První certifikační autorita, a.s.



Certificate Policy

for Issuing Qualified Certificates for Website Authentication to Legal Persons

(RSA Algorithm)

Certificate Policy for Issuing Qualified Certificates for Website Authentication to Legal Persons (RSA Algorithm) is a public document, which is the property of První certifikační autorita, a.s., and has been prepared as integral part of comprehensive security documentation. No part of this document may be reproduced without the written consent of the copyright holder.

Version 1.085

Copyright © První certifikační autorita, a.s.

TABLE OF CONTENTS

1 Introduction 12
1.1 Overview 12
1.2 Document name and identification 13
1.3 PKI participants 13
1.3.1 Certification authorities (also as 'CA') 13
1.3.2 Registration authorities (also as 'RA') 13
1.3.3 Subscribers 14
1.3.4 Relying parties 14
1.3.5 Other participants 14
1.4 Certificate usage 14
1.4.1 Appropriate certificate uses 14
1.4.2 Prohibited certificate uses 14
1.5 Policy administration 14
1.5.1 Organization administering the document 14
1.5.2 Contact person 14
1.5.3 Person determining CPS suitability for the policy 15
1.5.4 CPS approval procedures 15
1.6 Definitions and acronyms 15
2 Publication and repository responsibilities 22
2.1 Repositories 22
2.2 Publication of certification information 22
2.3 Time or frequency of publication 23
2.4 Access controls on repositories 23
3 Identification and authentication 24
3.1 Naming 24
3.1.1 Types of names 24
3.1.2 Need for names to be meaningful 24
3.1.3 Anonymity or pseudonymity of subscribers 24
3.1.4 Rules for interpreting various name forms 24
3.1.5 Uniqueness of names 24
3.1.6 Recognition, authentication, and role of trademarks 24
3.2 Initial identity validation 25
3.2.1 Method to prove possession of private key 25
3.2.2 Authentication of organization and domain identity 25

3.2.3 Authentication of individual identity 28
3.2.4 Non-verified subscriber information 29
3.2.5 Validation of authority 29
3.2.6 Criteria for interoperation 30
3.3 Identification and authentication for re-key requests 30
3.3.1 Identification and authentication for routine re-key 30
3.3.2 Identification and authentication for re-key after revocation 30
3.4 Identification and authentication for revocation request 30
4 Certificate life-cycle operational requirements 32
4.1 Certificate application 32
4.1.1 Who can submit a certificate application 32
4.1.2 Enrollment process and responsibilities 32
4.2 Certificate application processing 33
4.2.1 Performing identification and authentication functions 33
4.2.2 Approval or rejection of certificate applications 33
4.2.3 Time to process certificate applications 33
4.3 Certificate issuance 33
4.3.1 CA actions during certificate issuance 33
4.3.2 Notification to subscriber by the CA of issuance of certificate 34
4.4 Certificate acceptance 34
4.4.1 Conduct constituting certificate acceptance 34
4.4.2 Publication of the certificate by the CA 34
4.4.3 Notification of certificate issuance by the CA to other entities 34
4.5 Key pair and certificate usage 34
4.5.1 Subscriber private key and certificate usage 34
4.5.2 Relying party public key and certificate usage 35
4.6 Certificate renewal 35
4.6.1 Circumstance for certificate renewal 35
4.6.2 Who may request renewal 35
4.6.3 Processing certificate renewal requests 35
4.6.4 Notification of new certificate issuance to subscriber 35
4.6.5 Conduct constituting acceptance of a renewal certificate 35
4.6.6 Publication of the renewal certificate by the CA 36
4.6.7 Notification of certificate issuance by the CA to other entities 36
4.7 Certificate re-key 36
4.7.1 Circumstance for certificate re-key 36

4.7.2 Who may request certification of a new public key....36
4.7.3 Processing certificate re-keying requests....36
4.7.4 Notification of new certificate issuance to subscriber....36
4.7.5 Conduct constituting acceptance of a re-keyed certificate....36
4.7.6 Publication of the re-keyed certificate by the CA....36
4.7.7 Notification of certificate issuance by the CA to other entities....36
4.8 Certificate modification....36
4.8.1 Circumstance for certificate modification....37
4.8.2 Who may request certificate modification....37
4.8.3 Processing certificate modification requests....37
4.8.4 Notification of new certificate issuance to subscriber....37
4.8.5 Conduct constituting acceptance of modified certificate....37
4.8.6 Publication of the modified certificate by the CA....37
4.8.7 Notification of certificate issuance by the CA to other entities....37
4.9 Certificate revocation and suspension....37
4.9.1 Circumstances for revocation....38
4.9.2 Who can request revocation....39
4.9.3 Procedure for revocation request....40
4.9.4 Revocation request grace period....41
4.9.5 Time within which CA must process the revocation request....41
4.9.6 Revocation checking requirement for relying parties....42
4.9.7 CRL issuance frequency (if applicable)....42
4.9.8 Maximum latency for CRLs (if applicable)....42
4.9.9 On-line revocation/status checking availability....42
4.9.10 On-line revocation checking requirements....42
4.9.11 Other forms of revocation advertisements available....43
4.9.12 Special requirements re key compromise....43
4.9.13 Circumstances for suspension....43
4.9.14 Who can request suspension....43
4.9.15 Procedure for suspension request....43
4.9.16 Limits on suspension period....43
4.10 Certificate status services....43
4.10.1 Operational characteristics....43
4.10.2 Service availability....44
4.10.3 Optional features....44
4.11 End of subscription....44

4.12 Key escrow and recovery 44
4.12.1 Key escrow and recovery policy and practices 44
4.12.2 Session key encapsulation and recovery policy and practices 44
5 Facility, manegement, and operational controls 45
5.1 Physical controls 45
5.1.1 Site location and construction 45
5.1.2 Physical access 45
5.1.3 Power and air conditioning 45
5.1.4 Water exposures 45
5.1.5 Fire prevention and protection 46
5.1.6 Media storage 46
5.1.7 Waste disposal 46
5.1.8 Off-site backup 46
5.2 Procedural controls 46
5.2.1 Trusted roles 46
5.2.2 Number of persons required per task 46
5.2.3 Identification and authentication for each role 47
5.2.4 Roles requiring separation of duties 47
5.3 Personnel controls 47
5.3.1 Qualifications, experience, and clearance requirements 47
5.3.2 Background check procedures 47
5.3.3 Training requirements 48
5.3.4 Retraining frequency and requirements 48
5.3.5 Job rotation frequency and sequence 48
5.3.6 Sanctions for unauthorized actions 48
5.3.7 Independent contractor requirements 48
5.3.8 Documentation supplied to personnel 48
5.4 Audit logging procedures 49
5.4.1 Types of events recorded 49
5.4.2 Frequency of processing log 49
5.4.3 Retention period for audit log 49
5.4.4 Protection of audit log 49
5.4.5 Audit log backup procedures 50
5.4.6 Audit collection system (internal vs. external) 50
5.4.7 Notification to event-causing subject 50
5.4.8 Vulnerability assessments 50

5.5 Records archival 50
5.5.1 Types of records archived 50
5.5.2 Retention period for archive 50
5.5.3 Protection of archive 51
5.5.4 Archive backup procedures 51
5.5.5 Requirements for time-stamping of records 51
5.5.6 Archive collection system (internal or external) 51
5.5.7 Procedures to obtain and verify archive information 51
5.6 Key changeover 51
5.7 Compromise and disaster recovery 52
5.7.1 Incident and compromise handling procedures 52
5.7.2 Computing resources, software, and/or data are corrupted 52
5.7.3 Entity private key compromise procedures 52
5.7.4 Business continuity capabilities after a disaster 52
5.8 CA or RA termination 52
6 Techical security controls 54
6.1 Key pair generation and installation 54
6.1.1 Key pair generation 54
6.1.2 Private key delivery to subscriber 54
6.1.3 Public key delivery o certificate issuer 54
6.1.4 CA public key delivery to relying parties 54
6.1.5 Key sizes 55
6.1.6 Public key parameters generation and quality checking 55
6.1.7 Key usage purposes (as per X.509 v3 key usage extension) 55
6.2 Private key protection and cryptographic module engineering controls 55
6.2.1 Cryptographic module standards and controls 55
6.2.2 Private key (n out of m) multi-person control 55
6.2.3 Private key escrow 55
6.2.4 Private key backup 55
6.2.5 Private key archival 56
6.2.6 Private key transfer into or from a cryptographic module 56
6.2.7 Private key storage on cryptographic module 56
6.2.8 Method of activating private key 56
6.2.9 Method of deactivating private key 57
6.2.10 Method of destroying private key 57
6.2.11 Cryptographic module rating 57

6.3 Other aspects of key pair management 57
6.3.1 Public key archival 57
6.3.2 Certificate operational periods and key pair usage periods 58
6.4 Activation data 58
6.4.1 Activation data generation and installation 58
6.4.2 Activation data protection 58
6.4.3 Other aspects of activation data 58
6.5 Computer security controls 58
6.5.1 Specific computer security technical requirements 58
6.5.2 Computer security rating 58
6.6 Life cycle technical controls 61
6.6.1 System development controls 61
6.6.2 Security management controls 61
6.6.3 Life cycle security controls 61
6.7 Network security controls 61
6.8 Time-stamping 62
7 Certificate, CRL, and OCSP profiles 63
7.1 Certificate profile 63
7.1.1 Version number(s) 66
7.1.2 Certificate extensions 66
7.1.3 Algorithm object identifiers 70
7.1.4 Name forms 70
7.1.5 Name constraints 70
7.1.6 Certificate policy object identifier 70
7.1.7 Usage of Policy Constraints extension 70
7.1.8 Policy qualifiers syntax and semantics 70
7.1.9 Processing semantics for the critical Certificate Policies extension 70
7.2 CRL profile 70
7.2.1 Version number(s) 71
7.2.2 CRL and CRL entry extensions 71
7.3 OCSP profile 72
7.3.1 Version number(s) 72
7.3.2 OCSP extensions 72
8 Compliance audits and other assessments 73
8.1 Frequency or circumstances of assessment 73

8.2 Identity/qualifications of assessor 73
8.3 Assessor's relationship to assessed entity 73
8.4 Topics covered by assessment 73
8.5 Actions taken as a result of deficiency 73
8.6 Communication of results 74
8.7 Regular quality evaluation self-audits 74
9 Other business and legal matters 75
9.1 Fees 75
9.1.1 Certificate issuance or renewal fees 75
9.1.2 Certificate access fees 75
9.1.3 Revocation or status information access fees 75
9.1.4 Fees for other services 75
9.1.5 Refund policy 75
9.2 Financial responsibility 75
9.2.1 Insurance coverage 75
9.2.2 Other assets 75
9.2.3 Insurance or warranty coverage for end-entities 76
9.3 Confidentiality of business information 76
9.3.1 Scope of confidential information 76
9.3.2 Information not within the scope of confidential information 76
9.3.3 Responsibility to protect confidential information 76
9.4 Privacy of personal information 76
9.4.1 Privacy plan 76
9.4.2 Information treated as private 76
9.4.3 Information not deemed private 76
9.4.4 Responsibility to protect private information 77
9.4.5 Notice and consent to use private information 77
9.4.6 Disclosure pursuant to judicial or administrative process 77
9.4.7 Other information disclosure circumstances 77
9.5 Intellectual property rights 77
9.6 Representations and warranties 77
9.6.1 CA representations and warranties 77
9.6.2 RA representations and warranties 78
9.6.3 Subscriber representations and warranties 78
9.6.4 Relying party representations and warranties 78
9.6.5 Representations and warranties of other participants 78

9.7 Disclaimers of warranties 78
9.8 Limitations of liability 79
9.9 Indemnities....79
9.10 Term and termination 80
9.10.1 Term....80
9.10.2 Termination 80
9.10.3 Effect of termination and survival....80
9.11 Individual notices and communications with participants 80
9.12 Amendments....81
9.12.1 Procedure for amendment....81
9.12.2 Notification mechanism and period....81
9.12.3 Circumstances under which OID must be changed 81
9.13 Dispute resolution provisions....81
9.14 Governing law 81
9.15 Compliance with applicable law....81
9.16 Miscellaneous provisions 81
9.16.1 Entire agreement....81
9.16.2 Assignment....82
9.16.3 Severability....82
9.16.4 Enforcement (attorneys' fees and waiver of rights) 82
9.16.5 Force majeure 82
9.17 Other provisions....82
10 Final provisions 83

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 EVCG (chapters 3.2.2.4, 4.9.1, 4.9.5.2).
1.03	7 March 2020	CEO of První certifikační autorita, a.s.	Certificate Transparency support.

1.04	1 April 2020	CEO of První certifikační autorita, a.s.	Specification of issuing certificates for gTLD domains (in accordance with BRG).
1.05	28 November 2020	CEO of První certifikační autorita, a.s.	Classification of document marked, revision, more accurate text.
1.06	1 July 2021	CEO of První certifikační autorita, a.s.	More accurate text in chapter 3.2.2.1, attribute userNotice modification.
1.07	27 November 2021	CEO of První certifikační autorita, a.s.	Update and specification in accordance with EVCG v.1.7.8 and BRG v.1.8.0.
1.08	11 June 2022	CEO of První certifikační autorita, a.s.	Cryptographic module evaluation updated. Modification of requirements to comply with BRG up to version 1.8.4 – chapters 4.1.1, 4.2.1, 5.4.1 and 5.5.1. Revision of text.
1.081	26 April 2023	CEO of První certifikační autorita, a.s.	Clarification of requirements in relation to BRG. Using the reasons of revocation in compliance with BRG 1.8.7 added – chapters 4.9.1.1, 4.9.3 and 7.2.2. Revision of text.
1.082	27 February 2024	CEO of První certifikační autorita, a.s.	PSD2 attributes removed from certificate profile. Clarification of requirements in relation to BRG. Revision of text.
1.083	23 April 2025	CEO of První certifikační autorita, a.s.	Procedure for checking the domain name registrant's authority and certificate profile modified in accordance with the new version of BRG. List of referenced standards updated.
1.084	23 April 2026	CEO of První certifikační autorita, a.s.	Document updated according to BRG requirements. Revision of text.

1.085	12 September 2026	CEO of První certifikační autorita, a.s.	Committing to CCADB policy requirements. Clarification of CA actions during certificate issuance. New organizational chart taken into account.

1 INTRODUCTION

This document 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 certificate policy (also as the CP).

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

Note: Any reference to technical standard, norm or legislation is always a reference to that technical standard, norm or legislation or to replacing technical standard, norm or legislation. If this document is in conflict with any technical standard, norm or legislation that replaces the current technical standard, norm or legislation, a new version will be released.

1.1 Overview

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

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

Note: This is English translation of CP; Czech version always takes precedence. I.CA attests that the translation is not materially different to the original.

1.2 Document name and identification

This document's title:	Certificate Policy for Issuing Qualified Certificates for Website Authentication to Legal Persons (RSA Algorithm), version 1.085
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 relevant legislation and technical and other standards. This Authority issues Certificates under this CP and certificates for its own OCSP responder.

1.3.2 Registration authorities (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 conclude Service contracts on behalf of I.CA;
- Is authorized, 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 relevant 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 CEO of I.CA. Contact information is as described in chapter 2.2.

E-mail address certproblem@ica.cz maintains continuous 24x7 ability to accept and respond to certificate problem reports.

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
authorization domain name	FQDN used to obtain authorization for a given FQDN to be included in a Certificate; CA may use the FQDN returned from a DNS CNAME lookup as the FQDN for the purposes of domain validation
base domain name	part of FQDN, which is first node of domain name left from: • the one (name) checked by register; or • public extension plus the name checked by register public extension
CA/Browser Forum	organization, consensual association of certification authorities
Classified Information Protection Act	the Czech Republic's Act No. 412/2005 Coll., regulating classified information protection and security competence, as amended
contracting partner	provider of services contracted by I.CA for certification services or parts thereof – usually, it is a contracted RA
domain label	ordered list of zero or more octets that makes up a portion of a domain name (see also RFC 8499); using graph theory, a label identifies one node in a portion of the graph of all possible domain names
domain name	ordered list of one or more Domain Labels assigned to a node in the Domain Name System
domain name registrant/ registrant	sometimes referred to as a domain name owner, but more accurately a person or entity registered by a domain registrar as having the right to oversee the use of a domain name, a natural or legal person listed as a "Registrant" by WHOIS or a domain registrar

domain name registrar/ registrar	person or entity that registers domain names by mandate or with consent: • Internet Corporation for Assigning Names and Numbers (ICANN) - Administrator of DNS Root Space; • TLD administrator (e.g. .com) or ccTLD (e.g. .CZ, national administrator)
domain name space	a set of all possible domain names that are subordinate to one node in the domain name system
electronic seal	advanced electronic seal or recognized electronic seal or qualified electronic seal under trust services legislation
electronic signature	advanced electronic signature or recognized electronic signature or qualified electronic signature under trust services legislation
GET method	method of communication between client and http server by request for retrieving/downloading data from the server, preferred method to send http requests for OCSP responses to OCSP server using http protocol
hash function	transformation which receives, as an input, a string of characters of arbitrary length, and the result is a string of characters of fixed length (hash)
key pair	private key and corresponding public key
Labour Code	the Czech Republic's Act No. 262/2006 Coll., Labour Code, as amended
LDH label	type of domain label in DNS - a string consisting of ASCII letters, digits, and the hyphen with the further restriction that the hyphen cannot appear at the beginning or end of the string, and its total length must not exceed 63 octets (see also RFC 5890) note: abbreviation LDH means Letters, Digits, Hyphen
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
P-label	XN-Label that contains valid output of the Punycode algorithm (see RFC 3492, Section 6.3)
phishing	in an electronic communication attempt to obtain sensitive information (usernames, passwords, and credit card details) for malicious reasons
POST method	method of communication between client and http server by sending data from client to server (e.g., sending request to OCSP responder via http protocol)

private key	unique data to create electronic signature / seal
public key	unique data to verify electronic signature / seal
PSP registrar	authority responsible for approving or rejecting authorization of payment services providers in their state, usually National Bank, in ETSI TS 119 495 called NCA (National Competent Authority)
qualified certificate for electronic signature or for electronic seal or for website authentication	certificate defined by trust services legislation
qualified signature / seal creation device	device meeting the requirements of eIDAS, annex II, intended for electronic signature / seal creation
relying party	party relying on a certificate in its operations
root CA	certification authority which issues certificates to subordinate certification authorities
secure cryptographic device	device on which the private key is stored
softcard	software emulation of smartcard for access to private key stored in HSM
SSL certificate	certificate for identification and encryption within SSL/TLS protocol communication
subordinate CA	CA issuing certificates to end users
supervisory body	the body supervising qualified trust services providers
trust service / qualified trust service	trust service / qualified trust service defined by eIDAS
trust services legislation	current legislation on trust services
TWINS	commercial product of I.CA consisting of: • qualified certificate for electronic signature; • non-qualified certificate which issuance is based only on contractual relationship between I.CA and end-user
two-factor authentication	authentication employing two of three factors – I know something (the password), I have something (a smartcard or a hardware token) or I am something (fingerprint, retina or iris reading)
wildcard certificate	certificate containing at least one wildcard domain name within the subjectAlternativeName extensions in the Certificate
wildcard domain name	string starting with “*.” immediately followed by a FQDN
written contract	text of the contract in electronic or paper form
XN-label	class of LDH labels prefixed by "xn--" (from RFC 5890)

Table 3 – Acronyms

Acronym	Explanation
ARC	Alarm Receiving Centre
ASCII	American Standard Code for Information Interchange, table containing binary codes of English alphabets, numbers and other common symbols
BIH	Bureau International de l'Heure – The International Time Bureau
bit	from English *binary digit* – a binary system digit – the fundamental and the smallest unit of information in digital technologies
BRG	document "Baseline Requirements for the Issuance and Management of Publicly-Trusted TLS Server Certificates" published by CA/Browser Forum
CA	certification authority
CAA	DNS Resource Record - see RFC 6844
CCADB	The Common CA Database (CCADB), a repository of information about CAs whose root and intermediate certificates are included within the products and services of several Root Store Operators.
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	certificate policy
CPS	certification practice statement
CR	Czech Republic
CRL	Certificate Revocation List – the list of revoked certificates, which are not held as valid any longer
CT	Certificate Transparency, the system to mitigate misissuance of certificate based on adding new certificate (or rather precertificate) to public logs making possible to detect the misissuance (especially fraudulent getting the certificate by other than authorized applicant)
ČSN	Czech Technical Norm
DER, PEM	methods of certificate encoding (certificate formats)
DV	Domain Validation, SSL certificate type
DNS	Domain Name System, a hierarchical decentralized naming system implemented by DNS servers which are exchanging information via DNS protocol to translate domain names to the numerical IP addresses
EBA	European Banking Association

EC	Elliptic Curve
ECC	Elliptic Curve Cryptography
eIDAS	REGULATION (EU) no 910/2014 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 23 July 2014 on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC, as amended
EN	European Standard, a type of ETSI standard
ESI	Electronic Signatures and Infrastructures
ETSI	European Telecommunications Standards Institute, a European standardization institute for information and communication technologies
EU	European Union
EV	Extended Validation, type of SSL certificate or certificate intended for websites authentication
EVCG	document "Guidelines For The Issuance And Management Of Extended Validation Certificates" published by CA/Browser Forum
EVCP	Extended Validation Certificate Policy, type of certificate policy
FAS	Fire Alarm System
FIPS	Federal Information Processing Standard, standards for information technologies for U.S. non-military state organizations
FQDN	Fully Qualified Domain Name, a Domain Name that includes the Domain Labels of all superior nodes in the Internet Domain Name System
GDPR	General Data Protection Regulation, REGULATION (EU) 2016/679 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation)
gTLD	generic TLD, top level domain (e.g. .org for non-profit organizations)
html	Hypertext Markup Language, markup language for creating hypertext documents
http	Hypertext Transfer Protocol, protocol for exchanging html documents
https	Hypertext Transfer Protocol, protocol for secure exchanging of html documents
I.CA	První certifikační autorita, a.s.
IAS	Intrusion Alarm System
ICA_OID	OID belonging to OID space allocated to I.CA
ICANN	Internet Corporation for Assigned Names and Numbers, organization which among others assigns and administrates domain names and IP addresses
IEC	International Electrotechnical Commission, the global organization publishing standards for electrical and electronic engineering, communication technologies and related industries

IP	Internet Protocol, principal communications protocol in the Internet protocol suite for relaying packets across network and routing used in the Internet
IPS	Intrusion Prevention System
ISMS	Information Security Management System
ISO	International Organization for Standardization, an international organization of national standardization organizations; designation of standards
IT	Information Technology
ITU	International Telecommunication Union
ITU-T	Telecommunication Standardization Sector of ITU
MPSV	Ministry of Labor and Social Affairs of the Czech Republic
NCA	National Competent Authority - authority responsible for approving or rejecting authorization of payment services providers and assigning PSP numbers to them in particular state; see also PSP registrar above
NCP	Normalized Certificate Policy, non-qualified certificates certificate policy, qualitatively the same as certificate policy for issuing qualified certificates
NCP+	Extended Normalized Certificate Policy, NCP certificate policy requiring a secure cryptographic device
OCSP	Online Certificate Status Protocol, the protocol to identify public key certificate status
OID	Object Identifier
OSVČ	self-employed person
OV	Organization Validation, SSL certificate type
PDCA	Plan-Do-Check-Act, Deming cycle, management method for control and continuous improvement
PDS	PKI Disclosure Statement
PKCS	Public Key Cryptography Standards, designation for a group of standards for public key cryptography
PKI	Public Key Infrastructure
PSD	Payment Services Directive, DIRECTIVE 2007/64/EC OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL on payment services in the internal market
PSD2	DIRECTIVE (EU) 2015/2366 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL, superseding PSD and coming into effect January 13th 2018
PSP	Payment Service Provider
PSS	Probabilistic Signature Scheme, electronic signature schema developed by M. Bellar and P. Rogaway and standardized as part of PKCS#1 v2.1
PTC	Publicly-Trusted Certificate

PUB	Publication, FIPS standard designation
QSCD	Qualified Electronic Signature/Seal Creation Device (defined by eIDAS)
QWAC	Qualified Website Authentication Certificate
RA	registration authority
RFC	Request for Comments, designation for a range of standards and other documents describing web protocols, systems, etc.
RSA	signing and encrypting public key cipher (acronym from the names of the original authors - Rivest, Shamir and Adleman)
RTS	COMMISSION DELEGATED REGULATION (EU) 2018/389 of 27 November 2017 supplementing Directive (EU) 2015/2366 of the European Parliament and of the Council with regard to regulatory technical standards for strong customer authentication and common and secure open standards of communication
SCT	Signed Certificate Timestamp, signed timestamp from relevant CT log which confirms adding the precertificate
sha, SHA	type of hash function
SSL	Secure Sockets Layer, communication protocol, layer inserted between transport layer and application layer, providing securing of communication via encryption and authentication of communicating parties
TLD	Top Level Domain, top level Internet domain, in domain name the top-level domain is placed at the end
TLS	Transport Layer Security, communication protocol superseding SSL
TS	Technical Specification, type of ETSI standard
TSA	Time-Stamping Authority
TSS	Time-Stamp Server
TSU	Time-Stamp Unit
UPN	User Principal Name, username based on RFC 822
UPS	Uninterruptible Power Supply/Source
URI	Uniform Resource Identifier, defined-structure text string for accurate specification of a source of information
UTC	Coordinated Universal Time, the standard adopted on 1 January 1972 for the global coordinated time – Bureau International de l'Heure (BIH) plays the role of the 'official keeper' of the atomic time for the whole world
WHOIS	database including domain name registrant technical, billing and administrative contact information
ZOOÚ	current personal data protection legislation

2 PUBLICATION AND REPOSITORY RESPONSIBILITIES

2.1 Repositories

První certifikační autorita, a.s., sets up and operates repositories of both public and non-public information 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, data box of I.CA ID is a69fvfb.

The aforesaid website provides information about:

- Certificates of certification authorities and time-stamping authorities;
- Public certificates – the following information is published (and more information can be obtained from the Certificate):
  - Certificate number;
  - Content of commonName;
  - Valid from date (specifying the hour, minute and second);
  - Link to where the certificate can be obtained in the specified format (DER, PEM, TXT).
- Certificate revocation 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, practice statements and other public information.

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

Any revocation of certification authority certificate because of suspected or actual compromise of a given private key will be announced by I.CA on its web Information Address and in Hospodářské noviny or Mladá fronta Dnes, daily newspapers with national distribution.

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.

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

The Certification Authority issuing the Certificates complies with the requirements of the current version of the CCADB policy available at https://www.ccadb.org/policy.

2.3 Time or frequency of publication

I.CA publishes information with the following periodicity:

- Certificate policy - after approval and release of the new version, updates depending on changes of normative requirements concerning issued Certificates; revision at least once a year;
- Certification practice statement - immediately (if intended for publication);
- List of the certificates issued – updated immediately after issuing a new certificate to be published;
- Certificate revocation list (CRLs) - see chapter 4.9.7;
- Information about certification authority's certificate revocation with the reason of revocation – immediately;
- Other public information - not predetermined, but generally this information must reflect the current status of the services provided.

2.4 Access controls on repositories

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

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

3 IDENTIFICATION AND AUTHENTICATION

3.1 Naming

3.1.1 Types of names

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

3.1.2 Need for names to be meaningful

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

3.1.3 Anonymity or pseudonymity of subscribers

Certificates issued under this CP do not support either anonymity or pseudonymity.

3.1.4 Rules for interpreting various name forms

The data are transferred to subject attribute or subjectAlternativeName extension of the Certificate in the form they are specified in the application.

3.1.5 Uniqueness of names

The Authority guarantees that the subject field in a Certificate of 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 one of 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 and domain 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).

Data sources which are used for organization in Certificates legal identity and existence validation are stated on webpages www.ica.cz (part "Quick link labels" on homepage and then "PKI Disclosure Statement").

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. In case of government entities only legal identity and existence are validated. Any other entity must fulfil at least one of following conditions:

- 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 holds an active (current or deposit) account with a financial institution subject to the national bank's supervision; this is verified:
  - By getting the proof of the account's existence 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;

Entity is listed in the current list of tax subjects maintained by tax administration (Qualified Government Tax Information Source - QTIS) or in generally recognized independent register (Qualified Independent Information Source - QIIS).

3.2.2.4 Validation of Domain Authorization or Control

From March 15, 2025, in accordance with BRG, only the following method is used to validate domain name authorization or control:

- BRG, chapter 3.2.2.4.4 "Constructed Email to Domain Contact".

Previously also used methods:

- BRG, chapter 3.2.2.4.2 „Email, Fax, SMS, or Postal Mail to Domain Contact"; and
- BRG, chapter 3.2.2.4.7 „DNS Change";

are not used from March 15, 2025.

From March 15, 2026, in accordance with BRG. the DNSSEC protocol is used when validating domain authorization or control from the I.CA network (Primary Network Perspective).

Domain names constraints are stated in Certificate profile in chapter 7.1.2 (dNSName attribute).

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

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 "ica.cz“.

In an opposite case the application in rejected.

From March 15, 2026, in accordance with BRG, the DNSSEC protocol is used when validating CAA records.

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.

3.2.2.7 Multi-Perspective Issuance Corroboration

Before issuing a Certificate I.CA performs, in accordance with BRG, multi-perspective validation of domain authorization or control and CAA records.

3.2.3 Authentication of individual identity

Two documents, primary and secondary, 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 validated in this document:
  - Full civil name;
  - Date and place of birth or the birth certification number if shown in the primary document;
  - Number of the primary personal document;
  - Permanent address (if shown in the primary document).
- The secondary document must contain a unique identification, such as birth certification number or personal identity card number, matching it to the primary document and must show at least one of these items:
  - Date of birth (or birth certification number if specified);
  - Permanent address;
  - Photograph of the face.

  The secondary personal document data closely 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;
- At least 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 for 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 concluding the contract, submitting 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 signing the Certificate issuance contract and of the person approving the data in the Certificate;
- Validation of 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.

Cross certificates are not used.

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.

I.CA can use for issuing the Certificate (same user and domain) information collected by previous validation as described in chapter 3.2 under conditions stated in chapter 4.2.1.

3.3.2 Identification and authentication for re-key after revocation

I.CA does not support re-keying of revoked Certificates. The only way is to obtain a new Certificate with a new public key. The same requirements as those in the initial identity authorization apply.

3.4 Identification and authentication for revocation request

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

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

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

- Using the form on the company's website (and using the Certificate revocation password);
- Using an unsigned electronic message containing the Certificate revocation password and sent to revoke@ica.cz from the contact e-mail address indicated during enrollment process;
- Using a signed electronic message sent to revoke@ica.cz from the contact mailing address indicated during enrollment process, electronic signature must be created using private key related to the public key contained in the certificate of the defined person authorized to represent the Organization in the contractual relationship with I.CA;
- Using the data box of I.CA (and using the Certificate revocation password);

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

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

I.CA reserves the right to accept also other Certificate revocation identification and authentication procedures, which, however, must not be contrary to trust services legislation or to requirements of technical standards regarding this type of Certificates.

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.

4.1.2 Enrollment process and responsibilities

Before submission of an application the applicant must conclude the 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 others, 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 concluding the Certificate issuance contract;
- Conclude with the subscriber or the Organization such a Certificate issuance contract that meets the requirements of trust service legislation and relevant technical standards and norms;
- During the Certificate issuance process, check with RA all the data which can be validated specified in the application against the documents submitted;
- Require the proof of fact that private key was generated and stored on QSCD;
- Issue a Certificate that contains materially correct data on the basis of the information available to the Service provider as at the issuance of the Certificate;
- Publish public information in accordance with 2.2;
- Publish the Authority's certificates and the root CA's certificates;
- Provide any Service-related activity in accordance with trust services legislation, this CP, the relevant CPS, the System Security Policy – Trustworthy Systems and the operational 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:

- 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.

In the data validation process (for the same applicant and domain), I.CA may use information validated previously, provided that it is not older than the maximum validity period of the verified data specified in BRG.

4.2.2 Approval or rejection of certificate applications

I.CA does not issue certificates for gTLD domain .onion. 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

When issuing the Certificate:

- CA operators or software installed on their workstations can perform:
  - Visual check of the consistency of the data contained in the Certificate application (PKCS#10 structure) and the data entered by the RA employee;
  - Visual check of the formal correctness of the data;
  - Checking of the private key possession, supported hash functions in the Certificate request (minimum sha-256), and checking the formal correctness of the data;

- CA system core software always performs checking of private key possession, checks of supported hash functions in the Certificate request (minimum sha-256) and checks of formal data correctness.

Compliance of the Certificate profile with BRG requirements ("linting") and checking for known weak keys are automatically performed by the CA system core using recommended tools.

If any of these checks gives a fail result, the Certificate issuance procedure is terminated.

The Certificate is issued after willful and electronically signed (advanced electronic signature based on non-qualified certificate) command of authorized Operator to issue the Certificate.

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 take the Certificate. The only way to refuse taking over the Certificate is to request 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 legislation concerning personal data protection;
- 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 Service contract;
- 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 this CP in a manner as to prevent any unauthorized use of the private key;
- Notify immediately the Service provider of everything that leads to the Certificate's revocation, in particular of:
  - Suspected abuse of the private key; or
  - Invalidity or inaccuracy of entries in Certificate;

  In this case request for the Certificate's revocation and stop using the pertinent private key.

4.5.2 Relying party public key and certificate usage

Relying parties must, among other things:

- Obtain from a secure source (eg., www.ica.cz, RA, relevant trust list) the certification authority certificates related to the end user certificate issued under a specific CP, and verify the checksum and validity of these Certificates;
- Perform all actions necessary for them to verify that the Certificate is valid;
- Abide by any provision of this CP and relevant legislation and technical standards which relate to the relying party's duties.

4.6 Certificate renewal

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

Certificate renewal 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 under this CP means the issuance of a new Certificate (subsequent Certificate) with new public key without changing any other information in the Certificate.

The Certificate re-key is not provided.

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

Certificate modification under this CP means the issuance of a new Certificate in which at minimum one change is made to the content of the attributes concerning the Certificate's

subscriber (the subject field or the subjectAlternativeName extension) or in which one field requiring content validation is deleted or added.

The Certificate modification 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 via using the form on the company's website.

Certificate revocation requests may be submitted irrespective of the time of the day via e-mail, data box or letter. In these cases, the request is accepted no later than the new working day after delivery.

Certificate revocation requests may be submitted to RA only during opening hours of specific RA. In this case the request is accepted immediately.

Certificate suspension is not provided by I.CA, just as the revocation at a certain date and time in the future.

4.9.1 Circumstances for revocation

4.9.1.1 Certificate revocation reasons

I.CA revokes the Certificate within 24 hours and enters the corresponding CRLReason (see chapter 7.2.2) if one or more of the following reasons occurs:

1. Subscriber submits the Certificate revocation request in writing (unspecified(0); this code is not entered in CRLReason);
2. Subscriber notifies I.CA that the original Certificate application was not authorized and does not retroactively grant authorization (CRLReason #9, privilegeWithdrawn);
3. I.CA obtains evidence that Subscriber's private key corresponding to the public key in the Certificate suffered a key compromise (CRLReason #1, keyCompromise);
4. I.CA is made aware of a demonstrated or proven method that can easily compute the Subscriber's Private Key based on the Public Key in the Certificate (such as a Debian Weak Key (CRLReason #1, keyCompromise);
5. I.CA obtains evidence that the validation of domain authorization or control any FQDN contained in the Certificate should not be relied upon (CRLReason #4, superseded).

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

6. Certificate no longer complies with the requirements for cryptographic algorithms and their parameters (quality, see 6.1.5 and 6.1.6) CRLReason #4, superseded);
7. I.CA obtains evidence that the Certificate was misused (CRLReason #9, privilegeWithdrawn);
8. I.CA is made aware that a Certificate subscriber has violated one or more of his material obligations under Service contract or under the contract on the terms and conditions of use of the Certificate (CRLReason #9, privilegeWithdrawn);
9. I.CA is made aware of any circumstances indicating that the fully qualified domain name (FQDN) in the Certificate is no longer legally permitted (i.e., a court or an arbitrator has revoked the domain name registrant's right to use the domain name, a relevant licensing or services agreement between the domain name registrant and the subscriber has terminated, or the domain name registrant has failed to renew the domain name) (CRLReason #5, cessationOfOperation);
10. Wild card certificate – not applicable for Certificates issued by I.CA (CRLReason #9, privilegeWithdrawn);
11. I.CA is made aware of a material change in the information contained in the Certificate (CRLReason #9, privilegeWithdrawn);
12. I.CA is made aware that the Certificate was not issued in compliance with CP or CPS (CRLReason #4, superseded);
13. I.CA determines or is made aware that some information contained in the Certificate is inaccurate (CRLReason #9, privilegeWithdrawn);
14. I.CA's right to issue Certificate under BRG and this CP expired or is revoked or terminated, unless I.CA has made arrangements to continue maintaining CRL/OCSP repository (unspecified(0); this code is not entered in CRLReason);
15. Revocation is required by CP or CPS;
16. CRLReason #1, keyCompromise when I.CA is made aware of:

- Demonstrated or proven method that exposes subscriber's private key to compromise;
- Clear evidence that the specific method used to generate private key was flawed.

4.9.1.2 Reasons to revoke the Authority's certificate

I.CA revokes the Authority's certificate within seven days if one or more of the following reasons occurs:

1. Authority requests revocation in writing;
2. Authority notifies the root certification authority that original Certificate application was not authorized and does not retroactively grant authorization;
3. Root certification authority obtains evidence that the Authority's private key corresponding to the public key in the Certificate suffered a key compromise or no longer complies with the cryptographic algorithm requirements and the required parameters (quality, see 6.1.5 and 6.1.6);
4. Root certification authority obtains evidence that 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
   - No longer complies with the requirements of CP or CPS;
6. I.CA determines that any of the information appearing in the Authority's certificate is inaccurate or misleading;
7. Root CA or Authority ceases operations for any reason and has not made arrangements for another CA to provide revocation support for the Certificates;
8. Root CA's or Authority's right to issue Certificates under this CP expires or is revoked or terminated unless root CA has made arrangements to continue maintaining 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;
- Subject explicitly specified therefore in Service (under this CP) contract;
- Provider of this Service (CEO of I.CA or his deputy is the person authorized to request for the revocation of a certificate issued by I.CA, subscriber of the Certificate is informed by electronically signed e-mail sent to contact e-mail address indicated during enrollment process):
  - If the Certificate is issued on the basis of false data;
  - If demonstrably finds out that the private key belonging to the public key specified in the Certificate has been compromised;
  - If demonstrably finds out that the Certificate is issued in spite of noncompliance with the requirements of trust services legislation;

- If demonstrably finds out 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 certificate revocation request, the subscriber must immediately stop using the Certificate along with the corresponding private key.

In addition to this third parties (supervisory bodies, relying parties, application software suppliers etc.) can send report on problem with Certificate informing Authority about sufficient reasons for Certificate's revocation - 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 request:

- Using the form on the information web page http://www.ica.cz. The Certificate revocation date and time are the date and time when the valid certificate revocation request is dealt with in the CA's information system. The requestor receives a notice if the request is accepted;
- Using e-mail:
  - Electronic message signed electronically – body must contain the 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 either in decimal or hexadecimal format (introduced by the string '0x');
  - Electronic message not signed electronically - body must contain the 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 either in decimal or hexadecimal format (introduced by the string '0x').

    Note: If the request meets the requirements of options listed above, the employee in charge immediately revokes the Certificate in the CA's system, and the date and time when the request is processed by the CA's information system are the date and time of the Certificate's revocation. The requestor receives a notice if the request is accepted.
- Using registered post letter or data box - the request must contain the text (in Czech or Slovak with or without diacritics, or in English):

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

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

where '*xxxxxxx*' is the Certificate's serial number and '*yyyyyy*' the revocation password. The serial number must be given either in decimal or hexadecimal format (introduced by the string '0x'). Requestor may specify the reason of revocation (see 4.9.1.1). If the request meets these requirements, the I.CA employee in charge immediately revokes the Certificate in the CA's system, and the date and time the request is processed by the CA's information system are the date and time of the Certificate's revocation. If the request cannot be accepted (wrong revocation password), the certificate revocation request will be rejected. Requestor is informed in the same way as the request was sent i.e., by a registered letter sent to postal address of requestor or by data box, how the request was handled.

4.9.3.2 Suspected key compromise and abuse of Certificate

Report on suspected compromise of private key related to public key in the Certificate, Certificate misuse, or other types of fraud, compromise, misuse, inappropriate conduct, or any other matter related to Certificate may be sent to e-mail address referred to in chapter 1.5.2, or by registered letter to address of I.CA registered office or by data box.

4.9.4 Revocation request grace period

Revocation request must be submitted immediately; request grace is not permissible.

4.9.5 Time within which CA must process the revocation request

4.9.5.1 Certificate revocation request

Any certificate revocation request 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 problems

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 Certificate revocation is necessary, both subscriber and person who reported the problem are informed about the decision.

If revocation of the Certificate is necessary, then the Certificate revocation date is determined based on the following 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 the 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

EVCG require the validity of CRL (difference between nextUpdate and thisUpdate) to be 10 days at maximum. I.CA issues CRL immediately after revocation of any Certificate, if no Certificate is revoked then new CRL is issued usually 8 hours after issuing the previous CRL, but no more than 24 hours after issuing the previous CRL.

4.9.7.2 Status of the certificate of the CA issuing certificates

EVCG require the validity of root CA CRL (difference between nextUpdate and thisUpdate) to be 12 months at maximum. I.CA issues CRL immediately after revocation of any subordinate CA certificate, if no subordinate CA certificate is revoked then new root CA CRL is issued usually 6 months after issuing the previous root CA CRL, but no more than 12 months after issuing the previous root CA CRL.

4.9.8 Maximum latency for CRLs (if applicable)

CRL is released immediately after the issuance, conditions described in chapters 4.9.5 are 4.9.7 always observed.

4.9.9 On-line revocation/status checking availability

On-line revocation/status checking using the OCSP protocol is a service available to the general public. Every certificate issued under this CP includes a link to the pertinent (authorized) OCSP responder.

OCSP responses comply with RFC 6960 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 both GET and POST methods. OCSP responses to status requests of unissued certificate do not return good status.

4.9.10.1 Certificate status

EVCG require OCSP response validity to be between 8 hours and 10 days (now set to 24 hours).

After any Certificate revocation the OCSP response is actualized immediately (Certificate suspension is not provided by I.CA).

OCSP responses are automatically actualized (i.e., the validity of the item in internal cache of OCSP responder expires) when earlier of following conditions is met:

- half of OCSP response validity period (for responses with validity less than 16 hours);

- 8 hours before the end of OCSP response validity period (for responses with validity 16 hours and more).

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 for this document; the Certificate suspension service is not provided.

4.9.14 Who can request suspension

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

4.9.15 Procedure for suspension request

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

4.9.16 Limits on suspension period

Not applicable for 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; certificate revocation 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 is specified in the certificates issued by these authorities.

Information about revocation in CRL or in OCSP response is held at least till the expiration of revoked Certificate.

4.10.2 Service availability

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

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

Continuous availability 24x7 is ensured via e-mail address referred to in chapter 1.5.2. Due to this I.CA can internally react to serious problem report and, if necessary, to forward information about the received report to relevant body or to revoke the Certificate which is subject of the report.

4.10.3 Optional features

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

4.11 End of subscription

The certificate issuance contract expires when the last certificate issued under this contract expires.

4.12 Key escrow and recovery

Not applicable for this document; the key escrow and recovery service is not provided.

4.12.1 Key escrow and recovery policy and practices

See 4.12.

4.12.2 Session key encapsulation and recovery policy and practices

See 4.12.

5 FACILITY, MANEGEMENT, AND OPERATIONAL CONTROLS

Facility, management, and operational controls primarily deal with:

- Trustworthy systems supporting trust services;
- All processes supporting trust services.

The facility, management, and operational controls are addressed in the fundamental documents Corporate Security Policy, System Security Policy – Trustworthy Systems, Certification Practice Statement, Business Continuity Plan and Recovery Plan as well as 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 supporting trust services are situated on reserved premises of operating sites. These premises are secured in a manner similar to that required by the Classified Information Protection Act for the ‘Confidential’ category secure areas.

5.1.2 Physical access

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

5.1.3 Power and air conditioning

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

5.1.4 Water exposures

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

5.1.5 Fire prevention and protection

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

5.1.6 Media storage

Archive 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 where the records originated.

Any paper media required to be archived are stored in a site geographically different from the site of the operating office where the records originated.

5.1.7 Waste disposal

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

5.1.8 Off-site backup

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

5.2 Procedural controls

5.2.1 Trusted roles

Trusted roles are defined for selected activities conducted 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.

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

5.2.2 Number of persons required per task

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

- Initialization of cryptographic module;
- Generating key pairs of certification authorities and their OCSP responders;
- Destroying private keys of certification authorities and their OCSP responders, including their backups;

- Backup and restore of private keys of certification authorities and their OCSP responders;
- Activation and deactivation of private keys of certification authorities and their OCSP responders.

Data in Certificate application are validated by two trustworthy employees in the roles "validation specialist" and "cross checking specialist". Their activity is described in internal documentation.

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

5.2.3 Identification and authentication for each role

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

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

5.2.4 Roles requiring separation of duties

The roles requiring 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

Trusted roles employees are in I.CA selected and hired using the following criteria:

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

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

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

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

5.3.2 Background check procedures

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

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

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

5.3.3 Training requirements

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

5.3.4 Retraining frequency and requirements

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

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

5.3.5 Job rotation frequency and sequence

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

5.3.6 Sanctions for unauthorized actions

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

5.3.7 Independent contractor requirements

I.CA may or must procure some activities from independent contractors and is fully liable for the job they deliver. These business relations are regulated by 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 certificate policies, the relevant parts of internal documentation provided for them, and the required normative documents. Contractual penalties are applied for a breach of the obligations or duties specified in the said documents, or the contract with the contractor in breach is terminated immediately.

5.3.8 Documentation supplied to personnel

In addition to the certificate policy, the certificate practice statement and the security and operational 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

All events required by the trust services legislation and relevant technical standards and norms, including those from delegated third parties involved in the certificate lifecycle, are recorded. The generating of CRLs and OCSP responses is recorded too.

Both CRL generating and OCSP answers are logged.

The certification authorities' key pair generating is a special case of event logging. All this process complies with trust services legislation and the relevant technical and other standards. Generating is conducted according to a pre-determined scenario in a physically secure environment and under the control of more I.CA employees in trusted roles. Protocol on key pair generating with data required by technical standards is signed by present employees in trusted roles. When the key pair of subordinate certification authority issuing SSL type certificates for end users is generated then the process is also video recorded.

When the key pair of root certification authority is generated, an auditor qualified in accordance with current technical standards personally attends the process, signs also the created protocol to confirm that the generating followed the pre-determined scenario and the measures to ensure integrity and confidentiality were in place.

Logging of security events in systems, on network components and operation sites entrances is done in compliance with chapters 6.5 and 6.6 of this document and meets requirements of EVCG.

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 ten years of the day they are made.

5.4.4 Protection of audit log

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

Electronic audit records are archived in two copies. Printed audit records are kept outside the operating premises of I.CA.

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

5.4.5 Audit log backup procedures

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

5.4.6 Audit collection system (internal vs. external)

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

5.4.7 Notification to event-causing subject

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

5.4.8 Vulnerability assessments

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

5.5 Records archival

The archiving of records, i.e., information and documentation, performs I.CA according to internal documentation.

5.5.1 Types of records archived

I.CA archives the following electronic or printed records pertaining to the trust services provided, including those recorded by third parties involved in certificate life-cycle, such as:

- Records / protocols on the course of certification authorities key pair generating;
- For subordinate CAs issuing SSL type certificates to end users:
  - Video recording of the key pair generating process;
- Life cycle records for the certificates (especially the documents relating to validation of certificate issuance applications and certificate revocation requests);
- Audit logs according to 5.4.1;
- Information handling records, such as takeover, handover, saving, check, conversion from printed to electronic, etc.;
- Operational and security documentation.

5.5.2 Retention period for archive

Records relating to the certificates of all I.CA certification authorities and corresponding OCSP responders, excluding appropriate private keys, are kept throughout the existence of I.CA. Other records are kept in accordance with chapter 5.4.3.

The record archiving procedures are regulated by internal documentation.

5.5.3 Protection of archive

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

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

5.5.4 Archive backup procedures

The record backup procedures are regulated by internal documentation.

5.5.5 Requirements for time-stamping of records

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

5.5.6 Archive collection system (internal or external)

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

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

5.5.7 Procedures to obtain and verify archive information

Archived information and records are stored in designated locations and are accessible to:

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

A written record is made of any such permitted access.

5.6 Key changeover

In standard situations (expiration of a certification authority certificate), the key is replaced by issuing a new certificate a good time in advance (no later than one year prior to the expiration).

In non-standard situations, for instance such progress in cryptanalytic methods that could compromise the security of certificate issuance (e.g., changes to cryptanalytic algorithms or key length), the key is replaced as soon as possible.

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

5.7 Compromise and disaster recovery

5.7.1 Incident and compromise handling procedures

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

In case of need to quickly revoke a large number of Certificates, I.CA has developed a mass revocation plan (Plán pro hromadnou revokaci certifikátů).

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

See 5.7.1.

5.7.3 Entity private key compromise procedures

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

- Stops using the private key;
- Revokes immediately and permanently the pertinent certificate and destroys the corresponding private key;
- Revokes all valid certificates issued by pertinent certification authority;
- Immediately informs about this fact, including the reason of revocation, in accordance with Chapter 2.2; the list of revoked certificates is also 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 procedure will be applied in the event that cryptanalytic methods develop to such an extent (e.g., changes in cryptographic algorithms, key lengths, etc.) that the security of trust services could be immediately threatened.

5.7.4 Business continuity capabilities after a disaster

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

5.8 CA or RA termination

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

- The termination of the Authority's operations must be notified in writing to the supervisory body, all subscribers of valid Certificates, and the parties having a contract with I.CA that directly concerns the provision of trust services;
- The termination of the Authority's operations must be published on the web page pursuant to 2.2;

- If the Authority's certificate's expiration is part of the termination of operations, this information plus the reason for expiration must be included in that notice;
- The termination of operations is a controlled process following a pre-defined plan, which includes the description of the procedure to preserve and disclose information for judicial or administrative proceedings discovery and for arranging the continuity of services;
- The Authority or its successor must be able to revoke Certificates and publish CRLs as long as any Certificate issued by the Authority is valid;
- After that the Authority must demonstrably destroy its private key, make a record of this destruction and keep this record in accordance with this CP.

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

- The information must be notified in writing or electronically to all subscribers of valid Certificates, and the parties having 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

Key pairs of certification authorities and their corresponding OCSP responders are generated in designated secured areas of operating sites, according to a pre-defined scenario, in accordance with 5.2 and 5.4.1. Generating is conducted in cryptographic modules fulfilling requirements of trust service legislation, i.e., ETSI and CEN standards.

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

Key pairs of the employees taking part in the issuing Certificates are generated on smartcards meeting the QSCD requirements. The private keys of these key pairs are stored on smartcard in non-exportable form and PIN needs to be entered to use the keys.

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

Before issuing the Certificate, checks are conducted in accordance with BRG (see chapters 4.3.1, 6.1.5, 6.1.6).

6.1.2 Private key delivery to subscriber

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

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

6.1.3 Public key delivery o certificate issuer

Public keys are delivered to certificate issuer in the certificate application (the PKCS#10 format).

6.1.4 CA public key delivery to relying parties

Following options for obtaining the Authority's public key contained in its certificate are guaranteed:

- Handover from RA;
- From the trust list of the Czech Republic;
- Via web information addresses of I.CA, relevant supervisory body or its journal;
- Every subscriber gets relevant certification authorities' certificates together with his primary certificate.

6.1.5 Key sizes

The size of the key of I.CA root certification authority using RSA algorithm is 4096 bits, the size of the keys in certificates of subordinate certification authorities issued by this root certification authority is 2048 bits at minimum, the size of the keys of OCSP responders is 2048 bits at minimum. The minimum size of the keys in the Certificates issued under this CP is 2048 bits.

6.1.6 Public key parameters generation and quality checking

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

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

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

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

6.2 Private key protection and cryptographic module engineering controls

6.2.1 Cryptographic module standards and controls

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

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

Using cryptographic modules by end users is fully within their competence.

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

If cryptographic module related operations require the presence of more persons, then each of them knows only part of the code required for these operations.

6.2.3 Private key escrow

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

6.2.4 Private key backup

The private keys of CAs and their corresponding OCSP responders protected by cryptographic modules are backed up in an encrypted form that provides the same level of protection as cryptographic module.

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

Backup of private keys related to Certificates of end users is fully within the competence of these end users.

6.2.5 Private key archival

When certification authorities' and their corresponding OCSP responders' private keys expire, they are not archived but destroyed including their backup copies.

Archiving period of private keys of employees taking part in issuing certificates is limited by the memory capacity of the smartcard

Archiving private keys related to Certificates of end users is fully within the competence of these end users.

6.2.6 Private key transfer into or from a cryptographic module

Private keys of certification authorities and their corresponding OCSP responders are generated (as non-exportable) in cryptographic modules (operated in certified mode) and there is no way to export them outside the cryptographic module[1]. Import of private keys into the cryptographic module is not performed.

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

Transferring private keys related to Certificates of end users is fully within the competence of these end users.

6.2.7 Private key storage on cryptographic module

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

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

Possible storing private keys related to Certificates of end users on cryptographic modules is fully within the competence of these end users.

6.2.8 Method of activating private key

Activation of certification authorities' and their corresponding OCSP responders' private keys (allowing the use of these private keys) is done:

- In case of smartcard activation by inserting the smartcard into card reader and entering the password;
- In case of softcard activation by entering the softcard and password.

[1] Encrypted backup is the only one exception, this backup can be used only in cryptographic module (or in HA/LB modules), where the key was generated.

Private keys of employees taking part in issuing certificates are activated by inserting the smartcard into card reader and entering PIN.

Activation private keys related to Certificates of end users is fully within the competence of these end users and depends on the way of storing these private keys.

6.2.9 Method of deactivating private key

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

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

Deactivation private keys related to Certificates of end users is fully within the competence of these end users and depends on the way of storing these private keys.

6.2.10 Method of destroying private key

After expiration of specific certification authority's private key and based on subsequent decision of CEO of I.CA this private key is destroyed according to specific procedure including all backups of this key. Destroying is documented in a written record.

Private keys of OCSP responders are destroyed on the decision of I.CA representative when issuing OCSP responder's certificate. Destroying is documented in a written record.

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

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

6.2.11 Cryptographic module rating

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

Smartcards used for generating of key pairs and storing corresponding private keys of employees taking part in issuing certificates meet QSCD requirements.

Usage of cryptographic modules by end users (including evaluation these modules) is fully within the competence of these end users.

6.3 Other aspects of key pair management

6.3.1 Public key archival

All public keys as part of Certificates are archived throughout the existence of I.CA.

6.3.2 Certificate operational periods and key pair usage periods

The validity period of each Certificate issued in accordance with BRG is specified in the body of that Certificate and is the same as key pair usage period (see chapter 7).

6.4 Activation data

6.4.1 Activation data generation and installation

Activation data of certification authorities' and their corresponding OCSP responders' private keys (smartcard or softcard) of are created before or during the generating of the corresponding key pair.

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

Usage of activation data by end users is fully within the competence of these end users.

6.4.2 Activation data protection

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

Activation data of employees' taking part in issuing certificates private keys protection is fully within the competence of these employees.

Activation data of end users' private keys protection is fully within the competence of these employees.

6.4.3 Other aspects of activation data

Not applicable for this document.

6.5 Computer security controls

6.5.1 Specific computer security technical requirements

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

6.5.2 Computer security rating

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

- CEN/TS 419261 Security Requirements for Trustworthy Systems Managing Certificates and Time-stamps;

- ČSN ETSI EN 319 401 Electronic Signatures and Infrastructures (ESI) – General Policy Requirements for Trust Service Providers;
- ETSI EN 319 401 Electronic Signatures and Infrastructures (ESI); General Policy Requirements for Trust Service Providers;
- ČSN ETSI EN 319 403-1 Electronic Signatures and Infrastructures (ESI); Trust Service Provider Conformity Assessment; Part 1: Requirements for conformity assessment bodies assessing Trust Service Providers;
- ETSI EN 319 403-1 Electronic Signatures and Infrastructures (ESI); Trust Service Provider Conformity Assessment; Part 1: Requirements for conformity assessment bodies assessing Trust Service Providers;
- ČSN ETSI EN 319 411-1 Electronic Signatures and Infrastructures (ESI) – Policy and Security Requirements for Trust Service Providers Issuing Certificates – Part 1: General Requirements;
- ETSI EN 319 411-1 Electronic Signatures and Infrastructures (ESI); Policy and Security Requirements for Trust Service Providers Issuing Certificates; Part 1: General Requirements;
- ČSN ETSI EN 319 411-2 Electronic Signatures and Infrastructures (ESI) – Policy and Security Requirements for Trust Service Providers Issuing Certificates – Part 2: Requirements for Trust Service Providers Issuing EU Qualified Certificates;
- ETSI EN 319 411-2 Electronic Signatures and Infrastructures (ESI); Policy and Security Requirements for Trust Service Providers Issuing Certificates; Part 2: Requirements for Trust Service Providers Issuing EU Qualified Certificates;
- ČSN ETSI EN 319 412-1 Electronic Signatures and Infrastructures (ESI); Certificate Profiles; Part 1: Overview and Common Data Structures;
- ETSI EN 319 412-1 Electronic Signatures and Infrastructures (ESI); Certificate Profiles; Part 1: Overview and Common Data Structures;
- ČSN ETSI EN 319 412-2 Electronic Signatures and Infrastructures (ESI); Certificate Profiles; Part 2: Certificate Profile for Certificates Issued to Natural Persons;
- ETSI EN 319 412-2 Electronic Signatures and Infrastructures (ESI); Certificate Profiles; Part 2: Certificate Profile for Certificates Issued to Natural Persons;
- ČSN ETSI EN 319 412-3 Electronic Signatures and Infrastructures (ESI); Certificate Profiles; Part 3: Certificate Profile for Certificates Issued to Legal Persons;
- ETSI EN 319 412-3 Electronic Signatures and Infrastructures (ESI); Certificate Profiles; Part 3: Certificate Profile for Certificates Issued to Legal Persons;
- ČSN ETSI EN 319 412-4 Elektronické podpisy a infrastruktury (ESI) - Profily certifikátu – Část 4: Profil certifikátu pro certifikáty webových stránek;
- ETSI EN 319 412-4 Electronic Signatures and Infrastructures (ESI); Certificate Profiles; Part 4: Certificate profile for web site certificates;
- ČSN ETSI EN 319 412-5 Electronic Signatures and Infrastructures (ESI); Certificate Profiles; Part 5: QC Statements;
- ETSI EN 319 412-5 Electronic Signatures and Infrastructures (ESI); Certificate Profiles; Part 5: QCStatements;
- ČSN EN 419 221-5 Protection profiles for TSP Cryptographic modules - Part 5 Cryptographic Module for Trust Services;

- EN 419 221-5 Protection profiles for TSP Cryptographic modules - Part 5 Cryptographic Module for Trust Services;
- FIPS PUB 140-2 Requirements for Cryptographic Modules;
- ČSN ISO/IEC 15408-1 Information security, cybersecurity and privacy protection - Evaluation criteria for IT security - Part 1: Introduction and general model;
- ISO/IEC 15408-1:2022 Information security, cybersecurity and privacy protection - Evaluation criteria for IT security - Part 1: Introduction and general model;
- ČSN ISO/IEC 15408-2 Information security, cybersecurity and privacy protection - Evaluation criteria for IT security - Part 2: Security functional components;
- ISO/IEC 15408-2:2022 Information security, cybersecurity and privacy protection - Evaluation criteria for IT security - Part 2: Security functional components;
- ČSN ISO/IEC 15408-3 Information security, cybersecurity and privacy protection - Evaluation criteria for IT security - Part 3: Security assurance components;
- ISO/IEC 15408-3:2022 Information security, cybersecurity and privacy protection - Evaluation criteria for IT security - Part 3: Security assurance components;
- ETSI TS 119 312 Electronic Signatures and Infrastructures (ESI); Cryptographic Suites;
- European Cybersecurity Certification Group Sub-group on Cryptography - Agreed Cryptographic Mechanisms;
- CA/Browser Forum - Baseline Requirements for the Issuance and Management of Publicly-Trusted TLS Server Certificates (Baseline Requirements);
- CA/Browser Forum - Guidelines for The Issuance and Management of Extended Validation Certificates;
- ČSN EN ISO/IEC 27006 Information Technology – Security Techniques – Requirements for Bodies Providing Audit and Certification of Information Security Management Systems.
- ISO/IEC 17021 Conformity Assessment -- Requirements for Bodies Providing Audit and Certification of Management Systems;
- ISO/IEC 17065 Conformity Assessment -- Requirements for Bodies Certifying Products, Processes and Services.
- ISO 3166-1 Codes for the Representation of Names of Countries and Their Subdivisions – Part 1: Country Codes;
- ITU-T - X.501 Information Technology – Open Systems Interconnection – The Directory: Models;
- ITU-T - X.509 Information Technology – Open Systems Interconnection – The Directory: Public-key and Attribute Certificate Frameworks;
- ITU-T - X.520 Information Technology – Open Systems Interconnection – The Directory: Selected Attribute Types;
- RSA Laboratories - PKCS#10: Certification Request Syntax Standard;
- RFC 6960 X.509 Internet Public Key Infrastructure Online Certificate Status Protocol – OCSP;
- RFC 3647 Internet X.509 Public Key Infrastructure Certificate Policy and Certification Practices Framework;

- RFC 5019 The Lightweight Online Certificate Status Protocol (OCSP) Profile for High-Volume Environments;
- RFC 5280 Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile;
- EN 301 549 Accessibility requirements for ICT products and services.

6.6 Life cycle technical controls

6.6.1 System development controls

System development is carried out in accordance with internal documentation.

6.6.2 Security management controls

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

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

- ČSN EN ISO/IEC 27000 Information Technology – Security Techniques – Information Security Management Systems – Overview and Vocabulary;
- ČSN EN ISO/IEC 27001 Information security, cybersecurity and privacy protection - Information security management systems – Requirements;
- ČSN EN ISO/IEC 27002 Information security, cybersecurity and privacy protection - Information security controls.

6.6.3 Life cycle security controls

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

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

6.7 Network security controls

Network infrastructure of the operating site is protected with a firewall-type commercial product with an integrated intrusion prevention system. The detailed network security management

solution is described in internal documentation. All communication between RA and the operating sites is encrypted.

6.8 Time-stamping

See 5.5.5 for the time-stamping solution.

7 CERTIFICATE, CRL, AND OCSP PROFILES

7.1 Certificate profile

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 – Certificate basic fields

Field	Content
version	v3 (0x2)
serialNumber	unique serial number of the Certificate, greater than zero, random part at least 64 bits generated by random number generator used for cryptosystems
signatureAlgorithm	sha256WithRSAEncryption at minimum
issuer	issuer of the Certificate
validity	
notBefore*	start of the Certificate's validity (UTC)
notAfter*	notBefore + at most the maximum certificate validity period in accordance with BRG (UTC)
subject	see Table 5 below - subject field attributes may not consist only of single character ".", "-", " " (space) or of any other indication that the value is not present, is incomplete or not applicable
subjectPublicKeyInfo**	must meet the requirements under 6.1.5 and 6.1.6
algorithm	rsaEncryption
subjectPublicKey	2048 bits at minimum
extensions	extension of issued Certificate - see Table 6
signature	advanced electronic seal of Certificate's issuer

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

** Changes to relevant legislation, technical norms or standards may result in changes to the algorithm or minimum key length of the Certificate. Details may be provided in the PKI Disclosure Statement.

Table 5 – Subject field attributes

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

[2] 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).

Subject field attribute	Content	Comments
Address of Entity's Physical Site		
countryName	two-letter country code (ISO 3166-1)	mandatory
stateOrProvinceName	state of a federation or region/province	mandatory
localityName	town or city	mandatory
postalCode	postal code	optional
streetAddress	street and street number of entity's address	optional
Identification of the Entity – SSL/TLS Server Owner		
organizationName	MUST specify the full registered legal name of the entity; plus may contain business name at the beginning if it is followed by the entity's full legal name given in parentheses	mandatory CA may shorten the name/ accept shortening the name so that the text is the maximum of 64 characters long, if no third party can be misled that it communicates with a different organization
businessCategory (2.5.4.15)	MUST contain one of following strings according to the category of the entity (EVCG, chapter 8.5): • '**Private Organizations**' – 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;	mandatory

	• '**Non-commercial Entities**' – international organizations set up under treaties signed by multiple 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 country 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 for 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 jurisdictionStateOrP

		rovinceName MUST be specified • not applicable for CZ but may need to be specified for entities registered in other countries
serialNumber	• **Private Organization**: 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
commonName	if specified, it MUST be the only one server dNSName as specified in the first attribute of subjectAlternativeName (see Table 6)	optional, because of compatibility recommended to enter must be public DNS name wildcards are not allowed

* 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[3]

Extension	Content	Comments
subjectAlternativeName		non-critical

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

dNSName (1 .. 10 occurrences)	as per the application DNS name of the host (SSL/TLS server) / DNS domain under these conditions: • MUST be the public domain name; • at least one but no more than 10 dNSName attributes allowed; • all dnsName attributes must contain: - either the same basic domain that the applicant has registered or controls, of the second (e.g., ica.cz) or third (e.g., mv.gov.cz) level, i.e., the same two or three domain labels listed on the far right; or - FQDNs over which the applicant demonstrates control; • Certificates for domain names containing wildcards (for example *.company.cz) ARE NOT be issued; • Certificates for gTLD domain .onion ARE NOT issued; • Certificates for domain names containing underscore character ("_") ARE NOT issued; • FQDN must consist only of LDH labels (see the definitions) concatenated with dots, dot may not be the last character of FQDN (wrong example is example.com.); • Certificates for domain names using mixed byte-character set (i.e., Internationalized Domain Names – IDN, LDH label prefixed with "xn--") ARE NOT issued; • Domain name must not contain an IP Reverse Zone suffix (containing ip6.arpa, in-addr.arpa)	content of the first dNSName attribute MUST be identical to that of the attribute subject.commonName if commonName is specified
certificatePolicies		non-critical

.policyInformation(1)		
policyIdentifier	EV (2.23.140.1.1)	OID specified in EVCG policy identifier according to Microsoft requirements
.policyInformation(2)		
policyIdentifier	see 1.2.	mandatory
policyQualifiers		
cPSuri	http://www.ica.cz	
userNotice*	Tento kvalif. certifikat pro autentizaci internetovych stranek byl vydan v souladu s nariz. EU c. 910/2014. This is a EU qualified certificate for website auth. according to Reg. (EU) No 910/2014.	optional
.policyInformation(3)		recommended by EN 319411-2 for QCP-w certificates
policyIdentifier	QCP-w (0.4.0.194112.1.4)	
QCStatements		non-critical
	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 stored 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 attribute id-etsi-qcs-QcType = id-etsi-qct-web
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
authorityInformationAccess		non-critical
id-ad-ocsp**	http://ocsp.ica.cz/qcw*YY*_rsa	
id-ad-caIssuers**	http://q.ica.cz/qcw*YY*_rsa.cer	

basicConstraints		critical
cA	False	
keyUsage	digitalSignature, keyEncipherment	critical
extendedKeyUsage***	as per the application: • included must be at least id-kp-serverAuth; or • id-kp-serverAuth and id-kp-clientAuth	non-critical, mandatory attribute; 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	non-critical
authorityKeyIdentifier	hash of the certificate issuer's (Authority's) public key	non-critical
keyIdentifier	hash of the certificate issuer's (Authority's) public key	
Signed Certificate Timestamp	time-stamp tokens from at least two Certificate Transparency (CT) logs	time-stamp token = signed confirmation from relevant CT log that precertificate has been added

* The issuer may modify the text of the attribute.

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

*** Supported set; the specific EKU is taken over from the certificate application.

For extensions containing URLs (where relevant), an additional URL can be added to obtain the object.

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 comply with the relevant technical standards.

7.1.4 Name forms

Name forms included in the Authority-issued Certificates comply with RFC 5280.

Names and Certificate attributes constraints – see the profile above. The provisions of 3.1 also apply.

Domain authority or control validation is described in chapter 3.2.2.4.

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

Certificate policy OIDs are specified in the attribute certificatePolicies (see Table 6).

7.1.7 Usage of Policy Constraints extension

Not applicable for 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 for this document – not classified as critical.

7.2 CRL profile

Table 7 – CRL profile[4]

Field	Content
version	v2(0x1)
signatureAlgorithm	sha256withRSAEncryption at minimum
issuer	issuer of the CRL
thisUpdate	date and time when the CRL was issued (UTC)
nextUpdate*	date and expected time when the next CRL will be issued (UTC)

[4] 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).

revokedCertificates	list of revoked certificates
userCertificate	revoked certificate's serial number
revocationDate	certificate revocation date and time
crlEntryExtensions	list attribute extensions – see Table 8
crlExtensions	CRL extensions – see Table 8
signature	advanced electronic seal of CRL's issuer

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

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[5]

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

* For end user Certificates are (according to the reason of revocation) used only these CRLReason codes:

- keyCompromise (RFC 5280 CRLReason #1);
- affiliationChanged (RFC 5280 CRLReason #3);
- superseded (RFC 5280 CRLReason #4);
- cessationOfOperation (RFC 5280 CRLReason #5);
- privilegeWithdrawn (RFC 5280 CRLReason #9) – this code cannot be used by subscriber, it is entered by CA (from January 1, 2023, at the latest).

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

If the user certificate revocation reason is unspecified (RFC 5280 CRLReason #0), the reasonCode extension is not specified for the item in accordance with the RFC5280 recommendation.

Actualization of revocation code and date of previously revoked CRL entries, when verifiable proof of key compromise is obtained, is not implemented.

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.

Only http is used as the transmission protocol.

See the chapter 4.9.10 and 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 trust services legislation and the technical standards referred to therein regulating the assessment procedure.

The evaluation periodicity for the Microsoft Trusted Root 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 trust services legislation are defined in this legislation and the technical standards referred to therein.

The identity (accredited conformity assessment entity) and the qualification of the assessor carrying out assessment defined by Microsoft Trusted Root Program are described in ETSI EN 319 403-1.

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 property or personal relation to I.CA.

8.4 Topics covered by assessment

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

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

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

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

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 Organization. Certificate renewal is not provided.

9.1.2 Certificate access fees

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

9.1.3 Revocation or status information access fees

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

9.1.4 Fees for other services

Not applicable for this document.

9.1.5 Refund policy

Not applicable for this document.

9.2 Financial responsibility

9.2.1 Insurance coverage

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

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

9.2.2 Other assets

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

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

9.2.3 Insurance or warranty coverage for end-entities

Not applicable for this document.

9.3 Confidentiality of business information

9.3.1 Scope of confidential information

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

- All private keys, which are employed in providing the trust services;
- Business information of I.CA;
- Any internal information and documentation;
- Any personal data.

9.3.2 Information not within the scope of confidential information

Public information is marked as public or published in the manner pursuant to 2.2.

9.3.3 Responsibility to protect confidential information

I.CA employee who comes in contact with confidential information may not disclose this information to a third party without consent of CEO of I.CA.

9.4 Privacy of personal information

9.4.1 Privacy plan

I.CA protects personal data and other non-public information in accordance with the relevant legislation, which means ZOOU and GDPR in particular. Information on the client's personal data protection policy is provided in the document "Principles for Clients' Personal Data Processing" displayed on the company's website - see chapter 2.2.

9.4.2 Information treated as private

Any personal data subject to protection under applicable legislation are treated as private.

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

9.4.3 Information not deemed private

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

9.4.4 Responsibility to protect private information

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

9.4.5 Notice and consent to use private information

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

9.4.6 Disclosure pursuant to judicial or administrative process

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

9.4.7 Other information disclosure circumstances

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

9.5 Intellectual property rights

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

9.6 Representations and warranties

9.6.1 CA representations and warranties

I.CA warrants that:

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

The warranties also include:

- Verification of authorization to apply for the Certificate;
- Validation of the Certificate subscriber's control over the e-mail box with the address specified in the Certificate;

- Validation of the data provided in the Certificate application, including checking the completion of the items contained in the application (PKCS#10 format), and identity;
- Compliance of the Certificate issuance contract with applicable legislation;
- 24x7 operation of the certificate status information repository;
- Possibility to revoke the Certificate for the reasons specified in the trust service legislation and in this CP.

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

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

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

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 Certificate application if the applicant refuses to provide necessary data or is not authorized to submit the application;
- Is responsible, in the case of personal submission of a Certificate revocation request, for timely submission of this request for processing to the Authority;
- 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 for this document.

9.7 Disclaimers of warranties

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

9.8 Limitations of liability

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

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

První certifikační autorita, a.s.:

- Undertakes to discharge all the obligations defined in relevant legislation (including 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.

První certifikační autorita, a.s., **is not responsible for:**

- Any defect in the services rendered which is due to the Certificate subscriber's incorrect or unauthorized use of the services rendered under the 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 submitted by:

- E-mail to reklamace@ica.cz;
- Message to data box of I.CA;
- Registered post letter to the registered office of the company;
- Hand at the registered office of the company.

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

- Most concise description of the defect and its symptoms;
- 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 otherwise.

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

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

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

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

9.10 Term and termination

9.10.1 Term

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

9.10.2 Termination

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

9.10.3 Effect of termination and survival

The obligations of I.CA arising from 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, personal meetings and other channels.

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

9.12 Amendments

9.12.1 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

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

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

9.13 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 legal order of the Czech Republic.

9.15 Compliance with applicable law

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

9.16 Miscellaneous provisions

9.16.1 Entire agreement

Not applicable for this document.

9.16.2 Assignment

Not applicable for this document.

9.16.3 Severability

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

9.16.4 Enforcement (attorneys' fees and waiver of rights)

Not applicable for this document.

9.16.5 Force majeure

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

9.17 Other provisions

Not applicable for this document.

10 FINAL PROVISIONS

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