První certifikační autorita, s.r.o.



Certificate Policy

for Issuing Qualified Certificates for Remote Signing

According to the Legislation of the Slovak Republic

(RSA Algorithm)

Certificate Policy for Issuing Qualified Certificates for Remote Signing According to the Legislation of the Slovak Republic (RSA Algorithm) is a public document, which is the property of První certifikační autorita, s.r.o., 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 1.003

Copyright © První certifikační autorita, s.r.o.

CONTENT

1 Introduction 11
1.1 Overview 12
1.2 Document name and identification 13
1.2.1 Certificates for electronic signatures 13
1.2.2 Mandate certificates 13
1.3 PKI Participants 13
1.3.1 Certification authorities 13
1.3.2 Registration authorities 13
1.3.3 Subscribers 14
1.3.4 Relying parties 14
1.3.5 Other participants 14
1.4 Certificate usage 14
1.4.1 Appropriate certificate uses 14
1.4.2 Prohibited certificate uses 14
1.5 Policy administration 14
1.5.1 Organization administering the document 14
1.5.2 Contact person 14
1.5.3 Person determining CPS suitability for the policy 14
1.5.4 CPS approval procedures 15
1.6 Definitions and acronyms 15
2 Publication and repository responsibilities 20
2.1 Repositories 20
2.2 Publication of certification information 20
2.3 Time or frequency of publication 21
2.4 Access controls on repositories 21
3 Identification and authentication 22
3.1 Naming 22
3.1.1 Types of names 22
3.1.2 Need for names to be meaningful 22
3.1.3 Anonymity or pseudonymity of subscribers 22
3.1.4 Rules for interpreting various name forms 22
3.1.5 Uniqueness of names 22
3.1.6 Recognition, authentication, and role of trademarks 22
3.2 Initial identity validation 22

3.2.1 Method to prove possession of private key 22
3.2.2 Authentication of organization identity 22
3.2.3 Authentication of individual identity 23
3.2.4 Non-verified subscriber information 23
3.2.5 Validation of authority 23
3.2.6 Criteria for interoperation 23
3.2.7 Validation of e-mail address 23
3.3 Identification and authentication for re-key requests 23
3.3.1 Identification and authentication for routine re-key 23
3.3.2 Identification and authentication for re-key after revocation 23
3.4 Identification and authentication for revocation request 24
4 Certificate life cycle operational requirements 25
4.1 Certificate application 25
4.1.1 Who can submit a certificate application 25
4.1.2 Enrollment process and responsibilities 25
4.2 Certificate application processing 25
4.2.1 Performing identification and authentication functions 25
4.2.2 Approval or rejection of certificate applications 25
4.2.3 Time to process certificate applications 25
4.3 Certificate Issuance 26
4.3.1 CA actions during certificate issuance 26
4.3.2 Notification to subscriber by the CA of issuance of certificate 26
4.4 Certificate acceptance 26
4.4.1 Conduct constituting certificate acceptance 26
4.4.2 Publication of the certificate by the CA 26
4.4.3 Notification of certificate issuance by the CA to other entities 26
4.5 Key pair and certificate usage 27
4.5.1 Subscriber private key and certificate usage 27
4.5.2 Relying party public key and certificate usage 27
4.6 Certificate renewal 27
4.6.1 Circumstance for certificate renewal 27
4.6.2 Who may request renewal 27
4.6.3 Processing certificate renewal requests 27
4.6.4 Notification of new certificate issuance to subscriber 27
4.6.5 Conduct constituting acceptance of a renewal certificate 27
4.6.6 Publication of the renewal certificate by the CA 28

4.6.7 Notification of certificate issuance by the CA to other entities 28
4.7 Certificate re-key 28
4.7.1 Circumstance for certificate re-key 28
4.7.2 Who may request certification of a new public key.....28
4.7.3 Processing certificate re-keying requests 28
4.7.4 Notification of new certificate issuance to subscriber 28
4.7.5 Conduct constituting acceptance of a re-keyed certificate 28
4.7.6 Publication of the re-keyed certificate by the CA.....28
4.7.7 Notification of certificate issuance by the CA to other entities 28
4.8 Certificate modification 29
4.8.1 Circumstance for certificate modification 29
4.8.2 Who may request certificate modification 29
4.8.3 Processing certificate modification requests 29
4.8.4 Notification of new certificate issuance to subscriber 29
4.8.5 Conduct constituting acceptance of modified certificate.....29
4.8.6 Publication of the modified certificate by the CA 29
4.8.7 Notification of certificate issuance by the CA to other entities 29
4.9 Certificate revocation and suspension.....29
4.9.1 Circumstances for revocation 29
4.9.2 Who can request revocation 30
4.9.3 Procedure for revocation request.....30
4.9.4 Revocation request grace period 30
4.9.5 Time within which CA must process the revocation request 30
4.9.6 Revocation checking requirement for relying parties.....31
4.9.7 CRL issuance frequency.....31
4.9.8 Maximum latency for CRLs.....31
4.9.9 On-line revocation/status checking availability 31
4.9.10 On-line revocation checking requirements.....31
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.....32
4.9.15 Procedure for suspension request 32
4.9.16 Limits on suspension period 32
4.10 Certificate status services 32
4.10.1 Operational characteristics 32

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

5.4.6 Audit collection system (internal vs. external) 39
5.4.7 Notification to event-causing subject....39
5.4.8 Vulnerability assessments 39
5.5 Records archival 39
5.5.1 Types of records archived 39
5.5.2 Retention period for archive....40
5.5.3 Protection of archive....40
5.5.4 Archive backup procedures 40
5.5.5 Requirements for time-stamping of records 40
5.5.6 Archive collection system (internal or external)....40
5.5.7 Procedures to obtain and verify archive information 40
5.6 Key changeover 40
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 41
5.7.4 Business continuity capabilities after a disaster 41
5.8 CA or RA termination 41
6 Technical security controls 43
6.1 Key pair generation and installation....43
6.1.1 Key pair generation 43
6.1.2 Private key delivery to subscriber 43
6.1.3 Public key delivery to certificate issuer 43
6.1.4 CA public key delivery to relying parties 43
6.1.5 Key sizes....44
6.1.6 Public key parameters generation and quality checking....44
6.1.7 Key usage purposes (as per X.509 v3 key usage extension)....44
6.2 Private key protection and cryptographic module engineering controls 44
6.2.1 Cryptographic module standards and controls....44
6.2.2 Private key (n out of m) multi-person control....44
6.2.3 Private key escrow 44
6.2.4 Private key backup 45
6.2.5 Private key archival 45
6.2.6 Private key transfer into or from a cryptographic module 45
6.2.7 Private key storage on cryptographic module 45
6.2.8 Method of activating private key 46

6.2.9 Method of deactivating private key 46
6.2.10 Method of destroying private key 46
6.2.11 Cryptographic module rating 46
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 47
6.4 Activation data 47
6.4.1 Activation data generation and installation 47
6.4.2 Activation data protection 47
6.4.3 Other aspects of activation data 47
6.5 Computer security controls 47
6.5.1 Specific computer security technical requirements 47
6.5.2 Computer security rating 48
6.6 Life cycle technical controls 50
6.6.1 System development controls 50
6.6.2 Security management controls 50
6.6.3 Life cycle security controls 51
6.7 Network security controls 51
6.8 Time-stamping 51
7 Certificate, CRL and OCSP profiles 52
7.1 Certificate profile 52
7.1.1 Version number(s) 59
7.1.2 Certificate extensions 59
7.1.3 Algorithm object identifiers 65
7.1.4 Name forms 65
7.1.5 Name constraints 65
7.1.6 Certificate policy object identifier 66
7.1.7 Usage of Policy Constraints extension 66
7.1.8 Policy qualifier syntax and semantics 66
7.1.9 Processing semantics for the critical certificate policies extension 66
7.2 CRL profile 66
7.2.1 Version number(s) 67
7.2.2 CRL and CRL entry extensions 67
7.3 OCSP profile 68
7.3.1 Version number(s) 68

7.3.2 OCSP extensions 68
8 Conformity assessments and other assessments 69
8.1 Frequency or circumstances of assessment 69
8.2 Identity/qualifications of assessor 69
8.3 Assessor's relationship to assessed entity 69
8.4 Topics covered by assessment 69
8.5 Actions taken as a result of deficiency 69
8.6 Communication of results 70
8.7 Self audits 70
8.8 Review of delegated parties 70
9 Other business and legal matters 71
9.1 Fees 71
9.1.1 Certificate issuance or renewal fees 71
9.1.2 Certificate access fees 71
9.1.3 Revocation or status information access fees 71
9.1.4 Fees for other services 71
9.1.5 Refund policy 71
9.2 Financial responsibility 71
9.2.1 Insurance coverage 71
9.2.2 Other assets 71
9.2.3 Insurance or warranty coverage for end-entities 72
9.3 Confidentiality of business information 72
9.3.1 Scope of confidential information 72
9.3.2 Information not within the scope of confidential information 72
9.3.3 Responsibility to protect confidential information 72
9.4 Privacy of personal information 72
9.4.1 Privacy plan 72
9.4.2 Information treated as private 72
9.4.3 Information not deemed private 72
9.4.4 Responsibility to protect private information 73
9.4.5 Notice and consent to use private information 73
9.4.6 Disclosure pursuant to judicial or administrative process 73
9.4.7 Other Information disclosure circumstances 73
9.5 Intellectual property rights 73
9.6 Representations and warranties 73
9.6.1 CA Representations and warranties 73

9.6.2 RA representations and warranties....74
9.6.3 Subscriber representations and warranties....74
9.6.4 Relying parties representations and warranties....74
9.6.5 Representations and warranties of other participants....74
9.7 Disclaimers of warranties....75
9.8 Limitations of liability....75
9.9 Indemnities....75
9.10 Term and termination....75
9.10.1 Term....75
9.10.2 Termination....75
9.10.3 Effect of termination and survival....75
9.11 Individual notices and communications with participants....75
9.12 Amendments....76
9.12.1 Amending procedure....76
9.12.2 Notification mechanism and period....76
9.12.3 Circumstances under which OID must be changed....76
9.13 Disputes resolution provisions....76
9.14 Governing law....76
9.15 Compliance with applicable law....76
9.16 Miscellaneous provisions....76
9.16.1 Entire agreement....76
9.16.2 Assignment....76
9.16.3 Severability....76
9.16.4 Enforcement (attorneys' fees and waiver of rights)....77
9.16.5 Force Majeure....77
9.17 Other provisions....77
10 Final provisions....78

Table 1 – Document history

Version	Date of Release	Approved by	Comments
1.00	15 October 2022	Ing. Ctirad Fischer, Managing Director of První certifikační autorita, s.r.o.	First release.
1.001	22 June 2024	Ing. Ctirad Fischer, Managing Director of	List of referenced standards updated.

		První certifikační autorita, s.r.o.	Mandate certificate - clarifying the presence of Mandator part attributes in the subject field and adding the directoryName attribute in the subjectAlternativeName extension of the certificate.
1.002	26 August 2024	Ing. Ctirad Fischer, Managing Director of První certifikační autorita, s.r.o.	List of referenced standards updated, requirements of ETSI TS 119 411-6 taken into account.
1.003	16 August 2025	Ing. Ctirad Fischer, Managing Director of První certifikační autorita, s.r.o.	Certificate profile refinement. Updates related to S/MIME BR.

1 INTRODUCTION

První certifikační autorita, s.r.o., (also as I.CA SK) is the subsidiary company of První certifikační autorita, a.s., (also as I.CA) and I.CA is one hundred percent owner of I.CA SK. I.CA SK is the qualified service provider and I.CA on the basis of contractual relationship ensures:

- Complete technical infrastructure necessary to ensure providing qualified trust services by I.CA SK;
- Creation and management of documentation related to trust services provided by I.CA SK;
- Management of lists related to trust services provided by I.CA SK (list of issued certificates, CRLs),
- Operation of the on-line revocation/status checking service (OCSP) of the certificates issued by I.CA SK;
- Permanent cooperation in the provision of trust service;
- Methodological assistance.

I.CA SK operation is governed by internal and external documents (policies, directives) of I.CA unless otherwise stated.

This document determines the principles applied by I.CA SK, the qualified provider of trust services, in providing qualified trust service of issuing qualified certificates for remote signing according to the legislation of the Slovak Republic (also as the Service or the Certificate). There are two types of Certificates analogous with:

- Qualified certificates for electronic signatures according to the legislation of the Slovak Republic – also as certificates for electronic signatures; and
- Qualified mandate certificates according to the legislation of the Slovak Republic – also as mandate certificates; more detailed information concerning specific mandate is contained in the document “Podmínky pro přidělení mandátu Mandanta” / “Conditions for granting the mandate of the Mandator” (also as Conditions).

The RSA 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 Slovak Republic No. 272/2016 Coll., on Trust Services for Electronic Transactions in the Internal Market and on granting Amendment and Supplementing of certain Acts (Trust Services Act);
- Legislation concerning personal data protection in compliance with Regulation (EU) no 2016/679 of the European Parliament and of the Council on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation).

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

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

1.1 Overview

The document **Certificate Policy for Issuing Qualified Certificates for Remote Signing According to the Legislation of the Slovak Republic (RSA Algorithm)** prepared by I.CA on behalf of I.CA SK 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 Slovak 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 detail on the fulfillment of fields and extensions of Certificates issued under this CP and on Certificate administration may be included in the relevant certification practice statement (also as the CPS) and also in the document I.CA RemoteSign Policy (remote electronic signing) also as RSign_Policy.

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 Remote Signing According to the Legislation of the Slovak Republic (RSA Algorithm), version 1.003

1.2.1 Certificates for electronic signatures

Policy OID:	1.3.6.1.4.1.23624.10.1.193.1.0

1.2.2 Mandate certificates

Policy OID:	1.3.6.1.4.1.23624.10.1.194.1.0

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 on behalf of I.CA SK, 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

I.CA SK services are provided through registration authorities (stationary or mobile) – in the terminology of remote signing the term contact points is used – which can be:

- in case of **certificates for electronic signatures** either public (providing services for the general public) or client (providing services for their customers). These registration authorities;
- in case of **mandate certificates** designated.

These registration authorities:

- Accept applications for the services listed in this CP (Certificate issuance applications, in particular), arrange the handover of Certificates and certificate revocation lists, provide required information, handle complaints, etc.;
- Are authorized, for urgent operational or technical reasons, to suspend, in whole or in part, the performance of their activities;
- Are authorized to conclude Service contracts on behalf of I.CA SK;
- Are authorized to charge for the I.CA SK services provided through RA unless otherwise agreed in a contract;
- Contractual registration authorities perform on behalf of I.CA SK the same function as the registration authorities owned by I.CA SK on the basis of contractual relationship.

1.3.3 Subscribers

Subscriber of a Certificate may be 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 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 may only be used in the processes of verification of an electronic signature created within the framework of the remote electronic signature creation service, in accordance with the legal regulation for trust services.

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 is administered by I.CA SK, corresponding CPS is administered by I.CA.

1.5.2 Contact person

The contact person in respect of this CP and its CPS is the managing director of I.CA SK. 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 I.CA and managing director of I.CA SK are jointly responsible for making decisions about compliance of the procedures of I.CA or I.CA SK as set out in CPS with this CP.

1.5.4 CPS approval procedures

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

1.6 Definitions and acronyms

Table 2 – Definitions

Term	Explanation
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 document	digitally encoded document, stored on physical medium, transferred or processed by technical means, in electronic, magnetic or optical form
electronic seal	advanced electronic seal or qualified electronic seal under trust services legislation
electronic signature	qualified electronic signature under trust services legislation
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
mandator	person or public authority on behalf of who or which the mandatary acts
mandatary	natural person authorized by law to act on behalf of any other person or public authority, or person performing the activity or function according to a special regulation
mandate	confirmation of the right to act for or on behalf of any other person or public authority
mandate certificate	qualified certificate for electronic signature issued to the person who is authorized by law or in accordance with law to act for or on behalf of any other person or public authority, or who or which performs the activity or function according to a special regulation
OCSP responder	server using the OCSP protocol to provide data on public key certificate status
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	certificate defined by trust services legislation
qualified signature / seal creation device	device meeting the requirements of eIDAS, annex II, intended for electronic signature / seal creation
relying party	party relying on a certificate in its operations
root CA	certification authority which issues certificates to subordinate certification authorities
secure cryptographic device	device on which the private key is stored
Softcard	software emulation of smartcard for access to private key stored in HSM
subordinate CA	CA issuing certificates to end users
supervisory body	the body supervising qualified trust services providers
trust service / qualified trust service	trust service / qualified trust service defined by eIDAS
trust services legislation	current legislation on trust services
TWINS/DUAL	commercial product of I.CA or I.CA SK consisting of: • qualified certificate for electronic signature; • non-qualified certificate
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
CA	certification authority
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)
eIDAS	REGULATION (EU) no 910/2014 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 23 July 2014 on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC, as amended
EN	European Standard, a type of ETSI standard
ESI	Electronic Signatures and Infrastructures
ETSI	European Telecommunications Standards Institute, a European standardization institute for information and communication technologies
EU	European Union
FAS	Fire Alarm System
FIPS	Federal Information Processing Standard, standards for information technologies for U.S. non-military state organizations
GDPR	Global 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.
I.CA SK	První certifikační autorita, s.r.o.
IAS	Intrusion Alarm System
IEC	International Electrotechnical Commission, the global organization publishing standards for electrical and electronic engineering, communication technologies and related industries
IPS	Intrusion Prevention System
ISMS	Information Security Management System
ISO	International Organization for Standardization, an international organization of national standardization organizations; designation of standards
IT	Information Technology

ITU	International Telecommunication Union
ITU-T	Telecommunication Standardization Sector of ITU
MPSV	Ministry of Labor and Social Affairs of the Czech Republic
MTRP	Microsoft Trusted Root Program
NBÚ SR	National Security Authority of the Slovak Republic
NTR	National Trade Register
OCSP	Online Certificate Status Protocol, the protocol to identify public key certificate status
OID	Object Identifier
OSVČ	self-employed person
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
PTC	Publicly-Trusted Certificate
PUB	Publication, FIPS standard designation
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.
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
STN	Slovak Technical Norm
TS	Technical Specification, type of ETSI standard
TSA	Time-Stamping Authority
TSS	Time-Stamp Server
TSU	Time-Stamp Unit
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

I.CA SK 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 public information about I.CA SK and references where to find other pieces of information are as follows:

- Registered office:

  První certifikační autorita, s.r.o.

  Galvaniho 19045/19

  821 04 Bratislava – mestská časť Ružinov

  Slovenská republika
- Website: http://www.ica.cz;
- Registered offices of the registration authorities.

Electronic address for contact between general public and I.CA SK is info@ica.cz.

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 SK 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 or I.CA SK on its web Information

Address and in Hospodářské noviny or Mladá fronta Dnes and Hospodárske noviny or Sme, daily newspapers with national distribution.

The Certification authority that issues the Certificates meets the requirements of the current "CA/Browser Forum - Baseline Requirements for the Issuance and Management of Publicly-Trusted S/MIME Certificates", which is published on http://www.cabforum.org. If this CP and the S/MIME BR are in conflict, the S/MIME BR prevail.

2.3 Time or frequency of publication

I.CA SK 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 SK free of charge without any restrictions.

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

3 IDENTIFICATION AND AUTHENTICATION

3.1 Naming

3.1.1 Types of names

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

3.1.2 Need for names to be meaningful

For a Certificate to be issued, all names which can be validated given in the field subject must carry a meaning. See chapter 7 for the attributes supported for this field.

3.1.3 Anonymity or pseudonymity of subscribers

The Certificates issued under this CP do not support neither anonymity nor pseudonymity.

3.1.4 Rules for interpreting various name forms

The data specified in a Certificate application (format PKCS#10) 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

Certificate issued under this CP do not 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

Because the private keys are generated and stored in QSCD under the control of I.CA, its possession is not proved.

3.2.2 Authentication of organization identity

Procedure is described in RSign_Policy, chapter Authentication of organization identity.

3.2.3 Authentication of individual identity

Procedure is described in RSign_Policy, chapter Authentication of individual identity.

3.2.4 Non-verified subscriber information

All information provided in the Certificate is duly verified.

3.2.5 Validation of authority

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

Private keys are generated and stored in QSCD under the control of I.CA, corresponding attribute is inserted into all Certificates.

In case of **mandate certificates** mandatary proves the right to act for mandator or to act on behalf of him, to act as public authority, to operate on the basis of special legislation or to act on the basis of special legislation in accordance with requirements for granting this right stated in list of permissions kept by NBÚ SR.

3.2.6 Criteria for interoperation

Any collaboration between I.CA SK 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

Procedure is described in RSign_Policy, chapter Validation of e-mail address.

3.3 Identification and authentication for re-key requests

3.3.1 Identification and authentication for routine re-key

Identification and authentication for routine re-key (subsequent Certificate issuance) are not carried out, because re-keying is done automatically and electronically some time before the original Certificate expiration (user of the Service i.e., Certificate subscriber, is asked whether he wants to be issued subsequent Certificate). The Certificate subscriber is fully responsible for reporting any changes, this obligation is among others included in the remote signing contract.

3.3.2 Identification and authentication for re-key after revocation

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

3.4 Identification and authentication for revocation request

The Certificate is always revoked when the remote signing contract is terminated (the Client does not answer yes to the question whether he wants to be issued subsequent Certificate). revocation is possible in the ways described in RSign_Policy, in the chapter Certificate revocation and suspension.

Revocation may be also asked through authorized persons by subjects allowed to do it by applicable legislation.

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

4 CERTIFICATE LIFE CYCLE OPERATIONAL REQUIREMENTS

4.1 Certificate application

4.1.1 Who can submit a certificate application

Certificate application under this CP is submitted by natural person concluding the remote signing contract.

4.1.2 Enrollment process and responsibilities

Procedure is described in RSign_Policy, chapter Enrollment process and responsibilities.

4.2 Certificate application processing

4.2.1 Performing identification and authentication functions

When **the primary Certificate** is issued the identification and authentication procedure are done according to RSign_Policy, chapters Authentication of organization identity and Authentication of individual identity. When the **subsequent Certificate** is issued then chapter 3.3.1 applies.

4.2.2 Approval or rejection of certificate applications

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

- Check of the data in the documents submitted;
- Visual check as to the formal correctness of data.

Competence check and formal data correctness check are also carried out using the RA system software.

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

4.2.3 Time to process certificate applications

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

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

4.3 Certificate Issuance

4.3.1 CA actions during certificate issuance

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

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

The competence check and the formal data correctness check are carried out by both the software on CA operators' work stations and that on the CA system core. If any of these checks gives a fail result, the Certificate issuance procedure is terminated.

Subsequent Certificate issuance procedure is automatic without Operators' intervention and is based on Client's answer yes to the question whether he wants to be issued subsequent Certificate.

4.3.2 Notification to subscriber by the CA of issuance of certificate

During the **primary Certificate** issuance process, the Certificate subscriber receives information from the RA employee or is informed when the service of remote signing is activated. Then the Certificate is published and further handling with the Certificate may be specified in the contract between specific third party and I.CA SK.

Issuing subsequent Certificates is done automatically after Client's answer yes to the question whether he wants to be issued subsequent Certificate. Then the Certificate is published and further handling with the Certificate may be specified in the contract with a specific third party. The Certificate subscriber is fully responsible for correctness and accuracy of data in the Certificate.

4.4 Certificate acceptance

4.4.1 Conduct constituting certificate acceptance

If the Certificate issuance requirements are met, the Certificate is published. The Certificate subscriber accepts the Certificate wen the remote signing service is activated on his mobile device.

4.4.2 Publication of the certificate by the CA

I.CA SK publishes every Certificate it issues.

4.4.3 Notification of certificate issuance by the CA to other entities

Certificate issuance can be, depending on the contract between third party and I.CA SK, notified to this third party. Other subjects are not notified.

4.5 Key pair and certificate usage

4.5.1 Subscriber private key and certificate usage

Clients' obligations are described in RSign_Policy in chapter Enrollment process and responsibilities.

4.5.2 Relying party public key and certificate usage

Relying parties must, among other things:

- Obtain from a secure source (e.g., www.ica.cz, RA workplace or relevant trusted list) certification authority certificates linked with the Certificate issued under this CP, and verify those certificates' fingerprint values and validity;
- Carry out any operation necessary for them to verify that the Certificate is valid;
- Observe all and any provisions of this CP 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 still valid Certificate, or for revoked Certificate, or for expired Certificate without changing the public key or any other information in the Certificate.

Certificate renewal is not provided by I.CA SK.

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 identical content of the attributes under the subject field or the subjectAlternativeName extension of the Certificate the public key of which is requested to be re-keyed.

Issuing subsequent Certificates is done automatically, details are described in RSign_Policy in chapter Extending the validity of the Contract.

4.7.1 Circumstance for certificate re-key

Process is described in RSign_Policy in chapter Extending the validity of the Contract.

4.7.2 Who may request certification of a new public key

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

4.7.3 Processing certificate re-keying requests

Public key re-keying request is processed immediately after positive answer to the question whether the subsequent Certificate should be issued.

4.7.4 Notification of new certificate issuance to subscriber

See 4.3.2.

4.7.5 Conduct constituting acceptance of a re-keyed certificate

See 4.4.1.

4.7.6 Publication of the re-keyed certificate by the CA

See 4.4.2.

4.7.7 Notification of certificate issuance by the CA to other entities

See 4.4.3.

4.8 Certificate modification

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

Certificate modification is not provided by I.CA SK.

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 an inseparable part of remote signing service termination and is described in RSign_Policy, chapter Certificate revocation and suspension.

I.CA SK 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

See 4.9.

4.9.2 Who can request revocation

See 4.9.

4.9.3 Procedure for revocation request

See 4.9.

4.9.4 Revocation request grace period

See 4.9 and in addition to that upon receipt of a Certificate Problem Report, I.CA SK confirms its receipt, confirms the facts and circumstances of the reported problem, and provides a preliminary report to both the Certificate subscriber and the person who reported the problem.

I.CA SK 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 is necessary, then I.CA SK determines the date of revocation considering following criteria:

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

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

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

- The nature of the problem;

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

4.9.6 Revocation checking requirement for relying parties

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

4.9.7 CRL issuance frequency

The certificate revocation list is released immediately after a Certificate revocation request is handled affirmatively. If a Certificate is not revoked, the new CRL is usually released within 8 but no more than 24 hours after the previous CRL is released.

4.9.8 Maximum latency for CRLs

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

4.9.9 On-line revocation/status checking availability

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

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

4.9.10 On-line revocation checking requirements

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

4.9.10.1 Status of Certificates

The validity of OCSP response is set to 24 hours.

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

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

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

4.9.10.2 CA issuing Certificates certificate status

I.CA updates OCSP responses:

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

4.9.11 Other forms of revocation advertisements available

Not applicable for this document.

4.9.12 Special requirements re key compromise

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

4.9.13 Circumstances for suspension

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

4.9.14 Who can request suspension

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

4.9.15 Procedure for suspension request

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

4.9.16 Limits on suspension period

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

4.10 Certificate status services

4.10.1 Operational characteristics

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

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

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

4.10.2 Service availability

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

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

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

Termination of the Service is tied to revocation or expiration of the Certificate. If:

- Client does not approve issuing subsequent Certificate and the Certificate expires; or
- Client revokes the Certificate and the certificate is listed in CRL;

The Service contract is terminated.

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 of I.CA - 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 of I.CA. These documents take account of the results of periodic risk analyses.

5.1 Physical controls

5.1.1 Site location and construction

The I.CA operating site buildings are situated in geographically different locations, which are also different from the site of I.CA SK headquarters, the site of I.CA 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 of I.CA. Buildings are protected with intrusion alarm system (IAS), alarm receiving centre (ARC) and, as may be the case, a special system to monitor movement of persons and vehicles.

5.1.3 Power and air conditioning

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

5.1.4 Water exposures

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

5.1.5 Fire prevention and protection

The buildings of the operating sites and the information 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 of I.CA.

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 of I.CA.

I.CA employees 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 cryptographic module in which private keys corresponding with issued Certificates are stored.

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 of I.CA.

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

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

5.3.5 Job rotation frequency and sequence

I.CA or I.CA SK employees are encouraged to acquire knowledge necessary for working in other roles at I.CA or I.CA SK, 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 of I.CA 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 or I.CA SK provides some certificate issuance activities on a contractual basis, but is fully responsible for the activities of these independent contractors involved in the issuance of a Certificate. Further pays:

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

5.3.8 Documentation supplied to personnel

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

5.4 Audit logging procedures

5.4.1 Types of events recorded

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

The certification authorities' key pair generating is a special case of event logging. All this process complies with trust services legislation and the relevant technical and other standards. Generating is carried out according to a pre-determined scenario in a physically secure environment and under the control of more I.CA employees in trusted roles.

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

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

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

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

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

5.4.2 Frequency of processing log

Audit records are checked and assessed at the intervals defined in internal documentation of I.CA, 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 of I.CA.

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

I.CA carries out periodic vulnerability assessments as part of risk assessments. Vulnerability monitoring of the hardware and software related to the trustworthy systems designated to support trust services is described in internal documentation.

5.5 Records archival

The archiving of records, i.e., information and documentation, is at I.CA regulated in internal documentation of I.CA.

5.5.1 Types of records archived

I.CA or I.CA SK archives the following electronic or printed records pertaining to the trust services provided, including those from delegated third parties involved in the certificate lifecycle, such as:

- Records / protocols on the course of certification authorities key pair generating;
- Life cycle records for the certificates (especially the documents relating to validation of certificate issuance applications and certificate revocation requests);
- Audit records according to chapter 5.4.1;
- Information handling records, such as takeover, handover, saving, check, conversion from printed to electronic, etc.;
- Operational and security documentation.

5.5.2 Retention period for archive

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

The record archiving procedures are regulated in internal documentation of I.CA.

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 of I.CA.

5.5.4 Archive backup procedures

The record backup procedures are regulated in internal documentation of I.CA.

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 or by managing director of I.CA SK.

Internal documentation of I.CA 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 or I.CA SK employees if they need to have such an access for their job;
- Authorized supervising and inspection entities and law enforcement authorities if required by legislation.

A written record is made of any such permitted access.

5.6 Key changeover

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

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

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

5.7 Compromise and disaster recovery

5.7.1 Incident and compromise handling procedures

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

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

See. 5.7.1.

5.7.3 Entity private key compromise procedures

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

- Stops using the private key;
- Revokes immediately and permanently the pertinent certificate and destroys the corresponding private key;
- Revokes all valid certificates issued by pertinent certification authority;
- Immediately informs about this fact, including the reason of revocation, in accordance with Chapter 2.2; the list of revoked certificates is also used to make this information available;
- Notifies the supervisory body of that the pertinent certificate has been revoked and why it has been revoked.

A similar procedure will be applied in the event that cryptanalytic methods develop to such an extent (e.g. changes in cryptographic algorithms, key lengths, etc.) that the security of trust services could be immediately threatened.

5.7.4 Business continuity capabilities after a disaster

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

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 SK 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 or I.CA SK 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 or managing director of I.CA SK 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 of I.CA.

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

Key pairs related to Certificates are generated on QSCD devices which are placed in designated secured areas of I.CA operating sites.

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 related to Certificates – private keys are stored on cryptographic modules 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 relevant for public keys of end users of the Service, the public key was 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 may be published after issuance, further handling of the Certificate may depend on the contract between the third party and I.CA SK.

Other public keys are delivered to the 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 its are guaranteed:

- Handover from RA;
- From the trusted list of the Slovak Republic;
- Via web information addresses of I.CA or I.CA SK, relevant supervisory body or its journal;

- Every subscriber gets relevant certification authorities' certificates together with his primary certificate.

6.1.5 Key sizes

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

6.1.6 Public key parameters generation and quality checking

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

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

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

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

6.2 Private key protection and cryptographic module engineering controls

6.2.1 Cryptographic module standards and controls

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

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

End users use the device meeting the QSCD requirements.

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

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

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

When private keys related to Certificates of end users expire, they are not archived, but the access data allowing decryption and usage of these private keys are deleted.

6.2.6 Private key transfer into or from a cryptographic module

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

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

Private keys related to Certificates of end users are generated (as non-exportable) in 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.

Key pairs of end users are stored on QSCD device included in EU list.

[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.

6.2.8 Method of activating private key

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

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

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

Activation private keys related to Certificates of end users is 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 private keys related to Certificates of end users is done by revocation of specific Certificate or by issuing subsequent Certificate to the Certificate which private key should be deactivated.

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 or managing director of I.CA SK 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 or I.CA SK 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, that is ETSI and CEN standards and are used in accordance with their certification.

Smartcard 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 included 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. It complies with S/MIME BR requirements.

6.4 Activation data

6.4.1 Activation data generation and installation

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

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

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

6.4.2 Activation data protection

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

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

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

6.4.3 Other aspects of activation data

Not applicable for this document.

6.5 Computer security controls

6.5.1 Specific computer security technical requirements

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

6.5.2 Computer security rating

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

- CEN/TS 419261 Security Requirements for Trustworthy Systems Managing Certificates and Time-stamps;
- ČSN ETSI EN 319 401 Electronic Signatures and Infrastructures (ESI) – General Policy Requirements for Trust Service Providers;
- ETSI EN 319 401 Electronic Signatures and Infrastructures (ESI); General Policy Requirements for Trust Service Providers;
- ČSN ETSI EN 319 403-1 Electronic Signatures and Infrastructures (ESI); Trust Service Provider Conformity Assessment; Part 1: Requirements for conformity assessment bodies assessing Trust Service Providers;
- ETSI EN 319 403-1 Electronic Signatures and Infrastructures (ESI); Trust Service Provider Conformity Assessment; Part 1: Requirements for conformity assessment bodies assessing Trust Service Providers;
- ČSN ETSI EN 319 411-1 Electronic Signatures and Infrastructures (ESI) – Policy and Security Requirements for Trust Service Providers Issuing Certificates – Part 1: General Requirements;
- ETSI EN 319 411-1 Electronic Signatures and Infrastructures (ESI); Policy and Security Requirements for Trust Service Providers Issuing Certificates; Part 1: General Requirements;
- ČSN ETSI EN 319 411-2 Electronic Signatures and Infrastructures (ESI) – Policy and Security Requirements for Trust Service Providers Issuing Certificates – Part 2: Requirements for Trust Service Providers Issuing EU Qualified Certificates;
- ETSI EN 319 411-2 Electronic Signatures and Infrastructures (ESI); Policy and Security Requirements for Trust Service Providers Issuing Certificates; Part 2: Requirements for Trust Service Providers Issuing EU Qualified Certificates;
- ČSN ETSI EN 319 412-1 Electronic Signatures and Infrastructures (ESI); Certificate Profiles; Part 1: Overview and Common Data Structures;
- ETSI EN 319 412-1 Electronic Signatures and Infrastructures (ESI); Certificate Profiles; Part 1: Overview and Common Data Structures;
- ČSN ETSI EN 319 412-2 Electronic Signatures and Infrastructures (ESI); Certificate Profiles; Part 2: Certificate Profile for Certificates Issued to Natural Persons;
- ETSI EN 319 412-2 Electronic Signatures and Infrastructures (ESI); Certificate Profiles; Part 2: Certificate Profile for Certificates Issued to Natural Persons;
- ČSN ETSI EN 319 412-3 Electronic Signatures and Infrastructures (ESI); Certificate Profiles; Part 3: Certificate Profile for Certificates Issued to Legal Persons;
- ETSI EN 319 412-3 Electronic Signatures and Infrastructures (ESI); Certificate Profiles; Part 3: Certificate Profile for Certificates Issued to Legal Persons;
- ČSN ETSI EN 319 412-4 Elektronické podpisy a infrastruktury (ESI) - Profily certifikátu – Část 4: Profil certifikátu pro certifikáty webových stránek;
- ETSI EN 319 412-4 Electronic Signatures and Infrastructures (ESI); Certificate Profiles; Part 4: Certificate profile for web site certificates;

- ČSN ETSI EN 319 412-5 Electronic Signatures and Infrastructures (ESI); Certificate Profiles; Part 5: QC Statements;
- ETSI EN 319 412-5 Electronic Signatures and Infrastructures (ESI); Certificate Profiles; Part 5: QCStatements;
- ČSN EN 419 221-5 Protection profiles for TSP Cryptographic modules - Part 5 Cryptographic Module for Trust Services;
- EN 419 221-5 Protection profiles for TSP Cryptographic modules - Part 5 Cryptographic Module for Trust Services;
- 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;
- ETSI TS 119 411-6 Electronic Signatures and Infrastructures (ESI); Policy and security requirements for Trust Service Providers issuing certificates; Part 6: Requirements for Trust Service Providers issuing publicly trusted S/MIME certificates;
- FIPS PUB 140-2 Requirements for Cryptographic Modules;
- ČSN EN ISO/IEC 15408-1 Informační bezpečnost, kybernetická bezpečnost a ochrana soukromí - Kritéria pro hodnocení bezpečnosti IT - Část 1: Úvod a obecný model;
- ISO/IEC 15408-1:2022 Information security, cybersecurity and privacy protection - Evaluation criteria for IT security - Part 1: Introduction and general model;
- ČSN EN ISO/IEC 15408-2 Informační bezpečnost, kybernetická bezpečnost a ochrana soukromí - Kritéria pro hodnocení bezpečnosti IT - Část 2: Bezpečnostní funkční komponenty;
- ISO/IEC 15408-2:2022 Information security, cybersecurity and privacy protection - Evaluation criteria for IT security - Part 2: Security functional components;
- ČSN EN ISO/IEC 15408-3 Informační bezpečnost, kybernetická bezpečnost a ochrana soukromí - Kritéria pro hodnocení bezpečnosti IT - Část 3: Komponenty bezpečnostních záruk;
- ISO/IEC 15408-3:2022 Information security, cybersecurity and privacy protection - Evaluation criteria for IT security - Part 3: Security assurance components;
- ETSI TS 119 312 Electronic Signatures and Infrastructures (ESI); Cryptographic Suites;
- 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, resp. STN 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 of I.CA.

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 or STN 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 or STN 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 or STN 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 of I.CA. 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 – Basic fields of Certificates for electronic signatures

Field	Content
version	v3 (0x2)
serialNumber	unique serial number of the Certificate
signatureAlgorithm	according to the application type (depending on signature algorithm of the certificate) one of following options: • ***sha256withRSAEncryption*** (with parameters = NULL, pkcs#1 1v5) at minimum; or • ***rsassaPss*** (pkcs#1 2v1) with parameters: – hashAlgorithm: sha256 at minimum; – maskGenAlgorithm: mgf1 with the same hash function as in hashAlgorithm; – saltLength: depending on used hash function; – trailerField: 0xBC (default)
issuer	issuer of the Certificate
validity	
notBefore	start of the Certificate's validity (UTC)
notAfter	notBefore + at maximum 365 days, or 366 days in case of leap year (UTC)
subject	see Table 5
subjectPublicKeyInfo*	
Algorithm	rsaEncryption
subjectPublicKey	2048 bits at minimum
extensions	see Table 8
signature	advanced electronic seal of Certificate's issuer

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

Table 5 – Subject filed attributes of Certificates for electronic signatures

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

[3] I.CA SK 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).

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: • IDCss-nnnnnnnn; • PASss-nnnnnnnn; • PNO*ss-yyyyyyyyyy* (the Slovak Republic citizens only); where: • *ss* is the country code (ISO 3166) of document's issuer; • *nnnnnnn* is the document number; • *yyyyyyyyyy* is the birth certification number
serialNumber (3)	optional if serialNumber (2) contains birth certification number, one of following options: • IDCss-nnnnnnnn; • PASss-nnnnnnnn; where: • ss is the country code (does not have to be the same as countryName); • nnnnnnn is the document number
commonName*	mandatory; single occurrence; must contain givenName and surName
initials	optional; single occurrence
organizationName	natural person not doing business: must not be specified employee of the Organization, natural person doing business (OSVČ): mandatory, single occurrence

organizationIdentifier	natural person not doing business: must not be specified employee of the Organization, natural person doing business (OSVČ): mandatory in case of S/MIME BR type certificate, single occurrence: • NTR*ss-id*, (**N**ational **T**rade **R**egister, i.e., business/company identification number); where: • *ss* is the country code (ISO 3166) of the state where the employer of OSVČ is registered (does not have to be same as countryName); • *id* is the organization's identification number in the relevant register
organizationalUnitName	in case of S/MIME BR type certificate: • natural person not doing business: must not be specified; • optional, single occurrence in other cases: optional; multiple occurrences permitted
title	optional; multiple occurrences permitted
stateOrProvinceName**	optional; single occurrence
localityName**	optional; single occurrence
streetAddress**	optional; single occurrence in case of S/MIME BR type certificate: only if attributes localityName or stateOrProvinceName are given
postalCode**	optional; single occurrence

* The name under which the Certificate subscriber (private key holder) normally appears, the attribute may also contain verified degrees of the Certificate's subscriber.

** The attributes countryName, stateOrProvinceName, localityName, streetAddress and postalCode relate to data verified during initial identity authentication (see 3.2.3).

Table 6 – Basic fields of mandate Certificates

Field	Content
version	v3 (0x2)
serialNumber	unique serial number of the Certificate
signatureAlgorithm	according to the application type (depending on signature algorithm of the certificate) one of following options: • sha256withRSAEncryption (with parameters = NULL, pkcs#1 1v5) at minimum; or • ***rsassaPss*** (pkcs#1 2v1) with parameters: – hashAlgorithm: sha256 at minimum;

	– maskGenAlgorithm: mgf1 with the same hash function as in hashAlgorithm; – saltLength: depending on used hash function; – trailerField: 0xBC (default)
issuer	issuer of the Certificate
validity	
notBefore	start of the Certificate's validity (UTC)
notAfter	notBefore + at maximum 365 days, or 366 days in case of leap year (UTC)
subject	see Table 7
subjectPublicKeyInfo	
algorithm	rsaEncryption
subjectPublicKey	2048 bits at minimum
extensions	see Table 9
signature	advanced electronic seal of Certificate's issuer

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

Table 7 – Subject field attributes of mandate Certificates

All attributes[4] of the subject field are taken over from the Certificate application except the attributes created by the Authority.

	Subject field attributes	**Comments**
Mandatary	commonName	mandatory, consisting of givenName and surName attributes appended with text OPRÁVNENIE and with number of the authorization, i.e.: • givenName surName OPRÁVNENIE *xxxx* where *xxxx* is the number of the specific authorization
	givenName	mandatory
	surName	mandatory
	title	optional
	serialNumber (1)	unique identification of the Certificate's subscriber in the Authority's system (ICA - xxxxxxxx)

[4] I.CA SK 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).

	serialNumber (2)	mandatory, one of options: • IDCss-nnnnnnnn; • PASss-nnnnnnnn; • PNOss-yyyyyyyyyy (the Slovak Republic citizens only); • IDCss-DDD-*nnnnnnnn;* where: • ss is country code (ISO 3166); • nnnnnnnn is the document number; • yyyyyyyyyy is birth certification number; • DDD is specification of identification card type
	serialNumber (3)	optional and if serialNumber (2) attribute contains birth certification number one of following options: • IDCss-nnnnnnnn, • PASss-nnnnnnnn, where: • ss is country code (does not have to be identical to countryName attribute); • nnnnnnn is the document number
Employer* **	serialNumber (4)	mandatory, identification data of mandatary's employer (or mandatary operates or acts for this organization according to special regulation): • NTRss-*id*, (**N**ational **T**rade **R**egister, i.e., IČ), where: • ss is country code (ISO 3166); • id is identification number of the organization in the specific register
	organizationName	natural person not doing business: must not be specified; employee, natural person doing business (OSVČ): mandatory, single occurrence Note: mandatory's employer (or mandatory operates or acts for this organization according to special regulation)

		if mandatary provides his services as natural person his first name and surname (as entered in register) is entered
	organizationIdentifier	natural person not doing business: must not be specified; employee, natural person doing business (OSVČ): mandatory: identification data of mandatory's employer (or mandatory operates or acts for this organization according to special regulation): • NTRss-*id*, (**N**ational **T**rade **R**egister, i.e., IČ), where: • ss is country code (ISO 3166), • id is identification number of the organization in the specific register
	organizationalUnitName	natural person not doing business: must not be specified; employee, natural person doing business (OSVČ): optional, name of partial organizational unit
	countryName*	mandatory, country code (ISO 3166), single occurrence
	stateOrProvinceName*	optional, single occurrence
	localityName*	optional; single occurrence
	streetAddress*	optional; single occurrence in case of S/MIME BR type certificate: only if attributes localityName or stateOrProvinceName are given
	postalCode*	optional; single occurrence
Mandator**		specified if the directoryName attribute of the subjectAlternativeName extension is not specified (see tab. 6)
	givenName	natural person: mandatory others: must not be specified
	surName	natural person: mandatory others: must not be specified
	serialNumber (5)	natural person: mandatory, one of following options:

		• IDCss-nnnnnnnn; • PASss-nnnnnnnn; • PNOss-yyyyyyyyyy (the Slovak Republic citizens only); • IDCss-DDD-nnnnnnnn; where: • ss is country code (ISO 3166); • nnnnnnnn is the document number; • yyyyyyyyyy is birth certification number; • DDD is specification of identification card type; for subscribers other than natural persons the attribute must not be specified
	serialNumber (6)	optional and if serialNumber (5) attribute contains birth certification number one of following options: • IDCss-nnnnnnnn; • PASss-nnnnnnnn; • IDCss-DDD-nnnnnnnn; where: • ss is country code (ISO 3166); • nnnnnnnn is the document number; • DDD is specification of identification card type
	serialNumber (7)	mandatory in case of employee or legal person/public authority: • NTR*ss-id*, (**N**ational **T**rade **R**egister, i.e., IČ), where: • ss is country code (ISO 3166), • id is identification number of the organization in the specific register
	organizationName	natural person not doing business: must not be specified; natural person doing business, employee or legal person / public authority: mandatory: • MANDANT *mandator's employer*; eg., MANDANT Company Ltd.

	organizationIdentifier	natural person not doing business: must not be specified; employee or legal person / public authority: mandatory • NTRss-*id*, (**N**ational **T**rade **R**egister, i.e., IČ), where: • *ss* is country code (ISO 3166), • id is identification number of the organization in the specific register

* The attributes countryName, stateOrProvinceName, localityName, streetAddress and postalCode relate to data verified during initial identity authentication of natural person (see 3.2.3).

** Content of mandator relating attributes always starts with word MANDANT followed by one space, i.e., MANDAT Jan Poslušný.

*** The "Employer" section is optional within the "Mandatary" section.

7.1.1 Version number(s)

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

7.1.2 Certificate extensions

Table 8 – Certificate for electronic signatures extensions[5]

Extension	Content	Comments
certificatePolicies		non-critical
.policyInformation (1)		
policyIdentifier	see 1.2	I.CA policy OID
policyQualifiers		
cPSuri	http://www.ica.cz	
.policyInformation (2)		
policyIdentifier	1.3.158.36061701.0.0.0.1.2.2	OID of NBÚ SR policy
policyQualifiers		
userNotice	EN: This is a qualified certificate for electronic signature according to Regulation (EU) No 910/2014. SK:	issuer can change the text depending on the Slovak

[5] I.CA SK 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).

	Kvalifikovany certifikat pre elektronicky podpis v sulade s nariadenim (EU) č. 910/2014.	Republic legislation requirements
.policyInformation (3)		
policyIdentifier	OID (QCP-n-qscd): 0.4.0.194112.1.2	ETSI policy identifier (private key is generated and stored on QSCD)
.policyInformation (4)		in case of S/MIME BR type certificate (Multipurpose)
policyIdentifier	one of following options: • Sponsor-validated: 2.23.140.1.5.3.2; • Individual-validated: 2.23.140.1.5.4.2	
QCStatements		non-critical
	0.4.0.1862.1.1	Id-etsi-qcs-QcCompliance
	0.4.0.1862.1.4	Id-etsi-qcs-QcSSCD; specified if 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/2qcask*YY*_rsa.crl http://qcrldp2.ica.cz/2qcask*YY*_rsa.crl http://qcrldp3.ica.cz/2qcask*YY*_rsa.crl	non-critical
authorityInformationAccess		non-critical
id-ad-ocsp*	http://ocsp.ica.cz/2qcask*YY*_rsa	
id-ad-caIssuers*	http://q.ica.cz/2qcask*YY*_rsa.cer	
id-ad-caIssuers	directoryName.serialNumber **= TLISK-yyy**	optional

		nnn - number assigned by supervisory body
basicConstraints		non-critical
cA	False	
keyUsage	TWINS/DUAL: • digitalSignature, nonRepudiation other cases: depending on the content of Certificate application - one of following options: • digitalSignature, nonRepudiation; • digitalSignature, nonRepudiation and keyEncipherment	critical, mandatory DUAL – creates Authority; others - if this extension is missing in the application, the following will be added: • digitalSignature, nonRepudiation
extendedKeyUsage	depending on the content of Certificate application - one of following options: • id-kp-emailProtection; • id-kp-emailProtection, ms-DocumentSigning	non-critical, mandatory if EKU is not specified in the application, or if id-kp-emailProtection is not specified in the EKU, the following will be added: • id-kp-emailProtection
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		specified if the Mandator part is not specified in the subject field of the certificate (see table 5)
serialNumber	personal number or identifier of certificate subscriber - mandator	mandatory
organizationName	the name of the organization that assigns and registers the personal number of the mandator (i.e. without the MANDANT prefix)	mandatory
organizationIdentifier	the number of the organization that assigns and registers the personal number of the mandator (i.e. without the MANDANT prefix)	optional format NTRss-id - see description of the subject field attribute organizationIdentifier in part Mandator
nsComment	QSCD identification number	non-critical; may be inserted when generating and storing of the private key on QSCD was verified
I.CA_TWIN_ID: 1.3.6.1.4.1.23624.4.3	Certificate application number	non-critical
I.CA_CERT_INTERCONNECTION: 1.3.6.1.4.1.23624.4.7	if more certificate types are issued to a single entity (entity's connection to the certificates issued)	non-critical

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

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

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

Table 9 – Mandate Certificate extensions

Extension	Content	Comments
certificatePolicies		non-critical
.policyInformation (1)		
policyIdentifier	see 1.2	I.CA policy OID
policyQualifiers		
cPSuri	http://www.ica.cz	

.policyInformation (2)		
policyIdentifier	1.3.158.36061701.0.0.0.1.2.2	NBÚ SR policy OID
policyQualifiers		
userNotice	EN: This is a qualified certificate for electronic signature according to Regulation (EU) No 910/2014. SK: Kvalifikovany certifikat pre elektronicky podpis v sulade s nariadenim (EU) č. 910/2014.	issuer can change the text depending on the Slovak Republic legislation requirements
.policyInformation (3)		
policyIdentifier	1.3.158.36061701.1.1.*xxxx*	specific mandatary policy OID *xxxx* – specific authorization number
userNotice*	EN: Authorization *xxxx N*, SK: Opravnenie *xxxx N*	*xxxx* – specific authorization number *N* – specific name of authorization
.policyInformation (4)		
policyIdentifier	OID (QCP-n-qscd): 0.4.0.194112.1.2	ETSI policy OID (private key is generated and stored on QSCD)
.policyInformation (5)		in case of S/MIME BR type certificate (Multipurpose)
policyIdentifier	one of following options: • Sponsor-validated: 2.23.140.1.5.3.2; • Individual-validated: 2.23.140.1.5.4.2	
QCStatements		non-critical
	0.4.0.1862.1.1	Id-etsi-qcs-QcCompliance
	0.4.0.1862.1.4	Id-etsi-qcs-QcSSCD; specified if the private key is generated and stored on QSCD

	0.4.0.1862.1.5	id-etsi-qcs-QcPDS; link (URI, https) to disclosure statement (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/qcask*YY*_rsa.crl http://qcrldp2.ica.cz/qcask*YY*_rsa.crl http://qcrldp3.ica.cz/qcask*YY*_rsa.crl	non-critical
authorityInformationAccess		non-critical
id-ad-ocsp**	http://ocsp.ica.cz/qcask*YY*_rsa	
id-ad-caIssuers**	http://q.ica.cz/qcask*YY*_rsa.cer	
id-ad-caIssuers	directoryName.serialNumber **= TLISK-yyy**	optional yyy – number assigned by supervisory body
basicConstraints		non-critical
cA	False	
keyUsage	depending on the content of Certificate application - one of following options: • digitalSignature, nonRepudiation; • digitalSignature, nonRepudiation and keyEncipherment	critical, mandatory if this extension is missing in the application, the following will be added: • digitalSignature, nonRepudiation
extendedKeyUsage	depending on the content of Certificate application - one of following options: • id-kp-emailProtection; • id-kp-emailProtection and ms-DocumentSigning	non-critical, mandatory if EKU is not specified in the application, or if id-kp-emailProtection is not specified in the EKU, the following will be added: • id-kp-emailProtection
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
nsComment	QSCD identification number	non-critical; may be inserted when generating and storing of the private key on QSCD was verified
I.CA_CERT_INTERCONNECTION: 1.3.6.1.4.1.23624.4.7	if more certificate types are issued to a single entity (entity's connection to the certificates issued)	non-critical, optional

* English text is optional and is entered only if it is contained in register of authorizations.

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

I.CA SK inserts in the Certificates issued the following certificate policy object identifiers:

- OID of the I.CA SK certificate policy under which the Certificate is issued;
- OID of the NBÚ SR certificate policy;
- OID of the specific mandatory policy (in case of mandate Certificate);
- OID of the relevant certificate policy defined by ETSI EN 319 411-2 for a certificate issued to the natural person with regard to the storing of the private key and declaring that the Certificate is in compliance with eIDAS;
- OID of the relevant policy specified by S/MIME BR and MTRP in case of S/MIME BR type certificates.

7.1.7 Usage of Policy Constraints extension

Not applicable for Certificates issued to end users.

7.1.8 Policy qualifier syntax and semantics

See Certificate extensions in 7.1.2 above.

7.1.9 Processing semantics for the critical certificate policies extension

Not applicable for this document, extension not classified as critical.

7.2 CRL profile

Table 10 – CRL profile[6]

Field	Content
version	v2(0x1)
signatureAlgorithm	sha256withRSAEncryption at minimum
issuer	issuer of the CRL
thisUpdate	date and time when the CRL was released (UTC)
nextUpdate*	date and expected time when the next CRL will be released (UTC)
revokedCertificates	list of revoked certificates
userCertificate	revoked certificate's serial number
revocationDate	certificate revocation date and time
crlEntryExtensions	list attribute extensions – see Table 11
crlExtensions	CRL extensions – see Table 11

[6] I.CA SK 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).

signature	advanced electronic seal of CRL's issuer

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

7.2.1 Version number(s)

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

7.2.2 CRL and CRL entry extensions

Table 11 – CRL Extensions[7]

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

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

- keyCompromise (RFC 5280 CRLReason #1),
- affiliationChanged (RFC 5280 CRLReason #3),
- superseded (RFC 5280 CRLReason #4),
- cessationOfOperation (RFC 5280 CRLReason #5),
- privilegeWithdrawn (RFC 5280 CRLReason #9) – this code cannot be used directly by Certificate subscriber, it is determined by CA (no later than July 15, 2023).

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

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

[7] I.CA SK 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).

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 not 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 or I.CA SK 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 and managing director of I.CA SK, 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 or I.CA SK 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 of I.CA or the security manager of I.CA, or to the managing director of I.CA SK.

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

8.7 Self audits

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

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

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

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

8.8 Review of delegated parties

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

9 OTHER BUSINESS AND LEGAL MATTERS

9.1 Fees

9.1.1 Certificate issuance or renewal fees

The fees for Certificate issuance are specified in the contract with the specific third party (can be flat fee per specific period, paying for every successful signature creation etc.).

9.1.2 Certificate access fees

No fee is charged by I.CA or I.CA SK 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 or I.CA SK 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

I.CA represents that it holds a valid business risk insurance policy that covers financial damage.

I.CA 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

I.CA represents that it has available financial resources and other financial assurances sufficient for providing trust services, including the trust services provided by I.CA SK, 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 or I.CA SK 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 or I.CA SK;
- Any internal information and documentation;
- Any personal data.

9.3.2 Information not within the scope of confidential information

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

9.3.3 Responsibility to protect confidential information

I.CA or I.CA SK employee who comes in contact with confidential information may not disclose the same to a third party without consent of CEO of I.CA or managing director of I.CA SK.

9.4 Privacy of personal information

9.4.1 Privacy plan

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

9.4.2 Information treated as private

Any personal data subject to protection under relevant legislation is treated as private.

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

9.4.3 Information not deemed private

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

9.4.4 Responsibility to protect private information

CEO of I.CA or managing director of I.CA SK are responsible for the protection of personal data.

9.4.5 Notice and consent to use private information

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

9.4.7 Other Information disclosure circumstances

I.CA or I.CA SK provides access to personal data strictly as regulated in relevant legislation.

9.5 Intellectual property rights

This CP, all related documents, the website content and the procedures facilitating the operation of trustworthy systems providing trust services are copyrighted by I.CA or I.CA SK and are important know-how thereof.

9.6 Representations and warranties

9.6.1 CA Representations and warranties

I.CA SK warrants that:

- It will use the private keys of certification authorities 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 end users are stored in the way which guarantees their confidentiality and integrity; only the owner of the Certificate can access corresponding key;
- 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.

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

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

- The relying party did not violate any obligation arising from this CP.

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

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

The warranties 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;
- Ensuring that the Certificate may be revoked for reasons specified in trust services legislation and this CP;
- Possibility to revoke the Certificate for the reasons specified in the trust service legislation and in this CP.

9.6.2 RA representations and warranties

The designated RA:

- Assumes the obligation that the services which the RA provides are correct;
- Does not accept the Certificate application if the Certificate applicant refuses to provide necessary data or if the Certificate applicant is not authorized to submit the application;
- Is responsible for passing a hand-delivered Certificate revocation application to an Authority office in due time for the office to handle the application;
- Is responsible for handling objections and complaints.

9.6.3 Subscriber representations and warranties

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

9.6.4 Relying parties representations and warranties

Relying parties observe this CP.

9.6.5 Representations and warranties of other participants

Not applicable for this document.

9.7 Disclaimers of warranties

I.CA SK provides only the warranties as given in 9.6.

9.8 Limitations of liability

I.CA or I.CA SK is not responsible for any damage suffered by relying parties where the relying party breaches its obligations under trust services legislation and particular CP. I.CA or I.CA SK is also not responsible for any damage resulting from breach of its obligations as a result of force majeure.

9.9 Indemnities

Described in RSign_Policy, chapter Indemnities.

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

Jointly CEO of I.CA and managing director of I.CA SK are authorized to approve the termination of this CP.

9.10.3 Effect of termination and survival

The obligations of I.CA SK arising from CP survive the expiration thereof until the expiration of the last Certificate issued under this CP.

9.11 Individual notices and communications with participants

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

Communication with I.CA SK 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 of I.CA.

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

Described in RSign_Policy, chapter Disputes resolution provisions.

9.14 Governing law

The business of I.CA SK is governed by the legal order of the Slovak Republic.

9.15 Compliance with applicable law

The system of providing trust services is in compliance with the legislation EU, the Czech Republic, the Slovak 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

I.CA SK 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 I.CA SK company takes force and effect on the date mentioned above in Table 1.