/32 characters, acceptable characters: 0..9, A..Z, a..z). The password shall be used by the subscriber for the revocation of the certificate, if any.

An applicant for a **subsequent certificate** shall create an application for the issuance of a certificate (in the PKCS#10 format) meeting the following requirements:

1. the fields of the Subject attribute (see Chapter 7.1) must be identical to those appearing in the certificate with respect to which the subsequent certificate is requested,
2. the data for the verification of electronic marks (public key) must be different from those contained in the original certificate,
3. the other fields of the application are governed by the up-to-date rules for the issuance of certificates under this CP,
4. as regards the quality of the password for certificate revocation, I.CA shall accept one of the following options: acceptable characters: 0..9, A..Z, a..z, minimum/maximum length of the password: 4 characters/32 characters, or the password for the revocation of the subsequent certificate may be identical to the password for the revocation of the original certificate,
5. ownership of the data for the creation of electronic marks (private key) is proven in the manner specified in Chapter 3.2.1,

and choose one of the following alternatives:

1. appearance of the applicant for a certificate or the applicant's agent in person at an RA – the procedure is the same as in the event of the issuance of a first (initial) certificate,
2. not necessary for the applicant for a certificate to appear in person at an RA – during the inspections in the process of issuance of a subsequent certificate in an electronic way, the RA will also use key pair which is subject to replacement or a "signature certificate" (see Chapter 3.3.1).

4.2.2 Approval or Rejection of Certificate Applications

In the event that the result of the inspections (see the relevant parts of Chapter 4.2.1) performed during the process of application for a **first (initial) certificate** is positive, an RA employee shall copy the submitted personal identification documents or the certified copies thereof (unless otherwise agreed in a subscriber agreement). The RA employee shall then request the applicant for a certificate or the applicant's agent to sign the "Report on the Filing of an Application for a Qualified System I.CA Certificate" containing the sentence **"The applicant hereby grants První certifikační autorita, a.s., his consent to store copies of the applicant's personal identification documents in accordance with the applicable legislation."**. If the applicant for a certificate or the applicant's agent refuses to sign the Report, the RA employee shall terminate the certificate issuance procedure and destroy (shred) the copies of the personal identification documents (unless otherwise agreed in a subscriber agreement.

In the event of the handling of an application for a **subsequent qualified certificate** in an electronic way, the provisions of Chapter 4.7.3 shall apply.

4.2.3 Time to Process Certificate Applications

I.CA has not defined any fixed time limit within which an application for a certificate is to be processed, since it is a sequence of activities, some of which depend only on the applicant for a certificate. The time information is specified in the following list:

- generation of an application for a certificate – within minutes,
- issuance of the certificate (within business days, unless otherwise agreed in a subscriber agreement):
    - first (initial) certificate (the applicant MUST appear in person at the RA) – the time limit for the issuance of the certificate is within 15 minutes and only in exceptional cases it may take longer,
    - subsequent certificate (the applicant DOES NOT HAVE TO appear in person at the RA) – within minutes (the prerequisite is the previous payment of the relevant fee).

4.3 Certificate Issuance

4.3.1 CA Actions during Certificate Issuance

During the process of issuance of a certificate, the operators of the operational office of a certification authority perform necessary inspections (in particular of the formal correctness of the data contained in the application and of the proper filling-in of the application fields) and other activities (communication with RA employees, etc.).

4.3.2 Notification to subscriber by the CA of issuance of certificate

During the process of issuance of a **first (initial) certificate**, the applicant for a certificate or the applicant's agent shall be notified by an RA employee, and if the application contains an electronic address, the issued certificate shall be mailed to that address.

In the event that the applicant for a **subsequent certificate** submitted the application in an electronic way and the applicant's electronic mail address is known, the subsequent certificate shall be sent to that address electronically.

4.4 Certificate Acceptance

4.4.1 Conduct Constituting Certificate Acceptance

If all the conditions for the issuance of a **first (initial) certificate** have been met, i.e.:

- the enrollment conditions have been met,
- the relevant fee has been paid (unless otherwise agreed in a subscriber agreement),
- ownership of the data for the creation of electronic marks corresponding to the data for the verification of electronic marks to be contained in the issued certificate has been proven,
- the relevant subscriber agreement has been signed,

the applicant for a certificate shall be obligated to accept the certificate. The only possibility for an applicant who does not want to accept the certificate is to request its revocation under this CP. An RA employee shall hand the applicant a storage medium containing the requested certificate and the corresponding CA certificate (in the required formats). If an electronic address has been indicated in the application, the issued certificate and the I.CA signing certificate (in the required formats) shall be sent to that address.

In the event of an application for the issuance of a **subsequent certificate** filed in an electronic way, I.CA shall send the issued certificate and the corresponding I.CA signing certificate to the applicant's electronic address, and if the application is handled at an RA, the applicant shall be handed the issued certificate or the corresponding I.CA signing certificate by an RA employee.

This CP shall be available to the applicant at an RA, or it may be downloaded from the information address.

I.CA may stipulate in an agreement with a contractual partner a procedure different from these provisions of the CP. However, this shall be without prejudice to the relevant provisions of the applicable legislation concerning the provision of certification services or business activities related thereto.

4.4.2 Publication of the Certificate by the CA

I.CA shall ensure that issued certificates are immediately published, with the exception of those for which the client has requested that they will not be published.

4.4.3 Notification of Certificate Issuance by the CA to Other Entities

In the event of issuance of a first (initial) certificate or a subsequent certificate during the applicant's/agent's appearance in person, a notification of the issued certificate shall be sent to an RA employee. In addition, the provisions of Chapter 4.4.2 shall apply, as well as the requirements of the applicable legislation under which I.CA was granted accreditation.

4.5 Key Pair and Certificate Usage

4.5.1 Subscriber Private Key and Certificate Usage

Subscribers and signatories shall in particular:

- provide I.CA, without undue delay, with accurate, true and complete information relating to the issued certificate,
- abide by all the relevant provisions of the subscriber agreement on the provision of certification services,
- familiarize themselves with the relevant provisions of the subscriber agreement on the provision of certification services concerning the issuance and use of the certificate, and abide by such provisions,
- treat the means and data for the creation of a advanced electronic signature or electronic mark with due diligence so as to prevent their unauthorized use,
- immediately notify the provider of certification services which has issued the certificate (i.e. I.CA) of any threat of misuse of their data for the creation of an electronic signature or electronic mark,
- use the data for the creation of electronic signatures or electronic marks relating to the issued certificate in accordance with the provisions of relevant certification policies,
- abide by all the relevant provisions of ESA, ESR and relevant certification policies during any activities relating to the data for the creation of a advanced electronic signature or electronic mark.

4.5.2 Relying Party Public Key and Certificate Usage

Relying parties shall in particular:

- perform all activities required to verify that an electronic mark is valid and that the relevant certificate has not been revoked,
- abide by all the provisions of this CP, under which the certificate has been issued,
- abide by all the relevant provisions of ESA, ESR and this CP during any activities relating to the use of the issued certificate.

4.6 Certificate Renewal

In the context of this document, the certificate renewal service shall be understood to mean the renewal of a previously revoked certificate and/or the issuance of a subsequent certificate with the same data for the verification of electronic marks and with a new term.

4.6.1 Circumstance for Certificate Renewal

The service of renewal of a previously revoked certificate is not provided.

4.6.2 Who May Request Renewal

The service of renewal of a previously revoked certificate is not provided.

4.6.3 Processing Certificate Renewal Requests

The service of renewal of a previously revoked certificate is not provided.

4.6.4 Notification of New Certificate Issuance to Subscriber

The service of renewal of a previously revoked certificate is not provided.

4.6.5 Conduct Constituting Acceptance of a Renewal Certificate

The service of renewal of a previously revoked certificate is not provided.

4.6.6 Publication of the Renewal Certificate by the CA

The service of renewal of a previously revoked certificate is not provided.

4.6.7 Notification of Certificate Issuance by the CA to Other Entities

The service of renewal of a previously revoked certificate is not provided.

4.7 Certificate Re-Key

In the event that a certificate contains an electronic address, information about expiration of this certificate, as well as instructions concerning the steps to be taken in the event of an application for subsequent certificate, shall be sent to that address.

4.7.1 Circumstances for Certificate Re-Key

The circumstances for the replacement of the data for the verification of electronic marks are defined in Chapter 3.3.1. I.CA reserves the right to accept other forms of procedures as well.

4.7.2 Who May Request Certification of a New Public Key

Replacement of the data for the verification of electronic marks may be requested by subscribers.

4.7.3 Processing Certificate Re-Keying Requests

If the verification of electronic marks is positive (see the relevant parts of Chapters 3.3.1 and 4.2.1) and the content of the fields of the application for replacement of the data for the verification of electronic marks in a certificate meets the requirements defined in Chapter 3.3.1, the provisions of Chapter 4.3 shall apply, otherwise the certificate issuance procedure shall be terminated.

4.7.4 Notification of New Certificate Issuance to Subscriber

See the relevant parts of Chapter 4.3.2.

4.7.5 Conduct Constituting Acceptance of a Re-Keyed Certificate

See the relevant parts of Chapter 4.4.1.

4.7.6 Publication of the Re-Keyed Certificate by the CA

See Chapter 4.4.2.

4.7.7 Notification of Certificate Issuance by the CA to Other Entities

See Chapter 4.4.3.

4.8 Certificate Modification

Service is not provided.

4.8.1 Circumstances for Certificate Modification

Service is not provided.

4.8.2 Who May Request Certificate Modification

Service is not provided.

4.8.3 Processing Certificate Modification Requests

Service is not provided.

4.8.4 Notification of New Certificate Issuance to Subscriber

Service is not provided.

4.8.5 Conduct Constituting Acceptance of Modified Certificate

Service is not provided.

4.8.6 Publication of the Modified Certificate by the CA

Service is not provided.

4.8.7 Notification of Certificate Issuance by the CA to Other Entities

Service is not provided.

4.9 Certificate Revocation and Suspension

Applications for the revocation of a certificate are continuously received by I.CA in an electronic way and by regular mail. Handover in person at an RA is possible only during the business hours of the respective RA. The procedures specified in this chapter are described in detail in the internal documentation. Revocation of a certificate shall be also carried out by I.CA if requested by the parties entitled to do so by law.

I.CA does not provide the service of certificate suspension.

4.9.1 Circumstances for Revocation

A certificate may be revoked under the following circumstances:

- the data for the creation of electronic marks have been compromised or there is a reasonable suspicion that the data have been compromised,
- violation of the provisions of the subscriber agreement on the provision of certification services by the subscriber or by the signatory/marking person,
- by request of the subscriber or of the signatory/marking person,
- if the situation defined in ESA and ESR (for example invalidity of the data in the certificate) occurs.

I.CA reserves the right to accept other conditions for certificate revocation as well. Such conditions, however, must not be contrary to ESA or ESR.

4.9.2 Who Can Request Revocation

A request for the revocation of a certificate may be filed by:

- the signatory/marking person, the subscriber or the person who was explicitly authorized to do so in the subscriber agreement on the provision of certification services (for example in the event of issuing certificates for employees),
- person entitled by inheritance proceedings,

- the provider of certification services – the person authorized to apply for the revocation of a certificate issued by I.CA is the Chief Executive Officer of I.CA,
- other parties defined in ESA or ESR.

4.9.3 Procedure for Revocation Request

In the event of **submission of an application for certificate revocation in person at an RA**, the application must contain the serial number of the certificate, either in a decimal or hexadecimal format (beginning with "0x"), the full name of the individual to whom the certificate was issued, and the revocation password. If that person does not remember the revocation password, this must be explicitly stated in the written application, as well as the number of the primary personal identification document submitted when applying for the issuance of the certificate. This primary personal identification document must then be shown to an RA employee. The RA employee shall forward the application (via remote access) to the operational office of a certification authority. The responsible employee of the CA shall decide whether the application is justified or not, and communicate the decision through the RA employee. In the event that the application is justified, the moment of receipt of the application at the operational office of the certification authority shall be deemed to be the date and time of revocation of the relevant certificate. In the event that the application cannot be accepted (incorrect revocation password, unprovable identity of the individual), the RA employee shall, in cooperation with the individual, attempt to take any available corrective measure, and if this is not possible for any reason, the application for certificate revocation shall be rejected. The provisions of the subchapters of Chapter 3.2.3 shall apply to an agent.

In the case of **submission of an application for certificate revocation in an electronic way**, the following alternatives are acceptable:

- Electronically marked/signed (by relevant private key) electronic message – the body of the message must be in the following form (in Czech or Slovak, with or without diacritics):

  Zadam o zneplatneni certifikatu cislo = xxxxxxx

  or

  Žádám o zneplatnění certifikátu číslo = xxxxxxx

  where "xxxxxxx" is the serial number of the certificate, which must be in a decimal or hexadecimal format (beginning with "0x").

- Electronically unmarked/unsigned electronic message – the body of the message must be in the following form (in Czech or Slovak, with or without diacritics):

  Zadam o zneplatneni certifikatu cislo = xxxxxxx

  Heslo pro zneplatneni = yyyyyy

  or

  Žádám o zneplatnění certifikátu číslo = xxxxxxx

  Heslo pro zneplatnění = yyyyyy

  where "xxxxxxx" is the serial number of the certificate and "yyyyyy" is the revocation password. The serial number must be in a decimal or hexadecimal format (beginning with "0x").

  If the application meets one of the above two requirements (electronically signed or unsigned message), the responsible employee of the operational office of the certification authority shall immediately revoke the certificate. The revocation date and time shall be determined by the moment of receipt of a valid application for certificate revocation by the I.CA server. If the application does not meet the above requirements, it shall be rejected and the applicant shall be notified of this in an electronic way (if an electronic address has been filled in). If the application is granted, the applicant shall not be explicitly notified of this, and the information about the revocation shall be available in the next release of the certificate revocation list.

- Via the form available at the on-line information address reserved for this purpose: http://www.ica.cz/.

In the above three alternatives, the date and time of certificate revocation shall be determined by the moment of receipt of a valid application for certificate revocation by the I.CA server. If the application does not meet the above requirements, it shall be rejected and the applicant shall be notified of this. If the application is granted, the applicant shall not be explicitly notified of this, and the information about the revocation shall be available in the next release of the certificate revocation list.

In the event of **use of an item of correspondence to submit an application for certificate revocation**, the item of correspondence must contain an application in the following form (in Czech language):

Žádám o zneplatnění certifikátu číslo = xxxxxxx

Heslo pro zneplatnění = yyyyyy

where "xxxxxxx" is the serial number of the certificate and "yyyyyy" is the revocation password.

The serial number must be in a decimal or hexadecimal format (beginning with "0x"). If the applicant does not remember the revocation password, this must be explicitly stated in the written application, as well as the number of the primary personal identification document submitted when applying for the issuance of the certificate, and the application must be signed in the applicant's own hand. In the event that the application is justified, the moment of receipt of the registered item of correspondence at I.CA shall be deemed to be the date and time of revocation of the relevant certificate. The applicant shall be notified of the disposal of the application in a registered letter delivered to the mail address indicated as the sender's address.

4.9.4 Revocation Request Grace Period

The service is not provided.

4.9.5 Time within which CA Must Process the Revocation Request

I.CA's response to the receipt of a valid application for certificate revocation shall be its immediate revocation. The relevant certificate shall be blocked[11] until a certificate revocation list is published. The maximum time elapsed between the revocation of a certificate and its first publication in a certificate revocation list shall not exceed 24 hours.

I.CA shall not allow the unblocking of any certificate that has been previously blocked in accordance with a valid application for revocation.

4.9.6 Revocation Checking Requirement for Relying Parties

The relying parties are obligated to perform any and all activities necessary to verify that the electronic marks are valid and that the relevant certificates have not been revoked. For these purposes, the relying parties shall use the CRLs issued and electronically marked or signed by I.CA. In addition, the provisions of Chapter 4.5.2 shall apply.

4.9.7 CRL Issuance Frequency

První certifikační autorita, a.s., shall release a certificate revocation list on a regular basis, but no later than 24 hours after the release of the previous CRL (usually every 8 hours).

4.9.8 Maximum Latency for CRLs

The provisions of Chapter 4.9.5 shall always be observed in the process of CRL publication with regard to the applicable legislation.

[11] The state in which a certificate is after having been revoked by I.CA until I.CA publishes the CRL in which the certificate is listed for the first time.

4.9.9 On-line Revocation/Status Checking Availability

The service may be provided to contractual partners under specific conditions.

4.9.10 On-line Revocation Checking Requirements

See Chapter 4.9.9.

4.9.11 Other Forms of Revocation Advertisements Available

The service is not provided.

4.9.12 Special Requirements Re-Key Compromise

The service is not provided.

4.9.13 Circumstances for Suspension

The service is not provided.

4.9.14 Who Can Request Suspension

The service is not provided.

4.9.15 Procedure for Suspension Request

The service is not provided.

4.9.16 Limits on Suspension Period

The service is not provided.

4.10 Certificate Status Services

4.10.1 Operational Characteristics

Lists of public certificates are provided in the form of publication of information. Certificate revocations lists are provided both in the form of publication of information and indication of CRL distribution points in issued certificates.

4.10.2 Service Availability

The service of provision of public certificates in the form of publication of information is available 7 days a week and 24 hours a day.

I.CA guarantees continuous availability (7 days a week, 24 hours a day) and integrity of certificate revocation lists (up-to-date CRLs).

4.10.3 Optional Features

No other characteristics of certificate status services are provided. I.CA may extend the provision of characteristics of certificate status services without giving reasons. In doing so, I.CA must abide by the relevant provisions of ESA and ESR.

4.11 End of Subscription

I.CA shall terminate the provision of services to a subscriber or to a marking person upon:

- expiry of the term of the certificate where no application for the issuance of a subsequent certificate has been filed in accordance with this CP,
- termination of the subscriber agreement on the provision of certification services entered into between the subscriber and I.CA, with the exception of the certificate revocation service, which shall be provided throughout the term of the relevant certificate.

4.12 Key Escrow and Recovery

4.12.1 Key Escrow and Recovery Policy and Practices

The service is not provided.

4.12.2 Session Key Encapsulation and Recovery Policy and Practices

The service is not provided.

5 Facility, Management, and Operational Controls

The management of the security of the provided certification services focuses in particular on:

- systems that issue and electronically mark certificates and certificate revocation lists,
- all processes of the provision of certification services under ESA and ESR.

The fields of management, operational and physical security are dealt with both in the fundamental documents, it means Corporate Security Policy, CA System Security Policy, Certification Practice Statement for the Issuance of Qualified Certificates and/or Qualified System Certificates, Crisis Management Plan and Recovery Plan and also in specific security standards and guidelines. The above documents reflect the results of the performed risk analysis.

5.1 Physical Controls

5.1.1 Site Location and Construction

Location of the operational office is geographically different from the location of the company head office, commercial and development offices, registration authority offices and business points.

Devices providing the certification services are located in the restricted areas of the operational office. These areas are secured similarly to the secured areas of the “Confidential” security clearance.

5.1.2 Physical Access

The requirements for the physical access to restricted areas (protected by mechanical and electronic means) of the operational office are specified in the company’s internal regulations. The structure is protected by an electronic security system (ESS), by connection to a centralized protection panel (CPP) and by a special system for the monitoring, transmission and display of the movement of persons and vehicles.

5.1.3 Power and Air-Conditioning

In the areas dedicated for the performance of certification services, there is sufficiently dimensioned active air-conditioning, which keeps the temperature at 20℃ ± 5℃ all year round. The sup ply of electricity is backed-up by UPS (Uninterruptible Power Supply) or a diesel unit.

5.1.4 Water Exposures

All the critical systems of the operational office are located so as not to be flooded with a 100-year flood.

5.1.5 Fire Prevention and Protection

There is an automatic fire alarm system installed in the building of the operational office. The entrance door of the restricted areas, in which the devices providing certification services are located, is equipped with fireproof insulation. In the areas themselves, there is a fire extinguisher.

5.1.6 Media Storage

Storage media containing operational backups and records in an electronic form are stored in metal boxes or safes.

Paper media which must be archived under ESA and ESR are stored in a location that is geographically different from the location of the operational office.

5.1.7 Waste Disposal

All office paper waste is shredded before leaving the premises of a I.CA.

5.1.8 Off-Site Backup

Copies of operational and working backups are stored at a place specified by the Chief Executive Officer of I.CA.

5.2 Procedural Controls

5.2.1 Trusted Roles

Trusted roles have been defined for certain activities carried out in I.CA. The roles are defined in internal documents together with the relevant activities and responsibilities.

5.2.2 Number of Persons Required per Task

In První certifikační autorita, a.s., there are activities defined for the processes of the provision of certification services, which must be carried out only in the presence of two or more persons. These are in particular:

- generation of key pair for the creation/verification of electronic marks of certificates and certificate revocation lists issued by I.CA,
- destruction of data for the creation of electronic marks of certificates and certificate revocation lists issued by I.CA,
- backup/restore of data for the creation of electronic marks of certificates and certificate revocation lists issued by I.CA,
- activation of a cryptographic module containing the data for the creation of electronic marks of certificates and certificate revocation lists issued by I.CA.

The number of persons required to be present during the performance of other activities is not specified, but they must only be authorized employees.

5.2.3 Identification and Authentication for each Role

The employees of each role are given means for proper identification (name, certificate) and authentication (password, private key) for the components which are necessary for their activities.

5.2.4 Roles Requiring Separation of Duties

The roles requiring separation of duties in the process of the provision of certification services defined in the internal security documentation.

5.3 Personnel Controls

5.3.1 Qualifications, Experience, and Clearances Requirements

I.CA's employees for trusted roles are selected and hired according to the staffing criteria described below:

- absolutely no criminal records – proven by a statement of criminal records or by an affirmation,
- university degree achieved in an accredited bachelor or master study program and at least three years experience in the field of information and communications technologies, or secondary education and at least five years' experience in the field of information and communications technologies, of which at least one year in the field of the provision of certification services,
- proficiency of the area of public key infrastructure and information security,
- in individual cases, the time period of the experience may be reduced by up to one third of the required length if the employee has passed an examination and proven sufficient knowledge required for his/her position.

Other I.CA's employees are hired according to the following criteria:

- university degree achieved in an accredited bachelor or master study program, or secondary education,
- basic knowledge of public key infrastructure and information security.

5.3.2 Background Check Procedures

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

- the employees themselves,
- persons who know the employees,
- public information sources.

Employees provide the initial information during a personal interview at the time of the hiring, and the information is updated in regular interviews with their superior employees taking place during the course of the employment.

5.3.3 Training Requirements

I.CA's employees are professionally trained in the use of the relevant software and of special devices. The training is carried out by the combination of the method of self-preparation and methodological leadership by a previously trained employee. The regular period of the training is one month.

5.3.4 Retraining Frequency and Requirements

At least once a year, I.CA organizes an internal learning seminar focusing on the issue of information security for its own employees.

5.3.5 Job Rotation Frequency and Sequence

Due to possibility of deputizing in exceptional cases, I.CA's employees are motivated to acquire knowledge required for the performance of a different role within I.CA.

5.3.6 Sanctions for Unauthorized Actions

In the event of discovery of an unauthorized activity, the relevant employee shall be treated in the manner defined in the company's internal documents and in accordance with the Labor Code (this procedure shall be without prejudice to any criminal proceedings, if initiated, if the seriousness of the discovered unauthorized activities substantiates this).

5.3.7 Independent Contractor Requirements

I.CA may or must ensure certain activities contractually. These business relationships are governed by bilateral commercial contracts. They include for example contractual registration authorities, programmers of application software, hardware suppliers, suppliers of system software, external auditors, etc. These parties are obligated to abide by the relevant public certification policies, by the relevant parts of I.CA's internal documents that have been provided to them, and by the relevant normative documents. In the event of violation of any obligation defined in these documents, contractual penalties shall be imposed or the contract entered into with the contractor shall be terminated with immediate effect.

5.3.8 Documentation Supplied to Personnel

In addition to the certification policy, the certification practice statement and security and operational documents, I.CA's own employees shall be provided with any and all other standards, guidelines, manuals and instructions required for the performance of their duties and responsibilities.

5.4 Audit Logging Procedures

5.4.1 Types of Events Recorded

With regard to the fact that I.CA is an accredited provider of certification services, all the events required by ESA and ESR are recorded in the process of the provision of such services.

All audit records shall be, to the necessary extent, created, stored and processed while maintaining the provability of the origin, integrity, availability, confidentiality and time authenticity thereof.

The audit system has been designed and operated in a way that guarantees the storage of audit data, reservation of sufficient space for audit data, automatic non-rewriting of the audit file, presentation of audit records to users in a suitable manner, and access to the audit file restricted only to defined users.

5.4.2 Frequency of Processing Log

Audit records are checked and assessed in the intervals defined in internal security documents, or immediately in the event of a security incident.

5.4.3 Retention Period for Audit Log

Unless the relevant legislation enacts otherwise, audit records shall be archived for at least 10 years after the creation thereof.

5.4.4 Protection of Audit Log

Audit records in an electronic and paper form are stored in a manner ensuring protection against any modification, theft or destruction thereof (whether intentional or unintentional).

Electronic audit records are stored in two copies. Each copy is located in a different room of I.CA's operational premises. At least once a month, the audit records are stored in a medium that is stored outside I.CA's operational premises.

Audit records in a paper form are stored outside I.CA's operational premises.

The protection of the above types of audit records is defined in internal security documents.

5.4.5 Audit Log Back Up Procedures

The backup of audit records is performed in a similar method as the backup of other electronic information. The backup of audit records in a paper form is not performed.

5.4.6 Audit Collection System (Internal vs. External)

The system of collection of audit records is internal in relation to I.CA, and external in relation to contractual partners.

5.4.7 Notification to Event-Causing Subject

The party shall not be informed about the inclusion of the event in an audit record.

5.4.8 Vulnerability Assessment

The assessment of vulnerability is performed in První certifikační autorita, a.s., on a regular basis, or immediately in the event of an incident having an impact on the security of the provided services.

5.5 Records Archival

The storage of information and documents is carried out by I.CA in accordance with the requirements of ESA and ESR.

5.5.1 Types of Records Archived

I.CA stores the following types of information and documents (in an electronic or paper form) relating to the provision of certification services, and in particular:

- subscriber agreements on the provision of certification services, including applications for the provision of a service,
- copies of documents submitted at the time of the concluding of the subscriber agreement for the provision of certification services,

- confirmations of receipt of a certificate by the subscriber or the subscriber's agent, or the subscriber's consent to the publication of the certificate in a list of issued certificates,
- declaration of the certificate holder that prior to concluding the subscriber agreement on the provision of certification services he was given written information on the exact conditions for the use of such services as well as on the conditions for complaints and settlement of disputes, and on whether the provider of certification services was accredited or not,
- documents and records relating to the life cycle of an issued certificate, including this certificate,
- other records required by ESA and ESR,
- application software and all the company's documents that are necessary for the performance of inspections,
- identification of the location where the information and documents the storage of which is required by ESA and ESR are stored ,
- all certificate revocation lists,
- identification data of the person who verified the identity of an applicant for a certificate or of the applicant's agent, including the business name of the contractual partner performing such activities for I.CA, if any,
- report on the handling (for example acceptance, handover, storage, inspection, conversion into an electronic form, etc.) information,
- operational and security documents.

5.5.2 Retention Period for Archive

I.CA shall ensure that the information and documents specified in Chapter 5.5.1 are stored at least for 10 years since the creation thereof (unless otherwise provided by the relevant legislation).

Information relating to CA signing certificates, with the exception of the relevant data for the creation of an electronic mark, has been stored for the entire time of I.CA's existence.

The procedures for the storage of information and documents are defined in I.CA's internal documents.

5.5.3 Protection of Archive

Stored information and documents contain also the personal data of clients, and therefore because of the applicable legislation, the data are protected to a greater extent. The premises within which the stored information and documents are located are secured in the form of measured based on the requirements for structural and physical security.

The procedures for the protection of repositories of stored information and documents are defined in I.CA's internal documents.

5.5.4 Archive Backup Procedures

The procedures for the backup of stored information and documents are defined in I.CA's internal documents.

5.5.5 Requirements for Time-Stamping of Records

In the event that timestamps are used, these are qualified timestamps issued by I.CA.

5.5.6 Archive Collection System (Internal or External)

Information and documents are stored in the place specified by the Chief Executive Officer of I.CA. Registration authorities shall perform pre-archiving within the specified time limits and hand the acquired data to the authorized employees of I.CA.

The issue of preparation and the method of storage of information and documents in an electronic or paper form are described in internal standards and regulations. The collection of stored information is recorded.

5.5.7 Procedures to Obtain and Verify Archive Information

Stored information and documents are kept in the dedicated locations and they are accessible by:

- I.CA's employees, if this is required for their activities,
- authorized inspectors, authorities engaged in criminal proceedings, and courts, if this is required by the applicable legislation.

A written record shall be made of each such authorized access.

5.6 Key Changeover

In standard situations (expiry of the term of a certificate), the replacement of data for the verification of electronic marks in the I.CA parent qualified system certificate (I.CA signing certificate) shall be performed sufficiently in advance (at least one year prior to the expiry of the term of the certificate) in the form of issuance of a new I.CA signing certificate. In the event of non-standard situations (for example in the event of a development of cryptanalytic methods that may endanger the security of the process of creation of electronic marks, i.e. a change in encryption algorithms, key length, etc.), the replacement shall be performed at the adequate time.

Both in the event of standard and non-standard situations, the replacement of data for the verification of electronic marks/signatures in the I.CA parent qualified system certificate shall be notified to the subscribers and to the general public in advance (if possible) and in an appropriate manner.

5.7 Compromise and Disaster Recovery

5.7.1 Incident and Compromise Handling Procedures

In the event of occurrence of such circumstances, I.CA shall proceed in accordance with the internal document Crisis Management Plan and Recovery Plan and with any documents to which the Plan refers.

5.7.2 Computing Resources, Software, and/or Data are Corrupted

In the event of damage to computer equipment, software or data, I.CA shall proceed in accordance with the internal document Crisis Management Plan and Recovery Plan and with any documents to which the Plan refers.

5.7.3 Entity Private Key Compromise Procedures

In the event of occurrence of a reasonable concern regarding the compromising of the data for the creation of electronic marks for the marking of certificates and certificate revocation lists, I.CA shall:

- terminate the use thereof,
- immediately and permanently revoke the relevant I.CA signing certificate and the corresponding data for the creation of electronic marks (private key),
- revoke all the valid certificates that have been electronically marked with the above data,
- immediately announce this, including the reason, at its information website and at least in one nationally distributed daily newspaper; it is also possible to use a certificate revocation list to make this information available,
- notify the relevant authority of the information on the revocation of the I.CA signing certificate with specification of the grounds for revocation,

- if possible, notify the subscribers of valid certificates of the revocation of these certificates by sending them a message via electronic mail to the electronic addresses indicated by them in their applications for the issuance of a certificate; the notification shall also mention the reason for the termination of the validity of the relevant I.CA signing certificate.

An analogous procedure shall be applied in the event of a development of cryptanalytic methods (for example a change in encryption algorithms, key length, etc.) that may immediately endanger the security of the process of issuance of certificates and certificate revocation lists.

5.7.4 Business Continuity Capabilities after a Disaster

In the event of a disaster, I.CA shall proceed in accordance with the internal document Crisis Management Plan and Recovery Plan and with any documents to which the Plan refers.

5.8 CA or RA Termination

In the event of planned termination of the activities of I.CA as a qualified provider of certification services, i.e. on grounds other than extraordinary events, such as strikes, civil unrests, war, natural disasters of a national scale or other results of force majeure, it's necessary to ensure following activities and I.CA shall:

- notify the relevant authority of its intention to terminate the activities of provision of certification services at least 3 months prior to the planned termination of the activities,
- put forth maximum effort to ensure that the records kept under the applicable legislation are taken over by another qualified provider of certification services, notify this at least 30 days prior to the planned date of termination of the activities to the relevant authority, and ensure that the records are handed over to the relevant authority – include this information in a message sent to all its clients that are holders of effective subscriber agreements on the provision of certification services, if this is known at least 2 months prior to the planned termination of the activities,
- inform about the termination of I.CA's activities in the field of issuance of certificates at its information website at least 2 months prior to the planned termination of activities,
- terminate the provision of certification services,
- destruct its data for the creation of electronic marks used to mark issued certificates and certificate revocation list in a provable manner.

In the event of termination of the activity of a particular RA office, this shall be announced at the website http://www.ica.cz or on the notice board (if possible) at the RA office.

In the event of termination of I.CA's accreditation, I.CA shall immediately notify this not only to the parties to which it provides its certification services, but also to other involved parties in the manner specified in Chapters 2.2 and 2.3.

6 Technical Security Controls

6.1 Key Pair Generation and Installation

6.1.1 Key Pair Generation

The generation of I.CA key pair (the private key with which I.CA electronically marks issued certificates and certificate revocation lists, and the public key used to verify such marks), which takes place in a secured area in accordance with the CA System Security Policy and the course of which is recorded in a written report, shall be carried out in a cryptographic module complying with ESA and ESR. All the requirements for the process of generation of I.CA key pair used to mark or sign issued certificates and certificate revocation lists are defined in internal security documents.

For fundamental security reasons, I.CA does not provide the service of generation of key pair of an applicant for a certificate on its own devices. The keys must support the RSA algorithm.

6.1.2 Private Key Delivery to Subscriber

With regard to the fact that an applicant for a certificate generates the private key exclusively on devices and in an environment that are under the applicant's exclusive control at the moment of the generation, this process shall not be enforced.

6.1.3 Public Key Delivery to Certificate Issuer

The public key must be delivered to I.CA. I.CA supports the following methods of delivery of the data for the verification of an electronic mark – in person on a storage medium and/or in an electronic way.

6.1.4 CA Public Key Delivery to Relying Parties

The data for the verification of electronic marks of certificates and certificate revocation lists issued by I.CA are contained in an I.CA signing certificate, the receipt of which is guaranteed in the following methods:

- handover at an RA (personal visit),
- via I.CA's website or the relevant authority or the bulletin of the relevant authority,
- each applicant for a certificate shall receive an I.CA signing certificate at the time of receipt of the first (initial) certificate at an RA.

The methods of acquisition of the data for the verification of electronic marks of marking persons are specified in Chapter 2.

6.1.5 Key Sizes

In the process of the provision of certification services, I.CA uses exclusively the most credible classical asymmetric algorithm – RSA. The size of the keys (or the parameters of the relevant algorithm) used for the marking or signing of issued certificates and certificate revocation lists is 2048 bits, and the size of the keys (or the parameters of the relevant algorithm) on the part of the client is 2048 bits.

6.1.6 Public Key Parameters Generation and Quality Checking

The algorithms used to generate integer values necessary for an electronic mark to be functional (such as a prime-number test) must match the specifications defined in the applicable legislation (ESA, ESR) and relevant technical standards.

I.CA shall check for the possibility of double occurrence of the same data for the verification of electronic marks in issued certificates. In the event of duplicate occurrence of the data for the verification of electronic marks, the applicant for a certificate shall be requested to generate new key pair. The previously issued certificate shall be immediately revoked and the subscriber shall be immediately and in an appropriate manner notified of this and requested to generate new key pair.

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

Specified in Chapters 1.4 and 7.1.2.

6.2 Private Key Protection and Cryptographic Module Engineering Controls

6.2.1 Cryptographic Module Standards and Controls

The generation of I.CA key pair and the storage of the I.CA private key used to create electronic marks of issued certificates and certificate revocation lists takes place in a cryptographic module meeting the requirements of the FIPS PUB 140-2 Level 3 and of ESR.

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

The protection by secret sharing is performed by the means of a cryptographic module. During the performance of individual sensitive activities related to crucial activities of I.CA (see Chapters 6.1.1 and 6.2.10), the presence of three authorized I.CA employees, two of whom know a part of the code necessary to perform such activities, is required.

6.2.3 Private Key Escrow

The service is not provided.

6.2.4 Private Key Backup

The cryptographic module used for the administration of I.CA key pair allows backups of the private key used for the creation of electronic marks of issued certificates and certificate revocation lists. The private key is stored in an encrypted form via smart card.

6.2.5 Private Key Archival

Upon expiry of the term of the private key for the electronic marking of issued certificates and certificate revocation lists, the private key (and all its backups) shall be destroyed and no further backups thereof shall be performed. The archiving of the privates keys is a security risk, and it is therefore prohibited in I.CA.

6.2.6 Private Key Transfer into or from a Cryptographic Module

The private key used for the creation of electronic marks of issued certificates and certificate revocation lists is generated directly in the cryptographic module.

In the event of restore of a private key from an encrypted backup, the insertion of the private key into the cryptographic module shall take place in the direct personal presence of at least two designated employees of I.CA. At the time of the insertion, the dedicated workstation and the cryptographic module must be disconnected from the computer network. The insertion of the private key shall be logged (in writing).

6.2.7 Private Key Storage on Cryptographic Module

The private key used for the creation of electronic marks shall be stored in a secure manner in the cryptographic module meeting the requirements of applicable legislation.

6.2.8 Method of Activating Private Key

The activation of the private key used for the creation of electronic marks of issued certificates and certificate revocation lists, generated in the cryptographic module, shall be performed by the designated employees of I.CA through the activation of the cryptographic module itself and of an activation smart card in accordance with the specific procedure defined in the relevant internal documents. After the activation, the system will be ready for the electronic marking or signing of issued certificates and certificate revocation lists, and the activation card shall be removed. After the activation, the device shall be accessible only to the designated responsible employees of I.CA.

6.2.9 Method of Deactivating Private Key

The deactivation of the private key used for the creation of electronic marks of issued certificates and certificate revocation lists shall be performed by the designated employees of I.CA through the cryptographic module and the activation smart card in accordance with the specific procedure defined in the relevant internal documents. After the deactivation, a written report shall be executed and signed by the designated employees of I.CA.

6.2.10 Method of Destroying Private Key

The private key used for the marking of issued certificates and certificate revocation lists shall be stored in the cryptographic module. The destruction of the private key shall be performed through the means of the cryptographic module. Private key backups, stored in an encrypted form on external media, shall also be destroyed. The destruction shall consist in the physical destruction of said media. All the requirements for the process of destruction of the private key used for marking of issued certificates and certificate revocation lists are defined in the internal security documents.

6.2.11 Cryptographic Module Rating

Cryptographic module used for the electronic marking or signing of issued certificates and certificate revocation lists has been certified for conformity with the requirements of the FIPS PUB 140-2 Level 3 standard.

6.3 Other Aspects of Key Pair Management

6.3.1 Public Key Archival

The issue of archiving of the data for the verification of electronic marks is dealt with in accordance with ESA and ESR.

6.3.2 Certificate Operational Periods and Key Pair Usage Periods

The maximum term of any issued certificate is indicated in the body of that certificate.

6.4 Activation Data

6.4.1 Activation Data Generation and Installation

The activation data are created during the process of installation, when I.CA key pair used to create and verify electronic marks of issued certificates and certificate revocation lists is generated.

6.4.2 Activation Data Protection

The above activation data are protected by I.CA's employees in the manner specified in the internal security documents.

6.4.3 Other Aspects of Activation Data

The above activation data are intended solely for the processes of the provision of certification services and must not be used for any other purposes or transferred or kept in a clear form.

6.5 Computer Security Controls

6.5.1 Specific Computer Security Technical Requirements

The level of security of components used for the provision of certification services is defined by ESA and ESR.

A detailed solution of the specific technical requirements for computer security is described in the relevant internal documents.

6.5.2 Computer Security Rating

The security evaluation of I.CA is based on national and international standards:

- CWA 14167-1 – Security Requirements for Trustworthy Systems Managing Certificates for Electronic Signatures – Part 1: System Security Requirements,
- ETSI TS 101 456 – Electronic Signatures and Infrastructures; Policy Requirements for Certification Authorities Issuing Qualified Certificates,
- ČSN ISO/IEC 17799 – Information Technology – Code of Practice for Information Security Management,
- ČSN ISO/IEC 27001 – Information Technology – Security Techniques – Information Security Management Systems – Requirements,
- ČSN ISO/IEC TR 13335 – Information Technology – Guidelines for the Management of IT Security 1–3,
- ČSN EN ISO 19011 – Guidelines for Quality and/or Environmental Management Systems Auditing.

6.6 Life Cycle Technical Controls

6.6.1 System Development Controls

The system development shall be governed by the relevant internal documents.

6.6.2 Security Management Controls

Complying with the standards (see Chapter 6.5.2), ESA and ESR is verified by regular audits of the information security management system, performed by employees of independent audit companies, and by security conformity inspections performed by I.CA's employees. This issue is described in the relevant internal documents. I.CA reserves the right to perform also other types of inspections and audits.

6.6.3 Life Cycle Security Controls

The management of life cycle security is performed in I.CA by the procedural approach of "Plan-Do-Check-Act", which consists of several consecutive processes:

- establishing – definition of the security policy, plans, objectives, processes and procedures with regard to the risk management and security of information so as to make sure that they are consistent with the corporate security policy,
- implementation and operation – of the security policy, plans, objectives, processes and procedures,
- monitoring and reconsidering – evaluation of the process with regard to the security policy and handover of the findings to the company management for assessment,
- application – performance of remedial measures resulting from the decision of the company management.

6.7 Network Security Controls

In the environment of I.CA, the means performing the certification services themselves are not directly accessible from the Internet public network. Among other things, the information system is protected by a firewall (commercial product). All communications between an RA and the operational office of a certification authority is performed in an encrypted manner. Detailed information on the management of the network security is available in the relevant internal documents.

6.8 Time stamping

The solution is specified in Chapter 5.5.5.

7 Certificate, CRL and OCSP Profiles

7.1 Certificate Profile

Table 3 – Data of an Issued Qualified System Certificate

Field	Content	Comments
Version	v3 (0x2)	mandatory, generated by I.CA
serialNumber	unique serial number of the issued certificate (assigned by I.CA)	mandatory, generated by I.CA
Signature	identifier of the algorithm used by I.CA for the electronic mark of the issued certificate (i.e. of this certificate)	mandatory, generated by I.CA
Issuer	Information on the issuer of the certificate – see Table 4	mandatory, generated by I.CA
Validity		mandatory, generated by I.CA
• notBefore	beginning of the term of the issued certificate (UTC[12])	
• notAfter	end of the term of the issued certificate (UTC)	
Subject	information on the marking person/subscriber: • countryName(C) • commonName (CN) • stateOrProvinceName (S) • localityName (L) • organizationName (O) • organizationalUnitName (OU) • emailAddress (E) • initials (I) • name (N) • title (T) • serialNumber • generationQualifier	see Chapter 3.1
subjectPublicKeyInfo		mandatory, generated by I.CA
• algorithm	algorithm identifier used by the public key indicated in the issued certificate	
• subjectPublicKey	public key of the signatory (2048 bits)	
Extensions	extensions of the issued certificate	see Table 5

Table 4 – Issuer

Field	Content
Organization (O)	První certifikační autorita, a.s.
OrganizationalUnitName (OU)	I.CA – Accredited Provider of Certification Services
CommonName (CN)	I.CA – Qualified Certification Authority, MM/YYYY
Country (C)	CZ

Note: MM/YYYY is the month and year of the beginning of the term of the CA certificate.

[12] Universal Co-ordinated Time, a standard accepted on January 1, 1972 for the Coordinated Universal Time (UTC) – the function of the "official timekeeper" of the atomic time for the whole world is performed by Bureau International de l'Heure (BIPM).

7.1.1 Version Number(s)

All the issued certificates are consistent with X.509, version 3.

7.1.2 Certificate Extensions

Table 5 – Extending Fields in a Qualified Certificate

Field	Content	Specification
SubjectAlternativeName	otherName, rfc822Name, dNSName, URI, iPAddress	non-critical and optional field see Chapter 3.1.1.13
AuthorityKeyIdentifier		non-critical and mandatory field, generated by I.CA
• KeyIdentifier	hash of the public key of the certificate issuer	
Subject Key Identifier	hash of the public key of the issued certificate	non-critical and mandatory field, generated by I.CA
Certificate Policies		non-critical and mandatory field, generated by I.CA
• Policy	see Chapter 7.1.6	
• Explicit Text	see Chapter 7.1.8	
CRL Distribution Points	list of CRL distribution points, accessible via http protocol	non-critical and mandatory field, in the event of a written contract with a client, it is possible to add other distribution points requested by the client, generated by I.CA
Key Usage		critical and mandatory field; only digitalSignature, nonRepudiation, keyEncipherment, dataEncipherment, keyAgreement bits are generally accepted; if the application for the issuance of a certificate contains any other bit, it will be rejected and the certificate will not be issued
	if the field is missing in the application: digitalSignature, nonRepudiation, **if the field is not missing in the application:** if the nonRepudiation bit is not set, the application shall be rejected and the certificate shall not be issued, otherwise the setting of the bits will be taken from the application – due to compatibility with third-party products, I.CA recommends the setting of the digitalSignature bit – implemented in the application generators created by I.CA	(generated by I.CA) note: The application or non-application of digitalSignature, keyEncipherment, dataEncipherment, keyAgreement bits may be modified – the liability for losses incurred as a result of such modification will be borne by the applicant
Extended Key Usage	anyExtendedKeyUsage, id-kp-serverAuth, id-	optional field, taken from

	kp-clientAuth, id-kp-emailProtection	the application for a certificate, in the event of anyExtendedKeyUsage, I.CA will set this field as non-critical, in other events it will be taken from the application
nsComment	smart card number	non-critical and mandatory field only in the event of issuance of the certificate on a smart card, generated by I.CA

I.CA reserves the right to extend or reduce the above set of extending fields.

7.1.3 Algorithm Object Identifiers

The process of the provision of certification services uses the algorithms specified by the applicable legislation or by the relevant technical standards to which the applicable legislation refers.

7.1.4 Name Forms

Specified in Chapter 3.1.

7.1.5 Name Constraints

There is no constraint on the name of the subject with the exception of those specified in Chapter 3.1.2. The acceptability of particular content of individual fields of the subject shall be finally determined by the registration authority employee who handles the request for the issuance of a certificate. In the event of disapproval, the applicant may proceed in accordance with Chapter 9.13.

7.1.6 Certificate policy OID

This CP is designed for the issuance and administration of qualified system certificates, and it has been allocated the OID specified in Chapter 1.2.

7.1.7 Usage of Policy Constraints Extension

Not applicable.

7.1.8 Policy Qualifiers Syntax and Semantics

The text of the user notice of the mandatory “Policy Qualifiers” extending field shall be as follows:

Tento kvalifikovany certifikat je vydan podle zakona Ceske republiky c. 227/2000 Sb. v platnem zneni/This is qualified certificate according to Czech Act No. 227/2000 Coll.

7.1.9 Processing Semantics for the Critical Certificate Policies Extension

See Table 5.

7.2 CRL Profile

7.2.1 Version Number(s)

Certificate revocation lists are issued in accordance with X 509, version 2.

7.2.2 CRL and CRL Entry Extensions

Table 6 – CRL Fields

Field	Content
Version	v2
SignatureAlgorithm	identifier and parameters of the algorithm used by I.CA for the electronic mark of the issued CRL
Issuer	identification of the issuer of the CRL (see Table 5)
thisUpdate	date and time of issuance of the CRL (UTC)
nextUpdate	date and expected time of issuance of the next CRL (UTC)
revokedCertificates • userCertificates • revocationDate	certificate revocation list unique serial number of the revoked certificate date and time of revocation of the certificate
crlExtensions	CRL extension (see Table 7)

Table 7 – CRL extensions

Field	Content	Critical
AuthorityKeyIdentifier • KeyIdentifier	hash of the public key of the issuer of the certificate	NO
CRL Number	CRL number	NO
IssuingDistributionPoint	the http address(es) from which the CRL can be acquired	YES

7.3 OCSP Profile

See Chapter 4.9.9.

7.3.1 Version Number(s)

The service is not provided.

7.3.2 OCSP Extensions

The service is not provided.

8 Compliance Audit and Other Assessment

8.1 Frequency or Circumstances of Assessment

With regard to the fact that První certifikační autorita, a.s., is an accredited provider of certification services, the frequencies of assessments, including the circumstances for the performance of assessments, are strictly defined by the requirements of ESA and ESR – this concerns in particular an audit of the information security management system, inspection of security conformity and audit of the security of the provision of certification activities.

První certifikační autorita, a.s., reserves the right to perform other forms of assessment as well.

8.2 Identity / Qualification of the Assessor

The identity and qualification of the assessor performing an assessment required by ESA and ESR shall be defined by the applicable legislation, and in other cases the assessor shall be required to be certified for the relevant activities.

8.3 Assessor's Relationship to Assessed Entity

In the event of performance of an assessment required by ESA and ESR, the relation of the assessor to the provider of certification services is specified by the applicable legislation, and in other cases it shall be an external assessor.

8.4 Topics Covered by Assessment

In the event of performance of an assessment required by ESA and ESR, the assessed areas are specified by the applicable legislation, and in other cases the assessed areas shall be those specified in the standards under which the assessment is performed.

8.5 Actions Taken as a Result of Deficiency

The findings of all types of performed assessments shall be notified to the security manager, who shall ensure that any discovered deficiencies are corrected.

8.6 Communication of Results

The announcement of assessment results shall be performed in the form of a written final report which shall be handed over by the assessor to the Chief Executive Officer or to the security manager of the company.

The security manager shall convene a meeting of the security committee as soon as possible. In addition to the company management, the meeting shall be attended by the heads of individual departments, and the security manager shall inform them of the results of the assessment.

The announcement of assessment results shall be also governed by the requirements of ESA and ESR.

9 Other Business and Legal Matters

9.1 Fees

9.1.1 Certificate Issuance or Renewal Fees

The fees for a first (initial) or subsequent certificate are defined in the up-to-date price list of services, which is available at the on-line information address of I.CA. The service of certificate renewal is not provided.

9.1.2 Certificate Access Fees

I.CA does not charge any fees for the access to issued public certificates in an electronic way.

9.1.3 Revocation or Status Information Access Fees

I.CA does not charge any fees for the access to information about revoked certificates (up-to-date URL) or about certificate statuses in an electronic way.

9.1.4 Fees for Other Services

The fee for the handover of a certificate (first - initial, subsequent) on a storage medium (such as a floppy disk) is defined in the up-to-date price list of services, which is available at the on-line information address of I.CA.

Certificate revocation and downloading the electronic version of the CP (in the generally used PDF format) is provided for free.

Fees for above-standard services are defined contractually.

9.1.5 Refund Policy

I.CA reserves the right to change the fee for the issuance of a first (initial) certificate or a subsequent certificate. I.CA shall also have the right to determine different fees in individually concluded contracts.

9.2 Financial Responsibility

9.2.1 Insurance Coverage

První certifikační autorita, a.s., declares, that it has an insurance policy covering business risks to such an extent so as to cover financial losses, if any.

9.2.2 Other Assets

První certifikační autorita, a.s., declares that it has sufficient financial resources and other assets ensuring the operation of the certification services in accordance with the requirements of ESA and corresponding to the risk of liability for damage.

Detailed information on the assets of První certifikační autorita, a.s., is available in the Annual Report of I.CA.

9.2.3 Insurance or Warranty Coverage for End-Entities

The service is not provided.

9.3 Confidentiality of Business Information

9.3.1 Scope of Confidential Information

Sensitive or confidential information of I.CA shall be any and all pieces of information that are not published in the way described in Chapter 2.2, in particular:

- data for the creation of electronic marks, corresponding to the data for the verification of electronic marks, contained in I.CA signing certificates,
- data for the creation of electronic signatures / marks, corresponding to the data for the verification of electronic signatures / marks, contained in I.CA purpose certificates (for example keys for communication with an RA),
- other cryptographically significant information used for the operation of I.CA and RA,
- selected business information of I.CA,
- any and all internal information and documents concerning the provision of certification services under ESA,
- any and all personal data.

9.3.2 Information not within the Scope of Confidential Information

Public information shall be in particular those pieces of information that do not belong to any of the groups specified in Chapter 9.3.1.

9.3.3 Responsibilities to Protect Confidential Information

Each employee being in contact with the information specified in Chapter 9.3.1 must not disclose them to any third party without the consent of the Chief Executive Officer of I.CA.

I.CA's employees or any other individuals who are in contact with personal data shall be obligated to maintain the confidentiality of such information and the confidentiality of any data and security measures the disclosure of which would endanger the security of such information and data. The confidentiality obligation shall survive the termination of employment or any other similar relationship, as well as the completion of the relevant work.

9.4 Privacy of Personal Information

9.4.1 Privacy Plan

The protection of personal data and other non-public information is dealt with in I.CA in accordance with the requirements of the applicable legislation.

9.4.2 Information Treated as Private

Private information shall be any and all personal data of clients, users or employees that are protected under the applicable legislation.

9.4.3 Information not Deemed Private

In general, non-private data shall be the data published in the manner specified in Chapter 2.2.

9.4.4 Responsibility to Protect Private Information

The protection of personal data and other private information is the responsibility of I.CA.

9.4.5 Notice and Consent to Use Private Information

The issues of notification of the use of confidential information and of the consent to the use of sensitive information (see the relevant provisions of Chapters 3 and 4) are dealt with in I.CA in accordance with the requirements of the applicable legislation.

9.4.6 Disclosure Pursuant to Judicial or Administrative Process

The disclosure of sensitive information for judicial or administrative purposes is dealt with in I.CA in accordance with the requirements of the applicable legislation.

9.4.7 Other Information Disclosure Circumstances

In the event of disclosure of personal data, I.CA shall strictly abide by the requirements of the applicable legislation.

The persons specified in Chapter 9.3.3 may be relieved of the confidentiality obligation by the party in the interest of which they are so obligated or by a court of law.

9.5 Intellectual Property Rights

This CP, all related documents, the content of websites, CA certificates, I.CA keys and the procedures ensuring the operation of the system providing the certification services are protected by the copyright of První certifikační autorita, a.s., and represent its significant know-how.

9.6 Representations and Warranties

9.6.1 CA Representations and Warranties

I.CA represents and warrants that:

- it shall use the private keys corresponding to CA certificates only for the purposes of the electronic marking or signing of the issued certificates and certificate revocation lists,
- the issued certificates meet the requirements defined in ESA and ESR,
- it shall revoke any certificate for which the revocation was requested in the manner defined in this CP.

Any representations and warranties and performances thereunder may be recognized only if:

- the client has not violated any obligation under the contract on the provision of certification services and under this CP,
- the relying party has not violated any obligation under this CP.

The clients shall file their warranty claims with the RA which handled their initial applications. If the RA is unable to dispose of the warranty claims within its jurisdiction, it shall delegate them to I.CA and notify the client of this. The representations and warranties shall not apply to the use of any certificate not issued by I.CA.

9.6.2 RA Representations and Warranties

An RA shall assume the liability for the correct provision of the services defined in Chapter 1.3.2. An RA shall reject the application if the applicant has not proven his/her/its identity beyond reasonable doubt, has not submitted the documents mentioned in the application for the service, has refused to provide any required information, or has refused to sign the relevant documents (see the relevant chapters of this CP). In addition, an RA shall be responsible for:

- timely handover of applications for revocation of issued certificates to CA,
- the handling of the client's complaints and objections.

9.6.3 Subscriber Representations and Warranties

The subscriber or the signatory shall act in compliance with ESA and ESR and shall guarantee the correctness of the information provided by them during the entire life cycle of the use of the provided certification service.

9.6.4 Relying Parties Representations and Warranties

The relying parties shall act in accordance with ESA and ESR.

9.6.5 Representations and Warranties of Other Participants

The service is not provided.

9.7 Disclaimers of Warranties

První certifikační autorita, a.s., strictly abides by ESA and cannot disclaim the representations and warranties defined therein.

9.8 Limitation of Liability

The limits of the liability of První certifikační autorita, a.s., in the field of provision of certification services are governed by the applicable legislation.

9.9 Indemnities

In the process of the provision of certification services, the representations and warranties agreed between První certifikační autorita, a.s., and the applicant for a particular service shall apply. The subscriber agreement must not be contrary to the applicable legislation and must always be in writing.

První certifikační autorita, a.s.:

- undertakes that it will perform all the obligations defined both in the applicable legislation and in the relevant certification policies,
- grants the above representations and warranties for the entire term of the subscriber agreement on the provision of certification services entered into with the customer,
- does not grant any representations and warranties other than those above.

Other possible damages shall result from the provisions of the applicable legislation and their amounts may be determined by a court.

První certifikační autorita, a.s., **shall not be liable for**:

- any shortcomings in the provided services occurred as the result of incorrect or unauthorized use of the services provided as part of the performance of the subscriber agreement on the provision of certification services by the subscriber, in particular for the operation contrary to the terms and conditions specified in the certification policy, as well as for any shortcomings occurred as a result of force majeure, including a temporary downtime of telecommunications connection, etc.,
- any losses resulting from the use of a certificate during the period after requesting for its revocation, if První certifikační autorita, a.s., has observed the defined time limit for the publication of the revoked certificate in the certificate revocation list (CRL).

A justified complaint may be filed in the following ways:

- by e-mail to the address: reklamace@ica.cz,
- by a registered letter sent to the registered address of the company,
- in person at the registered address of the company.

The person filing a complaint (the subscriber) must provide:

- the subscriber agreement number,
- the receipt number,
- an in-depth description of the shortcomings and their implications.

Obligations of I.CA:

I.CA shall decide a complaint at the latest within three business days after the delivery of the complaint, and shall notify the complainant of the decision (in the form of an electronic mail or a registered letter), unless otherwise agreed between the parties.

A new certificate shall be issued to a subscriber free of charge in the following cases:

- if there is reasonable suspicion that the data for the creation of electronic marks with which I.CA electronically marks issued certificates and certificate revocation lists have been compromised, I.CA shall offer the subscriber free issuance of a new certificate – any and all costs of the issuance of such new certificates shall be borne by I.CA, and I.CA shall also bear the entire liability for any losses incurred in relation to the misuse of such certificates,
- if I.CA finds out during the receipt of an application for the issuance of a certificate that there is another certificate with the same public key, the applicant for a certificate shall be requested to generate a new application – and therefore new key pair, and the subscriber of the existing certificate, who owns the same public key as the applicant for the issuance of a certificate, shall be requested to generate new key pair and his original certificate shall be immediately revoked and the subscriber shall be notified of this.

9.10 Term and Termination

9.10.1 Term

This CP shall enter into force on the date indicated in Chapter 10 and shall continue in force at least for the period of the term of the last certificate issued hereunder.

9.10.2 Termination

The only person entitled to approve the termination of this CP shall be the Chief Executive Officer of První certifikační autorita, a.s.

9.10.3 Effects of Termination and Survival

This CP shall remain in force and effect for the period of the term of the last certificate issued hereunder.

9.11 Individual Notices and Communications with Participants

For the individual notifications and communication with the subscriber or the signatory, I.CA may use the e-mail addresses, mail addresses or telephone numbers provided by them, or discuss in person.

It is also possible to communicate with I.CA in the methods specified at http://www.ica.cz/.

9.12 Amendments

9.12.1 Procedure for Amendment

The procedure is implemented in a controlled process, specified in an internal document.

9.12.2 Notification Mechanism and Period

The procedure is implemented in a controlled process, specified in an internal document.

9.12.3 Circumstances under which OID Must Be Changed

A new OID shall be assigned in the event of a release of a new version of this document.

9.13 Dispute Resolution Provisions

This CP and the relevant certification practice statement and the interpretation and application thereof shall be governed by ESA and ESR.

In the event that a subscriber, signatory, relying party or contractual partner does not agree to the presented interpretation, they may use the following levels of appeal:

- the responsible employee of the RA,
- the responsible employee of I.CA (a submission in writing is mandatory),

- the Chief Executive Officer of I.CA (a submission in writing and payment of a financial security, which will be returned in the event of a positive disposal of the complaint, is mandatory).

The above procedure gives a disagreeing party an opportunity to enforce its will quicker then legal proceeding.

9.14 Governing Law

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

9.15 Compliance with Applicable Law

The system of provision of certification services is carried out in compliance with the requirements of ESA and ESR.

9.16 Miscellaneous Provisions

9.16.1 Entire Agreement

These matters are irrelevant for the application of the release of this document.

9.16.2 Assignment

These matters are irrelevant for the application of the release of this document.

9.16.3 Severability

These matters are irrelevant for the application of the release of this document.

9.16.4 Enforcement (attorneys' fees and waiver of rights)

These matters are irrelevant for the application of the release of this document.

9.16.5 Force Majeure

The subscriber agreement on the provision of certification services may contain provisions concerning force majeure.

9.17 Other Provisions

These matters are irrelevant for the application of the release of this document.

10 Final Provisions

This CP, released by První certifikační autorita, a.s., shall enter into force and effect on April 1, 2011.