První certifikační autorita, a.s.



Certificate Policy

for Issuing Commercial Technological Certificates

(RSA Algorithm)

Certificate Policy for Issuing Commercial Technological Certificates (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 1.145

Copyright © První certifikační autorita, a.s.

CONTENT

1 Introduction 11
1.1 Overview 11
1.2 Document name identification 12
1.3 PKI Participants 12
1.3.1 Certification authorities 12
1.3.2 Registration authorities 12
1.3.3 Subscribers 13
1.3.4 Relying parties 13
1.3.5 Other participants 13
1.4 Certificate usage 13
1.4.1 Appropriate certificate uses 13
1.4.2 Prohibited certificate uses 13
1.5 Policy administration 13
1.5.1 Organization administering the document 13
1.5.2 Contact person 13
1.5.3 Person determining CPS suitability for the policy 14
1.5.4 CPS approval procedures 14
1.6 Definitions and acronyms 14
2 Publication and repository responsibilities 21
2.1 Repositories 21
2.2 Publication of certification information 21
2.3 Time or frequency of publication 22
2.4 Access controls on repositories 22
3 Identification and authentication 23
3.1 Naming 23
3.1.1 Types of names 23
3.1.2 Need for names to be meaningful 23
3.1.3 Anonymity or pseudonymity of subscribers 23
3.1.4 Rules for interpreting various name forms 23
3.1.5 Uniqueness of names 23
3.1.6 Recognition, authentication, and role of trademarks 23
3.2 Initial identity validation 23
3.2.1 Method to prove possession of private key 23
3.2.2 Authentication of organization identity 24

3.2.3 Authentication of individual identity 24
3.2.4 Non-verified subscriber information 24
3.2.5 Validation of authority 24
3.2.6 Criteria for interoperation 25
3.2.7 Validation of e-mail address 25
3.3 Identification and authentication for re-key requests 25
3.3.1 Identification and authentication for routine re-key 25
3.4 Identification and authentication for revocation request 25
4 Certificate life cycle operational requirements 27
4.1 Certificate application 27
4.1.1 Who can submit a certificate application 27
4.1.2 Enrollment process and responsibilities 27
4.2 Certificate application processing 28
4.2.1 Performing identification and authentication functions 28
4.2.2 Approval or rejection of certificate applications 28
4.2.3 Time to process certificate applications 28
4.3 Certificate Issuance 28
4.3.1 CA actions during certificate issuance 28
4.3.2 Notification to subscriber by the CA of issuance of certificate 29
4.4 Certificate acceptance 29
4.4.1 Conduct constituting certificate acceptance 29
4.4.2 Publication of the certificate by the CA 29
4.4.3 Notification of certificate issuance by the CA to other entities 29
4.5 Key pair and certificate usage 29
4.5.1 Subscriber private key and certificate usage 29
4.5.2 Relying party public key and certificate usage 30
4.6 Certificate renewal 30
4.6.1 Circumstance for certificate renewal 30
4.6.2 Who may request renewal 30
4.6.3 Processing certificate renewal requests 30
4.6.4 Notification of new certificate issuance to subscriber 30
4.6.5 Conduct constituting acceptance of a renewal certificate 30
4.6.6 Publication of the renewal certificate by the CA 31
4.6.7 Notification of certificate issuance by the CA to other entities 31
4.7 Certificate re-key 31
4.7.1 Circumstance for certificate re-key 31

4.7.2 Who may request certification of a new public key....31
4.7.3 Processing certificate re-keying requests....31
4.7.4 Notification of new certificate issuance to subscriber....31
4.7.5 Conduct constituting acceptance of a re-keyed certificate....31
4.7.6 Publication of the re-keyed certificate by the CA....32
4.7.7 Notification of certificate issuance by the CA to other entities....32
4.8 Certificate modification....32
4.8.1 Circumstance for certificate modification....32
4.8.2 Who may request certificate modification....32
4.8.3 Processing certificate modification requests....32
4.8.4 Notification of new certificate issuance to subscriber....32
4.8.5 Conduct constituting acceptance of modified certificate....32
4.8.6 Publication of the modified certificate by the CA....33
4.8.7 Notification of certificate issuance by the CA to other entities....33
4.9 Certificate revocation and suspension....33
4.9.1 Circumstances for revocation....33
4.9.2 Who can request revocation....35
4.9.3 Procedure for revocation request....35
4.9.4 Revocation request grace period....37
4.9.5 Time within which CA must process the revocation request....37
4.9.6 Revocation checking requirement for relying parties....37
4.9.7 CRL issuance frequency....37
4.9.8 Maximum latency for CRLs....37
4.9.9 On-line revocation/status checking availability....38
4.9.10 On-line revocation checking requirements....38
4.9.11 Other forms of revocation advertisements available....38
4.9.12 Special requirements re key compromise....38
4.9.13 Circumstances for suspension....38
4.9.14 Who can request suspension....38
4.9.15 Procedure for suspension request....39
4.9.16 Limits on suspension period....39
4.10 Certificate status services....39
4.10.1 Operational characteristics....39
4.10.2 Service availability....39
4.10.3 Optional features....39
4.11 End of subscription....39

4.12 Key escrow and recovery 39
4.12.1 Key escrow and recovery policy and practices 40
4.12.2 Session key encapsulation and recovery policy and practices 40
5 Facility, management, and operational controls 41
5.1 Physical controls 41
5.1.1 Site location and construction 41
5.1.2 Physical access 41
5.1.3 Power and air conditioning 41
5.1.4 Water exposures 41
5.1.5 Fire prevention and protection 41
5.1.6 Media storage 42
5.1.7 Waste disposal 42
5.1.8 Off-site backup 42
5.2 Procedural controls 42
5.2.1 Trusted roles 42
5.2.2 Number of persons required per task 42
5.2.3 Identification and authentication for each role 43
5.2.4 Roles requiring separation of duties 43
5.3 Personnel controls 43
5.3.1 Qualification, experience, and clearance requirements 43
5.3.2 Background check procedures 43
5.3.3 Training requirements 43
5.3.4 Retraining frequency and requirements 44
5.3.5 Job rotation frequency and sequence 44
5.3.6 Sanctions for unauthorized actions 44
5.3.7 Independent contractor requirements 44
5.3.8 Documentation supplied to personnel 44
5.4 Audit logging procedures 45
5.4.1 Types of events recorded 45
5.4.2 Frequency of processing log 45
5.4.3 Retention period for audit log 45
5.4.4 Protection of audit log 45
5.4.5 Audit log backup procedures 46
5.4.6 Audit collection system (internal vs. external) 46
5.4.7 Notification to event-causing subject 46
5.4.8 Vulnerability assessments 46

5.5 Records archival 46
5.5.1 Types of records archived 46
5.5.2 Retention period for archive 46
5.5.3 Protection of archive 47
5.5.4 Archive backup procedures 47
5.5.5 Requirements for time-stamping of records 47
5.5.6 Archive collection system (internal or external) 47
5.5.7 Procedures to obtain and verify archive information 47
5.6 Key changeover 47
5.7 Compromise and disaster recovery 48
5.7.1 Incident and compromise handling procedures 48
5.7.2 Computing resources, software, and/or data are corrupted 48
5.7.3 Entity private key compromise procedures 48
5.7.4 Business continuity capabilities after a disaster 48
5.8 CA or RA termination 48
6 Technical security controls 50
6.1 Key pair generation and installation 50
6.1.1 Key pair generation 50
6.1.2 Private key delivery to subscriber 50
6.1.3 Public key delivery to certificate issuer 50
6.1.4 CA public key delivery to relying parties 50
6.1.5 Key sizes 50
6.1.6 Public key parameters generation and quality checking 51
6.1.7 Key usage purposes (as per X.509 v3 key usage extension) 51
6.2 Private key protection and cryptographic module engineering controls 51
6.2.1 Cryptographic module standards and controls 51
6.2.2 Private key (n out of m) multi-person control 51
6.2.3 Private key escrow 51
6.2.4 Private key backup 51
6.2.5 Private key archival 52
6.2.6 Private key transfer into or from a cryptographic module 52
6.2.7 Private key storage on cryptographic module 52
6.2.8 Method of activating private key 52
6.2.9 Method of deactivating private key 53
6.2.10 Method of destroying private key 53
6.2.11 Cryptographic module rating 53

6.3 Other aspects of key pair management 53
6.3.1 Public key archival 53
6.3.2 Certificate operational periods and key pair usage periods 53
6.4 Activation data 54
6.4.1 Activation data generation and installation 54
6.4.2 Activation data protection 54
6.4.3 Other aspects of activation data 54
6.5 Computer security controls 54
6.5.1 Specific computer security technical requirements 54
6.5.2 Computer security rating 54
6.6 Life cycle technical controls 57
6.6.1 System development controls 57
6.6.2 Security management controls 57
6.6.3 Life cycle security controls 57
6.7 Network security controls 57
6.8 Time-stamping 58
7 Certificate, CRL and OCSP profiles 59
7.1 Certificate profile 59
7.1.1 Version number(s) 61
7.1.2 Certificate extensions 61
7.1.3 Algorithm object identifiers 63
7.1.4 Name forms 63
7.1.5 Name constraints 63
7.1.6 Certificate policy object identifier 63
7.1.7 Usage of Policy Constraints extension 63
7.1.8 Policy qualifier syntax and semantics 64
7.1.9 Processing semantics for the critical certificate policies extension 64
7.2 CRL profile 64
7.2.1 Version number(s) 64
7.2.2 CRL and CRL entry extensions 64
7.3 OCSP profile 65
7.3.1 Version number(s) 65
7.3.2 OCSP extensions 65
8 Conformity assessments and other assessments 66
8.1 Frequency or circumstances of assessment 66
8.2 Identity/qualifications of assessor 66

8.3 Assessor's relationship to assessed entity 66
8.4 Topics covered by assessment 66
8.5 Actions taken as a result of deficiency....66
8.6 Communication of results....66
8.7 Self audits 67
8.8 Review of delegated parties 67
9 Other business and legal matters....68
9.1 Fees....68
9.1.1 Certificate issuance or renewal fees 68
9.1.2 Certificate access fees....68
9.1.3 Revocation or status information access fees....68
9.1.4 Fees for other services 68
9.1.5 Refund policy....68
9.2 Financial responsibility 68
9.2.1 Insurance coverage 68
9.2.2 Other assets 68
9.2.3 Insurance or warranty coverage for end-entities 69
9.3 Confidentiality of business information 69
9.3.1 Scope of confidential information....69
9.3.2 Information not within the scope of confidential information 69
9.3.3 Responsibility to protect confidential information 69
9.4 Privacy of personal information 69
9.4.1 Privacy plan....69
9.4.2 Information treated as private 69
9.4.3 Information not deemed private 69
9.4.4 Responsibility to protect private information....70
9.4.5 Notice and consent to use private information 70
9.4.6 Disclosure pursuant to judicial or administrative process 70
9.4.7 Other Information disclosure circumstances 70
9.5 Intellectual property rights 70
9.6 Representations and warranties....70
9.6.1 CA Representations and warranties 70
9.6.2 RA representations and warranties....71
9.6.3 Subscriber representations and warranties....71
9.6.4 Relying parties representations and warranties 71
9.6.5 Representations and warranties of other participants 71

9.7 Disclaimers of warranties 71
9.8 Limitations of liability 71
9.9 Indemnities....72
9.10 Term and termination 73
9.10.1 Term....73
9.10.2 Termination 73
9.10.3 Effect of termination and survival....73
9.11 Individual notices and communications with participants 73
9.12 Amendments....73
9.12.1 Amending procedure 73
9.12.2 Notification mechanism and period....73
9.12.3 Circumstances under which OID must be changed 73
9.13 Disputes resolution provisions....74
9.14 Governing law 74
9.15 Compliance with applicable law....74
9.16 Miscellaneous provisions 74
9.16.1 Entire agreement....74
9.16.2 Assignment....74
9.16.3 Severability....74
9.16.4 Enforcement (attorneys' fees and waiver of rights) 75
9.16.5 Force Majeure 75
9.17 Other provisions....75
10 Final provisions 76

Table 1 – Document history

Version	Date of Release	Approved by	Comments
1.00	29 March 2016	CEO of První certifikační autorita, a.s.	First release.
1.10	3 March 2017	CEO of První certifikační autorita, a.s.	Modified to match the requirements of Microsoft Trusted Root Certificate Program.
1.11	30 April 2019	CEO of První certifikační autorita, a.s.	More detailed description of filling up subject field attributes. Annual revision, formal errors correction.

1.12	10 December 2019	CEO of První certifikační autorita, a.s.	Support of RSA-PSS (pkcs#1 2v1) algorithm when creating advanced electronic of the certificate.
1.13	28 November 2020	CEO of První certifikační autorita, a.s.	Classification of document marked, change of CA actions during certificate issuance, revision, more accurate text.
1.14	11 June 2022	CEO of První certifikační autorita, a.s.	Cryptographic module evaluation updated. ExtendedKeyUsage attribute more specified. Revision of text.
1.141	26 April 2024	CEO of První certifikační autorita, a.s.	Revision of text.
1.142	2 July 2024	CEO of První certifikační autorita, a.s.	List of referenced standards updated.
1.143	26 August 2024	CEO of První certifikační autorita, a.s.	List of referenced standards updated, requirements of ETSI TS 119 411-6 taken into account.
1.144	16 August 2025	CEO of První certifikační autorita, a.s.	Certificate profile refinement. Updates related to S/MIME BR.
1.145	16 August 2026	CEO of První certifikační autorita, a.s.	Clarification of CA actions during certificate issuance. Committing to CCADB policy requirements. Revision of the text.

1 INTRODUCTION

This document determines the principles applied by První certifikační autorita, a.s. (also as the I.CA), a qualified provider of trust services, when issuing commercial (non-qualified) certificates (also as the Service or the Certificate) to legal persons or government authorities (also as Organizations). The RSA algorithm is used for the Service provided under this certificate policy (also as the CP).

Certificates issued under this CP are intended for verification of electronic signatures created by technological components operated by Organizations, for client authentication and for encryption.

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

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

The Service is provided to all end users on the basis of a contract. I.CA imposes no restrictions on potential end users, and the provision of the Service is non-discriminatory and the Service is also available to the disabled.

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 Commercial Technological Certificates (RSA Algorithm)** is prepared by První certifikační autorita, a.s., deals with the issues related to life cycle processes of Certificates and follows a structure matching the scheme of valid RFC 3647 standard while taking account of valid technical and other standards and rules of the European Union and the laws of the Czech Republic pertinent to this sphere (therefore, each chapter is preserved in his document even if it is irrelevant to this sphere). The document is divided into nine basic chapters and these are briefly introduced in the following list:

- Chapter 1 identifies this document with the allocated unique identifier, generally describes the entities and individuals taking part in the provision of this Service, and defines the acceptable use of the Certificates available to be issued;
- Chapter 2 deals with the responsibility for the publication and information or documents;
- Chapter 3 describes the processes of identification and authentication of an applicant for the issuance or revocation of a Certificate, and defines the types and contents of the names used in Certificates;
- Chapter 4 defines life cycle processes of Certificates, i.e., Certificate issuance application, the issuance of the Certificate, Certificate revocation request, the revocation

of the Certificate, the services related to checking of Certification status, termination of the provision of the Service, etc.;

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

More details 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 identification

Document's title:	Certificate Policy for Issuing Commercial Technological Certificates (RSA Algorithm), version 1.145
Policy OID:	1.3.6.1.4.1.23624.10.1.71.1.1

1.3 PKI Participants

1.3.1 Certification authorities

The root certification authority of První certifikační autorita, a.s., issued a certificate to a subordinate certification authority (also as the Authority) operated by I.CA, in a two-tier certification authority structure, in accordance with 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

The services of První certifikační autorita, a.s., are provided through registration authorities (stationary or mobile), which are either public (providing services for the general public) or client (providing services for their customers). These registration authorities:

- Accept applications for the services listed in this CP (Certificate issuance applications, in particular), arrange the handover of Certificates and certificate revocation lists, provide required information, handle complaints, etc.;
- Are authorized, for urgent operational or technical reasons, to suspend, in whole or in part, the performance of their activities;
- Are authorized to conclude Service contracts on behalf of I.CA;

- Are authorized to charge for the I.CA services provided through RA unless otherwise agreed in a contract;
- If contracted RA, exercise similar duties and responsibilities on behalf of I.CA as the RA proper, under a written contract concluded between I.CA and the operator of the contracted RA.

1.3.3 Subscribers

Subscriber of a Certificate is an Organization which applied for Certificate for itself and which is identified in the Certificate as the owner of the private key connected with the public key specified in the Certificate.

1.3.4 Relying parties

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

1.3.5 Other participants

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

1.4 Certificate usage

1.4.1 Appropriate certificate uses

Certificates issued under this CP may be used in electronic signature verification processes encryption and client authentication.

1.4.2 Prohibited certificate uses

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

1.5 Policy administration

1.5.1 Organization administering the document

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

1.5.2 Contact person

The contact person of První certifikační autorita, a.s., in respect of this CP and its CPS is COO of I.CA. The contact information given in chapter 2.2 applies.

The e-mail address certproblem@ica.cz is monitored continuously 24x7 and is intended to report problems with the Certificate, i.e. suspicion of key compromise or misuse of the Certificate.

1.5.3 Person determining CPS suitability for the policy

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

1.5.4 CPS approval procedures

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

1.6 Definitions and acronyms

Table 2 – Definitions

Term	Explanation
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
client portal	web platform enabling designated representatives of Organizations that have a contract with I.CA to manage information about issued certificates and perform other defined actions
contracting partner	provider of services contracted by I.CA for certification services or parts thereof – usually, it is a contracted RA
domain name	node name in domain name system
domain name registrant/ registrant	sometimes referred to as a domain name owner, but more accurately a person or entity registered by a domain registrar as having the right to oversee the use of a domain name, a natural or legal person listed as a "Registrant" by WHOIS or a domain registrar
domain name registrar/ registrar	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	standard preferred method for sending http requests to OCSP responder via http, the method allows caching (the second method is POST)
hash function	transformation which receives, as an input, a string of characters of arbitrary length, and the result is a string of characters of fixed length (hash)
key pair	private key and corresponding public key
Labour Code	the Czech Republic's Act No. 262/2006 Coll., Labour Code, as amended
OCSP responder	server using the OCSP protocol to provide data on public key certificate status
OCSP stapling	way of minimizing queries for OCSP Responder, RFC 4366 - TLS Extensions; allows the TLS server to return the once-received answer to the question about certificate status from the OCSP (during its validity) to all end users accessing the TLS server
phishing	in an electronic communication attempt to obtain sensitive information (usernames, passwords, and credit card details) for malicious reasons
private key	unique data to create electronic signature / 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 on 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)
written contract	text of the contract in electronic or paper form

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), the certificate application can also be in PEM format (DER format is the binary version of PEM format)
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, domain name that specifies all domain levels in 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
MTRP	Microsoft Trusted Root Program
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
S/MIME BR	CA/Browser Forum document „Baseline Requirements for the Issuance and Management of Publicly-Trusted S/MIME Certificates"
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.

2.2 Publication of certification information

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

- Registered office:

  První certifikační autorita, a.s.

  Podvinný mlýn 2178/6

  190 00 Praha 9

  The Czech Republic
- Website: http://www.ica.cz;
- Registered offices of the registration authorities.

Electronic address for contact between general public and I.CA is 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 list (CRL) – the following information is published (and more information can be obtained from the CRL):
  - Date of CRL release;
  - CRL number;
  - Link to where the CRL can be obtained in the specified format (DER, PEM, 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's 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 - Baseline Requirements for the Issuance and Management of Publicly-Trusted S/MIME Certificates", which is published on http://www.cabforum.org. If this CP and the S/MIME BR are in conflict, the S/MIME BR prevail.

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 as follows:

- Certificate policy – after a new version is approved and issued;
- Certification practice statement – immediately, update depends on changes in normative requirements for issued Certificates, revision is carried out at least once a year;
- List of the certificates issued – updated immediately after issuing a new certificate to be published;
- Certificate revocation list (CRL) – see 4.9.7;
- Information about certification authority's certificate revocation with the reason of revocation – immediately;
- Other public information – no specific time limit, the general rule is that this information must correspond to the current state of the services provided.

2.4 Access controls on repositories

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

Non-public information is available only to authorized employees of I.CA or the parties specified by the 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 field subject must carry a meaning. See chapter 7 for the attributes supported for this field.

3.1.3 Anonymity or pseudonymity of subscribers

The Certificates issued under this CP do not support 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 specific subscriber is unique.

3.1.6 Recognition, authentication, and role of trademarks

Any Certificate issued under this CP may only contain a trademark with evidenced ownership or license. The Certificate's subscriber bears any consequence resulting from unauthorized use of a trademark.

3.2 Initial identity validation

The entities authorized to apply for a Certificate are listed in 4.1.1. The following chapters specify the rules for the initial validation of the identity of these entities.

3.2.1 Method to prove possession of private key

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

3.2.2 Authentication of organization identity

The following must be submitted to authenticate the identity of an Organization:

- Original or certified copy of the entry in the Commercial Register or in another register specified by law, of a trade license, of a deed of incorporation, or of another document of the same legal force; or
- Printed extract from public registers to be submitted by the applicant or prepared by the RA operator.

This document must contain full business name, identification number (if any), registered office, the name(s) of the person(s) authorized to act on behalf of the legal entity (authorized representatives).

3.2.3 Authentication of individual identity

The person's representing Organization identity validation procedure requires personal document that shows the data specified further in this chapter.

Valid personal identity card or passport must be used as the personal document for the citizens of the Czech Republic. Valid passport is the 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 personal document;
- Permanent address (if shown in the personal document).

If the person representing Organization is not an authorized representative of the Organization then the officially certified power of attorney signed by authorized representative of the Organization is required. The power of attorney may also be submitted in electronic form. It must be in PDF format and electronically signed by a person authorized to act on behalf of the Organization, using at least a guaranteed electronic signature based on a qualified electronic signature certificate, or, in justified cases, a qualified electronic signature.

3.2.4 Non-verified subscriber information

All information provided in the Certificate is duly verified.

3.2.5 Validation of authority

E-mail address may be placed in the Certificate extension, that is, in the rfc822Name attribute of the subjectAlternativeName extension, if this has been validated for the given application during the Certificate issuance procedure.

The attribute that the key pair was generated and stored on secure cryptographic device may only be in the Certificate if this has been validated for the given application during the Certificate issuance procedure.

3.2.6 Criteria for interoperation

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

Cross-certificates are not used.

3.2.7 Validation of e-mail address

E-mail address validation is performed in two ways, by checking whether the address belongs to a registered DNS domain (validating authority over mailbox via domain) or by validation the owner of the e-mail address using the content of the e-mail being sent (validating control over mailbox via e-mail). The use of the appropriate validation method depends on the type of contractual relationship with the client.

3.2.7.1 Validation via registered DNS domain

Validation of the e-mail address against the registered DNS domain is intended for business customers, where the contractual partner has control over the relevant DNS domain. In such a case, the correspondence of the domain part of e-mail address to the internally maintained list of registered company domains is verified (the company has a contract with I.CA and control over the DNS domain has been verified).

3.2.7.2 Validation using the content of the validation e-mail

In this case, validation of the ownership of the e-mail address from the application is carried out by sending a validation e-mail containing unique random information (validation link) with a time-limited validity. The Certificate applicant confirms the check of the e-mail address by clicking on the appropriate button or validation link, thereby activating the validation procedure on the side of the I.CA system.

3.3 Identification and authentication for re-key requests

3.3.1 Identification and authentication for routine re-key

The identification and authentication in routine re-key request (subsequent Certificate issuance) are as follows - the application for the issuance of subsequent Certificate in PKCS#10 structure must be:

- Electronically sealed with the use of a private key matching the public key contained in the valid Certificate which is to be re-keyed; or
- Contained in an e-mail signed by private key matching the public key in signing certificate (certificate issued to the subscriber of Certificate uniquely linked to this Certificate).

3.4 Identification and authentication for revocation request

The entities authorized to request for Certificate revocation are listed in 4.9.2. Possible methods of identification and authentication are described later in this chapter.

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 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;
- Using a signed electronic message, where:
  - the electronic signature must be created using the private key matching the public key in signing certificate relating with the Certificate to be revoked; or
  - the electronic signature must be created with the private key belonging to the Certificate to be revoked or
  - the electronic seal must be created using the private key matching the private key in the valid Certificate to be revoked;

  sent to revoke@ica.cz;
- Using the data box of I.CA (and using the Certificate revocation password);
- Using a defined person assigned to represent the Organization in the contractual relationship with I.CA.

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 conflict with trust services legislation or with the requirements of technical standards for this type of Certificates.

4 CERTIFICATE LIFE CYCLE OPERATIONAL REQUIREMENTS

4.1 Certificate application

4.1.1 Who can submit a certificate application

Certificate application can be submitted by Organization via the person representing the Organization.

4.1.2 Enrollment process and responsibilities

Process is performed only when the primary Certificate is issued. The person representing the Organization initiates the registration procedure by appearing at an RA office and bringing all the required documents plus the Certificate application (if already existing); at the RA office, the data in the submitted documents are entered into the Authority's information system and the Certificate application is processed.

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

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

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

- Inform the Certificate subscriber about the terms and conditions prior to concluding the Certificate issuance contract;
- Conclude with the Certificate subscriber such a Certificate issuance contract that meets the requirements of 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 a proof of fact that the private key was generated and stored on secure cryptographic device;
- 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 Service contract, 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

The identification and authentication procedure for the **primary Certificate** follows the rules given in 3.2.3, or 3.2.2 where applicable, and the procedure for **subsequent Certificates** follows the rules given in 3.3.1.

4.2.2 Approval or rejection of certificate applications

RA employees (also as the Employees) do the following in the procedure leading to the decision accepting or dismissing the issuance of the **primary Certificate**:

- Make a visual check as to conformity of the data in the Certificate application (the PKCS#10 structure) with the data in the documents submitted;
- Make a visual check as to the formal correctness of data.

The private key ownership verification, competence check and formal data correctness check are also carried out using the RA system software.

If any of these checks gives a fail result, the Certificate issuance procedure is terminated; otherwise, the procedure continues in accordance with 4.3.

See 4.3 for the procedure for the issuance of **subsequent Certificates**.

4.2.3 Time to process certificate applications

I.CA must issue the Certificate immediately after Certificate issuance is granted. The following list gives tentative times for issuing Certificates unless other agreement is stipulated in the contract:

- Primary Certificate – is usually (only on business days and during business hours) issued within 15 minutes, exceptionally it can take longer;
- Subsequent Certificates – within units of minutes.

4.3 Certificate Issuance

4.3.1 CA actions during certificate issuance

When issuing **the primary 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.

If any check ends negatively, the Certificate issuance procedure is terminated.

Subsequent Certificate issuance procedure is automated. The verification of private key ownership, the supported hash function in the Certificate application (not weaker than sha-256) and the competence check are carried out by software on the CA system core. If any of these checks gives a fail result, the Certificate issuance procedure is terminated.

4.3.2 Notification to subscriber by the CA of issuance of certificate

During the **primary Certificate** issuance process, the Certificate subscriber or more precisely the person representing the Organization applying for the Certificate receives information from the RA employee and the Certificate is sent to the contact e-mail provided during registration as mandatory data.

Subsequent Certificates are 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 over. The only way to refuse to take over the Certificate is applying for the Certificate's revocation in accordance with this CP.

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

4.4.2 Publication of the certificate by the CA

I.CA publishes every Certificate it issues, except any Certificate:

- Containing data 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

Chapter 4.4.2 applies.

4.5 Key pair and certificate usage

4.5.1 Subscriber private key and certificate usage

Subscribers must, among other things:

- Observe all relevant provisions of the Service contract;
- Use the private key and corresponding Certificate 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;
- Notify immediately the Service provider of everything that leads to the Certificate's revocation, in particular of:
  - Suspected abuse of the private key; and
  - Invalid or inaccurate attributes of 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 (e.g., www.ica.cz, RA workplace) certification authority certificates linked with the Certificate issued under this CP, and verify those certificates' fingerprint values and validity;
- Carry out any operation necessary for them to verify that the Certificate is valid;
- Observe all and any provisions of this CP.

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

Certificate re-key under this CP means the issuance of a new Certificate (subsequent Certificate) with a different public key but with identical content of the attributes under the subject field and the subjectAlternativeName extension of the Certificate which is requested to be re-keyed.

If the whole new Certificate issuance procedure is handled solely electronically without requiring any natural person to be present at an RA office, it is the issuance of a subsequent Certificate. See 4.7.1 for the requirements in respect of validating electronic applications for subsequent Certificates; if these requirements are not met, it is the primary Certificate issuance procedure, which starts with the enrollment process.

4.7.1 Circumstance for certificate re-key

Applications for Certificate re-key (the PKCS#10 structure) must meet the following requirements:

- The attributes under the subject field and the subjectAlternativeName extension must be identical to those in the Certificate which is to be re-keyed;
- The public key must be different from that in the Certificate which is to be re-keyed;
- The electronic subsequent Certificate application is validated in accordance with 3.3.1.

4.7.2 Who may request certification of a new public key

Certification of a new public key in a Certificate may be requested by the Certificate's subscriber.

4.7.3 Processing certificate re-keying requests

If the re-keying requirements are met, the procedure continues in accordance with 4.2 and 4.3.1, otherwise the Certificate issuance procedure is terminated.

4.7.4 Notification of new certificate issuance to subscriber

See 4.3.2.

4.7.5 Conduct constituting acceptance of a re-keyed certificate

See 4.4.1.

4.7.6 Publication of the re-keyed certificate by the CA

See 4.4.2.

4.7.7 Notification of certificate issuance by the CA to other entities

See 4.4.3.

4.8 Certificate modification

Certificate modification under this CP means the issuance of a new Certificate in which a minimum of one modification made to the content of the attributes, concerning the Certificate's subscriber, under the subject field or the subjectAlternativeName extension or in which one field which requires content validation is deleted or added. The public key must be different from that in the Certificate which is to be modified.

If the whole new Certificate issuance procedure is handled solely electronically without requiring any natural person to be present at an RA office, it is the issuance of a subsequent Certificate. See 4.8.1 for the requirements in respect of validating electronic applications for subsequent Certificates; if these requirements are not met, it is the primary Certificate issuance procedure, which starts with the registration procedure.

4.8.1 Circumstance for certificate modification

Application for the subsequent Certificate (the PKCS#10 structure) with modified data must meet the following requirements:

- The attributes to be modified or added in the subject field or the subjectAlternativeName extension must be duly validated;
- The public key must be different from that in the original Certificate;
- The electronic subsequent Certificate application is validated in accordance with 3.3.1.

4.8.2 Who may request certificate modification

Change to the data in a Certificate may be requested by the Certificate's subscriber.

4.8.3 Processing certificate modification requests

If the Certificate modification requirements are met, the procedure continues in accordance with 4.2 and 4.3.1, otherwise the Certificate issuance procedure is terminated.

4.8.4 Notification of new certificate issuance to subscriber

See 4.3.2.

4.8.5 Conduct constituting acceptance of modified certificate

See 4.4.1.

4.8.6 Publication of the modified certificate by the CA

See 4.4.2.

4.8.7 Notification of certificate issuance by the CA to other entities

See 4.4.3.

4.9 Certificate revocation and suspension

Certificate revocation requests are accepted irrespective of the time of the day through the form on the company's website

Irrespective of the time it is also possible to submit the Certificate revocation request via e-mail, data box and letter. An application submitted in this way is accepted no later than the next working day after its delivery.

Handing over and accepting the Certificate revocation request at the RA is possible only during the working hours of the relevant RA.

I.CA does not provide certificate suspension, nor does it provide the possibility to request a revocation at a certain date in the future.

4.9.1 Circumstances for revocation

4.9.1.1 User 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 mailbox control for any mailbox address in the Certificate should not be relied upon.

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 circumstance indicating that use of an email address or Fully-Qualified Domain Name in the Certificate is no longer legally permitted (e.g., a court or arbitrator has revoked the right to use an email address or Domain Name, a relevant licensing or services agreement between the Subscriber has terminated, or the accountholder has failed to maintain the active status of the email address or Domain Name) (CRLReason #5, cessationOfOperation);
10. I.CA is made aware of a material change in the information contained in the Certificate (CRLReason #9, privilegeWithdrawn);
11. I.CA is made aware that the Certificate was not issued in compliance with S/MIME BR, CP or CPS (CRLReason #4, superseded);
12. I.CA determines or is made aware that some information contained in the Certificate is inaccurate (CRLReason #9, privilegeWithdrawn);
13. I.CA's right to issue Certificate under S/MIME BR 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);
14. Revocation is required by CP or CPS;
15. 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 made aware that Authority's certificate:
    - □ Was not issued in compliance with S/MIME BR, corresponding CP or CPS; or
    - □ Does not meet requirements of S/MIME BR, corresponding CP or CPS;
6. I.CA determines that some information appearing in the Authority's certificate was inaccurate or misleading;
7. Root CA or Authority ceased operation for any reason a did not made arrangement for another CA to provide revocation support for certificates issued by them;
8. Root CA's or Authority's right to issue Certificate under S/MIME BR or CP requirements expired, was revoked or terminated and root CA did not make arrangement 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

Certificate revocation request may be submitted by:

- Certificate's subscriber;
- Subject explicitly specified therefore in the Service (under this CP) contract;
- Subjects designated by legislation through an authorized person;
- Provider of this Service (CEO of I.CA or his representative is the person authorized to request for the revocation of a Certificate issued by I.CA) and the subject is informed of the revocation by a signed e-mail to the address entered during registration:
  - 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 was used contrary to the restrictions defined in 1.4.2;
  - If demonstrably finds out that the Certificate's subscriber has terminated or the data by which the Certificate was issued are no longer valid;
  - If the public key in the Certificate application is the same as the public key in a certificate already issued.

After requesting the revocation of the Certificate, the subscriber is obliged to immediately stop using this Certificate and the corresponding private key.

In addition, third parties (e.g. supervisory bodies, law enforcement authorities, relying parties, suppliers of application SW) may send a report of a problem with the Certificate informing the Authority of the reasons for possible revocation of the Certificate.

4.9.3 Procedure for revocation request

Any Certificate revocation request delivered to RA in person must include the Certificate's serial number in the decimal or hexadecimal format (introduced by the string '0x'), the full name of the person authorized to request for the Certificate's revocation, and the Certificate revocation password. If the person authorized to request for revocation does not know the Certificate revocation password, s/he must explicitly state this in the written application, along with the number of the primary personal document submitted in the Certificate application procedure or the number of the new personal document if the original document has been replaced. The person must use this personal document to prove their identity with the RA employee. If the request is legitimate, the RA employee revokes the Certificate, and the Certificate revocation date and time are the date and time when the request is processed by CA's information system. If the Certificate revocation application cannot be accepted (wrong revocation password or no proof of identity of the person authorized to request for Certificate revocation) the RA employee seeks to rectify these defects in collaboration with that natural person and dismisses the request if the defects cannot be rectified for any reason. The RA employee always notifies the requestor of the result.

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

- Using the form on the information web page. The Certificate revocation date and time are the date and time a valid Certificate revocation request is dealt with in the CA's information system. The request receives a notice if the request is granted;
- Electronic message signed electronically – the body text must contain (in Czech or Slovak with or without diacritics, or in English):

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

where '*xxxxxxx*' is the Certificate's serial number and must be given either in the decimal or hexadecimal format (introduced by the string '0x').

The message must be electronically signed with the private key corresponding to the public key in the signing certificate, or the private key corresponding to the public key in the Certificate to be revoked;

- Electronic message not signed electronically – the body text must contain (in Czech or Slovak with or without diacritics, or in English):

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

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

  where '*xxxxxxx*' is the Certificate's serial number and '*yyyyyy*' the revocation password. The Certificate's serial number must be given either in the decimal or hexadecimal format (introduced by the string '0x');

- Electronic message signed electronically, or electronic message not signed electronically in special cases, and sent by a defined person authorized to represent the Organization in the contractual relationship with I.CA:

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

  where '*xxxxxxx*' is the Certificate's serial number. The Certificate's serial number must be given in the decimal or hexadecimal format (introduced by the string '0x').

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

If Certificate revocation request is submitted as a registered post letter, the request must contain following 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 is to be given either in the decimal or hexadecimal format (introduced by the string '0x'). 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 by a registered letter sent to postal address of request sender how the request was handled.

Report of suspected compromise of the private key related to the public key in the Certificate, misuse of the Certificate or other types of fraud, compromise, misuse, inappropriate behavior associated with the issued Certificate can be sent to the e-mail address specified in chapter 1.5.2, or as registered letter to the company's headquarters, or via a data box - see chapter 2.2.

4.9.4 Revocation request grace period

Certificate revocation request must be made immediately.

4.9.5 Time within which CA must process the revocation request

4.9.5.1 Certificate revocation request

The revocation request is carried out without delay after receiving a legitimate revocation request. The CRL containing the serial number of the revoked Certificate is issued immediately after the revocation of this Certificate.

4.9.5.2 Certificate Problem Report

I.CA reviews the facts and circumstances of the reported problem and within 24 hours of receiving the Certificate Problem Report provides a preliminary report to both the Certificate subscriber and the person reporting the problem.

I.CA, in cooperation with the Certificate subscriber and the person reporting the problem, decides whether it is necessary to revoke the Certificate and informs both the Certificate subscriber and the person who reported the problem about the decision.

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

- The nature of the problem;
- The consequences of revocation for both subscriber and relying parties;
- The number of Certificate Problem Reports received about a particular Certificate or subscriber;
- The entity making the complaint (for example, a complaint from a law enforcement official should be addressed with higher priority); and
- Relevant legislation.

4.9.6 Revocation checking requirement for relying parties

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

4.9.7 CRL issuance frequency

The certificate revocation list is released immediately after a Certificate revocation request is handled affirmatively. If a Certificate is not revoked, the new CRL is usually released two times daily and no more than 24 hours after the previous CRL is released.

4.9.8 Maximum latency for CRLs

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 OCSP responder.

OCSP responses comply with the 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 supports both GET and POST method. If the OCSP responder receives a request for the status of a certificate serial number that is "unused", then the response is not "good".

4.9.10.1 Status of Certificates

The validity of OCSP response is set to 24 hours.

When the Certificate is revoked, the OCSP response is updated immediately (Certificate suspension or renewal of revoked Certificate is not provided).

OCSP responses are automatically updated (i.e. an entry in the responder's internal OCSP cache expires) at the latest when the earlier of the following conditions is met:

- In the middle of the OCSP response validity (for responses with a validity of less than 16 hours);
- 8 hours before the response expires (for responses valid for 16 hours or longer).

4.9.10.2 CA issuing Certificates certificate status

I.CA updates OCSP responses:

- Within 24 hours after revoking the certificate of the CA issuing the Certificates; and
- At least every twelve months.

4.9.11 Other forms of revocation advertisements available

Not applicable for this document.

4.9.12 Special requirements re key compromise

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

4.9.13 Circumstances for suspension

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

4.9.14 Who can request suspension

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

4.9.15 Procedure for suspension request

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

4.9.16 Limits on suspension period

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

4.10 Certificate status services

4.10.1 Operational characteristics

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

The fact that the Authority provides Certificate status information in the form of OCSP is specified in the Certificates issued by the Authority.

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

4.10.2 Service availability

The Authority guarantees round-the-clock (24/7) availability and integrity of the list of the Certificates it has issued and the list of revoked certificates (CRLs), plus the availability of the OCSP service.

The response time to a certificate status request using CRL or OCSP is less than 10 seconds under normal operating conditions.

I.CA maintains continuous 24x7 availability through the e-mail address specified in chapter 1.5.2 in order to react internally to the Certificate Problem Report and, if necessary, to forward the information about the received report to the competent authority and, if necessary, to revoke the Certificate that is the 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, MANAGEMENT, AND OPERATIONAL CONTROLS

Facility, management, and operational controls primarily deal with:

- Systems provided to support the Service;
- All processes supporting the provision of the Service.

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 in the more detailed internal documentation. This documentation takes account of the results of periodic risk analysis.

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

5.1.4 Water exposures

The trustworthy systems supporting the Service 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 electronic fire alarm system (FAS). Fireproof insulation is installed in the entrance doors to the restricted

areas in which the trustworthy systems are situated. The fire extinguishers are fitted in these areas.

5.1.6 Media storage

Archiving 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 carried out at I.CA. The trusted role employee appointment procedure, the trusted roles and their responsibilities are defined 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.

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

5.2.3 Identification and authentication for each role

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

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

5.2.4 Roles requiring separation of duties

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

5.3 Personnel controls

5.3.1 Qualification, experience, and clearance requirements

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 a similar area as is provision of the Service;
- Knowledge in public key infrastructure and information security.

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

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

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

5.3.2 Background check procedures

The sources of information about all 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 provides some certificate issuance activities on a contractual basis but is fully responsible for the activities of these independent contractors involved in the issuance of a Certificate. Further pays:

- Commercial and legal relations are regulated by bilateral commercial agreements;
- These independent contractors:
  - Must meet personnel and event recording requirements analogously to those for providing activities with own resources od I.CA;
  - Are required to comply with the relevant certification policies, the certification practice statement, relevant internal documents provided to them and prescribed normative documents.

5.3.8 Documentation supplied to personnel

In addition to the certificate policy, the certification 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.

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 carried out 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.

Protocol on key pair generating with data required by technical standards is created and signed by present I.CA 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.

The recording of security events in systems, network elements and entrances to the operating sites is carried out in accordance with the requirements of the standards in chapters 6.5 and 6.6 of this document and meets the requirements of the S/MIME BR.

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

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

5.4.2 Frequency of processing log

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

5.4.3 Retention period for audit log

Unless the relevant legislation provides otherwise, audit records are kept for a minimum of 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 the trustworthy systems designated to support trust services is described in internal documentation.

5.5 Records archival

The archiving of records, i.e., information and documentation, at První certifikační autorita, a.s., is regulated by 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 from delegated third parties involved in the certificate lifecycle, 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 records according to chapter 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 records 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 archiving 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 sites designated therefore and are accessible to:

- I.CA employees if they need to have such access for their job;
- Authorized supervising and inspection entities and law enforcement authorities 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.

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 authority 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;
- Where appropriate 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 all subscribers of valid Certificates, to the parties having contract with I.CA that directly concerns the provision of the Service and, when appropriate to supervisory body;
- 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 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 provision of the Service is terminated, then the next procedure will be consistent with valid Service contracts and possibly in accordance with technical and other standards.

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

6 TECHNICAL 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 carried out 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.

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 to certificate issuer

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

6.1.4 CA public key delivery to relying parties

Following options for obtaining the Authority's public key contained in this certification authority’s certificate are guaranteed:

- Handover from RA;
- From the trusted 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, that 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 some 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 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 on 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 in 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 and entering the password;
- In case of softcard activation by entering the softcard and password.

Private keys of employees taking part in issuing certificates are activated by inserting the smartcard 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.

[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.

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 or by terminating the specific application.

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

Deactivation private keys related to Certificates of end users is fully within the competence of these end users and deepens 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.

Possible 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 maximum period of validity of each Certificate issued is specified in the body of that Certificate and is the same as key pair usage period. It complies with S/MIME BR requirements.

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.

Possible 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 trusted services is, including the scope of necessary evaluations and assessments and also trustworthy systems configuration checks, and their periodicity, defined in effective technical standards.

6.5.2 Computer security rating

The assessment of I.CA computer security is based on the requirements set out in 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;
- ETSI TS 119 411-6 Electronic Signatures and Infrastructures (ESI); Policy and security requirements for Trust Service Providers issuing certificates; Part 6:

Requirements for Trust Service Providers issuing publicly trusted S/MIME certificates;

- FIPS PUB 140-2 Requirements for Cryptographic Modules;
- ČSN EN ISO/IEC 15408-1 Informační bezpečnost, kybernetická bezpečnost a ochrana soukromí - Kritéria pro hodnocení bezpečnosti IT - Část 1: Úvod a obecný model;
- ISO/IEC 15408-1:2022 Information security, cybersecurity and privacy protection - Evaluation criteria for IT security - Part 1: Introduction and general model;
- ČSN EN ISO/IEC 15408-2 Informační bezpečnost, kybernetická bezpečnost a ochrana soukromí - Kritéria pro hodnocení bezpečnosti IT - Část 2: Bezpečnostní funkční komponenty;
- ISO/IEC 15408-2:2022 Information security, cybersecurity and privacy protection - Evaluation criteria for IT security - Part 2: Security functional components;
- ČSN EN ISO/IEC 15408-3 Informační bezpečnost, kybernetická bezpečnost a ochrana soukromí - Kritéria pro hodnocení bezpečnosti IT - Část 3: Komponenty bezpečnostních záruk;
- 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 S/MIME 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

Table 4 – Certificate basic fields

Field	Content
version	v3 (0x2)
serialNumber	unique serial number of the Certificate
signatureAlgorithm	on the basis of application (depending on signature algorithm of the certificate) one of following options: • sha256withRSAEncryption (with parameters = NULL, pkcs#1 1v5) at minimum; or • rsassaPss (pkcs#1 2v1) with parameters: – hashAlgorithm: sha256 at minimum; – maskGenAlgorithm: mgf with the same hash function as v hashAlgorithm; – saltLength: depending on used hash function; – trailerField: 0xBC (default)
issuer	issuer of the Certificate
validity	
notBefore	start of the Certificate's validity (UTC)
notAfter	notBefore + at maximum 365 days, or 366 days in case of leap year (UTC)
subject	see Table 5
subjectPublicKeyInfo*	
Algorithm	rsaEncryption
subjectPublicKey	2048 bits at minimum
extensions	see Table 6
signature	advanced electronic seal of Certificate's issuer

* 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.

Subject field attributes	Comments
countryName*	mandatory, single occurrence country code (ISO 3166), state where organization is registered - context of all other subject attributes
serialNumber	unique identification of the Certificate's subscriber in the Authority's system (ICA - xxxxxxxx)
commonName	mandatory; single occurrence in case of S/MIME BR type certificate: content identical to the content of the organizationName attribute other cases: • name under which the Certificate subject (private key owner) commonly acts, does not have to contain full registered name (can contain shortened name of organization), identification of equipment or ICT component creating electronic seals can be appended; • must not contain FQDN or IP address
emailAddress	this attribute must not be included in the primary Certificate
name	this attribute must not be included in the primary Certificate
organizationName	mandatory; single occurrence
organizationIdentifier	mandatory; single occurrence, one of following options: • NTR*ss-id*, (**N**ational **T**rade **R**egister, i.e., business/company identification number); • VAT*ss-id*, (**V**alue **A**dded **T**ax, i.e., tax identification number); • XX:ss-id; where: • *ss* is country code (ISO 3166) - same as countryName attribute; • *id* is identification number of the organization in corresponding register; • XX are two characters defined by the authority of specific state followed by the character ":" (colon) – national register different from VAT and NTR, for the Slovak Republic it is "SZ"

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

organizationalUnitName	optional; multiple occurrences permitted
stateOrProvinceName*	optional; single occurrence
localityName*	optional; single occurrence
streetAddress*	optional; single occurrence in case of S/MIME BR type certificate: only if attributes localityName or stateOrProvinceName are given
postalCode*	optional; single occurrence

* The attributes countryName, stateOrProvinceName, localityName, streetAddress and postalCode relate to the registered address of the Organization.

7.1.1 Version number(s)

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

7.1.2 Certificate extensions

Table 6 – Certificate extensions[3]

Extension	Content	Comments
certificatePolicies		non-critical
.policyInformation (1)		
policyIdentifier	see 1.2	
policyQualifiers		
cPSuri	http://www.ica.cz	
.policyInformation (2)		
policyIdentifier	one of following options: • OID (NCP): 0.4.0.2042.1.1 (the private key is not generated and stored on secure cryptographic device); • OID (NCP+): 0.4.0.2042.1.2 (the private key is generated and stored on secure cryptographic device)	
.policyInformation (3)		in case of S/MIME BR type certificate (Multipurpose)
policyIdentifier	Organization-validated: 2.23.140.1.5.2.2	
CRLDistributionPoints*	http://scrldp1.ica.cz/pca*YY*_rsa.crl	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).

	http://scrldp2.ica.cz/pca*YY*_rsa.crl	
authorityInformationAccess		non-critical
id-ad-ocsp*	http://ocsp.ica.cz/pca*YY*_rsa	
id-ad-caIssuers*	http://q.ica.cz/pca*YY*_rsa.cer	
basicConstraints		non-critical
cA	False	
keyUsage	depending on the content of Certificate application one of following options: • digitalSignature; • digitalSignature, nonRepudiation; • digitalSignature, keyEncipherment; • digitalSignature, keyEncipherment, nonRepudiation	critical, mandatory if the application contains not supported keyUsage, it will be removed if this extension is missing in the application, the following will be added: • digitalSignature, keyEncipherment
extendedKeyUsage	depending on the content of Certificate application - any combination of following options: • id-kp-clientAuth; • ms-DocumentSigning; • id-kp-emailProtection; • Microsoft SmartCard Logon excluding illegal separate ms-DocumentSigning	non-critical, mandatory if this extension is missing in the application, the following will be added: • id-kp-emailProtection if id-kp-emailProtection is not set in EKU, it will be added
subjectKeyIdentifier	hash of the public key (subjectPublicKey) in the Certificate	non-critical
authorityKeyIdentifier		non-critical
keyIdentifier	hash of the Authority's public key	
subjectAlternativeName		non-critical
otherName	I.CA_OID (1.3.6.1.4.1.23624.4.6): xxxxxxxx**	
otherName	User Principal Name: UPN	optional

		Microsoft OID
rfc822Name	e-mail address	optional; multiple occurrences permitted
nsComment	secure cryptographic device identification number	non-critical; optional – creates Authority when generating and storing of the private key on secure cryptographic device was verified
I.CA_CERT_INTERCONNECTION: 1.3.6.1.4.1.23624.4.7	if more certificate types are issued to a single entity (entity's connection to the certificates issued)	non-critical

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

** It is a selected sub-string from the subject field's serialNumber attribute created by the Authority (see Table 5).

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

7.1.3 Algorithm object identifiers

The algorithms used in providing the service comply with the relevant technical standards.

7.1.4 Name forms

Name forms in issued Certificates comply with RFC 5280 standard. The provisions of 3.1 also apply.

7.1.5 Name constraints

Not applicable for Certificates issued to end users.

7.1.6 Certificate policy object identifier

První certifikační autorita, a.s., inserts in the Certificates issued the following certificate policy object identifiers:

- OID of the I.CA certificate policy under which the Certificate is issued;
- OID of the relevant certificate policy defined by ETSI EN 319 411-1, or ČSN ETSI EN 319 411-1 as applicable with regard to the storing of the private key;
- OID of the relevant policy specified by S/MIME BR and MTRP in case of S/MIME BR type certificates.

7.1.7 Usage of Policy Constraints extension

Not applicable for Certificates issued to end users.

7.1.8 Policy qualifier syntax and semantics

See Certificate extensions in 7.1.2 above.

7.1.9 Processing semantics for the critical certificate policies extension

Not applicable for this document – extension is 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 released (UTC)
nextUpdate*	date and expected time when the next CRL will be released (UTC)
revokedCertificates	list of revoked certificates
userCertificate	revoked certificate's serial number
revocationDate	certificate revocation date and time
crlEntryExtensions	list 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 extension[5]

Extension	Content	Comments
crlEntryExtensions		
CRLReason*	certificate revocation reason	non-critical; optional

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

[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).

	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	non-critical
CRLNumber	unique number of the CRL to be released	non-critical

* For end user certificates, only the following CRLReason codes are used (according to the individual reasons for revocation - see chapter 4.9.1.1):

- 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 directly by Certificate subscriber, it is determined by CA (no later than July 15, 2023).

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 comply with RFC 6960 and RFC 5019.

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

Http only is used as the transmission protocol.

See the relevant certification practice statement for more detail.

7.3.1 Version number(s)

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

7.3.2 OCSP extensions

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

8 CONFORMITY ASSESSMENTS AND OTHER ASSESSMENTS

8.1 Frequency or circumstances of assessment

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

The intervals for other assessments are specified in the relevant technical standards, according to which the assessment is performed.

8.2 Identity/qualifications of assessor

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 the service.

External assessor is an assessor without any ties to I.CA both through property and person.

8.4 Topics covered by assessment

The areas to be assessed in an assessment required for Microsoft Trusted Root Program are strictly given by requirements of Microsoft Company.

The areas to be assessed in any other assessment are specified in the technical standards under which the assessment is made.

8.5 Actions taken as a result of deficiency

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

8.6 Communication of results

Assessment result notification is subject to the requirements of 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 Self audits

On at least quarterly basis, with the intervals immediately following each other, a randomly selected sample consisting of at least the greater number of the following options:

- thirty Certificates issued in the evaluation period; or
- three percent of the Certificates issued in the evaluation period;

a monitoring of adherence to this CP, corresponding CPS and S/MIME BR is performed. A report is created on the result.

If possible, a Linting process is used to verify the technical accuracy of the issued Certificates. The sample of Certificates is set independently of previous linting.

8.8 Review of delegated parties

I.CA performs on at least an annual basis monitoring of the delegated parties which do not undergo a regular annual audit whether they are in compliance with the provided relevant normative documents, corresponding certificate policies, certification practice statement and relevant internal documentation. In case of violation of the obligations set out in the above documents, contractual penalties are applied, or the contract with the supplier is immediately terminated. A protocol is created about the monitoring carried out.

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 a 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 Service 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, the service is not provided.

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 Service;
- 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 only the information marked as public and that 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, that is ZOOÚ 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 relevant legislation is 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 CP, all related documents, the website content and the procedures facilitating the operation of the trustworthy systems providing trust services are copyrighted by První certifikační autorita, a.s., and are important know-how thereof.

9.6 Representations and warranties

9.6.1 CA Representations and warranties

I.CA warrants that:

- It will use the certification authorities' private keys solely for issuing certificates to end users (except I.CA 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 requirements 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.

9.6.2 RA representations and warranties

The designated RA:

- Assumes the obligation that the services which the RA provides are correct;
- Does not accept the Certificate if the Certificate applicant refuses to provide necessary data or if the Certificate applicant 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

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

9.6.4 Relying parties 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 obligations under 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.

9.9 Indemnities

Applicable for the provision of the Service are the relevant provisions of the current legislation regulating provider–consumer relations and the warranties agreed between První certifikační autorita, a.s., and the applicant for the Service. The contract must always take an electronic or printed form.

První certifikační autorita, a.s.:

- Undertakes to discharge all the obligations defined in concluded Service contract and those in the relevant policies;
- Gives the aforesaid warranties throughout the term of the Service contract;
- 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 Service contract, 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 possible compensation is based on the relevant legislation and the amount of damage and may be determined by court.

9.10 Term and termination

9.10.1 Term

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

9.10.2 Termination

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

9.10.3 Effect of termination and survival

The obligations of I.CA arising from 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 Amending procedure

This procedure is a controlled process described in an 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 will have a significant effect on the acceptability of the Certificate in compliance with technical and other standards.

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

9.13 Disputes resolution provisions

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

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

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

9.14 Governing law

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

9.15 Compliance with applicable law

The system of providing the Service is in compliance with the legislation 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 there is a conflict between the requirements of the S/MIME BR or the referenced technical standards and the applicable legal regulation, the requirements specified in this CP will be minimized so that they are valid and in accordance with this applicable legal regulation. Immediately, and before the first issuance of the Certificate under the modified rules, a new version of the CP will be issued and a reference to the legal regulation that required the modification and a description of this modification will be added at the end of this chapter. Also, before the first issuance of the Certificate under the modified rules, a report on the modification will be sent to the CA/Browser Forum.

The modification of requirements made in accordance with these rules shall cease to apply if the corresponding provision of the legal regulation ceases to apply or if the requirements of the S/MIME BR or the referenced technical standards are changed.

All modifications and notifications mentioned above will be done within ninety days.

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.