První certifikační autorita, a.s.



Certificate Policy

for Issuing Qualified Certificates

for ZameKEP System

Certificate Policy for Issuing Qualified Certificates for ZameKEP System 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 1.001

Copyright © První certifikační autorita, a.s.

CONTENT

1 Introduction 10
1.1 Overview 10
1.2 Document name and identification 11
1.3 PKI Participants 11
1.3.1 Certification authorities 11
1.3.2 Registration authorities 11
1.3.3 Subscribers 11
1.3.4 Relying parties 12
1.3.5 Other participants 12
1.4 Certificate usage 12
1.4.1 Appropriate certificate uses 12
1.4.2 Prohibited certificate uses 12
1.5 Policy administration 12
1.5.1 Organization administering the document 12
1.5.2 Contact person 12
1.5.3 Person determining CPS suitability for the policy 12
1.5.4 CPS approval procedures 12
1.6 Definitions and acronyms 13
2 Publication and repository responsibilities 17
2.1 Repositories 17
2.2 Publication of certification information 17
2.3 Time or frequency of publication 18
2.4 Access controls on repositories 18
3 Identification and authentication 19
3.1 Naming 19
3.1.1 Types of names 19
3.1.2 Need for names to be meaningful 19
3.1.3 Anonymity or pseudonymity of subscribers 19
3.1.4 Rules for interpreting various name forms 19
3.1.5 Uniqueness of names 19
3.1.6 Recognition, authentication, and role of trademarks 19
3.2 Initial identity validation 19
3.2.1 Method to prove possession of private key 19
3.2.2 Authentication of organization identity 20

3.2.3 Authentication of individual identity 20
3.2.4 Non-verified subscriber information 21
3.2.5 Validation of authority 21
3.2.6 Criteria for interoperation 21
3.2.7 Validation of e-mail address 21
3.3 Identification and authentication for re-key requests 21
3.3.1 Identification and authentication for routine re-key 21
3.3.2 Identification and authentication for re-key after revocation 21
3.4 Identification and authentication for revocation request 21
4 Certificate life cycle operational requirements 23
4.1 Certificate application 23
4.1.1 Who can submit a certificate application 23
4.1.2 Enrollment process and responsibilities 23
4.2 Certificate application processing 23
4.2.1 Performing identification and authentication functions 23
4.2.2 Approval or rejection of certificate applications 24
4.2.3 Time to process certificate applications 24
4.3 Certificate Issuance 24
4.3.1 CA actions during certificate issuance 24
4.3.2 Notification to subscriber by the CA of issuance of certificate 24
4.4 Certificate acceptance 25
4.4.1 Conduct constituting certificate acceptance 25
4.4.2 Publication of the certificate by the CA 25
4.4.3 Notification of certificate issuance by the CA to other entities 25
4.5 Key pair and certificate usage 25
4.5.1 Subscriber private key and certificate usage 25
4.5.2 Relying party public key and certificate usage 25
4.6 Certificate renewal 26
4.6.1 Circumstance for certificate renewal 26
4.6.2 Who may request renewal 26
4.6.3 Processing certificate renewal requests 26
4.6.4 Notification of new certificate issuance to subscriber 26
4.6.5 Conduct constituting acceptance of a renewal certificate 26
4.6.6 Publication of the renewal certificate by the CA 26
4.6.7 Notification of certificate issuance by the CA to other entities 26
4.7 Certificate re-key 26

4.7.1 Circumstance for certificate re-key 27
4.7.2 Who may request certification of a new public key.....27
4.7.3 Processing certificate re-keying requests 27
4.7.4 Notification of new certificate issuance to subscriber 27
4.7.5 Conduct constituting acceptance of a re-keyed certificate 27
4.7.6 Publication of the re-keyed certificate by the CA.....27
4.7.7 Notification of certificate issuance by the CA to other entities 27
4.8 Certificate modification 27
4.8.1 Circumstance for certificate modification 27
4.8.2 Who may request certificate modification 27
4.8.3 Processing certificate modification requests 28
4.8.4 Notification of new certificate issuance to subscriber 28
4.8.5 Conduct constituting acceptance of modified certificate.....28
4.8.6 Publication of the modified certificate by the CA 28
4.8.7 Notification of certificate issuance by the CA to other entities 28
4.9 Certificate revocation and suspension.....28
4.9.1 Circumstances for revocation 28
4.9.2 Who can request revocation 30
4.9.3 Procedure for revocation request.....30
4.9.4 Revocation request grace period 31
4.9.5 Time within which CA must process the revocation request 31
4.9.6 Revocation checking requirement for relying parties.....31
4.9.7 CRL issuance frequency.....31
4.9.8 Maximum latency for CRLs.....32
4.9.9 On-line revocation/status checking availability 32
4.9.10 On-line revocation checking requirements.....32
4.9.11 Other forms of revocation advertisements available 32
4.9.12 Special requirements re key compromise 32
4.9.13 Circumstances for suspension.....32
4.9.14 Who can request suspension.....33
4.9.15 Procedure for suspension request 33
4.9.16 Limits on suspension period 33
4.10 Certificate status services 33
4.10.1 Operational characteristics 33
4.10.2 Service availability 33
4.10.3 Optional features 33

4.11 End of subscription....33
4.12 Key escrow and recovery....34
4.12.1 Key escrow and recovery policy and practices....34
4.12.2 Session key encapsulation and recovery policy and practices....34
5 Facility, management, and operational controls....35
5.1 Physical controls....35
5.1.1 Site location and construction....35
5.1.2 Physical access....35
5.1.3 Power and air conditioning....35
5.1.4 Water exposures....35
5.1.5 Fire prevention and protection....35
5.1.6 Media storage....36
5.1.7 Waste disposal....36
5.1.8 Off-site backup....36
5.2 Procedural controls....36
5.2.1 Trusted roles....36
5.2.2 Number of persons required per task....36
5.2.3 Identification and authentication for each role....37
5.2.4 Roles requiring separation of duties....37
5.3 Personnel controls....37
5.3.1 Qualification, experience, and clearance requirements....37
5.3.2 Background check procedures....37
5.3.3 Training requirements....38
5.3.4 Retraining frequency and requirements....38
5.3.5 Job rotation frequency and sequence....38
5.3.6 Sanctions for unauthorized actions....38
5.3.7 Independent contractor requirements....38
5.3.8 Documentation supplied to personnel....38
5.4 Audit logging procedures....39
5.4.1 Types of events recorded....39
5.4.2 Frequency of processing log....39
5.4.3 Retention period for audit log....39
5.4.4 Protection of audit log....39
5.4.5 Audit log backup procedures....39
5.4.6 Audit collection system (internal vs. external)....40
5.4.7 Notification to event-causing subject....40

5.4.8 Vulnerability assessments 40
5.5 Records archival 40
5.5.1 Types of records archived 40
5.5.2 Retention period for archive 40
5.5.3 Protection of archive 40
5.5.4 Archive backup procedures 41
5.5.5 Requirements for time-stamping of records 41
5.5.6 Archive collection system (internal or external) 41
5.5.7 Procedures to obtain and verify archive information 41
5.6 Key changeover 41
5.7 Compromise and disaster recovery 41
5.7.1 Incident and compromise handling procedures 41
5.7.2 Computing resources, software, and/or data are corrupted 41
5.7.3 Entity private key compromise procedures 42
5.7.4 Business continuity capabilities after a disaster 42
5.8 CA or RA termination 42
6 Technical security controls 44
6.1 Key pair generation and installation 44
6.1.1 Key pair generation 44
6.1.2 Private key delivery to subscriber 44
6.1.3 Public key delivery to certificate issuer 44
6.1.4 CA public key delivery to relying parties 44
6.1.5 Key sizes 45
6.1.6 Public key parameters generation and quality checking 45
6.1.7 Key usage purposes (as per X.509 v3 key usage extension) 45
6.2 Private key protection and cryptographic module engineering controls 45
6.2.1 Cryptographic module standards and controls 45
6.2.2 Private key (n out of m) multi-person control 45
6.2.3 Private key escrow 45
6.2.4 Private key backup 45
6.2.5 Private key archival 46
6.2.6 Private key transfer into or from a cryptographic module 46
6.2.7 Private key storage on cryptographic module 46
6.2.8 Method of activating private key 46
6.2.9 Method of deactivating private key 47
6.2.10 Method of destroying private key 47

6.2.11 Cryptographic module rating....47
6.3 Other aspects of key pair management....47
6.3.1 Public key archival....47
6.3.2 Certificate operational periods and key pair usage periods....48
6.4 Activation data....48
6.4.1 Activation data generation and installation....48
6.4.2 Activation data protection....48
6.4.3 Other aspects of activation data....48
6.5 Computer security controls....48
6.5.1 Specific computer security technical requirements....48
6.5.2 Computer security rating....48
6.6 Life cycle technical controls....51
6.6.1 System development controls....51
6.6.2 Security management controls....51
6.6.3 Life cycle security controls....51
6.7 Network security controls....52
6.8 Time-stamping....52
7 Certificate, CRL and OCSP profiles....53
7.1 Certificate profile....53
7.1.1 Version number(s)....54
7.1.2 Certificate extensions....54
7.1.3 Algorithm object identifiers....57
7.1.4 Name forms....57
7.1.5 Name constraints....57
7.1.6 Certificate policy object identifier....57
7.1.7 Policy qualifier syntax and semantics....57
7.1.8 Processing semantics for the critical certificate policies extension....57
7.2 CRL profile....58
7.2.1 Version number(s)....58
7.2.2 CRL and CRL entry extensions....58
7.3 OCSP profile....59
7.3.1 Version number(s)....59
7.3.2 OCSP extensions....59
8 Conformity assessments and other assessments....60
8.1 Frequency or circumstances of assessment....60
8.2 Identity/qualifications of assessor....60

8.3 Assessor's relationship to assessed entity 60
8.4 Topics covered by assessment 60
8.5 Actions taken as a result of deficiency.....60
8.6 Communication of results.....61
8.7 Self audits 61
8.8 Review of delegated parties 61
9 Other business and legal matters.....62
9.1 Fees.....62
9.1.1 Certificate issuance or renewal fees 62
9.1.2 Certificate access fees.....62
9.1.3 Revocation or status information access fees.....62
9.1.4 Fees for other services 62
9.1.5 Refund policy.....62
9.2 Financial responsibility 62
9.2.1 Insurance coverage 62
9.2.2 Other assets 62
9.2.3 Insurance or warranty coverage for end-entities 63
9.3 Confidentiality of business information 63
9.3.1 Scope of confidential information.....63
9.3.2 Information not within the scope of confidential information 63
9.3.3 Responsibility to protect confidential information 63
9.4 Privacy of personal information 63
9.4.1 Privacy plan.....63
9.4.2 Information treated as private 63
9.4.3 Information not deemed private 63
9.4.4 Responsibility to protect private information.....64
9.4.5 Notice and consent to use private information 64
9.4.6 Disclosure pursuant to judicial or administrative process 64
9.4.7 Other Information disclosure circumstances 64
9.5 Intellectual property rights 64
9.6 Representations and warranties.....64
9.6.1 CA Representations and warranties 64
9.6.2 RA representations and warranties.....65
9.6.3 Subscriber representations and warranties.....65
9.6.4 Relying parties representations and warranties 65
9.6.5 Representations and warranties of other participants 65

9.7 Disclaimers of warranties 65
9.8 Limitations of liability 65
9.9 Indemnities....66
9.10 Term and termination 66
9.10.1 Term....66
9.10.2 Termination 67
9.10.3 Effect of termination and survival....67
9.11 Individual notices and communications with participants 67
9.12 Amendments....67
9.12.1 Amending procedure 67
9.12.2 Notification mechanism and period....67
9.12.3 Circumstances under which OID must be changed 67
9.13 Disputes resolution provisions....67
9.14 Governing law 67
9.15 Compliance with applicable law....68
9.16 Miscellaneous provisions 68
9.16.1 Entire agreement....68
9.16.2 Assignment....68
9.16.3 Severability....68
9.16.4 Enforcement (attorneys' fees and waiver of rights) 68
9.16.5 Force Majeure 68
9.17 Other provisions....68
10 Final provisions 69

Table 1 – Document history

Version	Date of Release	Approved by	Comments
1.000	14 April 2026	CEO of První certifikační autorita, a.s.	First release.
1.001	17 September 2026	CEO of První certifikační autorita, a.s.	Committing to CCADB policy requirements. New organizational chart taken into account.

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, in providing qualified trust service of issuing qualified certificates for remote electronic signatures for ZameKEP system (also as the Service or the Certificate) to the employees of ČSOB group (also as Client). ECC algorithm is used for the Service provided under this certificate policy (also as the CP).

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

- Regulation (EU) no 910/2014 of the European Parliament and of the Council on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC, as amended;
- Act of the Czech Republic No. 297/2016 Coll., on trust services for electronic transactions;
- Legislation concerning personal data protection in compliance with Regulation (EU) no 2016/679 of the European Parliament and of the Council on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation).

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

The Service is provided to the employees of ČSOB group on the basis of a contract between I.CA and Československá obchodní banka, a.s., (also as Contract). I.CA imposes no other restrictions on potential end users, and the provision of the Service is non-discriminatory and the Service is also available to the disabled, unless the Bank has requested adaptation to its design requirements in a specific case.

1.1 Overview

Document **Certificate Policy for Issuing Qualified Certificates for ZameKEP System** 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 norms 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 and identification

Document's title:	Certificate Policy for Issuing Qualified Certificates for ZameKEP System, version 1.001
Policy OID (ECC):	1.3.6.1.4.1.23624.11.1.60.1.0

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 role of registration authorities is performed by employees of the HR department of the relevant member of the ČSOB group responsible for authentication the individual upon employment and by further defined employees responsible for additional physical authentication.

1.3.3 Subscribers

Subscriber of a Certificate is a natural person 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 electronic signatures created using the private keys corresponding to the Certificates issued under this CP is a relying party.

1.3.5 Other participants

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

1.4 Certificate usage

1.4.1 Appropriate certificate uses

Certificates issued under this CP can only be used in the processes of verifying an electronic signature created within the remote electronic signature creation service and in accordance with the trust services legislation.

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 CEO 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
contracting partner	provider of services contracted by I.CA for certification services or parts thereof – usually, it is a contracted RA
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
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
softcard	software emulation of smartcard for access to private key stored in HSM
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
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
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.
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
ČSN	Czech Technical Norm
DER, PEM	methods of certificate encoding (certificate formats)
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
ESAM	Entrust Signature Activation Module, certified component implementing QSCD functionality together with the relevant HSM
ESI	Electronic Signatures and Infrastructures
ETSI	European Telecommunications Standards Institute, a European standardization institute for information and communication technologies
EU	European Union
FAS	Fire Alarm System
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)
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.
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
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
PCO	Central Protection Desk, Pult centrální ochrany
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
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
QSCD	Qualified Electronic Signature/Seal Creation Device (defined by eIDAS)
RA	registration authority
RFC	Request for Comments, designation for a range of standards and other documents describing web protocols, systems, etc.
ROB	Register of Residents, Registr obyvatel
RSA	signing and encrypting public key cipher (acronym from the names of the original authors - Rivest, Shamir and Adleman)
S/MIME BR	CA/Browser Forum document „Baseline Requirements for the Issuance and Management of Publicly-Trusted S/MIME Certificates"
sha, SHA	type of hash function
TS	Technical Specification, type of ETSI standard
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
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 no later than 24 hours after the

incident to the supervisory body and, at its request, to the public on its web Information Address and in Hospodářské noviny or Mladá fronta Dnes, daily newspapers with national distribution.

The certification authority issuing the Certificates complies with the requirements of the current version of the document "CA/Browser Forum – Baseline Requirements for the Issuance and Management of Publicly-Trusted S/MIME Certificates", which is published at http://www.cabforum.org. In the event of any inconsistency between this CP and the aforementioned document, the aforementioned document shall 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, update depends on changes in normative requirements for issued Certificates, revision is carried out at least once a year;
- Certification practice statement – immediately;
- 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 subject field or in subjectAlternativeName extension must carry a meaning. See chapter 7 for the attributes supported for this field.

3.1.3 Anonymity or pseudonymity of subscribers

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

3.1.4 Rules for interpreting various name forms

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

3.1.5 Uniqueness of names

The Authority guarantees that the subject field in a Certificate of specific subscriber is unique.

3.1.6 Recognition, authentication, and role of trademarks

The Certificates issued under this CP don't contain any 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 generating of the key pair is initiated by the Client using his access data to the SAM or HSM. The used protocol guarantees that no one other than the Client has access to the private key and the Client is therefore its owner.

3.2.2 Authentication of organization identity

Authentication of organization identity is carried out in a standard manner when concluding a Contract.

3.2.3 Authentication of individual identity

The initial authentication of individual identity takes place upon hiring, when a face-to-face authentication is performed and, after authentication, the name, surname and date of birth are recorded in the ČSOB personnel system from the submitted personal document.

At regular intervals, this and some other information (e.g., the employee's unique identifier within the Bank's group member, a flag about physical verification upon hiring - whether it has been completed or whether additional physical authentication needs to be called up, a flag whether the MPSV identifier should be inserted, the employee's e-mail address, telephone number if listed and issuing country of personal identification document) are imported from the Bank's personnel system into the ZameKEP system (a system operated by the Bank designed to support remote signing). In addition, this import can be performed manually by the responsible employee via the Administrator Portal. In addition, through the Administrator Portal, the responsible employee can also manually insert data into the ZameKEP system about employee who is not entered into the Bank's personnel system. If the employee is in a contractual relationship other than an employment relationship, additional physical authentication is always performed when issuing the Certificate.

Note: Changes in data and data on Clients' leavings employment are also notified from the personnel system at regular intervals, so that the data in the ZameKEP system is always fully up-to-date. Even in this case, the responsible employee can enter data on changes in data or Client leaving employment into the ZameKEP system via the Administrator Portal.

At the moment when the Certificate is to be issued, i.e. the Client has logged in to the Bank's Self-service Portal and selected "Issue of certificate and activation of ČSOB ZameKEP", the Client is shown information about the organization within the Bank of which the Client is an employee, name, surname, date of birth and the conditions of issuance (including consent to the Bank to apply for certificates on his behalf, consent to verification personal data in the ROB). The Client fills in the number of the identification document, the date of its expiration and indicates agreement with the stated conditions.

The further procedure for issuing the Certificate varies depending on whether it is possible to perform verification in the ROB, or not (if the Client is a foreign national, the information provided does not include a telephone number, or the need for additional physical authentication is explicitly stated):

- in the case of a verification in the ROB (the Client has already expressed consent to the it – see above), it is checked based on the name, surname and number of the primary document whether the date of birth matches, whether it is not a document of a deceased person and whether the Client has not been deprived of legal capacity;
- without the possibility to verify data in the ROB, or if physical verification has not been performed, so-called additional physical authentication is necessary:
  - which is carried out by a designated employee of the Bank (i.e. has a special role assigned, is trained and, among other things, has a list of potential primary identification documents available);
  - which requires the presentation of a secondary personal document, which must either be an employee ID card of a member of the ČSOB group, or must be clearly linked

to the primary personal document (birth identification number, date of birth, number, etc.) and must contain at least one of the following data:

- date of birth (or birth identification number, if provided);
- photo of the face.

The data in the secondary personal document used to uniquely identify the Certificate subscriber must be identical to this data in the primary personal document.

3.2.4 Non-verified subscriber information

All information relating to the Certificate subscriber must be properly verified.

3.2.5 Validation of authority

Since the private key is always generated and used in QSCD device operated by I.CA, specific attribute is always inserted.

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 using the method of checking whether the address belongs to a registered DNS domain (validating authority over mailbox via domain) - the domain part of the e-mail address is verified against the list of verified domains managed by I.CA.

3.3 Identification and authentication for re-key requests

3.3.1 Identification and authentication for routine re-key

Identification and authentication are not performed in the case of routine re-key request (issuance of a subsequent Certificate), everything is done automatically and electronically.

3.3.2 Identification and authentication for re-key after revocation

Not relevant to this document as re-keying after Certificate revocation is not provided.

3.4 Identification and authentication for revocation request

Entities authorized to submit a request for revocation of a Certificate are listed in chapter 4.9.2.

The information that the request for revocation of the Certificate must contain is listed in chapter 4.6.3

I.CA reserves the right to accept also other Certificate revocation identification and authentication procedures, which, however, must not 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

The employee (Client or potential Certificate subscriber) applies the issuance of the Certificate but based on his consent – see chapter 3.2.3 – the Bank represents him when submitting the application.

4.1.2 Enrollment process and responsibilities

The registration process is carried out only in the case of establishing the Service, i.e. issuing the primary Certificate. Its course depends on the method of individual identity authentication - see chapter 3.2.3.

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

- Familiarize himself with this CP and contractually commit to act in accordance with it;
- Provide true and complete information for Certificate issuance.
- Check whether the data provided in the Certificate application and in the issued Certificate are correct and correspond to the required data.

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

- Inform the Client about the terms and conditions before concluding the Agreement;
- Conclude the Agreement that meets the requirements imposed by current legislation and technical standards and norms;
- During the process of issuing the Certificate validate all data specified in the application;
- 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 chapter 2.2;
- Publish the certificates of issuing and root certification authorities;
- Provide activities related to the Service in accordance with the trust service legislation, this CP, the relevant CPS, the System Security Policy – Trustworthy Systems and operational documentation.

4.2 Certificate application processing

4.2.1 Performing identification and authentication functions

When issuing a **primary Certificate**, identification and authentication are performed in accordance with chapter 3.2.3, in the case of issuing a **subsequent Certificate**, in accordance with chapter 3.3.1.

4.2.2 Approval or rejection of certificate applications

An application for the issuance of a primary Certificate, if the identity of the natural person is verified in the ROB, is approved upon successful completion of this verification. An application for the issuance of a primary Certificate without verification the identity of the natural person in the ROB is approved after successful additional physical verification of the identity of the natural person. It can then be rejected only in the event of failure of the checks performed by the CA core software – see chapter 4.3.1.

If the CA rejects the application, the Client (potential subscriber) is informed by e-mail to his employee e-mail address, the Bank's responsible employees are also informed and the rejection is recorded in the log. If the content of the identification data led to the rejection, the Client must arrange to update his personal data in the Bank's personnel system.

4.2.3 Time to process certificate applications

The process of issuing a primary Certificate with verification of the identity of a natural person in the ROB and the process of issuing a subsequent Certificate take place without intervention by the CA operator and the application processing time does not exceed minutes. The process of issuing a primary Certificate without verifying the identity of a natural person in the ROB includes additional physical authentication by a responsible Bank employee and the check by the CA operator ad the issuance time (only on business days and hours) is usually within 15 minutes. Only in exceptional cases may this time be longer.

4.3 Certificate Issuance

4.3.1 CA actions during certificate issuance

In the process of issuing the **primary Certificate**, the competence check and the formal correctness check of the data are performed by the software of the CA system core. In addition, if the authentication of the identity of the natural person did not include a verification in the ROB, the CA operator can perform a check of the Certificate application. If any of the above checks ends negatively, the Certificate issuance process is terminated.

The issuance of the **subsequent Certificate** is automated.

4.3.2 Notification to subscriber by the CA of issuance of certificate

In the process of issuing **the primary Certificate**, after the provision of the document "Documentation for the issuance and use of a qualified certificate for ZameKEP", hereinafter also "Agreement", an advanced electronic seal based on the Bank's qualified certificate, the Client is sent information to the employee's e-mail address and the issued Certificate can be viewed in the Self-service Portal. In addition, the issued Certificate can be published, the issuance is notified to the Bank and further handling of it can be by the Contract.

The issuance of a subsequent Certificate is automated at a certain time before the end of the validity of the original Certificate. After issuance the Certificate may be published, the issuance is notified to the Bank, the Client is sent information to the employee e-mail address and he has the option to revoke the issued Certificate. Further handling of the Certificate may be determined by the Contract.

4.4 Certificate acceptance

4.4.1 Conduct constituting certificate acceptance

If the conditions for issuing a Certificate have been met, it is issued. Subsequently, the Bank provides the Agreement with an advanced electronic seal based on a qualified certificate and makes it available to the Client in the Self-service Portal. The Client then has the option to revoke the issued Certificate.

4.4.2 Publication of the certificate by the CA

I.CA will ensure the publication of the Certificate after providing the Agreement with an advanced electronic seal based on a qualified certificate, unless it has been requested not to be published.

4.4.3 Notification of certificate issuance by the CA to other entities

The issuance of the Certificate is not notified to other entities.

4.5 Key pair and certificate usage

4.5.1 Subscriber private key and certificate usage

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

- Observe all relevant provisions of the Agreement;
- Use the private key and corresponding Certificate issued under this CP only for the purposes specified in this CP;
- Handle access data to the private key, which corresponds to the public key contained in the Certificate issued under this CP, in such a way that the private key cannot be abused;
- Immediately notify the Service provider of any facts that lead to the revocation of the Certificate, in particular:
  - Suspicion that the private key has been misused, and
  - Invalidity or inaccuracy of data in the Certificate.

  In such cases request revocation of the Certificate and terminate use of the relevant private key.

4.5.2 Relying party public key and certificate usage

Relying parties are obliged, among other things:

- Obtain, from a secure source (e.g., www.ica.cz, supervisory body web pages, relevant trusted list) certification authorities 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 and trust services legislation which relate to the relying party's duties.

4.6 Certificate renewal

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

Certificate renewal is not provided.

4.6.1 Circumstance for certificate renewal

See 4.6.

4.6.2 Who may request renewal

See 4.6.

4.6.3 Processing certificate renewal requests

See 4.6.

4.6.4 Notification of new certificate issuance to subscriber

See 4.6.

4.6.5 Conduct constituting acceptance of a renewal certificate

See 4.6.

4.6.6 Publication of the renewal certificate by the CA

See 4.6.

4.6.7 Notification of certificate issuance by the CA to other entities

See 4.6.

4.7 Certificate re-key

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 items listed in the subject field or subjectAlternativeName extension of the Certificate, whose public key is the subject of exchange.

A request for the issuance of a subsequent Certificate is made at a certain time before the expiration of the original Certificate, based on the Client's consent - see 3.2.3. Then the subscriber has the option to revoke the subsequent Certificate.

4.7.1 Circumstance for certificate re-key

The subsequent Certificate is issued automatically, without intervention by the Certificate subscriber or CA operators.

4.7.2 Who may request certification of a new public key

Certification of a new public key in the relevant Certificate may be, based on the Client's consent – see 3.2.3, requested by the Bank.

4.7.3 Processing certificate re-keying requests

The request to re-key the Certificate is processed immediately after receiving it.

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

Modifying Certificate data 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.

Certificate renewal is not provided.

4.8.1 Circumstance for certificate modification

See 4.8.

4.8.2 Who may request certificate modification

See 4.8.

4.8.3 Processing certificate modification requests

See 4.8.

4.8.4 Notification of new certificate issuance to subscriber

See 4.8.

4.8.5 Conduct constituting acceptance of modified certificate

See 4.8.

4.8.6 Publication of the modified certificate by the CA

See 4.8.

4.8.7 Notification of certificate issuance by the CA to other entities

See 4.8.

4.9 Certificate revocation and suspension

Certificate revocation is described in the following subsections.

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 in the Self-service Portal or the responsible Bank employee in the Administrator Portal 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 e-mail 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 e-mail 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 e-mail 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 or 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 make 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;
- Person authorized to act on behalf of the Bank;
- Person authorized to act on behalf the legal successor of the Bank;
- 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):
  - If the Certificate is issued on the basis of false data;
  - If demonstrably finds out that the Certificate was issued in spite of noncompliance with the requirements of trust services legislation;
  - If demonstrably finds out that the Certificate was used contrary to the restrictions defined in 1.4.2;
  - If demonstrably finds out that the Certificate's subscriber has died or been limited in legal capacity by court 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;
- Supervisory body and other entities as may be specified in trust services legislation.

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 – see 4.9.3.

4.9.3 Procedure for revocation request

Revocation of the Certificate by the Certificate subscriber or by the Bank based on consent – see 3.2.3 – is possible in two ways:

- Subscriber performs the revocation via the Self-service Portal; or
- Person authorized to act on behalf of the Bank performs the revocation via the Administrator Portal.

The result in both cases is the submission of a revocation request signed by the so-called system operator certificate (which has RA operator rights set in I.CA systems).

Notification 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 by registered mail to the address of the company's registered office or can be submitted via a data mailbox - 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.

The period until the publication of the revocation of the Certificate must not exceed the interval specified in chapter 4.9.1.

4.9.6 Revocation checking requirement for relying parties

Relying parties are obliged to perform all actions specified in chapter 4.5.2.

4.9.7 CRL issuance frequency

CRL is issued immediately after the positive processing of the revocation request. If no Certificate is revoked, a new CRL is usually issued at an interval of 8 hours, but no more than 24 hours after the previous CRL was issued.

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 service using the OCSP protocol is publicly available. Each Certificate issued under this CP contains a link to the relevant OCSP responder.

OCSP responses comply with RFC 6960 and RFC 5019. The OCSP responder's certificate contains an extension of type id-pkix-ocsp-nocheck 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 OSCP response is as of the release date of this CP version 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).

OSCP 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 issued Certificates.

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

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 procedure for terminating the Agreement is defined by the Contract.

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:

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

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

5.1 Physical controls

5.1.1 Site location and construction

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

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

5.1.2 Physical access

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

5.1.3 Power and air conditioning

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

5.1.4 Water exposures

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

5.1.5 Fire prevention and protection

The buildings of the operating sites and the information archiving sites have electronic fire alarm system (FAS). Fireproof insulation is installed in the entrance doors to the restricted

areas in which the trustworthy systems designated to support trust services are situated, and 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;
- Initialization of the security world of the cryptographic module, in which the private keys belonging to the public keys in the issued Certificates are used.

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 the provision of trust services;
- Knowledge in public key infrastructure and information security.

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

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

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

5.3.2 Background check procedures

The sources of information about all 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 twelve months.

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

5.3.5 Job rotation frequency and sequence

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

5.3.6 Sanctions for unauthorized actions

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

5.3.7 Independent contractor requirements

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

5.3.8 Documentation supplied to personnel

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

5.4 Audit logging procedures

5.4.1 Types of events recorded

Subject to logging are all the events required by trust services legislation or the relevant technical and other standards to be logged, that is, for example, the life cycle events of Certificates.

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 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.

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 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 described in internal documentation.

5.5.1 Types of records archived

I.CA archives the following electronic or printed records pertaining to the trust services provided, 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 of the certificates (especially the documents relating to validation of certificate issuance applications and certificate revocation requests);
- 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

All records pertaining to the certificates of all I.CA certification authorities and their respective OCSP responders, except for the pertinent private keys, are archived throughout the existence of I.CA. Other records are archived in accordance with 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 at 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 the case of reasonable concern that a private key of certification authorities has been compromised, I.CA does the following:

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

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

5.7.4 Business continuity capabilities after a disaster

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

5.8 CA or RA termination

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

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

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

- The information must be notified in writing or electronically to all subscribers of valid Certificates, and the parties having contract with I.CA that directly concerns the provision of trust services;
- The information must be published in accordance with 2.2. at all offices of registration authorities and must also communicate that certification authorities' certificates cannot be used in accordance with the purpose of their issuance any longer;

- The subsequent course of action will be decided by CEO of I.CA while taking account of the decision of the supervisory body.

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

6 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 the Certificates generating takes place in a QSCD-type device located in secure, dedicated areas of the operating site.

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.

Not applicable for the private keys of the Certificates - these private keys are stored in the cryptographic module, which is under the sole control of I.CA.

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

6.1.3 Public key delivery to certificate issuer

Not applicable for public keys od Service end users. These public keys are generated as part of the key pair in the cryptographic module under the sole control of I.CA. The public key as part of the issued Certificate is published immediately after issuance, further handling of the Certificate may depend on the contract between a specific third party and I.CA.

Public keys of other certificates 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 certification authority's public key contained in this certification authority’s certificate are guaranteed:

- Via web information addresses of I.CA, relevant supervisory body or its journal;
- From the trust list of the Czech Republic;
- By downloading it from the Bank’s Self-Service Portal.

6.1.5 Key sizes

The size of the key of I.CA root certification authority using ECC cryptography is 384 bits at minimum, the size of the keys in certificates od subordinate certification authorities issued by this root certification authority is 384, the size of the keys of OCSP responders is 256 bits at minimum. The minimum size of the keys in the Certificates issued under this CP is 256 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 used on cryptographic modules which meet the requirements of trust services legislation, that is ETSI and CEN standards and are used in accordance to their certification.

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

Key pairs of end users are generated and corresponding private keys are used in cryptographic module which is listed in EU list as QSCD.

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

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

The cryptographic modules used for the administration of end users' key pairs facilitates private key backup. Encryption of these backups ensures the same level of protection as the cryptographic module does.

6.2.5 Private key archival

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 devices.

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

Private keys related to Certificates of end users are not archived, after expiration the access data to these keys enabling their decryption and subsequent use are destroyed.

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) on 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.

Private keys related to Certificates of end users are generated (as non-exportable) on cryptographic modules (operated in certified mode) and there is no way to export them outside the cryptographic module[2]. Import of private keys into the cryptographic module is not performed.

6.2.7 Private key storage on cryptographic module

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

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

Private keys related to Certificates of end users are stored on cryptographic module which is listed in EU list as QSCD.

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:

[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.

[2] 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.

- 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 done by smartcard - inserting the smartcard and entering the password.

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 of private keys related to Certificates end users is done by terminating the specific application.

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 means deleting access data to these keys. Without these access data it is impossible to decrypt and use the key. This happens after revocation of specific Certificate or after issuing subsequent Certificate.

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.

Cryptographic modules used for generating of key pairs and storing corresponding private keys of end users are listed in EU list of QSCD devices.

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.

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.

Activation data of end users' private keys (softcard) of are created before or during the generating of the corresponding key pair.

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 are protected by passwords.

6.4.3 Other aspects of activation data

Not applicable for this document.

6.5 Computer security controls

6.5.1 Specific computer security technical requirements

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

6.5.2 Computer security rating

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

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

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

- EN 419 221-5 Protection profiles for TSP Cryptographic modules - Part 5 Cryptographic Module for Trust Services;
- 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.
- ČSN EN 419 241-1 – Trustworthy Systems Supporting Server Signing – Part 1: General System Security Requirements;
- EN 419 241-1 – Trustworthy Systems Supporting Server Signing - Part 1: General System Security Requirements;
- ČSN EN 419 241-2 – Trustworthy Systems Supporting Server Signing – Part 2: Protection profile for QSCD for Server Signing;
- EN 419 241-2 – Trustworthy Systems Supporting Server Signing - Part 2: Protection profile for QSCD for Server Signing;
- 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;
- FIPS PUB 140-2 Requirements for Cryptographic Modules;
- 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, greater than zero, with a random part of at least 64 bits from the random generator used for cryptosystems
signatureAlgorithm	ecdsa-with-SHA384
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	id-ecPublicKey, NIST P-256 (secp256r1), NIST P-384 (secp384r1)
subjectPublicKey	256 bits, 384 bits
extensions	see Table 6
signature	advanced electronic seal of Certificate's issuer

Table 5 – Subject field attributes

All attributes[3] of the subject field are taken over from the Certificate application except the attributes created by the Authority. The application must include the mandatory attributes.

Subject field attributes	Comments
countryName**	mandatory, country code (ISO 3166), single occurrence
givenName	mandatory, single occurrence
surName	mandatory, single occurrence
serialNumber (1)	unique identification of the Certificate's subscriber in the Authority's system (ICA - xxxxxxxx)
serialNumber (2)	optional; one of following options: • IDC*ss-nnnnnnnn*;

[3] 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).

	• PASss-*nnnnnnnn*; where *ss* is the country code (ISO 3166) of document's issuer, and *nnnnnnnn* is the document number
commonName*	mandatory, single occurrence, must contain givenName and surName
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 the country code (ISO 3166); • *id* is the organization's identification number in the relevant register; • XX are two characters defined by the given country's authority and followed by ':' (colon) – type of national register other than VAT and NTR

* The attribute may also contain validates degrees of the Certificate's subscriber.

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[4]

Extension	Content	Comments
certificatePolicies		non-critical
.policyInformation (1)		
policyIdentifier	see 1.2	
policyQualifiers		
cPSuri	http://www.ica.cz	
userNotice	Tento kvalifikovany certifikat pro elektronicky podpis byl vydan	

[4] 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).

	v souladu s narizenim EU c. 910/2014. This is a qualified certificate for electronic signature according to Regulation (EU) No 910/2014.	
.policyInformation (2)		
policyIdentifier	OID (QCP-n-qscd): 0.4.0.194112.1.2 (the private key is generated and stored on QSCD)	
QCStatements		non-critical
	0.4.0.1862.1.1	Id-etsi-qcs-QcCompliance
	0.4.0.1862.1.4	Id-etsi-qcs-QcSSCD; specified when the private key is generated and stored on QSCD
	0.4.0.1862.1.5	id-etsi-qcs-QcPDS; link (URI, https) to user notice (PDS)
	0.4.0.1862.1.6 = 0.4.0.1862.1.6.1	id-etsi-qcs-QcType = id-etsi-qct-esign
CRLDistributionPoints*	http://qcrldp1.ica.cz/2qca*YY*_ecc.crl http://qcrldp2.ica.cz/2qca*YY*_ecc.crl http://qcrldp3.ica.cz/2qca*YY*_ecc.crl	non-critical
authorityInformationAccess		non-critical
id-ad-ocsp*	http://ocsp.ica.cz/2qca*YY*_ecc	
id-ad-caIssuers*	http://q.ica.cz/2qca*YY*_ecc.cer	
basicConstraints		non-critical
cA	False	
keyUsage	digitalSignature, nonRepudiation	critical, mandatory
extendedKeyUsage	id-kp-emailProtection, ms-Document_Signing	non-critical, mandatory
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_User_ID(1.3.6.1.4.1.23624.4.6) : xxxxxxxx	
otherName	MPSV_IK (1.3.6.1.4.1.11801.2.1): numerical identifier supplied by MPSV	optional
rfc822Name	e-mail address	optional, multiple occurrences permitted
directoryName		
serialNumber	personal number or identifier of the Certificate subscriber	mandatory
organizationName	name of the organization that assigns and registers the personal number	mandatory
organizationIdentifier	number of the organization that assigns and registers the personal number	mandatory, single occurrence: • NTR*ss-id*, (National **T**rade **R**egister, i.e. IČ); • VAT*ss-id*, (**V**alue **A**dded **T**ax, i.e. DIČ); • XX:ss-id; where: • *ss* is the country code (ISO 3166); • *id* is the organization's identification number in the relevant register; • XX are two characters defined by the given country's authority and followed by ':' (colon) – type of national register other than VAT and NTR

givenName		see subject.givenName
surName		see subject.surName

* 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 trust services 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 319 411-2, or ČSN ETSI EN 319 411-2 as applicable, for a certificate issued to an individual with regard to the storing of the private key;
- OID defining Sponsor-validated type and Multipurpose generation S/MIME certificate (see S/MIME BR).

7.1.6.1 Usage of Policy Constraints extension

Not applicable for Certificates issued to end users.

7.1.7 Policy qualifier syntax and semantics

See Certificate extensions in 7.1.2 above.

7.1.8 Processing semantics for the critical certificate policies extension

Not applicable for this document – not classified as critical.

7.2 CRL profile

Table 7 – CRL profile[5]

Field	Content
version	v2(0x1)
signatureAlgorithm	ecdsa-with-SHA384
issuer	issuer of the CRL
thisUpdate	date and time when the CRL were 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 365 days at maximum, in case of subordinate CA 24 hours at maximum.

7.2.1 Version number(s)

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

7.2.2 CRL and CRL entry extensions

Table 8 – CRL extensions[6]

Extension	Content	Comments
crlEntryExtensions		
CRLReason*	certificate revocation reason as the *certificateHold* reason is not admissible, it is not used another reason than unspecified (0) is given when subordinate CA's certificate is revoked	non-critical; optional
crlExtensions		
authorityKeyIdentifier		
keyIdentifier	hash of the CRL issuer's public key	non-critical

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

[6] 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).

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.

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

The Microsoft Trusted Root Program assessment interval and circumstances are strictly defined by Microsoft, and the audit period is no longer than one year.

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

8.2 Identity/qualifications of assessor

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

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

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

8.3 Assessor's relationship to assessed entity

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

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

8.4 Topics covered by assessment

The areas to be assessed in an assessment required under trust services legislation are those as specified in that legislation.

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

8.6 Communication of results

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

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

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

8.7 Self audits

On at least quarterly basis, with the intervals immediately following each other, a randomly selected sample of S/MIME BR certificates 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

Fees for issuing Certificates are not charged, they are replaced by a flat-rate payment for using the remote electronic signature creation service.

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 trust services given the risk of a liability-for-damage claim.

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

9.2.3 Insurance or warranty coverage for end-entities

Not applicable for this document.

9.3 Confidentiality of business information

9.3.1 Scope of confidential information

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

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

9.3.2 Information not within the scope of confidential information

Public information is 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 information 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 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;
- Private keys of Certificate subscribers are stored in a way that ensures their confidentiality and integrity, and access to such a key is limited to the authorized subscriber of the Certificate;
- Certificates meet the statutory trust services requirements and those of the relevant technical standards;
- It will revoke any issued Certificate if the revocation request is filed in the manner defined in this CP;
- When issuing Certificates, during their validity period and in their administration, it will comply with its CP and its corresponding CPS.

The warranties also include:

- Verification of authorization to apply for the Certificate;

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

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

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

The manner in which the subscriber of a Certificate issued under this CP exercises the guarantee is defined in the Contract.

9.6.2 RA representations and warranties

RA warrants that:

- It assumes liability for the correctness of the services provided;
- The employee responsible for additional physical verification will not process the application positively if any of the application items could not be verified or the Client refuses to provide the necessary information or is not authorized to submit an application for the Service.

9.6.3 Subscriber representations and warranties

The guarantees of the Certificate subscriber are set out in the Agreement.

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 trust services legislation and particular

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

První certifikační autorita, a.s.:

- Undertakes to discharge all the obligations defined in current legislation (including the trust services legislation) and those in the relevant policies;
- Gives the aforesaid warranties throughout the term of the contract of trust services;
- Agrees that the application software suppliers with a valid contract with První certifikační autorita, a.s., for the distribution of the root certificate assume no obligation or liability, except for where damage or loss is directly attributable to the software of that supplier.

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, 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).

The method of filing a complaint is defined in the Contract. The complaining party is obliged to provide:

- The most concise description of the defect and its symptoms;
- The serial number of the product being complained about;
- The requested method of handling the complaint.

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.

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

In general, I.CA may use the e-mail addresses, postal addresses, telephone numbers, personal meetings, etc. provided by the parties for individual notifications and communication with the parties involved. However, in the case of this CP, this usually concerns communication between the parties to the Contract.

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 trust services legislation.

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

9.13 Disputes resolution provisions

The dispute resolution procedure is defined in the Contract.

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 trust services 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.