První certifikační autorita, a.s.

Certification Policy

for Issuing Qualified Certificates for Website Authentication to Legal Persons

(RSA Algorithm)

Version 1.03

TABLE OF CONTENTS

Table 1 – Document history

Version	Date of Release	Approved by	Comments
1.00	16 November 2017	CEO of První certifikační autorita, a.s.	First release.
1.01	31 January 2018	CEO of První certifikační autorita, a.s.	More specific text in chapters 3.2.2 and 3.2.3, more specific heading 3.2.2.6, language errors correction.
1.02	30 April 2019	CEO of První certifikační autorita, a.s.	More specific text required by BRG and EVCG.
1.03	7 March 2020	CEO of První certifikační autorita, a.s.	Certificate Transparency support.

1 INTRODUCTION

This documents determines the principles applied by První certifikační autorita, a.s. (also as I.CA), a qualified provider of trust services, in providing the trust service of issuing qualified website authentication certificates to end-client legal persons (also as the Service and the Certificate, respectively) which are legal persons or government authorities (also as the Organization).

The Certificates are to authenticate websites and secure data transferred over the SSL/TSL encrypting protocol based on asymmetric cryptography. In accordance with ETSI EN 319 411-2 (see 6.5.2), the Certificates are 'Extended Validation' certificates, i.e. it is the EVCP policy pursuant to ETSI EN 319 411-1 (see 6.5.2) and meet the requirements of *CA/Browser Forum – Guidelines for Issuance and Management of Extended Validation Certificates* (also as EVCG). The RSA algorithm is used for the Service provided under this certification policy (also as the CP).

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

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

In addition to that:

- The Certification Authority that issues the Certificates meets the requirements of the current *CA/Browser Forum – Guidelines for Issuance and Management of Extended Validation Certificates*, which is published on http://www.cabforum.org. If this CP and the Guidelines are in conflict, the Guidelines prevail.

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

1.1 Overview

The document **Certification Policy for Issuing Qualified Certificates for Website Authentication to Legal Persons (RSA Algorithm)**, is prepared by První certifikační autorita, a.s., deals with the issues related to life cycle processes of the certificates issued by I.CA and strictly follows the structure matching the scheme of valid RFC 3647 standard while taking account of valid standards and norms of the European Union and the laws of the Czech Republic pertinent to this sphere (therefore, each chapter is preserved in this document even if it is irrelevant to this sphere). The document is divided into nine basic chapters and these are briefly introduced in the following list:

- Chapter 1 identifies this document with the allocated unique identifier, generally describes the entities and individuals taking part in the provision of this Service, and defines the acceptable use of the Certificates available to be issued;
- Chapter 2 deals with the responsibility for the publication and information or documents;

- Chapter 3 describes the processes of identification and authentication of an applicant for the issuance or revocation of a Certificate, and defines the types and contents of the names used in Certificates;
- Chapter 4 defines life cycle processes of Certificates, i.e. application, the issuance of the Certificate, Certificate revocation request, the revocation of the Certificate, the services related to checking of Certification status, termination of the provision of the Service, etc.;
- Chapter 5 covers physical, procedural and personal security, including the definition of the set of events subject to logging, the keeping of these records and responses to emergency and compromising situations;
- Chapter 6 focuses on the technical security of the type of generating public and private keys, protection of private keys, including the computer and network protection;
- Chapter 7 defines the profile of issued Certificates and CRL;
- Chapter 8 focuses on assessing the Service delivered.
- Chapter 9 deals with commercial and legal aspects.

More detail on the fulfillment of the items of the certificates issued under this policy and the administration thereof are provided in the relevant certification practice statement (also as the CPS).

1.2 Document name and identification

This document's title:	Certification Policy for Issuing Qualified Certificates for Website Authentication to Legal Persons (RSA Algorithm), version 1.03
Policy OID:	1.3.6.1.4.1.23624.10.1.35.1.0

1.3 PKI participants

1.3.1 Certification authorities (also as 'CA')

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

1.3.2 Registration authorities (also as 'RA')

The acceptance of Certificate applications is not delegated to any party, and the physical receipt of applications and applicant authentication are only possible to be made at the designated RA offices of I.CA. Such an RA:

- Accepts applications for the services listed in this CP (Certificate applications, in particular), arranges the handover of Certificates and certificate revocation lists, provides required information, receives complaints, etc.;
- Communicates with relevant subjects when verifying Certificate applications;
- Is authorized to enter into contracts, on behalf of I.CA, on the provision of the Service;
- Is entitled, for urgent operational or technical reasons, to suspend, in whole or in part, the performance of their activities;
- Is authorized to charge for the I.CA services provided by this RA unless otherwise agreed in a contract.

1.3.3 Subscribers

Subscriber of a Certificate may be only the Organization, which made an agreement with První certifikační autorita, a.s., and applied for a Certificate.

1.3.4 Relying parties

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

1.3.5 Other participants

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

1.4 Certificate usage

1.4.1 Appropriate certificate uses

The certificates issued under this CP may only be used for websites authentication and for securing transferred data. The Certificate may be used only for authentication of websites the names of which are stated in this Certificate (subjectAlternativeName extension).

1.4.2 Prohibited certificate uses

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

1.5 Policy administration

1.5.1 Organization administering the document

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

1.5.2 Contact person

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

1.5.3 Person determining CPS suitability for the policy

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

1.5.4 CPS approval procedures

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

1.6 Definitions and acronyms

Table 2 - Definitions

Term	Explanation
CA/Browser Forum	organization, consensual association of certification authorities
Classified Information Protection Act	the Czech Republic's Act No. 412/2005 Coll., regulating classified information protection and security competence, as amended
contracting partner	provider of selected certification services contracted by I.CA for certification services or parts thereof – usually, it is a contracted RA
domain name	node name in domain name system
domain name registrant/ registrant	sometimes referred to as a domain name owner, but more accurately a person or entity registered by a domain registrar as having the right to oversee the use of a domain name, a natural or legal person listed as a "Registrant" by WHOIS or a domain registrar
domain name registrar/ registrar	a person or entity that registers domain names by mandate or with consent: ▪ Internet Corporation for Assigning Names and Numbers (ICANN) - Administrator of DNS Root Space, ▪ TLD administrator (e.g. .com) or ccTLD (e.g. .CZ, national administrator)
domain name space	a set of all possible domain names that are subordinate to one node in the domain name system
electronic signature	data in electronic form that are attached to or logically associated with a data message and which serve as a method

	for unique verifying the identity of the signer in relation to the data message
GET method	a standard preferred method for sending http requests to OCSP responder via http, the method allows caching (the second method is POST)
hash function	transformation which receives, as an input, a string of characters of arbitrary length, and the result is a string of characters of fixed length (hash)
issuing, subordinate CA	for this document, the CA issuing certificates to end users
key pair	a private key and the corresponding public key
Labour Code	the Czech Republic's Act No. 262/2006 Coll., Labour Code, as amended
OCSP responder	server using the OCSP protocol to provide data on public key certificate status
OCSP stapling	way of minimizing queries for OCSP Responder, RFC 4366 - TLS Extensions; allows the TLS server to return the once-received answer to the question about certificate status from the OCSP (during its validity) to all end users accessing the TLS server
phishing	in an electronic communication attempt to obtain sensitive information (usernames, passwords, and credit card details) for malicious reasons
private key	unique data to create electronic signature
public key	unique data to verify electronic signature
relying party	party relying on a certificate in its operations
root CA	certification authority which issues certificates to subordinate certification authorities
subscriber	an applicant for the certificate to whom the certificate was issued
two-factor authentication	authentication employing two of three factors – I know something (the password), I have something (a smart card or a hardware token) or I am something (fingerprint, retina or iris reading)

Table 3 - Acronyms

Acronym	Explanation
ASCII	American Standard Code for Information Interchange, table containing binary codes of English alphabets, numbers and other common symbols
bit	from English *binary digit* – a binary system digit – the fundamental and the smallest unit of information in digital technologies

BRG	document "Baseline Requirements for the Issuance and Management of Publicly-Trusted Certificates" published by CA/Browser Forum
CA	certification authority
CAA	DNS Resource Record - see RFC 6844
ccTLD	country code TLD, national top level domain, usually user for countries, sovereign states or dependent territories, ASCII ccTLD identifiers are two letters long
CEN	European Committee for Standardization, an association of national standardization bodies
CEO	Chief Executive Officer
COO	Chief Operating Officer
CP	certification policy
CPS	certification practice statement
CR	Czech Republic
CRL	Certificate Revocation List – the list of revoked certificates, which are not held as valid any longer
CT	Certificate Transparency, the system to mitigate misissuance of certificate based on adding new certificate (or rather precertificate) to public logs making possible to detect the misissuance (especially fraudulent getting the certificate by other than authorized applicant)
DER, PEM	methods of certificate encoding (certificate formats)
DNS	Domain Name System, a hierarchical decentralized naming system implemented by DNS servers which are exchanging information via DNS protocol to translate domain names to the numerical IP addresses
EBA	European Banking Association
eIDAS	REGULATION (EU) no 910/2014 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 23 July 2014 on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC
EN	European Standard, a type of ETSI standard
ETSI	European Telecommunications Standards Institute, a European standardization institute for information and communication technologies
EU	European Union
EV	extended validation, type of certificate intended for websites authentication
EVCG	document "Guidelines For The Issuance And Management Of

	Extended Validation Certificates" published by CA/Browser Forum
EVCP	Extended Validation Certificate Policy, type of certification policy
FIPS	Federal Information Processing Standard, standards for information technologies for U.S. non-military state organizations
FQDN	Fully Qualified Domain Name, domain name that specifies all domain levels in Internet domain name system
gTLD	generic TLD, top level domain (e.g. .org for non-profit organizations)
ICANN	Internet Corporation for Assigned Names and Numbers, organization which among others assigns and administrates domain names and IP addresses
IEC	International Electrotechnical Commission, the global organization publishing standards for electrical and electronic engineering, communication technologies and related industries
IP	Internet Protocol, principal communications protocol in the Internet protocol suite for relaying packets across network and routing used in the Internet
ISO	International Organization for Standardization, an international organization of national standardization organizations; designation of standards
IT	Information Technology
ITU	International Telecommunication Union
ITU-T	Telecommunication Standardization Sector of ITU
OCSP	Online Certificate Status Protocol, the protocol to identify public key certificate status
PKCS	Public Key Cryptography Standards, designation for a group of standards for public key cryptography
PKI	Public Key Infrastructure
PSD	Payment Services Directive, DIRECTIVE 2007/64/EC OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL on payment services in the internal market
PSD2	DIRECTIVE (EU) 2015/2366 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL, superseding PSD and coming into effect January 13th 2018
PSP	Payment Service Provider
PTC	Publicly-Trusted Certificate
PUB	Publication, FIPS standard designation
QSCD	Qualified Electronic Signature/Seal Creation Device

RA	registration authority
RFC	Request for Comments, designation for a range of standards and other documents describing web protocols, systems, etc.
RSA	signing and encrypting public key cipher (acronym from the names of the original authors: Rivest, Shamir and Adleman)
RTS	COMMISSION DELEGATED REGULATION (EU) 2018/389 of 27 November 2017 supplementing Directive (EU) 2015/2366 of the European Parliament and of the Council with regard to regulatory technical standards for strong customer authentication and common and secure open standards of communication
SCT	Signed Certificate Timestamp, signed timestamp from relevant CT log which confirms adding the precertificate
SHA, sha	type of hash function
SSCD	Secure Signature Creation Device, see Directive
SSL	Secure Sockets Layer, communication protocol, layer inserted between transport layer and application layer, providing securing of communication via encryption and authentication of communicating parties
TLD	Top Level Domain, top level Internet domain, in domain name the top level domain is placed at the end
TLS	Transport Layer Security, communication protocol superseding SSL
TS	Technical Specification, type of ETSI standard
URI	Uniform Resource Identifier, defined-structure text string for accurate specification of a source of information
UTC	Coordinated Universal Time, the standard adopted on 1 January 1972 for the global coordinated time – Bureau International de l'Heure (BIH) plays the role of the 'official keeper' of the atomic time for the whole world
WHOIS	database including domain name registrant technical, billing, and administrative contact information
ZOOÚ	current personal data protection legislation

2 PUBLICATION AND REPOSITORY RESPONSIBILITIES

2.1 Repositories

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

2.2 Publication of certification information

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

- address of the company's registered office:

  První certifikační autorita, a.s.

  Podvinný mlýn 2178/6

  190 00 Praha 9

  Česká republika
- website: http://www.ica.cz;
- registered offices of the registration authorities.

Electronic address for contact between the public and I.CA are ssl@ica.cz and info@ica.cz, I.CA's data box ID is a69fvfb.

The aforesaid website provides information about:

- Certificates – the following information is published (and more information can be obtained from the Certificate):
  - Certificate number;
  - Content of commonName;
  - Valid from date (specifying the hour, minute and second) ;
  - Link to where the certificate can be obtained in the specified format (DER, PEM, TXT).
- certificate revocation lists (CRL) – the following information is published (and more information can be obtained from the CRL):
  - Date of CRL release;
  - CRL number;
  - Links to where the CRL can be obtained in the specified formats (DER, PEM and TXT).
- certification and other policies and implementing regulations, certificates issued or revoked and other public information.

Http and https are the permitted protocols for access to public information. I.CA may terminate or suspend access to some information without cause.

Any revocation of a certificate employed in issuing certificates to end users, a release of certificate revocation list, and the provision of certificate status information (also as Infrastructure Certificates) because of suspected or actual compromise of a given private key will be announced by I.CA on its web Information Address and in a daily newspaper with national distribution – Hospodářské noviny or Mladá fronta Dnes.

There is website at https://test-evssl.ica.cz on which I.CA allows independent application software vendors to test their software with the various Certificates states.

2.3 Time or frequency of publication

I.CA publishes information with the following periodicity:

- Certification policy - after approval and release of the new version; the update depending on changes required by EVCG or BRG, or check at least one time a year;
- Certification practice statement - immediately (if intended for publication);
- List of issued certificates - updates every time a new certificate is issued;
- Certificate revocation list (CRLs) - see chapter 4.9.7;
- Information about revocation of the Infrastructure Certificate, stating the reason for revocation - without delay;
- Other public information - not predetermined, but generally this information must reflect the current status of the certification services provided.

2.4 Access controls on repositories

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

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

3 IDENTIFICATION AND AUTHENTICATION

3.1 Naming

3.1.1 Types of names

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

3.1.2 Need for names to be meaningful

For a Certificate to be issued all names which can be validated given in the attributes of the subject field and/or subjectAlternativeName extension must carry a meaning. See chapter 7 for the attributes supported for these field and extension.

3.1.3 Anonymity or pseudonymity of subscribers

Certificates issued under this CP do not support anonymity neither the use of a pseudonym.

3.1.4 Rules for interpreting various name forms

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

3.1.5 Uniqueness of names

The Authority guarantees that the subject field in a Certificate of this Certificate's subscriber is unique.

3.1.6 Recognition, authentication, and role of trademarks

The Certificates issued under this CP may also specify trade names (trademarks given as text) in subject.organizationName. The information must be validated by either of the following ways:

- In a register maintained by a government agency (for the Czech Republic, it is the Czech Industrial Property Office), in person, by post, e-mail, phone or from the agency's website;
- From independent competent information source created for providing information on trademarks if the information source has validated the trademark with the relevant government agency.

The following information is subject to validation:

- Whether the applicant has registered the use of the trademark with the relevant government agency in the jurisdiction for the registered and validated registered office of the organization;

- Whether the registration is valid (and shows no validity expiration date).

The Authority may rely on a notary certification that certifies the trade name, the agency which registered the trade name and the fact that the entry in the register is currently valid (and shows no validity expiration date).

3.2 Initial identity validation

The entities authorized to apply for a Certificate are listed in 4.1.1. The following chapters specify the rules for the initial validation of their identity; specific procedures are detailed in internal documentation. The validation procedure complies with *CA/Browser Forum – Guidelines for the Issuance and Management of Extended Validation Certificates*, that is, among other things:

- Validation is carried out by a validation specialist and cross-checked by another validation specialist;
- All the information acquired and the evidence gained during application validation is kept on file and each has a validity expiration date shown.

A legal opinion will be requested for specific cases to resolve any ambiguity in the interpretation of the said standard and internal documentation rules resulting from it.

3.2.1 Method to prove possession of private key

The ownership of the private key matching the public key in the Certificate application must be proved by submitting the application in the PKCS#10 format. The application is electronically signed with this private key and this way the subscriber provides evidence that he is the owner of the private key when the electronic signature is created.

3.2.2 Authentication of organization identity

The procedure is described in the following chapters.

3.2.2.1 Legal identity and organization existence

Authentication requirements are based on the organization category. Four organization categories exist:

- Private organization, i.e. company filed in the Czech Trade Register (the Register), entered or registered under a law or created by a government agency;
- Government entity;
- Entities entered in a register other than the Register, i.e. those registered by a registration agency (granting and verifying business licenses), the registration of which can be verified (business entities);
- International organizations created under treaties signed by multiple national governments (non-commercial entities).

The procedure to authenticate these organization types is described in internal documentation.

3.2.2.2 Validation of physical existence

The Authority validates whether the physical address provided by the applicant (the application attributes: subject.streetAddress, localityName, stateOrProvinceName, postalCode, and countryName) is the address where the applicant or his parent or subsidiary company physically exists and does business and is not just a P.O. box or an address of the company's representative.

3.2.2.3 Validation of applicant's operational existence

The Authority validates whether the applicant is able to do business by checking operational existence. Only legal identity and existence is validated in respect of government entities; any other entity is validated for the following:

- Data in the register of companies or the data of the registration agency show that the entity has existed for a minimum of three years;
- Entity is listed in the current QIIS or QTIS register (the financial administration's list of taxable entities);
- Entity holds an active (current or deposit) account with a financial institution subject to the national bank's supervision:
  - By getting the proof of the account from the financial institution; or
  - Through a notary certification certifying that the entity holds an active current account with a financial institution subject to the national bank's supervision.

3.2.2.4 Validation of required DNS names

For each domain (DNS, FQDN) name which is to be specified in the Certificate, the Authority must check whether, as at the Certificate issuance date, the applicant:

- Is the registrant (owner) of the domain name; or
- Has control over the domain name.

Specific validation procedure is described in internal documentation and is based on BRG (referenced from EVCG) requirements.

I.CA does not support domain names:

- With TLD .onion;
- Using mixed byte-character set (i.e. Internationalized Domain Names);
- Containing underscore character.

Note 1: Other limitations of dNSName are given in Certificate profile in 7.1.2.

Note 2: All DNS names, both in commonName and subjectAlternativeName.dnsName, must be public.

3.2.2.5 CAA records check

I.CA checks in DNS whether for domains contained in application Certification Authority Authorization Resource Records (according to RFC 6844, abbreviation CAA records) exist. CAA records specify certification authorities which exclusively can issue SSL certificates for given domain.

Because I.CA does not issue Certificates containing wild cards in DNS names only CAA records containing sign "**issue**" are considered; CAA records containing sign "**issuewild**" are disregarded.

In compliance with RFC 6844 updated by Errata 5065 for every domain contained in application the DNS tree is searched from verified domain up to the top until finding first set of CAA records for:

- Domain or some target of its CNAME or DNAME alias string; or
- For some superior domain or its alias;

until reaching TLD (in this case CAA records set stays empty).

Alias strings are checked to the depth of eight records.

Detailed description is in RFC 6844, chapter 4 updated by Errata 5065 in compliance with BRG.

I.CA carries out first check and:

- If the set of CAA records is found then it waits the amount of time which is maximum of TTL CAA record time and 8 hours;
- If no CA record exists then it waits 8 hours;

and then the repeated check is carried out.

Next steps of application validation and Certificate issuance will be performed only if the repeated check found:

- That no CAA record exists; or
- The set of CAA records was found; and
  - No CAA record of the set contains an unknown sign and is simultaneously marked as critical; and
  - The set of CAA records containing the sign **"issue"** is empty or some of these records contains the string „"ca.cz“.

In an opposite case the application in rejected.

3.2.2.6 Additional validation requirements

In addition to as given above, the following is also subject to validation:

- Whether the DNS name has been rejected because of suspected phishing or fraud or has been part of any Certificate revoked by the Authority for the said reason;
- Whether the DNS name is on the list of phishing sites;
- Whether the person applying for the Certificate, the person approving Certificate data, the country of entry, the country of registration or the place of business is on any government list of bans or undesirable persons or a list prohibiting any trade with such a country or Organization.

Procedures are detailed in internal documentation.

3.2.3 Authentication of individual identity

Two documents, a primary and a secondary document showing the information as given below, must be presented for authenticating the individual's identity in personal contact for private organizations and government entities.

- Valid personal identity card or passport must be used as the primary personal document for the citizens of the Czech Republic. Valid passport is the primary personal document for foreigners; citizens of EU member countries may use their valid personal identity card they use in their country as the proof of their identity. The following data are verified in this document:
  - Full civil name;
  - Date and place of birth or the birth identification number if shown in the primary document;
  - Number of the primary personal document;
  - Permanent address (if shown in the primary document).
- The secondary document must contain a unique identification, such as birth identification number or personal identity card number, matching it to the primary document and must show at least one of these items:
  - Date of birth (or birth identification number if specified);
  - Permanent address;
  - Photograph of the face.

  The secondary personal document data uniquely identifying persons representing the Organization must be identical to those in the primary personal document.

The following documents must be presented to authorize the individual's identity in personal contact for business entities:

- Personal statement containing:
  - Full name;
  - Permanent (or temporary) address;
  - Date of birth;
  - Statement that all the information given in the Certificate application is true and correct;
- Valid identification card issued by the country's authority, with the person's photograph and signature, such as:
  - Personal identity card;
  - Passport;
- No fewer than two secondary proofs of the person's identity showing the name of the person (one of them must be from a financial institution):
  - Driving license;
  - Accepted documents from a financial institution are:
    - Valid credit card from a financial institution subject to the national bank's supervision;

  - Valid debit card from a financial institution subject to the national bank's supervision;
  - Mortgage account statement from, which is dated no more than six months ago;
  - Bank account statement from a financial institution subject to the national bank's supervision, which is dated no more than six months ago;
- Accepted documents from a different institution are:
  - Original copy of the latest utility bill (not a phone bill) confirming utility supply to the person's address of residence;
  - Copy of rent charge dated no more than six months ago;
  - Certified copy of birth certificate;
  - Tax authority's tax assessment for the current year;
  - Certified copy of a judicial decision, such as a divorce judgment or an adoption decision;
  - Valid identification card issued by state administration, other than the primary document and showing the person's name.

Individuals must attend the authentication procedure because a notary certificate is required that the authentication procedure has been carried out. The authentication procedure along with the notary certification procedure is detailed in internal documentation.

3.2.4 Non-verified subscriber information

Not applicable to this document – all information must be duly verified.

3.2.5 Validation of authority

The following is subject to validation in the procedures related to making the contract, filing the Certificate application and issuing the Certificate:

- Reliable method of communication with the applicant, i.e. contact address, phone number, e-mail address;
- The authorization of the person executing the Certificate issuance contract and the person approving the data in the Certificate;
- Certified signature on the contract with the Certificate subscriber;
- Validation of Certificate application approval.

The specific procedures are described in internal documentation.

3.2.6 Criteria for interoperation

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

3.3 Identification and authentication for re-key requests

3.3.1 Identification and authentication for routine re-key

A new Certificate with a new public key needs to be issued. Before issuing I.CA must perform complete validation procedure. If the validation documentation was used for previous validation it is checked whether maximum period of applicability was not exceeded.

For Certificates issued since 1.8.2018 the information about ownership of domain name or control over domain name will not be used if it was collected by methods which are not allowed by BRG ever since:

- Using information contained in WHOIS register operated by organization administering TLD /ccTLD;
- Using domain authorization document (method #5).

3.3.2 Identification and authentication for re-key after revocation

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

3.4 Identification and authentication for revocation request

Acceptable ways of identification and authorization are as follows:

- Using the form on the company's website (and using the Certificate revocation password);
- Using an unsigned e-mail containing the Certificate revocation password and sent to ssl@ica.cz;
- Using a signed e-mail (the electronic signature must be created with the private key belonging to the Certificate to be revoked) and sent to ssl@ica.cz;
- Using the I.CA's data box (and using the Certificate revocation password);
- Using registered letter sent to address of the company's registered office and containing the Certificate revocation password;
- Using a defined person assigned to represent the Organization in the contractual relation with I.CA.

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

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

4 CERTIFICATE LIFE-CYCLE OPERATIONAL REQUIREMENTS

4.1 Certificate Application

4.1.1 Who can submit a certificate application

Certificates are issued to Organizations having contract with První certifikační autorita, a.s. – see 1.3.3.

I.CA keeps records about applications previously rejected because of phishing or fraud suspicion and about Certificates been revoked due to these reasons. These records are used when processing subsequently submitted applications.

4.1.2 Enrollment process and responsibilities

Before submission of an application the applicant must make a contract with První certifikační autorita, a.s., where the conditions of usage the Certificate are defined.

After it representative of the applicant can send an e-mail to ssl@ica.cz containing the Certificate application (PKCS#10) and declaration that all pieces of information contained in the application are true.

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

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

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

- Inform the subscriber or the Organization about the terms and conditions prior to executing the Certificate issuance contract;
- Conclude with subscriber or the Organization, such a Certificate issuance contract that meets the requirements imposed by valid trust services legislation and technical and other standards;
- During the Certificate issuance process, check with RA all the data which can be validated specified in the application against the documents submitted;
- Require a proof of QSCD private key generation if the private key is QSCD-generated;
- Issue a Certificate that contains materially correct data on the basis of the information available to the Service provider as at the issuance of the Certificate;
- Publish public information in accordance with 2.2;
- Publish the Authority's certificates and the root CA's certificates;

- Provide any Service-related activity in accordance with current trust services legislation, this CP, the relevant CPS, the System Security Policy of CA and TSA, and the operating documentation.

4.2 Certificate application processing

4.2.1 Performing identification and authentication functions

When processing application it is:

- Checked origin of application;
- Proved ownership of private key;
- Validated identity of the Organization;
- Checked whether application contains identification (Internet address) of device;
- Validated the permission to use second level domain name.

Before authorizing the application RA validates:

- Records of applications rejected previously because of phishing or fraud suspicion and records of Certificates revoked by I.CA due to same reasons – see 4.1.1;
- Required domain name in relation to the list of phishing websites;
- Other internal criteria to detect fraudulent applications;
- DNS for existence and content of CAA records for domains indicated in Certificate application - see 3.2.2.5.

For other entries validation (for the same subscriber and the same domain) I.CA may use information obtained when previous validation was carried out, if such information is not older than 13 months. In another cases the procedure described in chapter 3.2.2 is used.

4.2.2 Approval or rejection of certificate applications

I.CA doesn't issue certificates for gTLD domains. If some of validations and checks – see 4.2.1 - is not successful then issuing of the Certificate is terminated. In the opposite case RA employee authorizes issuing the Certificate.

4.2.3 Time to process certificate applications

If all items of application are validated the Certificate will be issued within five working days.

4.3 Certificate issuance

4.3.1 CA actions during certificate issuance

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

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

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

Issuing of the Certificate is executed after willful commanding to sign issued Certificate by Operator.

4.3.2 Notification to subscriber by the CA of issuance of certificate

Issued Certificate is always sent to the contact e-mail provided during registration as mandatory data.

4.4 Certificate acceptance

4.4.1 Conduct constituting certificate acceptance

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

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

4.4.2 Publication of the certificate by the CA

I.CA has to publish every Certificate it issues, except any Certificate:

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

4.4.3 Notification of certificate issuance by the CA to other entities

Notification of certificate issuance gets the subscriber only.

4.5 Key pair and certificate usage

4.5.1 Subscriber private key and certificate usage

Subscriber must, among other things:

- Observe all relevant provisions of the contract of the provision of this Service;

- Use the private key and the corresponding certificate issued under this CP solely for the purposes defined in this CP;
- Handle the private key corresponding to the public key contained in the Certificate issued under a this CP in a manner as to prevent any unauthorized use of the private key;
- Inform immediately the Service provider of everything that leads to the Certificate's revocation, in particular of:
  - Suspected abuse of the private key, apply for the Certificate's revocation and stop using the pertinent private key;
  - Invalidity or inaccuracy of entries in Certificate.

4.5.2 Relying party public key and certificate usage

Relying parties must, among other things:

- Obtain, from a secure source, the certification authority certificates related to the end user certificate issued under a specific CP, and verify those certificates' fingerprint values and validity;
- Carry out any operation necessary for them to verify that the certificate is valid;
- Abide by any provision of this CP and current legislation and technical standards which relate to the relying party's duties.

4.6 Certificate renewal

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

The certificate renewal service is not provided.

4.6.1 Circumstance for certificate renewal

See 4.6.

4.6.2 Who may request renewal

See 4.6.

4.6.3 Processing certificate renewal requests

See 4.6.

4.6.4 Notification of new certificate issuance to subscriber

See 4.6.

4.6.5 Conduct constituting acceptance of a renewal certificate

See 4.6.

4.6.6 Publication of the renewal certificate by the CA

See 4.6.

4.6.7 Notification of certificate issuance by the CA to other entities

See 4.6.

4.7 Certificate re-key

The certificate re-key service means the issuance of a Certificate with new public key without changing any other information in the Certificate. Requirements on 3.3.1 and from 4.1 to 4.4 are valid.

4.7.1 Circumstance for certificate re-key

See 4.7.

4.7.2 Who may request certification of a new public key

See 4.7.

4.7.3 Processing certificate re-keying requests

See 4.7.

4.7.4 Notification of new certificate issuance to subscriber

See 4.7.

4.7.5 Conduct constituting acceptance of a re-keyed certificate

See 4.7.

4.7.6 Publication of the re-keyed certificate by the CA

See 4.7.

4.7.7 Notification of certificate issuance by the CA to other entities

See 4.7.

4.8 Certificate modification

The certificate modification service means the issuance of a subsequent Certificate with:

- At least one change of entries in subject field or subjectAlternativeName extension concerning the subscriber; or
- With removed field; or
- With added field, which content must be validated.

The certificate modification service is not provided.

4.8.1 Circumstance for certificate modification

See 4.8.

4.8.2 Who may request certificate modification

See 4.8.

4.8.3 Processing certificate modification requests

See 4.8.

4.8.4 Notification of new certificate issuance to subscriber

See 4.8.

4.8.5 Conduct constituting acceptance of modified certificate

See 4.8.

4.8.6 Publication of the modified certificate by the CA

See 4.8.

4.8.7 Notification of certificate issuance by the CA to other entities

See 4.8.

4.9 Certificate revocation and suspension

Certificate revocation requests are accepted irrespective of the time of the day if submitted electronically or by post.

I.CA does not provide certificate suspension.

4.9.1 Circumstances for revocation

4.9.1.1 Certificate revocation reasons

I.CA revokes the Certificate within 24 hours if one or more of the following reasons occurs:

1. Subscriber submitted the Certificate revocation request in writing;
2. Subscriber notified the certification authority that the original Certification application had been unauthorized and he won't grant retrospective authorization;
3. I.CA obtains evidence that Subscriber's private key corresponding to the Certificate's public key has been compromised;
4. I.CA obtains evidence that the method for domain ownership validation (see 3.2.2.4) used for validation of FQDN contained in issued Certificate is no more reliable.

I.CA revokes the Certificate within five days if one or more of the following reasons occur:

1. Certificate does not meet the requirements for cryptographic algorithms and their parameters (quality, see 6.1.5 and 6.1.6);
2. I.CA obtains evidence that the Certificate has been misused;
3. I.CA is notified that the Certificate subscriber has breached any of his important obligations resulting from the Certificate issuance contract or the contract of the terms and conditions for using the Certificate;
4. I.CA is notified of circumstances indicating that the fully qualified domain name (FQDN) or the IP address specified in the certificate is no longer permitted by law (i.e. a court or an arbitration has deprived the registrant the right to use the domain name, cancelled the relevant contract or agreement, the license or service agreement between the domain name registrant and the certificate applicant has been cancelled or the domain name registrant failed to renew the domain name);
5. I.CA is notified of important changes to information contained in the Certificate;
6. I.CA is notified that the Certificate was not issued in compliance with CP or CPS.
7. I.CA finds out that some information contained in the Certificate is inaccurate or misleading;
8. I.CA's authorization to issue Certificate under this CP expired, was revocated or terminated and I.CA did not make arrangement how to maintain CRL/OCSP repository;
9. Revocation is required by CP or CPS;
10. I.CA is notified of:
    - □ Demonstrated or proven method to compromise Certificate subscriber's private key that allows to find this private key out when knowing public key contained in the Certificate (e.g. Debian Weak Key);
    - □ Clear evidence that the method used for private key generation contained a mistake.

4.9.1.2 Reasons to revoke the Authority's certificate

I.CA revokes the Authority's certificate within seven days in any of the following events:

1. Authority requests revocation in writing;

2. Authority reported to root certification authority that original Certification application had been unauthorized and it won't grant retrospective authorization;
3. Authority's private key has been compromised or no longer meets the cryptographic algorithm requirements and the required parameters (quality, see 6.1.5 and 6.1.6);
4. Authority's certificate was misused;
5. Root certification authority is notified that Authority's certificate:
   - □ Was not issued in compliance with corresponding CP or CPS; or
   - □ Does not meet requirements of corresponding CP or CPS;
6. I.CA finds out that some information contained in the Authority's certificate is inaccurate or misleading;
7. Root CA or Authority terminated their operation due to some reasons a did not transferred support of revocation to any other CA;
8. Root CA's or Authority's authorization to issue Certificate under this CP expired, was revocated or terminated and root CA did not make arrangement how to maintain CRL/OCSP repository;
9. Revocation is required by CP or CPS of root certification authority.

4.9.2 Who can request revocation

Revocation request may be submitted by:

- Subscriber;
- The entity explicitly specified therefore in the contract of providing the Service under this CP;
- Provider of this Service (CEO of I.CA is the person entitled to request for the revocation of a certificate issued by I.CA):
  - □ If the Certificate is issued on the basis of false data;
  - □ If CEO demonstrably establishes that the private key belonging to the public key specified in the Certificate has been compromised;
  - □ If CEO establishes that the Certificate is issued in spite of the failure to meet the requirements of current trust services legislation;
  - □ If CEO demonstrably establishes that the Certificate was used contrary to the restrictions defined in 1.4.2;
  - □ If the public key in the Certificate application is the same as the public key in a certificate already issued;

Having filled a Certification revocation request, the subscriber must immediately stop using the Certificate along with the corresponding private key.

Subscribers, relying parties, application SW suppliers and other third parties can send reports about problems with Certificates to inform Authority about sufficient reasons for revoking Certificate - see 4.9.3.2.

4.9.3 Procedure for revocation request

4.9.3.1 Revocation request made by subscriber

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

- Using the form on the information web page http://www.ica.cz. The Certificate revocation date and time are the date and time a valid Certificate revocation request is dealt with in the CA's information system. The applicant receives a notice if the application is carried out;
- Electronically signed e-mail – body must contain text (in Czech or Slovak with or without diacritics, or in English):

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

  where '*xxxxxxx*' is the Certificate's serial number and must be given in the decimal or hexadecimal format (introduced by the string '0x');
- Electronically unsigned e-mail - body must contain text (in Czech or Slovak with or without diacritics, or in English):

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

  Heslo pro zneplatneni = yyyyyy. [Revocation password = yyyyyy.],
- where '*xxxxxxx*' is the Certificate's serial number and '*yyyyyy*' the revocation password. The Certificate's serial number must be given in the decimal or hexadecimal format (introduced by the string '0x').

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

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

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

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

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

4.9.3.2 Suspected key compromise and abuse of Certificate

Suspected compromise of a private key (to the relevant Certificate), Certificate abuse or other types of fraud, compromise, abuse or misconduct connected with an issued Certificate may be reported by e-mail to ssl@ica.cz, by registered post or data box.

4.9.4 Revocation request grace period

Not applicable to this document; the revocation request grace period service is not provided.

4.9.5 Time within which CA must process the revocation request

4.9.5.1 Certificate revocation requested by subscriber

Any Certificate revocation request made by the subscriber is carried out immediately after the receipt of authorized revocation request. The CRL containing the serial number of the revoked Certificate is issued immediately after that Certificate's revocation.

4.9.5.2 Reporting certificate troubles

Within 24 hours after being reported the Certificate problem I.CA examines facts and circumstances and puts out the preliminary statement to Certificate's subscriber and to the person who reported the problem.

I.CA decides in cooperation with Certificate's subscriber and the person who reported the problem whether Certification revocation is necessary. If it is then the date of revocation will be determined depending on these criteria:

- Nature of the suspected issue;
- Impacts of revocation (both for subscriber and relying parties);
- Number of reported Certificate troubles concerning a specific Certificate or a subscriber;
- Who complains: for instance, a report from a law-enforcing organization that a site is engaged in illegal activities takes precedence over a customer's complaint about not receiving the goods ordered;
- Relevant legislation.

Period of publishing the revocation must not exceed interval stated in chapter 4.9.1.

4.9.6 Revocation checking requirement for relying parties

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

4.9.7 CRL issuance frequency (if applicable)

4.9.7.1 Certificate status

The certification revocation list (CRL) of the authority issuing Certificates is released:

- Immediately after a Certificate revocation request is carried out; and

- Within 24 hours of the release of the previous CRL

4.9.7.2 Status of the certificate of the CA issuing certificates

The CRL of the root CA is released:

- Within 24 hours of the revocation of the certificate of the CA issuing Certificates; and
- Every year or in a shorter interval.

The maximum validity of a CRL is twelve months.

4.9.8 Maximum latency for CRLs (if applicable)

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

4.9.9 On-line revocation/status checking availability

Checking certificate status online using the OCSP protocol is a service available to the general public. Every certificate issued under this CP includes a link to the pertinent OCSP responder.

OCSP responses satisfy the RFC 2560 and RFC 5019 standards. The OCSP responder's certificate includes an id-pkix-ocsp-nocheck extension as defined in RFC 6960.

4.9.10 On-line revocation checking requirements

OCSP allows checking requirements using GET method. OCSP responses concerning certificates which were not issued do not return good status.

4.9.10.1 Certificate status

I.CA updates the information returned by OCSP at least every four days. OCSP responses are valid no more than ten days.

4.9.10.2 CA issuing Certificates certificate status

I.CA updates the information returned by OCSP:

- No later than 24 hours after revocation of the CA issuing Certificates; and
- No later than every twelve months.

4.9.11 Other forms of revocation advertisements available

I.CA contractually obligates web server Certificate subscribers to configure servers for OCSP stapling pursuant to RFC 4366 for the distribution of OCSP responses.

4.9.12 Special requirements re key compromise

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

4.9.13 Circumstances for suspension

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

4.9.14 Who can request suspension

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

4.9.15 Procedure for suspension request

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

4.9.16 Limits on suspension period

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

4.10 Certificate status services

4.10.1 Operational characteristics

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

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

4.10.2 Service availability

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

Response time of Certificate status request using CRL or OCSP is usually less than 10 second.

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

Continuous availability 24x7 is ensured via e-mail address ssl@ica.cz, company's data box and registered letters. Due to this I.CA can internally react to serious problem report and, if necessary, to resend this report to relevant body or to revoke the Certificate which is subject of the report.

4.10.3 Optional features

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

4.11 End of subscription

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

4.12 Key escrow and recovery

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

4.12.1 Key escrow and recovery policy and practices

See 4.12.

4.12.2 Session key encapsulation and recovery policy and practices

See 4.12.

5 FACILITY, MANEGEMENT, AND OPERATIONAL CONTROLS

Facility, management, and operational controls primarily deal with:

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

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

5.1 Physical controls

5.1.1 Site location and construction

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

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

5.1.2 Physical access

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

5.1.3 Power and air conditioning

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

5.1.4 Water exposures

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

5.1.5 Fire prevention and protection

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

5.1.6 Media storage

Storage media containing operational backups and electronic records are stored in metal boxes or safes. Copies are kept at a site geographically different from the site of the operating office.

Any paper media required by current trust services legislation to be kept are stored at a site geographically different from the site of the operating office.

5.1.7 Waste disposal

Any paper office waste is shredded before it leaves I.CA operating sites.

5.1.8 Off-site backup

The copies of operating and working backups are stored at a place designated by the COO of I.CA and described in internal documentation.

5.2 Procedural controls

5.2.1 Trusted roles

Trusted roles are defined for selected activities carried out at I.CA. The trusted role employee appointment procedure, the trusted roles and their responsibilities are defined in internal documentation.

Validating information contained in Certificate application and authorizing Certificate issuance are performed by two trustworthy persons in the roles Validation Specialist and Cross-Correlation specialist. Their operation is described in internal documentation.

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

5.2.2 Number of persons required per task

Processes related to key pair of certifications authorities and OCSP responders are defined as activities which must be carried out with the participation of more than one person. These include in particular:

- Initializing cryptographic module;
- Generating key pair of any certification authority and of the OCSP responder of the root certification authority;

- Destroying the private keys of any certification authority and of the OCSP responder of the root certification authority;
- Making backups of the private keys of certification authorities (including the root certification authority), which issue qualified certificates to end users;
- Recovering the private keys of all certification authorities and their OCSP responders;
- Activating and deactivating the private keys of any certification authority and of the OCSP responder of the root certification authority.

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

5.2.3 Identification and authentication for each role

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

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

5.2.4 Roles requiring separation of duties

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

5.3 Personnel controls

5.3.1 Qualifications, experience, and clearance requirements

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

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

Any other I.CA employee taking part in providing trust services is accepted using the following criteria:

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

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

5.3.2 Background check procedures

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

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

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

5.3.3 Training requirements

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

5.3.4 Retraining frequency and requirements

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

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

5.3.5 Job rotation frequency and sequence

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

5.3.6 Sanctions for unauthorized actions

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

5.3.7 Independent contractor requirements

I.CA may or must procure some activities from independent contractors, and is fully liable for the job they deliver. These business relations are regulated in bilateral business contracts with parties such as contracted registration authorities, application software developers, hardware suppliers, system software suppliers, external auditors and other parties. These parties are required to observe the appropriate certification policies, the relevant parts of internal documentation provided for them, and the required normative documents. Contractual penalties are demanded for a breach of the obligations or duties specified in the said documents, or the contract with the contractor in breach is terminated immediately.

5.3.8 Documentation supplied to personnel

In addition to the certification policy, the certificate practice statement and the security and operating documentation, I.CA employees have available any other relevant standard, policy, manual and guidance they may need for their job.

5.4 Audit logging procedures

5.4.1 Types of events recorded

Subject to logging are all the events required by current trust services legislation or the relevant technical and other standards to be logged, that is, for example, the life cycle events for the Certificates, the certificates of the Authority and the root CA and their respective OCSP responders.

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

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

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

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

5.4.2 Frequency of processing log

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

5.4.3 Retention period for audit log

Unless the relevant legislation provides otherwise, audit records are kept for a minimum of 10 years of the day they are made.

5.4.4 Protection of audit log

Both electronic and printed audit records are stored in a manner ensuring they are protected against change, theft and destruction (willful or accidental).

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

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

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

5.4.5 Audit log backup procedures

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

5.4.6 Audit collection system (internal vs. external)

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

5.4.7 Notification to event-causing subject

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

5.4.8 Vulnerability assessments

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

5.5 Records archival

The storage of records, i.e. information and documentation performs První certifikační autorita, a.s. according to internal documentation.

5.5.1 Types of records archived

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

- Life cycle records for the Certificates issued, the Certificates issued and the certificates elated thereto;
- Video recordings, if any, of the generation of data pair of a certification Authority;
- Other records that may be necessary for issuing Certificates;
- Information handling records, such as takeover, handover, saving, check, conversion from printed to electronic, etc.;
- Application software, operating and security documentation.

5.5.2 Retention period for archive

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

The record storage procedures are regulated in internal documentation.

5.5.3 Protection of archive

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

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

5.5.4 Archive backup procedures

The record backup procedures are regulated in internal documentation.

5.5.5 Requirements for time-stamping of records

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

5.5.6 Archive collection system (internal or external)

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

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

5.5.7 Procedures to obtain and verify archive information

Stored information and records are located in designated locations and are accessible to:

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

A written record is made of any such permitted access.

5.6 Key changeover

In standard situations (expiration of a certificate authority's certificate), the key is replaced by issuing a new certificate a good time in advance (no later than one year prior to the expiration). In non-standard situations, for instance such developments in cryptanalytic methods that could compromise the security of certificate issuance (e.g. changes to cryptanalytic algorithms or key length), the key is replaced as soon as possible.

In both standard and non-standard situations, the replacement of the public key in certificate authority certificates is suitably notified to the public a good time in advance (if practicable).

5.7 Compromise and disaster recovery

5.7.1 Incident and compromise handling procedures

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

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

See 5.7.1.

5.7.3 Entity private key compromise procedures

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

- Stops using the private key;
- Revokes immediately and permanently the pertinent certificate and destroys the corresponding private key;
- Revokes all relevant valid certificates;
- Without delay about this fact, including the reason, informs in accordance with 2.2, the relevant list of invalidated certificates shall also be used to make this information available;
- Notifies the supervisory body of that the pertinent certificate has been revoked and why it has been revoked.

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

5.7.4 Business continuity capabilities after a disaster

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

5.8 CA or RA termination

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

- The discontinuance of the Authority's operations must be notified in writing to the supervisory body, all subscribers of valid Certificates, and the parties having a contract with I.CA that directly concerns the provision of trust services;
- The termination of the Authority's operations must published on the web page pursuant to 2.2;
- If the Authority's certificate's expiration is part of the discontinuance of operations, this information plus the reason for expiration must be included in that notice;
- The termination of operations is a controlled process following a pre-defined plan, which includes the description of the procedure to preserve and disclose information for judicial or administrative proceedings discovery and for arranging the continuity of services;
- The Authority or its successor must be able to revoke Certificates and publish CRLs as long as any Certificate issued by the Authority is valid;
- After that the Authority must demonstrably destroy its private key, make a record of this destruction and keep this record in accordance with this CP.

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

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

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

6 TECHICAL SECURITY CONTROLS

6.1 Key pair generation and installation

6.1.1 Key pair generation

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

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

Key pairs related to Certificates issued under this CP are generated on devices which are under sole control of the respective private key owners. These key pairs may be stored on hardware and in software.

6.1.2 Private key delivery to subscriber

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

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

6.1.3 Public key delivery to certificate issuer

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

6.1.4 CA public key delivery to relying parties

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

- Via RA;
- Via I.CA's web Information Addresses;
- Each applicant will receive an Authority certificate when obtaining the Certificate.

6.1.5 Key sizes

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

certificates issued by that root authority is 2048 bits. The minimum size of the keys in the Certificates issued under this CP is 2048 bits.

6.1.6 Public key parameters generation and quality checking

The parameters of the algorithms used in generating the public keys of certification authorities and their OCSP responder meet the requirements listed in current trust services legislation and the technical and other standards referred to therein.

For the RSA algorithm, the Authority must verify that the value of the public exponent is an odd number equal to three or more (at the same time it is recommended to be in the range $2^{16}+1$ to $2^{256}+1$).

Parameters of algorithms used to generate end-user public keys must also meet these requirements.

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

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

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

6.2 Private Key Protection and Cryptographic Module Engineering Controls

6.2.1 Cryptographic module standards and controls

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

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

If cryptographic module related operations require the presence of two I.CA management members, then each member only has knowledge of some part of the code required for these operations.

6.2.3 Private key escrow

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

6.2.4 Private key backup

The cryptographic module used for the administration of certificate authority and their OCSP responder key pairs allows private keys backup. Private keys are backed up using the native features of the cryptographic module in the encrypted form.

6.2.5 Private key archival

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

6.2.6 Private key transfer into or from a cryptographic module

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

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

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

Every actual transfer is documented in a written record.

6.2.7 Private key storage on cryptographic module

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

6.2.8 Method of activating private key

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

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

6.2.9 Method of deactivating private key

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

The private keys of OCSP responders of other certification authorities saved in the cryptographic module are deactivated under direct personal participation of a single I.CA

management member with the use of an activation chip card and pursuant to a strictly defined procedure described in internal documentation. Every actual deactivation is documented in a written record.

6.2.10 Method of destroying private key

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

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

6.2.11 Cryptographic module rating

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

6.3 Other aspects of key pair management

6.3.1 Public key archival

The public keys as part of certificates are stored throughout the existence of I.CA.

6.3.2 Certificate operational periods and key pair usage periods

The maximum period of validity of each Certificate issued is specified in the body of that Certificate.

6.4 Activation data

6.4.1 Activation data generation and installation

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

6.4.2 Activation data protection

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

6.4.3 Other aspects of activation data

The activation data of Authority and its OCSP responder must not be transferred or kept in an open form. All aspects are described in internal documentation.

6.5 Computer security controls

6.5.1 Specific computer security technical requirements

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

6.5.2 Computer security rating

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

- CEN/TS 419261 Security requirements for trustworthy systems managing certificates and time-stamps;
- ČSN ETSI EN 319 401 Electronic Signatures and Infrastructures (ESI) – Policy and Security Requirements for Trust Service Providers;
- ETSI EN 319 401 Electronic Signatures and Infrastructures (ESI); General Policy Requirements for Trust Service Providers;
- ČSN ETSI EN 319 403 Electronic Signatures and Infrastructures (ESI) – Trust Service Provider Conformity Assessment – Requirements for Conformity Assessment Bodies Assessing Trust Service Providers;
- ETSI EN 319 403 Electronic Signatures and Infrastructures (ESI); Trust Service Provider Conformity Assessment - Requirements for conformity assessment bodies assessing Trust Service Providers;
- ČSN ETSI EN 319 411-1 Electronic Signatures and Infrastructures (ESI) – Policy and Security Requirements for Trust Service Providers Issuing Certificates – Part 1: General Requirements;
- ETSI EN 319 411-1 Electronic Signatures and Infrastructures (ESI); Policy and security requirements for Trust Service Providers issuing certificates; Part 1: General requirements;
- ČSN ETSI EN 319 411-2 Electronic Signatures and Infrastructures (ESI) – Policy and Security Requirements for Trust Service Providers Issuing Certificates – Part 2: Requirements for Trust Service Providers Issuing EU Qualified Certificates;
- ETSI EN 319 411-2 Electronic Signatures and Infrastructures (ESI); Policy and security requirements for Trust Service Providers issuing certificates; Part 2: Requirements for trust service providers issuing EU qualified certificates;
- ETSI TS 119 312 Electronic Signatures and Infrastructures (ESI); Cryptographic Suites;
- CA/Browser Forum - Baseline Requirements for the Issuance and Management of Publicly-Trusted Certificates (Baseline Requirements);

- CA/Browser Forum - Guidelines for The Issuance and Management of Extended Validation Certificates;
- ČSN ISO/IEC 27006 Information Technology – Security Techniques – Requirements for Bodies Providing Audit and Certification of Information Security Management Systems;
- ISO/IEC 17021 Conformity assessment -- Requirements for bodies providing audit and certification of management systems;
- ISO/IEC 17065 Conformity assessment -- Requirements for bodies certifying products, processes and services;

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

- FIPS PUB 140-2 Requirements for Cryptographic Modules;
- ISO 3166-1 Codes for the representation of names of countries and their subdivisions -- Part 1: Country codes;
- ITU-T - X.501 Information technology – Open Systems Interconnection – The Directory: Models;
- ITU-T - X.509 Information technology – Open Systems Interconnection – The Directory: Public-key and attribute certificate frameworks;
- ITU-T - X.520 Information technology – Open Systems Interconnection – The Directory: Selected attribute types;
- RSA Laboratories - PKCS#10: Certification Request Syntax Standard;
- RFC 2560 X.509 Internet Public Key Infrastructure Online Certificate Status Protocol - OCSP;
- RFC 3647 Internet X.509 Public Key Infrastructure Certificate Policy and Certification Practices Framework;
- RFC 4366 Transport Layer Security (TLS) Extensions;
- RFC 5019 The Lightweight Online Certificate Status Protocol (OCSP) Profile for High-Volume Environments;
- RFC 5280 Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile;
- RFC 6844 DNS Certification Authority Authorization (CAA) Resource Record;
- RFC 6962 Certificate Transparency;
- EN 301 549 Accessibility requirements for ICT products and services;
- ČSN ETSI EN 319 412-1 Electronic Signatures and Infrastructures (ESI); Certificate Profiles; Part 1: Overview and Common Data Structures;
- ETSI EN 319 412-1 Electronic Signatures and Infrastructures (ESI); Certificate Profiles; Part 1: Overview and common data structures;
- ČSN ETSI EN 319 412-3 Electronic Signatures and Infrastructures (ESI); Certificate Profiles; Part 3: Certificate Profile for Certificates Issued to Legal Persons;
- ETSI EN 319 412-3 Electronic Signatures and Infrastructures (ESI); Certificate Profiles; Part 3: Certificate profile for certificates issued to legal persons;

- ČSN ETSI EN 319 412-4 Electronic Signatures and Infrastructures (ESI); Certificate Profiles; Part 4: Certificate profile for web site certificates;
- ETSI EN 319 412-4 Electronic Signatures and Infrastructures (ESI); Certificate Profiles; Part 4: Certificate profile for web site certificates.
- ČSN ETSI EN 319 412-5 Electronic Signatures and Infrastructures (ESI); Certificate Profiles; Part 5: „QC Statements“ Statement.
- ETSI EN 319 412-5 Electronic Signatures and Infrastructures (ESI); Certificate Profiles; Part 5: QCStatements.

6.6 Life cycle technical controls

6.6.1 System development controls

System development is carried out in accordance with internal documentation.

6.6.2 Security management controls

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

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

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

6.6.3 Life cycle security controls

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

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

6.7 Network security controls

In the I.CA environment the trustworthy systems destined for supporting trust services and situated at I.CA's operating sites are not directly accessible from the Internet. These systems are protected with a firewall-type commercial product with an integrated intrusion prevention system (IPS). All communication between RA and the operating sites is encrypted.

6.8 Time-stamping

See 5.5.5 for the time stamping solution.

7 CERTIFICATE, CRL, AND OCSP PROFILES

7.1 Certificate profile

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

Table 4 – Basic certificate fields

Field	Content	Comments
version	v3 (0x2)	
serialNumber	unique serial number of the Certificate	minimum of 64 bits from a random numbers generator (used for cryptosystems) greater than zero
signatureAlgorithm	sha256WithRSAEncryption at minimum	
issuer	issuer of the certificate (the Authority)	
validity		
notBefore*	start of the Certificate's validity (UTC)	
notAfter*	end of the Certificate's validity (UTC)	
subject	see Table 5 below	
subjectPublicKeyInfo		must meet the requirements under 6.1.5 and 6.1.6
algorithm	rsaEncryption	
subjectPublicKey	2048 at minimum	
extensions	extensions to the Certificate issued	see Table 6
signature	Certificate issuer's (Authority's) electronic seal	

* The period of validity is defined by the Authority and is in accordance with EVCG (usually twelve months).

Table 5 – Subject field attributes

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

Subject Field Attribute	Content	Comments
commonName	If specified, it MUST be the only server dNSName as specified in the first item subjectAlternativeName (see Table 6).	optional item wildcards are not permitted
Identification of the Entity – SSL/TLS Server Owner		
organizationName	MUST specify the full registered legal name of the entity; plus may have a business name field at the beginning provided it is followed by the entity's full legal name given in parentheses).	mandatory item The CA may cut the name shorter or accept an abbreviated name so that the text has a maximum of 64 characters, provided that no third party might be made to believe it communicates with a different organization.
businessCategory (2.5.4.15)	MUST contain one of the strings according to the category of the entity (EVCG, chapter 8.5): ▪ '**Private Organisations**' – companies entered or registered under a law or set up by a government agency; in the Czech Republic, this register is referred to as the Commercial Register; ▪ '**Government Entities**' – government authority (entity); ▪ '**Business Entities**' – entities registered by a registration agency that grants/validates business licenses or certificates (such as entities registered in a register other than the Commercial Register) where the registration of these entities can be validated; ▪ '**Non-commercial Entities**' – international organizations set up under treaties signed by multiple	mandatory item

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

	national governments	
The level of the registration agency which registered the entity and the registration number		
jurisdictionCountryName (1.3.6.1.4.1.311.60.2.1.3)	ISO 3166-1 country code	▪ mandatory if the registration of the entity was made (is managed) at the state level ▪ only this attribute for entities registered in the Czech Republic ▪ If not specified, then jurisdictionLocalityName and jurisdictionStateOrProvinceName MUST NOT be specified
jurisdictionStateOrProvinceName (1.3.6.1.4.1.311.60.2.1.2)	UTF8String, maximum length 128 characters (full text of the name of the administrative region/province)	▪ mandatory if the registration of the entity was made (is managed) at the level of 'province'/region; and ▪ jurisdictionCountryName MUST be specified and jurisdictionLocalityName must NOT be specified; ▪ not applicable to CZ but may need to be specified for entities registered in other countries
jurisdictionLocalityName (1.3.6.1.4.1.311.60.2.1.1)	UTF8String, maximum length 128 characters (full text of the name of the locality/town or city)	▪ mandatory if the registration of the entity was made (is managed) at the level of locality = town or city ▪ then both jurisdictionCountryName and jurisdictionStateOrProvinceName

		MUST be specified ▪ not applicable to CZ but may need to be specified for entities registered in other countries
serialNumber	• **Private Organisation**: registration number or registration date if registration number is not assigned • **Government Entity**: date the entity is set up/registered/created or the number of the law or a text expressing the entity is a government entity • **Business Entity**: unique registration number or registration date if registration number is not assigned • **Non-Commercial**: date the entity is set up or the number of the law or a text expressing the entity is an international organization	mandatory item
Address of Entity's Physical Site		
streetAddress	street and street number of entity's address	optional item
localityName	town or city	mandatory item
stateOrProvinceName	state of a federation or region/province	mandatory item
postalCode	postal code	optional item
countryName	two-letter country code (ISO 3166-1)	mandatory item

* More accurately, the entity controlling the server (the operator of the SSL server and/or the owner of the physical server may be someone else – a hosting company etc.).

7.1.1 Version number(s)

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

7.1.2 Certificate extensions

Table 6 – Certificate extensions[2]

Extension	Content	Comments
subjectAlternativeName		non-critical
dNSName (1 .. 10 occurrences)	Public DNS name of the host (of the SSL/TLS server)/ of the DNS domain on the basis of certificate application. The content of the first item dnsName must be identical to that of the item subject.commonName if commonName is specified (see Table 5).	▪ minimum of one occurrence is mandatory, multiple occurrence permitted – maximum of 10 occurrences of dnsName; ▪ wildcards not permitted (*.company.cz, for example); ▪ all dnsName attributes must contain the same part of second level domain (same second level domain); ▪ Certificates for new generic top-order domains MUST NOT be issued; ▪ MUST be public DNS name
PSD2 attributes*		
directoryName		mandatory for PSD2 certificates, not specified for other QC-web
description (2.5.4.13)	PSP's authorized roles; (comma-separated) list of one or multiple roles assigned by registrar (as text, in English)	see EBA RTS 1024 characters at maximum
DN Qualifier (2.5.4.46)	registrar's name in English	see EBA RTS 64 characters at

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

		maximum
DMDName (2.5.4.54)	PSP's authorization name available in public register	see EBA RTS
otherName	I.CA_User_ID (1.3.6.1.4.1.23624.4.6)	non-critical; created by the Authority for internal use
certificatePolicies		non-critical; created by the Authority
.policyInformation(1)		
policyIdentifier	See 1.2.	mandatory
policyQualifiers		
cPSuri	http://www.ica.cz	
userNotice	This is a qualified certificate for website authentication according to Regulation (EU) No 910/2014.	optional
.policyInformation(2)		
policyIdentifier	EV (2.23.140.1.1)	OID specified in EVCG, chapter 9.3.2, policy identifier according to Microsoft requirements
.PolicyInformation(3)		EN 319411-2 recommended for QCP-w certificates
policyIdentifier	QCP-w (0.4.0.194112.1.4)	
QCStatements		non-critical; created by the Authority
	id-etsi-qcs-QcCompliance (0.4.0.1862.1.1)	
	id-etsi-qcs-QcSSCD (0.4.0.1862.1.4)	may be specified if the private key is generated and saved on QSCD
	id-etsi-qcs-QcPDS (0.4.0.1862.1.5)	link (URI, https) to user notice (PDS)
	id-etsi-qcs-QcType (0.4.0.1862.1.6) = 0.4.0.1862.1.6.3	mandatory id-etsi-qcs-QcType = id-etsi-qct-web

	qcStatement-2 (1.3.6.1.5.5.7.11.2)	PSD2 certificates*, not specified for other QC-web link to the website of the registrar and the public register of PSPs (EU Directive 2015/2366, article 14
CRLDistributionPoints**	http://qcrldp1.ica.cz/qcw*YY*_rsa.crl http://qcrldp2.ica.cz/qcw*YY*_rsa.crl http://qcrldp3.ica.cz/qcw*YY*_rsa.crl	non-critical; created by the Authority
authorityInformationAccess		non-critical; created by the Authority
id-ad-ocsp**	http://ocsp.ica.cz/qcw*YY*_rsa	
id-ad-caIssuers**	http://q.ica.cz/qcw*YY*_rsa.cer	
basicConstraints		non-critical; created by the Authority
cA	False	
keyUsage	digitalSignature, keyEncipherment	critical; created by the Authority
extendedKeyUsage***	as per the application; ▪ included must be at least id-kp-serverAuth ▪ or id-kp-serverAuth and id-kp-clientAuth ▪ plus id-kp-emailProtection may be included as an option	non-critical, mandatory; if this extension is missing from the application, id-kp-serverAuth, id-kp-clientAuth will be added
subjectKeyIdentifier	the hash of the public key (subjectPublicKey) in the certificate issued (see Table 4)	non-critical; created by the Authority
authorityKeyIdentifier	hash of the certificate issuer's (Authority's) public key	non-critical; created by the Authority
keyIdentifier	hash of the certificate issuer's (Authority's) public key	
Signed Certificate Timestamp	timestamps from at least two Certificate Transparency (CT) logs	created by Authority timestamp = signed confirmation from relevant CT log that precertificate has been added

* Since 30 April 2019 the attributes PSD2 and subjectAlternativeName.otherName extension are not supported.

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

*** It is a supported set; the specific EKU is taken over from the Certificate application.

7.1.2.1 All certificates

Other fields and extensions are set in accordance with RFC 5280. The Authority will not issue a certificate containing a keyUsage attribute, extendedKeyUsage value, certificate extension or other data not specified in this chapter 7.1.2 unless it has a reason for putting such data in the certificate.

Also, the Authority will not issue certificates:

- With extensions that are irrelevant in the context of the public Internet;
- With semantics that might mislead the relying party.

7.1.2.2 Application RFC 5280

The 'pre-certificate' as described in RFC 6962 – Certificate Transparency is not considered a certificate meeting the RFC 5280 requirements.

7.1.3 Algorithm object identifiers

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

7.1.4 Name forms

Name forms included in the Authority-issued Certificates comply with RFC 5280. The provisions of 3.1 also apply.

7.1.5 Name constraints

The names in the Certificate must, if possible, accurately correspond to the data in the documents by which the subscriber proved his identity for registration.

7.1.6 Certificate policy object identifier

Certification policy OIDs are specified in the item CertificatePolicies (see Table 6).

7.1.7 Usage of Policy Constraints extension

Not applicable to Certificates issued to end users.

7.1.8 Policy qualifiers syntax and semantics

See Certificate extensions in 7.1.2 above.

7.1.9 Processing semantics for the critical Certificate Policies extension

Not applicable to this document – not classified as critical.

7.2 CRL profile

Table 7 – CRL profile[3]

Field	Content
version	v2(0x1)
signatureAlgorithm	sha256WithRSAEncryption
issuer	issuer of the CRL (the Authority)
thisUpdate	date and time the CRL is released (UTC)
nextUpdate	date and expected time the next CRL will be released (UTC)
revokedCertificates	list of revoked certificates (crlEntries)
crlEntries	
userCertificate	revoked certificate's serial number
revocationDate	certificate revocation date and time
crlEntryExtensions	list item extensions – see Table 8 below
crlExtensions	CRL extensions – see Table 8 below
signatureAlgorithm	sha256WithRSAEncryption
signature	CRL issuer's (Authority's) electronic seal

7.2.1 Version number(s)

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

7.2.2 CRL and CRL entry extensions

Table 8 – CRL extensions[4]

Extension	Content	Comments
crlEntryExtensions		
CRLReason	certificate revocation reason; the certificateHold reason is not admissible as it is out of use	non-critical, optional

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

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

crlExtensions		
authorityKeyIdentifier		
keyIdentifier	hash of the CRL issuer's (Authority's) public key	non-critical
CRLNumber	unique number of the CRL to be released	non-critical

7.3 OCSP profile

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

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

See the relevant certification practice statement for more detail.

7.3.1 Version number(s)

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

7.3.2 OCSP extensions

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

8 COMPLIANCE AUDITS AND OTHER ASSESSMENTS

8.1 Frequency or circumstances of assessment

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

The evaluation periodicity for the Microsoft Trusted Root Certificate Program, including the circumstances for the evaluation, is strictly determined by Microsoft's requirements. The Authority's term of office is divided into an uninterrupted sequence of audit periods, with an audit period not exceeding one year.

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

8.2 Identity/qualifications of assessor

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

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

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

8.3 Assessor's relationship to assessed entity

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

External assessor is an assessor without any ties to I.CA through property or organization.

8.4 Topics covered by assessment

In the case of the assessment required by current trust services legislation, the assessed areas are specified by this legislation.

Microsoft Trusted Root Certificate Program areas are strictly determined by Microsoft's requirements.

Assessed areas for other assessment are specified by the technical standards and standards under which the evaluation is performed.

8.5 Actions taken as a result of deficiency

The findings in any type of assessment are communicated to the I.CA security manager, who makes sure that any defect identified is remedied. If defects are identified that critically

prevent the provision of a specific trust service, I.CA must suspend that service until the defects are remedied.

8.6 Communication of results

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

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

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

8.7 Regular quality evaluation self-audits

The I.CA employee shall carry out at least quarterly, on a randomly selected sample of size of at least one Certificate, but on at least three percent of the Certificates issued in the period immediately following the selection of the sample for past self-audit, compliance check with CP and CPS.

9 OTHER BUSINESS AND LEGAL MATTERS

9.1 Fees

9.1.1 Certificate issuance or renewal fees

The fees for Certificate issuance are given in the current price list, which is available on the web Information Address of I.CA or in the contract if there is a contract between I.CA and the Organisation. Certificate renewal is not provided.

9.1.2 Certificate access fees

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

9.1.3 Revocation or status information access fees

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

9.1.4 Fees for other services

Not applicable to this document.

9.1.5 Refund policy

Not applicable to this document.

9.2 Financial responsibility

9.2.1 Insurance coverage

První certifikační autorita, a.s. represents it holds a business risk insurance policy that covers financial damage.

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

9.2.2 Other assets

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

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

9.2.3 Insurance or warranty coverage for end-entities

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

9.3 Confidentiality of business information

9.3.1 Scope of confidential information

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

- All private keys, which are employed in providing the Services;
- I.CA's business information;
- Any internal information and documentation;
- Any personal data.

9.3.2 Information not within the scope of confidential information

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

9.3.3 Responsibility to protect confidential information

No I.CA employee who comes in contact with confidential information may disclose the same to a third party without consent of CEO of I.CA.

9.4 Privacy of personal information

9.4.1 Privacy plan

I.CA protects personal data and other non-public information in accordance with the relevant legislation, that is, ZOOÚ.

9.4.2 Information treated as private

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

I.CA employees or the entities defined by current legislation that come into contact with personal data must maintain confidentiality of these data and the security controls the disclosure of which would put the security of these data at risk. The confidentiality duty survives the termination of employment or other similar relationship, or the completion of pertinent work.

9.4.3 Information not deemed private

Any information outside the scope of relevant legislation, that is, ZOOÚ, is not considered personal data.

9.4.4 Responsibility to protect private information

CEO of I.CA is responsible for the protection of personal data.

9.4.5 Notice and consent to use private information

I.CA deals with the notifying of personal data use and consents to personal data processing in accordance with the relevant legislation, that is, ZOOÚ.

9.4.6 Disclosure pursuant to judicial or administrative process

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

9.4.7 Other information disclosure circumstances

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

9.5 Intellectual property rights

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

9.6 Representations and warranties

9.6.1 CA representations and warranties

I.CA warrants that:

- It will use the certification authorities' private keys solely for issuing Certificates to end users (except I.CA's root certification authority), releasing certification revocation lists and issuing OCSP responder certificates;
- It will use the private keys of certification authorities' OCSP responders solely in the processes of providing responses to certificate status requests;
- Certificates issued to end users meet the statutory trust services requirements and those of the relevant technical standards;
- It will revoke any issued Certificate if the revocation request is submitted in the manner defined in this CP.

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

- The Certificate's subscriber does not breach any obligation out of the contract of Services and this CP;
- The relying party does not breach any obligation out of this CP.

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

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

The warranties include:

- Validating of the right to use the domain name mentioned in the Certificate;
- Checking of the right to apply for a Certificate on behalf of the Organization;
- Validating the information given in the Certificate application, checking due completion of the items in the Certificate application (PKCS#10 format) and checking the identity;
- Ensuring that certificate status information repository is maintained 24 hours a day and 7 days a week;
- Ensuring that the Certificate may be revoked for reasons specified in this CP.

9.6.2 RA representations and warranties

The designated RA:

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

9.6.3 Subscriber representations and warranties

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

9.6.4 Relying party representations and warranties

Relying parties observe this CP.

9.6.5 Representations and warranties of other participants

Not applicable to this document.

9.7 Disclaimers of warranties

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

9.8 Limitations of liability

První certifikační autorita, a.s., may not be held liable, in respect of this Service, for any damage suffered by relying parties where the relying party breaches its duty under current trust services legislation and this CP. První certifikační autorita, a.s. may also not be held liable for any damage resulting from breach of obligations of I.CA as a result of force majeure.

In all other cases the maximum compensation of damage caused to the single Certificate subscriber or to the single relying party is limited to the sum in Czech crowns equivalent to two thousand US dollars depending on exchange rate effective at the moment of damage origin.

9.9 Indemnities

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

První certifikační autorita, a.s.:

- Undertakes to discharge all the duties defined in current legislation (including the trust services legislation) and those in the relevant policies;
- Gives the aforesaid warranties throughout the term of the contract of trust services;
- Agrees that the application software suppliers with a valid contract with První certifikační autorita, a.s. for the distribution of the root certificate assume no obligation or liability, except for where damage or loss is directly attributable to the software of that supplier;
- Any other possible compensation is based on the relevant legislation and the amount of damages may be determined by court.

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

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

Claims and complaints may be made and delivered by:

- E-mail to reklamace@ica.cz;
- Message to I.CA's data box;

- Registered post letter to the registered office of the company;
- Hand at the registered office of the company.

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

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

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

The claim/complaint, including the defect, will be dealt with without undue delay, within 30 days of the date of the claim/complaint unless the parties agree otherwise.

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

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

9.10 Term and termination

9.10.1 Term

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

9.10.2 Termination

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

9.10.3 Effect of termination and survival

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

9.11 Individual notices and communications with participants

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

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

9.12 Amendments

9.12.1 Procedure for amendment

This procedure is a controlled process described in internal documentation.

9.12.2 Notification mechanism and period

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

9.12.3 Circumstances under which OID must be changed

The Policy's OID must be changed when the changes of the Policy materially reduce the assurance that the Certificate is trusted and have a significant effect on the acceptability of the Certificate within website authentication in compliance with valid technical standards.

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

9.13 Dispute resolution provisions

If the Certificate's subscriber or the relying party disagrees with the proposed way of resolving the dispute, they may use the following levels of appeal:

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

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

9.14 Governing law

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

9.15 Compliance with applicable law

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

9.16 Miscellaneous provisions

9.16.1 Entire agreement

Not applicable to this document.

9.16.2 Assignment

Not applicable to this document.

9.16.3 Severability

If a court or a public authority with jurisdiction over the activities covered by this CP establishes that the implementation of a mandatory requirement is illegal, the scope of that requirement will be so limited as to ensure the requirement is applicable and lawful. I.CA informs about this fact CA/Browser Forum.

9.16.4 Enforcement (attorneys' fees and waiver of rights)

Not applicable to this document.

9.16.5 Force majeure

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

9.17 Other provisions

Not applicable to this document.

10 FINAL PROVISIONS

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