První certifikační autorita, a.s.



I.CA RemoteSign Policy

(Remote Creation of Electronic Signatures)

I.CA RemoteSign Policy (Remote Creation of Electronic Signatures) is a public document, which is the property of První certifikační autorita, a.s., and has been prepared as integral part of comprehensive security documentation. No part of this document may be reproduced without the written consent of the copyright holder.

Version 1.10

Copyright © První certifikační autorita, a.s.

CONTENT

1 Introduction 8
1.1 Overview 9
1.2 Document name and identification 9
1.2.1 Signature creation policy 9
1.2.2 Supported signature formats and classes, their limitations 10
1.2.3 Passing the parameters of the signature 10
1.3 PKI Participants 10
1.3.1 Service provider 10
1.3.2 Contact points 10
1.3.3 Relying parties 11
1.3.4 Other participants 11
1.4 Service usage 12
1.4.1 Appropriate service uses 12
1.4.2 Prohibited service uses 12
1.5 Policy administration 12
1.5.1 Organization administering the document 12
1.5.2 Contact person 12
1.5.3 Person determining providing statement suitability for the policy 12
1.5.4 Providing statement approval procedures 12
1.6 Definitions and acronyms 12
2 Publication and repository responsibilities 15
2.1 Repositories 15
2.2 Publication of certification information 15
2.3 Time or frequency of publication 15
2.4 Access controls on repositories 15
3 Identification and authentication 16
3.1 Initial identity validation 16
3.1.1 Authentication of organization identity 16
3.1.2 Authentication of individual identity 16
3.1.3 Validation of e-mail address 24
3.2 Identity validation for service extending 25
3.3 Modification of data 25
4 Service life cycle requirements 26
4.1 Conclusion of the contract 26

4.2 Service activation 26
4.2.1 Enrollment process and responsibilities 26
4.2.2 Conduct constituting Certificate acceptance 27
4.3 Activation of the Service 27
4.4 Extending the validity of the Contract 27
4.5 Contract expiration 28
4.6 Certificate revocation and suspension 28
4.6.1 Circumstances for revocation 28
4.6.2 Who can request revocation 30
4.6.3 Submitting revocation request 31
4.6.4 Revocation request grace period 32
4.7 Blocking and unblocking of mobile or PC application 32
4.7.1 Blocking 32
4.7.2 Unblocking 33
4.8 Use of the Service 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 34
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 35
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 36
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 37
5.4 Audit logging procedures 37
5.4.1 Types of events recorded 37
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 38
5.4.6 Audit collection system (internal vs. external) 38
5.4.7 Notification to event-causing subject 38
5.4.8 Vulnerability assessments 38
5.5 Records archival 38
5.5.1 Types of stored records 38
5.5.2 Retention period for archive 39
5.5.3 Protection of archive 39
5.5.4 Archive backup procedures 39
5.5.5 Requirements for time-stamping of records 39
5.5.6 Archive collection system (internal or external) 39
5.5.7 Procedures to obtain and verify archive information 39
5.6 Compromise and disaster recovery 39
5.6.1 Incident and compromise handling procedures 39
5.6.2 Computing resources, software, and/or data are corrupted 40
5.6.3 Business continuity capabilities after a disaster 40
5.7 Service's provider termination 40
6 Technical security controls 41
6.1 Cryptography, private key and its protection 41
6.2 Computer security controls 41
6.2.1 Specific computer security technical requirements 41
6.2.2 Computer security rating 41
6.3 Life cycle technical controls 42
6.3.1 System development controls 42
6.3.2 Security management controls 43
6.3.3 Life cycle security controls 43
6.4 Network security controls 43
6.5 Protection against fraud and theft of data 43

7 Conformity assessments and other assessments 44
7.1 Frequency or circumstances of assessment 44
7.2 Identity/qualifications of assessor 44
7.3 Assessor's relationship to assessed entity 44
7.4 Topics covered by assessment 44
7.5 Actions taken as a result of deficiency 44
7.6 Communication of results 44
8 Other business and legal matters 46
8.1 Fees 46
8.1.1 Service fees 46
8.1.2 Fees for other services 46
8.1.3 Refund policy 46
8.2 Financial responsibility 46
8.2.1 Insurance coverage 46
8.2.2 Other assets 46
8.2.3 Insurance or warranty coverage for end-entities 46
8.3 Confidentiality of business information 46
8.3.1 Scope of confidential information 46
8.3.2 Information not within the scope of confidential information 47
8.3.3 Responsibility to protect confidential information 47
8.4 Privacy of personal information 47
8.4.1 Privacy plan 47
8.4.2 Information treated as private 47
8.4.3 Information not deemed private 47
8.4.4 Responsibility to protect private information 47
8.4.5 Notice and consent to use private information 47
8.4.6 Disclosure pursuant to judicial or administrative process 48
8.4.7 Other Information disclosure circumstances 48
8.5 Intellectual property rights 48
8.6 Representations and warranties 48
8.6.1 CA Representations and warranties 48
8.6.2 Contact points representations and warranties 48
8.6.3 Representations and warranties of other participants 48
8.7 Disclaimers of warranties 48
8.8 Limitations of liability 49
8.9 Indemnities 49

8.10 Term and termination 50
8.10.1 Term 50
8.10.2 Termination 50
8.10.3 Effect of termination and survival 50
8.11 Individual notices and communications with participants 50
8.12 Amendments 50
8.12.1 Amending procedure 50
8.12.2 Notification mechanism and period 50
8.12.3 Circumstances under which OID must be changed 50
8.13 Disputes resolution provisions 50
8.14 Governing law 51
8.15 Compliance with applicable law 51
8.16 Miscellaneous provisions 51
8.16.1 Entire agreement 51
8.16.2 Assignment 51
8.16.3 Severability 51
8.16.4 Enforcement (attorneys' fees and waiver of rights) 51
8.16.5 Force Majeure 51
8.17 Other provisions 51
9 Final Provisions 52

Table 1 – Document history

Version	Date of Release	Approved by	Comments
1.00	26 February 2020	CEO of První certifikační autorita, a.s.	First release.
1.01	27 August 2022	CEO of První certifikační autorita, a.s.	Classification of document marked, audit recommendation included, more accurate text. Possibility to use the certificates issued for the Slovak Republic included.
1.02	31 August 2022	CEO of První certifikační autorita, a.s.	Formal error correction.
1.03	2 December 2022	CEO of První certifikační autorita, a.s.	Possibility to use also the certificates issued by other trust services provider added.

1.04	23 November 2023	CEO of První certifikační autorita, a.s.	Two other ways to authorize individual identity added (other qualified certificate for qualified electronic signature validation of the same subscriber and remotely vis ZealiD).
1.05	26 August 2024	CEO of První certifikační autorita, a.s.	List of referenced standards updated, requirements of ETSI TS 119 411-6 taken into account.
1.06	22 November 2024	CEO of První certifikační autorita, a.s.	Two other ways to authorize individual identity remotely added (NKČR, NIA).
1.07	15 January 2025	CEO of První certifikační autorita, a.s.	Two other ways to authorize individual identity on contact point added (eDoklady and verification in ROB).
1.08	16 August 2025	CEO of První certifikační autorita, a.s.	Updates related to S/MIME BR.
1.09	25 August 2025	CEO of První certifikační autorita, a.s.	Formal errors correction.
1.10	12 September 2025	CEO of První certifikační autorita, a.s.	Error correction in chapter 1.2.

1 INTRODUCTION

This document determines the principles applied by První certifikační autorita, a.s. (also as the I.CA), a qualified provider of trust services, in providing trust service I.CA RemoteSign i.e., remote creation of electronic signatures (also as the Service). It also describes Service's end user (also as Client) actions relying to issuance and management of relevant qualified certificate.

The Service is primarily intended for electronic signing based on qualified certificates issued by I.CA, but can be also used for electronic signing based on qualified certificates issued by other trust services providers (currently the company První certifikační autorita, s.r.o., also I.CA SK).

Condition is the contractual relationship between I.CA and these trust services providers and also the fact, that the private key used for electronic signing was generated and is stored in secure cryptographic device or in QSCD, which are under sole control of I.CA.

In the following text these terms are used:

- Signing certificate in the meaning of qualified certificate for electronic signature issued under the legislation of the Czech Republic or under the legislation of the Slovak Republic;
- Mandate certificate in the meaning of qualified mandate certificate issued under the legislation of the Slovak Republic;
- The Certificate for all mentioned types of certificates.

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

- Regulation (EU) no 910/2014 of the European Parliament and of the Council on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC, as amended;
- Act of the Czech Republic No. 297/2016 Coll., on trust services for electronic transactions;
- 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);
- Act of the Czech National Council No. 358/1992 Coll., on Notaries and their Work Activities (Notarial Procedures);
- 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 of První certifikační autorita, a.s., creating remotely electronic signatures is provided to all Clients who need to create electronic signatures for subject sending them documents to be signed (also as third party). I.CA imposes no restrictions on potential end users, and the provision of the Service is non-discriminatory and the Service is also available to the disabled.

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

1.1 Overview

The document **I.CA RemoteSign Policy (Remote Creation of Electronic Signatures)** is prepared by První certifikační autorita, a.s., deals with the issues related to the Service while taking account of valid technical and other standards and norms of the European Union and the laws of the Czech Republic pertinent to this sphere and also contains information arising from the requirements for defining the signature creation policy. The document is divided into nine basic chapters and these are briefly introduced in the following list:

- Chapter 1 identifies this document, generally describes subjects taking part in the provision of this Service and defines the acceptable use of the Service;
- Chapter 2 deals with the responsibility for the publication and information or documents;
- Chapter 3 describes the processes of the Service identification and authentication;
- Chapter 4 defines life cycle processes of the Service up to Service's provision termination;
- 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 including the computer and network protection;
- Chapter 7 focuses on assessing the Service delivered;
- Chapter 8 deals with commercial and legal aspectsů
- Chapter 9 contains final provisions.

More details concerning the Service are given in two practice statements (also as Statements – not yet translated) required by ETSI TS 119 431-1 and ETSI TS 119 431-2 standards (see chapter 6.1.2), i.e. I.CA RemoteSign Practice Statement ETSI TS 119 431-1 (also as Statement1) and I.CA RemoteSign Practice Statement ETSI TS 119 431-2 (also as Statement2).

Note: This is English translation of the Policy; 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:	I.CA RemoteSign Policy (Remote Creation of Electronic Signatures), version 1.10
Supported OIDs:	**0.4.0.19431.2.1.2** (eu-advanced-x509, AdES based on X.509 certificates); and
	0.4.0.19431.1.1.2 (Normalized SSASC policy) – in case of storing signing keys on SCDev; or
	0.4.0.19431.1.1.3 (EU SSASC policy) - in case of storing signing keys on QSCD

1.2.1 Signature creation policy

A single signature creation policy is supported at any given time within the Service. It is implemented within the RSiCON component located in a third-party environment, which

securely communicates with the Client and the Service provider. The applied version of the signature creation policy is determined by the time when a particular electronic signature was created.

1.2.2 Supported signature formats and classes, their limitations

The Service supports the following formats. The characters "-B" at the end of the format name mean that it is a signature without included time-stamp, "-T" is a signature with included time-stamp.

CAdES

CAdES-B-B and CAdES-B-T according to the ETSI EN 319 122 standard, in internal and external versions.

PAdES

PAdES-B-B and PAdES-B-T according to ETSI EN 319 142, in invisible and visible versions.

For the foreground of the visible signature, it is possible to choose from three variants:

- Text only (which thus fills the entire rectangle for a visible representation of the signature).
- Image only (which thus fills the entire rectangle for a visible representation of the signature).
- Both text and image (when the rectangle is divided into left and right halves for visible representation. The left half will contain an image, the right half will contain text).

For all of these foreground variants, it is possible to optionally specify a background image that will always stretch to the full rectangle for visible representation.

1.2.3 Passing the parameters of the signature

Defining the signature parameters is a matter of the already mentioned RSiCON component, which on the provider's side creates a request for the creation of an electronic signature in the queue of the relevant Client, containing, among other things, the type of signature required (see chapter 1.2.2), the date and time of expiration of the request, an encrypted preview of the signed document or a link to it (both can only be decrypted by the relevant Client) and a checksum (hash) to create a signature. Neither the signed document nor its preview in open form is available to the service provider, only the hash is available.

1.3 PKI Participants

1.3.1 Service provider

První certifikační autorita, a.s., as the qualified trust services provider.

1.3.2 Contact points

Contact points serving in cases of physical presence of Client or of his agent (see chapter 3.1.2) are implemented via:

- Public registration authorities I.CA or I.CA SK; and
- Client registration authorities; and
- Specialized contact points oriented only to activities related to the Service.

Registration authorities can be stationary or mobile.

Contact points:

- Accept applications for the Service, provide required information, handle complaints, etc.;
- Are entitled, for urgent operational or technical reasons, to suspend, in whole or in part, the performance of their activities;
- Are authorized to conclude contracts “Contract about issuing the certificate and usage of I.CA RemoteSign service” (also as Contract) on behalf of I.CA or I.CA SK;
- Are authorized to charge for the I.CA services provided through contact point unless otherwise agreed in the Contract.

If the process takes place with the participation of the NKČR (see chapter 3.1.2.4), the contact point is the remote registration authority (also as DRA) operated by the NKČR. These registration authorities;

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

Authorized DRA operator can be:

- Notary – see Notarial Procedures, § 1/1;
- Notarial candidate – see Notarial Procedures, § 23 or § 24 /1;
- Notary trainee – see Notarial Procedures, § 19.

1.3.3 Relying parties

Any entity relying on electronic signature created using the Service is a relying party.

1.3.4 Other participants

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

1.4 Service usage

1.4.1 Appropriate service uses

Service provided under this Policy may be used in electronic signature creation processes for the benefit of specific third party in compliance with current legislation.

1.4.2 Prohibited service uses

Service provided under this Policy may not be used contrary to the acceptable use described in 1.4.1 or contrary to law. It also may not be used for electronic signing of any document which was not sent to Client by third party.

1.5 Policy administration

1.5.1 Organization administering the document

This Policy and its Statements are administered by První certifikační autorita, a.s.

1.5.2 Contact person

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

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

1.5.3 Person determining providing statement suitability for the policy

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

1.5.4 Providing statement approval procedures

If it is necessary to make changes to Statement1 or Statement2 to create new version thereof, CEO of První certifikační autorita, a.s., appoints a person authorized to perform such changes. No new version may take force unless it has been approved by CEO of První certifikační autorita, a.s.

1.6 Definitions and acronyms

Table 2 – Definitions

Term	Explanation
activation code	QR code or barcode inside of activation envelope under safety sticker used to activate the Service for specific Client

activation envelope	envelope which Client receives at contact point; at the front side or under transparent window at the front side there is an identification barcode, inside the activation envelope under safety sticker there is other, activation QR code or barcode
Citizen Identity	Identita občana, electronic document, primarily serves for secure and simple login to various public administration portals.
Citizen Portal	Portál občana, web service allowing access to various information and public administration services
Classified Information Protection Act	act of the Czech Republic no. 412/2005 Coll., on the protection of classified information and security eligibility
electronic signature	advanced electronic signature or recognized electronic signature or qualified electronic signature under trust services legislation
remote electronic signature	electronic signature created using private key stored in device operated by I.CA; this private key is under sole control of Client
identification code	barcode at front side of activation envelope or under transparent window at front side of activation envelope linking specific key pair to specific Client; identification code is also listed as number to allow typing
Labor Code	the Czech Republic's Act No. 262/2006 Coll., Labour Code, as amended
QR code	Quick Response code, means for automated data collection, stays readable after removal of substantial part of figure
seal (signature) creation policy	a set of rules and limitations related to the electronic seals (signatures) being created
supervisory body	the body supervising qualified trust services providers
trust service / qualified trust service	trust service / qualified trust service defined by trust services legislation
trust services legislation	current legislation on trust services
written contract	text of the contract in electronic or paper form

Table 3 – Acronyms

Acronym	Explanation
AdES	Advanced Electronic Signature
CAdES	CMS Advanced Electronic Signature
ARC	Alarm Receiving Centre
CR	Czech Republic
ČSN	Czech Technical Norm
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
ETSI	European Telecommunications Standards Institute, a European standardization institute for information and communication technologies
EU	European Union
FAS	Fire Alarm System
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)
http	Hypertext Transfer Protocol, protocol for exchanging html documents
https	Hypertext Transfer Protocol, protocol for secure exchanging of html documents
IAS	Intrusion Alarm System
IEC	International Electrotechnical Commission, the global organization publishing standards for electrical and electronic engineering, communication technologies and related industries
ISMS	Information Security Management System
ISO	International Organization for Standardization, an international organization of national standardization organizations; designation of standards
OID	Object Identifier
NIA	Národní identitní autorita, National Identity Authority
NKČR	Notářská komora České republiky, Notarial Chamber of the Czech Republic
PC	Personal Computer
PDCA	Plan-Do-Check-Act, Deming cycle, management method for control and continuous improvement
ROB	Registr obyvatel, Register of Residents
SCDev	Secure Cryptographic Device
S/MIME BR	CA/Browser Forum document „Baseline Requirements for the Issuance and Management of Publicly-Trusted S/MIME Certificates"
SSASC	Server Signing Application Service Component
TS	Technical Specification, type of ETSI standard
UPS	Uninterruptible Power Supply/Source
ZOOÚ	current personal data protection legislation

2 PUBLICATION AND REPOSITORY RESPONSIBILITIES

2.1 Repositories

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

2.2 Publication of certification information

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

- Registered office:

  První certifikační autorita, a.s.

  Podvinný mlýn 2178/6

  190 00 Praha 9

  The Czech Republic
- Website: http://www.ica.cz.

Electronic address for contact between general public and I.CA is info@ica.cz, ID of data box of I.CA is a69fvfb.

Information concerning the Service is also available at this web address.

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

2.3 Time or frequency of publication

I.CA publishes information as follows:

- Policy of the Service – after a new version is approved and issued;
- Practice statements of the Service – immediately;
- Other public information – no specific time limit, the general rule is that this information must correspond to the current state of the services provided.

2.4 Access controls on repositories

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

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

3 IDENTIFICATION AND AUTHENTICATION

3.1 Initial identity validation

Clients of third parties' services whose list the specific third party sent to I.CA can become Clients of the Service. Based on sent list the Contract can be concluded with them and then they can activate the Service.

3.1.1 Authentication of organization identity

Authentication of organization identity is relevant to third party authentication before concluding contract with this third party, for authentication of Client's employer identity or for identity authentication of Client who is self-employed. For such authentication the following must be submitted:

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

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

3.1.2 Authentication of individual identity

Individual identity authentication may be done in one of these ways:

- The presence of the Client on contact point;
- On the basis of another existing qualified certificate for validation of qualified electronic signature of the same Client;
- Remotely via certified ZealiD TRA Service using ZealiD application installed on Client's mobile device;
- Remotely via NKČR;
- Remotely via NIA.

Methods of individual identity authentication are described in following subchapters.

3.1.2.1 Presence on contact point

In this way it's possible to ask for:

- Qualified certificate for validation of qualified electronic signature created remotely;
- Qualified mandate certificate for validation of qualified electronic signature created remotely.

Third party first sends to I.CA (in a trustworthy way) the list of authorized applicants for Service activation containing their identification data. The next step depends on the type signing or mandate, of Certificate, which should be applied for. In both cases Client is, after issuing the

Certificate, to RemoteSign application, as the first transaction, the Contract. If the Contact is not signed by the specified time, the Certificate will be revoked.

3.1.2.1.1 Signing certificate

In case of signing certificate Client's identity authentication is possible in the following ways:

- By submitting two personal documents in paper form;
- By submitting an electronic personal document, namely a personal identity card, in the eDoklady application [1];
- By submitting one personal document in paper form and verifying it in the Register of Residents (Registr obyvatel - ROB) [2].

3.1.2.1.1.1 Two personal documents in paper form

The applicant is required to submit two personal documents, a primary and a secondary one. Valid personal identity card or passport must be used as the primary personal document for the citizens of the Czech Republic. Valid passport is the primary personal document for foreigners; citizens of EU member countries may use their valid personal identity card they use in their country as the proof of their identity. The secondary personal document must be clearly linked to the primary personal document (birth number, ID number, etc.) and must contain at least one of the following data:

- Date of birth (or birth identification number, if provided);
- Address of permanent residence;
- Photo of the face.

The data in the secondary personal document used to clearly identify the subscriber of the Certificate must be the same as the data in the primary personal document.

The RA operator compares the photo of the Client on the primary document with the actual appearance of the applicant, in case of doubt, he has the right to request the submitting of other document in paper form, or to end the authentication, if necessary. Other document must be clearly linked to the primary document (birth identification number, number of personal identity card etc.).

If the photo check ends with a positive result, the following data are validated from the submitted primary personal document:

- Full civil name;
- Date and place of birth or the birth identification number if shown in the primary document;
- Number of the primary personal document;
- Permanent address (if shown in the primary document).

If neither the primary nor the secondary personal document shows permanent address, no permanent address may be specified in the Certificate application and in the Certificate issued. The operator does not verify it; it only has to match the countryName attribute of the Certificate application.

For employees an employment certificate with the Organization is also required. This certificate is to be submitted by the Certificate subscriber to RA, but may be provided in the manner

[1] See chapter 9.

[2] See chapter 9.

defined in the contract concluded between I.CA and the Organization. The person authorized to act on behalf of the Organization must prove their identity through the primary personal document – see above, or the signature on the certificate of the Certificate subscriber's employment must be officially authenticated. If this person is not defined by law as a person authorized to represent the Organization, this person must also submit his/her officially authenticated power of attorney, signed by the Organization's authorized representative, for representing the Organization.

Employment certificate can be also submitted electronically. Must be .PDF format electronically signed by the person authorized to act on behalf of the Organization. Advanced (at least) electronic signature must be based on qualified certificate.

If an agent represents the Certificate subscriber vis-à-vis RA, officially authenticated authorization to act as agent is required.

If the individual who applies for a Certificate for themselves is OSVČ and this is to be specified in the Certificate, the relevant requirements under 3.2.2 apply.

3.1.2.1.1.2 Electronic personal document in eDoklady application

This option is only relevant for citizens of the Czech Republic with an active eDoklady mobile application for proving identity. It is required to submit a digital copy of the personal identity card. The applicant first uses the eDoklady application to scan the QR code of the registration authority, which is presented to him by the RA operator. After scanning the code, the applicant is shown information in the application about the request to transfer specific data to I.CA for the purpose of issuing the Certificate, and the applicant must agree to the transfer.

The RA operator compares the photo of the applicant on the digital copy of the personal identity card with his actual appearance, in case of doubt, he has the right to request the submission of other document in paper form, or to end the authentication, if necessary. Oher document must be clearly linked to the submitted digital copy of the personal identity card (birth identification number, ID number, etc.).

If the photo check ends with a positive result, the other necessary data (full civil name, date and place of birth, or social security number, if stated in the digital copy of the personal identity card, number of the submitted digital copy of the personal identity card, address of permanent residence (if stated in the digital copy of the personal identity card), are automatically transferred to the applicant's data in the CA information system. These data are the basis for creating the Certificate application.

If the digital copy of the personal identity card doesn't show permanent address it will be stated only in the Contract (not in the related Certificate). The operator does not verify it; it only has to match the countryName attribute of the Certificate application.

For employees an employment certificate with the Organization is also required. This certificate is to be submitted by the Certificate subscriber to RA, but may be provided in the manner defined in the contract concluded between I.CA and the Organization. The person authorized to act on behalf of the Organization must prove their identity through the primary personal document – see above, or the signature on the certificate of the Certificate subscriber's employment must be officially authenticated. If this person is not defined by law as a person authorized to represent the Organization, this person must also submit his/her officially authenticated power of attorney, signed by the Organization's authorized representative, for representing the Organization.

Employment certificate can be also submitted electronically. Must be .PDF format electronically signed by the person authorized to act on behalf of the Organization. Advanced (at least) electronic signature must be based on qualified certificate.

If an agent represents the Certificate subscriber vis-à-vis RA, officially authenticated authorization to act as agent is required.

If the individual who applies for a Certificate for themselves is OSVČ and this is to be specified in the Certificate, the relevant requirements under 3.2.2 apply.

3.1.2.1.1.3 One personal document in paper form and its verification in ROB

This option is only relevant for citizens of the Czech Republic. It is required to submit one personal document in paper forma, which can be personal identity card or passport.

The RA operator compares the photo of the Client on the document with his actual appearance, in case of doubt, he has the right to request the submission of other document in paper form, or to end the authentication, if necessary. Other document must be clearly linked to the submitted personal document (birth identification number, ID number, etc.).

If the photo check ends with a positive result, the RA operator retypes the name, surname, document number and document type from the submitted document, and these pieces of data are sent to the ROB for verification. Confirmation that the given document exists, belongs to a self-righteous and living person, or other information will be returned. The data from the ROB are taken over without the possibility of any further modification and stored together with the applicant's data in the CA information system. These data are the basis for the creation of the Certificate application and are subsequently verified once again by the CA against the ROB.

If the personal document doesn't show permanent address, no permanent address may be specified in the Certificate application and in the Certificate issued. The operator does not verify it; it only has to match the countryName attribute of the Certificate application.

For employees an employment certificate with the Organization is also required. This certificate is to be submitted by the Certificate subscriber to RA, but may be provided in the manner defined in the contract concluded between I.CA and the Organization. The person authorized to act on behalf of the Organization must prove their identity through the primary personal document – see above, or the signature on the certificate of the Certificate subscriber's employment must be officially authenticated. If this person is not defined by law as a person authorized to represent the Organization, this person must also submit his/her officially authenticated power of attorney, signed by the Organization's authorized representative, for representing the Organization.

Employment certificate can be also submitted electronically. Must be .PDF format electronically signed by the person authorized to act on behalf of the Organization. Advanced (at least) electronic signature must be based on qualified certificate.

If an agent represents the Certificate subscriber vis-à-vis RA, officially authenticated authorization to act as agent is required.

If the individual who applies for a Certificate for themselves is OSVČ and this is to be specified in the Certificate, the relevant requirements under 3.2.2 apply.

3.1.2.1.2 Mandate certificate

When the primary Certificate is applied, the **mandatary's** (Certificate subscriber's) identity authentication procedure, where mandatary always must be present in person on RA, requires two identification documents, the primary and the secondary one, and also the document identifying the mandator (including identification data) on behalf of which mandatary operates or acts and confirming authorization to act or operate.

Valid personal identity card or passport must be used as the primary personal document for the citizens of the Slovak Republic. Valid passport is the primary personal document for foreigners; citizens of EU member countries may use their valid personal identity card they use in their country as the proof of their identity.

The following data are validated in this document:

- Full civil name;
- Date and place of birth or the birth certification number if shown in the primary document;
- Number of the primary personal document;
- Permanent address (if shown in the primary document);
- Additional Identifier/identifiers (in compliance with the Slovak Republic legislation).

The secondary personal document must contain a unique identification, such as birth certification number or personal identity card number, matching it to the primary document and must show at least one of these items:

- Full civil name;
- Birth certification number in case of the Czech Republic or the Slovak Republic citizens, or date of birth of the applicant (foreigner who was not granted the birth certification number by public authority of the Czech Republic or the Slovak Republic);
- Permanent address;
- Photograph of the face.

The secondary personal document data uniquely identifying the Certificate subscriber must be identical to those in the primary personal document. RA employee decides whether the data are identical or not. If the applicant does not submit two personal documents fulfilling the above requirements the application will not be accepted. Acceptable secondary personal documents are passport, driving license, service card of state office, member of parliament card, service card of the police, gun license, military book, health insurance card, public transportation card, company card, student card etc.

The certificate of right to operate or act for person or public authority must be signed by person authorized to act for organization. If this person is not authorized to act for organization, i.e. is not statutory representative (is not listed in certificate of incorporation or in other register determined by law or in trade certificate in deed of foundation or in law, in case of organizational unit of state/public authority in special legislation) an other officially verified document (power of attorney, authorization, legal representation certificate) signed by statutory representative of the organization is required to confirm the right of this person to act on behalf of this organization.

When the **primary Certificate** is applied the **manadator** proves (mandate proving) through a power of attorney (depending on requirements stated in list on mandates published by NBÚ SR, unless otherwise specified) submitted by mandatary these data:

- In case of natural person:
  - Full civil name;
  - In case of employee organization name and organization identification of the employer;
  - Birth certification number in case of the Czech Republic or the Slovak Republic citizens, or date of birth of the applicant (foreigner who was not granted the birth certification number by public authority of the Czech Republic od the Slovak Republic);
  - Number of ID card or passport;
- In case of legal person or public authority the name and Identification data.

Procedure is described into detail in Conditions.

3.1.2.2 Another existing qualified certificate of the same Client

This way of identity authentication may be used only when the Client owns valid qualified certificate for qualified electronic signature validation which meets following requirements:

- Certificate was issued by I.CA;
- Corresponding private key is stored on smartcard Starcos 3.7 or higher;
- Certificate was issued on the basis of on-site identity authentication in the presence of the Client on contact point.

Issuing of these types of Certificates may be applied for:

- Qualified certificate for validation of qualified electronic signature created remotely on the basis of another qualified certificate for qualified signature validation of the same Client or of qualified mandate certificate for qualified electronic signature signing of the same Clients;
- Qualified mandate certificate for validation of qualified electronic signature created remotely on the basis of another qualified mandate certificate for qualified signature validation of the same Client;

when fulfillment of attributes corresponds with fulfillment of original certificate attributes.

Third party first sends to I.CA (in a trustworthy way) the list of authorized applicants for Service activation containing their identification data (at least name, surname and e-mail address). This list is entered into I.CA system and to the e-mail addresses are sent unique links allowing Clients to start Service activation and guiding them through the process of individual identity authentication.

Within the application processing it's checked if the data obtained from third party matches the data of the certificate based on which the Certificate is supposed to be issued. Negative result of any check means that the process of Certificate issuance is terminated and the Certificate is not issued.

After issuing the Certificate, Client is to RemoteSign application sent, as the first transaction, the Contract. If the Contact is not signed by the specified time, the Certificate will be revoked.

3.1.2.3 On-line identity authentication through ZealiD

This way of Client's identity authentication may be used only for issuing the qualified Certificate for verification of qualified electronic signature created remotely (other data relating to mandate certificate cannot be entered this way).

Third party first sends to I.CA (in a trustworthy way) the list of authorized applicants for Service activation containing their identification data (at least name, surname and e-mail address) who can use on-line identity authentication.

On-line identity authentication procedure uses certified ZealiD TRA Service using ZealiD application installed on the applicant's mobile phone or tablet. For this method of identity authentication, a primary personal document is required, which must be a valid personal identity card or passport for the citizens of the Czech Republic. Valid passport is the primary personal identity document for foreigners; citizens of EU member countries may use their valid personal identity card they use in their country as the proof of their identity. The guide with detailed instructions can be found at the I.CA website. The guide informs the applicant (Certificate subscriber) about the process of issuing the Certificate, including information for users about the conditions under which the Certificate can be issued in this way.

This list of authorized applicants is entered into I.CA system and to e-mail addresses are sent unique links allowing Clients to start Service activation and guiding them through the process of individual identity authentication.

Within the application processing it's checked if the data obtained from third party matches the data obtained via ZealiD. Negative result of any check means that the process of Certificate issuance is terminated and the Certificate is not issued.

The process of on-line authenticating the applicant's identity and issuing the Certificate consists of several successive steps and includes:

- Installation of the ZealiD application on the applicant's mobile device (supported platforms are Apple and Android);
- Registration of the mobile device to the system;
- Biometric facial analysis - for the required functionality, it is necessary to allow access to the camera when installing the ZealiD application;
- Verification of the personal document – scanning it and then biometric comparison of the photograph from the document with the applicant's face is performed;
- Generating Certificate application.

If any of the checks does not end with a positive result, e.g., if the verification of the form does not take place in required quality, the process is terminated and the Certificate is not issued.

After issuing the Certificate, Client is to RemoteSign application sent, as the first transaction, the Contract. The condition for the exposure of the Certificate on the list of issued certificates is its signing, otherwise the Certificate is revoked.

Restrictions for usage of the on-line individual identity authentication procedure is that the applicant cannot be represented by an agent.

3.1.2.4 On-line identity authentication through NKČR

This way of Client's identity authentication may be used only for issuing the qualified Certificate for verification of qualified electronic signature created remotely.

The list of authorized applicants for activation of the Service is not forwarded in this case, the Service is activated for each Client whose identity has been verified through the NKČR.

The condition for identity authentication of a natural person is a means for remote identification of this person according to Section 64 and (2) of the Notarial Procedures, i.e. registration through the National Identity Authority (NIA) with a high, or substantial level of assurance (only through bank identity - BankID).

In the process of identity authentication, the individual applicant is required to submit two personal documents, a primary and a secondary one, that show the data specified further in this chapter.

Valid personal identity card or passport must be used as the primary personal document for the citizens of the Czech Republic. Valid passport is the primary personal document for foreigners; citizens of EU member countries may use their valid personal identity card they use in their country as the proof of their identity.

The following data are validated in this document:

- Full civil name;
- Date and place of birth or the birth certification number if shown in the primary document;
- Number of the primary personal document;

- Permanent address (if shown in the primary document).

The secondary document must contain a unique identification, such as birth certification number or personal identity card number, matching it to the primary document and must show at least one of these items:

- Date of birth (or birth certification number if specified);
- Permanent address;
- Photograph of the face.

The secondary personal document data uniquely identifying the Certificate subscriber must be identical to those in the primary personal document.

If neither the primary nor the secondary personal document shows permanent address, no permanent address may be specified in the Certificate application and the Certificate issued.

After issuing the Certificate, Client is to RemoteSign application sent, as the first transaction, the Contract. The condition for the exposure of the Certificate on the list of issued certificates is its signing, otherwise the Certificate is revoked.

Restrictions for usage of the on-line individual identity authentication procedure is that the applicant cannot be represented by an agent.

3.1.2.4.1 Online Session to DRA Requirements

An online session to DRA must meet the following technical requirements:

- PC with Windows 10 operating system or higher and SW for making a video call;
- microphone and video camera with HD resolution (1280x720) or betterů
- network connectivity level ADSL2 (2.5 Mb/s or better).

The DRA operator is entitled to terminate the session if the quality of the established connection or the lighting conditions on the side of the QC applicant are not sufficient for the needs of facial recognition and/or the relevant verified documents (insufficient brightness, contrast or sharpness of the display), the sound is missing or dropped, or the video transmission is choppy and thus does not allow the acquisition of sufficient quality uninterrupted video evidence.

During an online session with to DRA, the DRA operator requires, among other things:

- Presentation of relevant documents from both sides in case of an identity card, or of the passport pages with a photograph and other identification data, in order to confirm that the person has the document under their control at the time of the initial identity authentication;
- Showing the face (including movement from side to side) so that it is possible to compare the applicant's likeness with a photo stored in one of the agenda information systems (citizenship cards, travel documents, foreigner records) - if the verification in the agenda information system fails the session ends with a negative result.

The DRA operator is entitled to terminate the session if the identity of the natural person cannot be sufficiently authenticated.

3.1.2.4.2 Online individual identity authentication records

Records are made of the course of online individual authentication, a log file is captured and archived. All requests and responses to and from the basic registers or agenda information systems are recorded in it, including time stamps, so that the course of online authentication can be reconstructed in the future. After passing the online individual authentication, the log

file is, together with the certificate application, transferred to I.CA and archived there. I.CA has the right to randomly check the log files.

3.1.2.5 On-line identity authentication through NIA

This way of Client's identity authentication may be used only for issuing the qualified Certificate for verification of qualified electronic signature created remotely (other data relating to mandate certificate cannot be entered this way).

This is a verification of the Client's identity through the Citizen Portal, high and substantial levels. The condition is that the latter has a personal computer with the Windows 10 operating system (or a higher version), a monitor with at least HD resolution and a functional Internet connection.

Third party first sends to I.CA (in a trustworthy way) the list of authorized applicants for Service activation containing their identification data (at least name, surname, phone number, e-mail address, type of identification document and its number) who can use on-line identity authentication.

This list of authorized applicants is entered into I.CA system and to e-mail addresses are sent unique links allowing Clients to start Service activation and guiding them through the process of individual identity authentication. The Service activation process can be started no earlier than twenty-four hours after entering the data into the I.CA system, for the next three days.

Clicking on the link will bring up a splash screen with basic information and related links. The applicant must agree to the procedure and conditions for the online issuance of the Certificate, otherwise it is not possible to issue the Certificate remotely. If he agrees, he is then redirected to the Citizen Portal, where he chooses how and at what level he wants to be verified. Subsequently, he selects the identification profile and the data from the Citizen Identity is displayed to him. When the correctness of the data on the Citizen's Portal is confirmed, these are automatically transferred to the certificate application and cannot be changed. The client adds to the application the e-mail address for communication with I.CA, the telephone number to which the password for the encrypted documentation is to be sent, the password for the Certificate revocation and the gender, agrees to the terms of Service provision and the Certificate is issued.

After issuing the Certificate, Client is to RemoteSign application sent, as the first transaction, the Contract. The condition for the exposure of the Certificate on the list of issued certificates is its signing, otherwise the Certificate is revoked.

Restrictions for usage of the on-line individual identity authentication procedure is that the applicant cannot be represented by an agent.

3.1.3 Validation of e-mail address

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

3.1.3.1 Validation via registered DNS domain

Validation of the e-mail address against the registered DNS domain is intended for business customers, where the contractual partner has control over the relevant DNS domain. In such a case, the correspondence of the domain part of e-mail address to the internally maintained

list of registered company domains is verified (the company has a contract with I.CA and control over the DNS domain has been verified).

3.1.3.2 Validation using the content of the validation e-mail

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

3.2 Identity validation for service extending

Service extending is automatic. I.CA as the third party inserts the query into Client's queue whether he wants to issue subsequent Certificate. If the answer is yes (answer is electronically signed, signature is based on private key corresponding with Certificate to which the subsequent should be issued) the Service is extended to the end of validity of subsequent Certificate. This way the Client also confirms continuing validity of his identification data validated as part of initial validity validation.

3.3 Modification of data

If it is not possible to issue subsequent Certificate because data has changed the Client is obliged to pass individual identity authentication process in one of the ways described in chapter 3.1.2.

4 SERVICE LIFE CYCLE REQUIREMENTS

In chapters below the Service life cycle is described.

4.1 Conclusion of the contract

The Contract for activation and usage of Service is concluded between I.CA and the Client.

4.2 Service activation

Activation the Service depends on the way of individual identity authentication (see chapter 3.1.2) when:

- The Contract is concluded;
- Certificate application is created;
- Depending on the way of individual identity authentication:
  - The Client is given activation envelope for Service activation and mobile application activation;
  - Unique QR code is sent to the Client to activate the Service and mobile application,
- Certificate is issued and published.

Further handling with Certificate may be specified in the contract concluded between specific third party and I.CA (I.CA is also special case of third party).

4.2.1 Enrollment process and responsibilities

Process is performed only in case of setting up the Service and so issuance of the primary Certificate. Its progress depends on the way of individual identity authentication – see chapter 3.2.1.

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

- Get acquainted with this Policy and with Certificate policy for issuing qualified certificates for remote electronic signatures (RSA algorithm) or with Certificate policy for issuing qualified certificates for remote electronic signatures according to the legislation of the Slovak Republic (RSA algorithm);
- Get acquainted with the Contract;
- Observe all relevant provisions the Contract;
- Use the Service in compliance with chapter 1.4;
- Use the identification and authentication data for access to the Servis so that they cannot be abused;
- Inform immediately the Service provider that the identification and authentication data for access to the Service were abused and ask for Certificate revocation;
- Provide true and complete information for setting up the Service;
- Check whether the data retyped from submitted documents are correct and correspond to the required data;

- Choose a suitable Certificate revocation password (the minimum/maximum password length is 4/32 characters; permitted characters: 0..9, A..Z, a..z).

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

- Inform the Client about the terms and conditions before concluding the Contract;
- Conclude with the Client contract that meets the requirements imposed by current legislation and technical standards;
- During the process of setting up the Service validate all validable data according to the submitted documents;
- Issue a Certificate that contains materially correct data on the basis of the information available to the Service provider as at the issuance of the Certificate;
- Publish the certificates of issuing and root certification authorities;
- Publish public information in accordance with 2.2;
- Provide any Service-related activity in accordance with current legislation, this Policy, the relevant certificate policy and certification practice statement, Corporate Security Policy, System Security Policy - Trustworthy Systems and the operational documentation.

4.2.2 Conduct constituting Certificate acceptance

Issued certificate is accepted by Client after signing the Contract. This Contract is sent to him as first transaction into RemoteSign application and if the Contract is not signed in specified time period, issued Certificate will be revoked.

4.3 Activation of the Service

Service is activated immediately after Certificate issuance. To use the Service, Client must install mobile or PC application (in case of remote client's identity authentication or client's identity authentication on the basis of his other existing qualified certificate the installation is linked with creation of Certificate application). Through this installation Client gains access to his private key, any other access to private key of specific Client is not possible.

4.4 Extending the validity of the Contract

Client is, before Certificate's expiration, notified and asked whether he wants to issue subsequent certificate with different public key, but with the same content of subject and subjectAlternatioveName fields. If Client does not answer in affirmative the Certificate expires and the Contract is terminated. In an opposite case (answer is electronically signed and the signature is based on private key corresponding with public key in Certificate, to which the subsequent one should be issued) Contract remains in force and the Service in provided continuously.

Client (subscriber of the Certificate) is obliged to inform the Service provider of all changes in Contractual data (and in subject and subjectAlternativeName fields od Certificate).

4.5 Contract expiration

Expiration of the Contract is closely tied with Certificate expiration. When:

- Client does not agree subsequent Certificate issuance;
- Clients revokes the Certificate and this one is listed on CRL;

the Contract expires.

4.6 Certificate revocation and suspension

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

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

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

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

4.6.1 Circumstances for revocation

4.6.1.1 User certificate revocation reasons

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

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

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

6. Certificate no longer complies with the requirements for cryptographic algorithms and their parameters (quality, see 6.1.5 and 6.1.6) CRLReason #4, superseded);
7. I.CA obtains evidence that the Certificate was misused (CRLReason #9, privilegeWithdrawn);
8. I.CA is made aware that a Certificate subscriber has violated one or more of his material obligations under Service contract or under the contract on the terms and conditions of use of the Certificate (CRLReason #9, privilegeWithdrawn);

9. I.CA is made aware of any circumstance indicating that use of an email address or Fully-Qualified Domain Name in the Certificate is no longer legally permitted (e.g., a court or arbitrator has revoked the right to use an email address or Domain Name, a relevant licensing or services agreement between the Subscriber has terminated, or the accountholder has failed to maintain the active status of the email address or Domain Name) (CRLReason #5, cessationOfOperation);
10. I.CA is made aware of a material change in the information contained in the Certificate (CRLReason #9, privilegeWithdrawn);
11. I.CA is made aware that the Certificate was not issued in compliance with S/MIME BR, CP or CPS (CRLReason #4, superseded);
12. I.CA determines or is made aware that some information contained in the Certificate is inaccurate (CRLReason #9, privilegeWithdrawn);
13. I.CA's right to issue Certificate under S/MIME BR and this CP expired or is revoked or terminated, unless I.CA has made arrangements to continue maintaining CRL/OCSP repository (unspecified(0); this code is not entered in CRLReason);
14. Revocation is required by CP or CPS;
15. CRLReason #1, keyCompromise when I.CA is made aware of:
    - □ Demonstrated or proven method that exposes subscriber's private key to compromise;
    - □ Clear evidence that the specific method used to generate private key was flawed.

4.6.1.2 Reasons to revoke the authority's certificate

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

1. Authority requests revocation in writing;
2. Authority notifies the root certification authority that original Certificate application was not authorized and does not retroactively grant authorization;
3. Root certification authority obtains evidence that the Authority's private key corresponding to the public key in the Certificate suffered a key compromise or no longer complies with the cryptographic algorithm requirements and the required parameters (quality, see 6.1.5 and 6.1.6);
4. Root certification authority obtains evidence that Authority's certificate was misused;
5. Root certification authority is made aware that Authority's certificate:
    - □ Was not issued in compliance with S/MIME BR, corresponding CP or CPS; or
    - □ Does not meet requirements of S/MIME BR, corresponding CP or CPS;
6. I.CA determines that some information appearing in the Authority's certificate was inaccurate or misleading;
7. Root CA or Authority ceased operation for any reason a did not made arrangement for another CA to provide revocation support for certificates issued by them;
8. Root CA's or Authority's right to issue Certificate under S/MIME BR and this CP expired, was revoked or terminated and root CA did not make arrangement to continue maintaining CRL/OCSP repository;
9. Revocation is required by CP or CPS of root certification authority.

4.6.2 Who can request revocation

Certificate revocation request may be submitted by:

- Provider of this Service (CEO of I.CA or his representative, or managing director of ICA SK in case of the Certificate issued by this company is the person authorized to request for the revocation of a Certificate issued:
  - If the Certificate is issued on the basis of false data;
  - If establishes that the Certificate was issued in spite of nonconformance with the requirements of trust services legislation;
  - If demonstrably establishes that the Certificate was used contrary to the restrictions defined in 1.4.2;
  - If demonstrably establishes that the Certificate's subscriber has died or been limited in legal capacity by court or the data by which the Certificate was issued are no longer valid;
  - If the public key in the Certificate application is the same as the public key in a certificate already issued;
- Supervisory body and other entities as may be specified in trust services legislation.

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

Additional options are listed in the following subsections.

4.6.2.1 Signing certificate

Request for revocation of the Certificate may be submitted by:

- Certificate's subscriber;
- In case of employee Certificate any person authorized to act on behalf of the Organization;
- Any person who is beneficiary in Certificate's subscriber probate proceedings;
- In case of employee Certificate any person authorized to act for the legal successor to the original entity (the Organization) to which the Certificate was issued for that entity's employee.

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

4.6.2.2 Mandate certificate

Request for revocation of the Certificate may be submitted by:

- Subscriber of the Certificate (Client, mandatary):
  - If there is the risk of his private key abuse;
  - If demonstrably establishes that the mandator died, was finally declared dead or ceased to exist;
  - If the status of a public authority for which the mandatory performed activities, was terminated;

- Mandator for whom the mandatory performed activity or function under specific regulation when mandatary's performance of activity creased of function under specific legislation was terminated;
- Subject explicitly specified therefore in the Service (under this CP) contract;
- Person who is beneficiary in mandatary probate proceedings.

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

4.6.3 Submitting revocation request

Options for submission the request for revocation by the Client are as follows:

- In case of personal handover at contact point (RA) the request must include the Certificate's serial number in the decimal or hexadecimal format (introduced by the string '0x'), the full name of the natural person authorized to request for Certificate's revocation, and the Certificate revocation password. If the natural person authorized to request for revocation does not know the Certificate revocation password, s/he must explicitly state this in the written application, along with the number of the primary personal document submitted in the Certificate application procedure or the number of the new primary personal document if the original document has been replaced. The person must use this primary personal document to prove their identity with the RA employee. If the request is legitimate, the RA employee revokes the Certificate, and the Certificate revocation date and time are the date and time the request is processed by CA's information system. If the Certificate revocation application cannot be accepted (wrong revocation password or no proof of identity of the natural person authorized to request for Certificate revocation) the RA employee seeks to rectify these defects, and dismisses the request if the defects cannot be rectified for any reason. The RA employee always notifies the requestor of the result.
- The following options are available in case of electronic submission:
  - Using the form on the information web page. The Certificate revocation date and time are the date and time when Certificate revocation request is dealt with in the CA's information system. The requestor receives a notice if the request was processed positively;
  - Electronic message not signed electronically – the body must contain the text (in Czech or Slovak with or without diacritics, or in English):

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

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

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

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

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

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

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

Request for revocation employee's Certificate submitted by the person authorized to act on behalf of Organization (given in organizationName attribute) must be in electronic form as electronically signed or unsigned (in special cases) message. The message must contain the text (in Czech or Slovak with or without diacritics, or in English):

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

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

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

4.6.4 Revocation request grace period

Certificate revocation request must be made immediately.

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.

4.7 Blocking and unblocking of mobile or PC application

Mobile or PC application may be blocked for example if mobile device or PC are stolen.

4.7.1 Blocking

Blocked mobile or PC application means that it is marked as blocked a cannot be used to access the Certificate. Certificate remains valid (and can be accessed through any other activated application of the same Client). Blocking is possible:

- Through any other activated mobile or PC application (of the same Client);
- By phone at +420 284 081 930, +420 284 081 931 or +420 284 081 933. Technical support employee finds out first name, surName and degree of the Client, number of his primary personal identification document and his residence. Technical support employee can ask any other information which is not present in the Certificate but was given in

application for Service's setting up. Technical support employee is in case of any ambiguity in Client's answers allowed to refer the Client to another way of blocking.

- By e-mail to podpora@ica.cz sent from address which was communicated by Client when setting up the Service. E-mail must contain the text:
  - Client *degree, first name (names), surname*, date of birth *dd.mm.yyyy*, number of primary identification document *abcdefghij*, residence *street, house number, zip code, town* requests blocking of mobile device for access to the service of remote electronic signature creation *identification of mobile device*.

  In case of any ambiguity blocking may be rejected, in all cases the Client is informed by e-mail about the result of processing the request for blocking.
- In person at contact point, it is necessary to submit primary and secondary personal identity document (secondary document necessary to submit primary and secondary personal identity document (secondary document may not be the same as the one submitted by initials identity validation as described in 3.1.1, but must contain one of items mentioned in 3.1.1).

4.7.2 Unblocking

Mobile or PC application can be unblocked only through any other activated application (of the same Client). If application was blocked for a limited time, it is unblocked automatically after this expiration period (set when blocking).

4.8 Use of the Service

Service provides remote creation of electronic signatures. Documents to be signed are sent by third parties, the procedure is as follows:

- Third party queues the request for electronic signing of specific document into the I.CA RemoteSign queue. The request contains identification of the Client who is to sign, encrypted preview of document to be signed (only authorized Client can decrypt it) and list of electronic signature parameters (AdES and CAdES are supported);
- Client runs the application and enters the password;
- After password verification all request for electronic signature creation are downloaded into the application;
- Client can check the details of the request including the display of signed data, or their preview. The established technical, personnel, procedural and cryptographic measures ensuring the storage of the private key and access to it allow the signatory to bear full guarantee for the created signature and therefore for the content of the signed document;
- If Client has decided to create specific electronic signature, he presses the button "Podepsat" ("Sign") and enters private key's password; by creating a qualified electronic signature, the Client expresses his undeniable consent to the signed content;
- If the password is correct the required electronic signature based on private key stored in secure cryptographic device or in QSCD will be created and sent back to the third party.

5 FACILITY, MANAGEMENT, AND OPERATIONAL CONTROLS

Facility, management, and operational controls primarily deal with:

- System designated to support the Service;
- All processes supporting the provision of the Service.

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

5.1 Physical controls

5.1.1 Site location and construction

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

Systems designated to support the Service are situated on reserved premises of operating sites. These premises are secured in a manner similar to that required by the Classified Information Protection Act for the 'Confidential' category secure areas.

5.1.2 Physical access

Requirements for physical access to the reserved premises (protected with mechanical and electronic features) of operating sites are described in internal documentation. Buildings are protected with intrusion alarm system (IAS), alarm receiving 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 systems supporting the Service have active air-conditioning of adequate capacity, which keeps the temperature at 20°C ± 5°C all year round. The supply of electricity is backed up with a UPS (Uninterruptible Power Supply) and a diesel unit.

5.1.4 Water exposures

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

5.1.5 Fire prevention and protection

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

5.1.6 Media storage

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

Any paper media required to be archived are stored at 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 at a place designated by the COO of I.CA and described in internal documentation.

5.2 Procedural controls

5.2.1 Trusted roles

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

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

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:

- Initializing cryptographic module designated for generation and stage of sensitive data which are necessary for providing the Service;
- Making backups of these data stored in cryptographic module;
- Restoring these data into cryptographic module.

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

5.2.3 Identification and authentication for each role

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

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

5.2.4 Roles requiring separation of duties

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

5.3 Personnel controls

5.3.1 Qualification, experience, and clearance requirements

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

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

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

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

Description of employee's activities is defined by the employment contract.

Before completion all entry checks employee is not granted both logical and physical access to systems supporting the Service.

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

5.3.2 Background check procedures

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

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

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

5.3.3 Training requirements

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

5.3.4 Retraining frequency and requirements

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

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

5.3.5 Job rotation frequency and sequence

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

5.3.6 Sanctions for unauthorized actions

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

5.3.7 Independent contractor requirements

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

5.3.8 Documentation supplied to personnel

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

5.4 Audit logging procedures

5.4.1 Types of events recorded

Subject to logging are all the events required by trust services legislation or the relevant technical and other standards to be logged.

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

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

5.4.2 Frequency of processing log

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

5.4.3 Retention period for audit log

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

5.4.4 Protection of audit log

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

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

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

5.4.5 Audit log backup procedures

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

5.4.6 Audit collection system (internal vs. external)

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

5.4.7 Notification to event-causing subject

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

5.4.8 Vulnerability assessments

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

5.5 Records archival

The storage of records i.e., information and documentation, at První certifikační autorita, a.s., is regulated in internal documentation.

5.5.1 Types of stored records

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

- Client's Contracts and amendments of these Contracts;

- Information handling records, such as takeover, handover, saving, check, conversion from printed to electronic, etc.;
- Application software, operating and security documentation.

5.5.2 Retention period for archive

All records are stored in accordance with 5.4.3.

The record storage procedures are regulated in internal documentation.

5.5.3 Protection of archive

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

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

5.5.4 Archive backup procedures

The record backup procedures are regulated in internal documentation.

5.5.5 Requirements for time-stamping of records

If time-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 stored at a place designated by COO of I.CA.

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

5.5.7 Procedures to obtain and verify archive information

Stored information and records are placed at sites designated therefore and are accessible to:

- I.CA 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 Compromise and disaster recovery

5.6.1 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.

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

See. 5.6.1.

5.6.3 Business continuity capabilities after a disaster

See. 5.6.1.

5.7 Service's provider termination

The following rules apply to the termination of qualified trusted services provider operations:

- The termination must be notified in writing to the supervisory body and all parties having valid Contract;
- The termination must be published on the web page pursuant to 2.2;
- 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.

In the event of withdrawal of the qualified trusted services provider status:

- The information must be notified in writing or electronically to all parties having valid Contract;
- The information must be published in accordance with 2.2;
- The subsequent course of action will be decided by CEO of I.CA while taking account of the decision of the supervisory body.

6 TECHNICAL SECURITY CONTROLS

6.1 Cryptography, private key and its protection

RSA cryptography is fundamentally used within the service. The length of the keys corresponds to the requirements of ETSI TS 119 312

Key pairs of Clients are generated and private keys stored in a cryptographic module, or in a QSCD-type device under the sole control of I.CA. Access to private keys is protected by a cryptographic protocol that ensures that only its authorized owner has access to the key.

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.

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 Computer security controls

6.2.1 Specific computer security technical requirements

The level of security of the components used in providing the Service 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.

6.2.2 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:

- ČSN EN 419241-1 Trustworthy Systems Supporting Server Signing - Part 1: Security Requirements;
- EN 419241-1 Trustworthy Systems Supporting Server Signing - Part 1: Security Requirements;
- ČSN EN 419241-2 Trustworthy Systems Supporting Server Signing - Part 2: Protection profile for QSCD for Server Signing;
- EN 419241-2 Trustworthy Systems Supporting Server Signing - Part 2: Protection profile for QSCD for Server Signing;
- ČSN EN 419221-5 – Protection Profiles for TSP Cryptographic Modules - Part 5 - Cryptographic Module for Trust Services;
- EN 419221-5 – Protection Profiles for TSP Cryptographic Modules - Part 5 - Cryptographic Module for Trust Services;
- ETSI TS 119 431-1 Electronic Signatures and Infrastructures (ESI); Policy and security requirements for trust service providers; Part 1: TSP service components operating a remote QSCD / SCDev;

- ETSI TS 119 431-2 Electronic Signatures and Infrastructures (ESI); Policy and security requirements for trust service providers; Part 2: TSP service components supporting AdES digital signature creation;
- ETSI TS 119 432 Electronic Signatures and Infrastructures (ESI); Protocols for remote digital signature creation;
- ETSI EN 319 102-1 Electronic Signatures and Trust Infrastructures (ESI); Procedures for Creation and Validation of AdES Digital Signatures; Part 1: Creation and Validation.
- 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;
- 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.
- EN 301 549 Accessibility requirements for ICT products and services.
- ETSI TS 119 312 Electronic Signatures and Infrastructures (ESI); Cryptographic Suites;
- ETSI TS 119 101 Electronic Signatures and Infrastructures (ESI); Policy and security requirements for applications for signature creation and signature validation;
- ČSN EN ISO/IEC 27006 Information Technology – Security Techniques – Requirements for Bodies Providing Audit and Certification of Information Security Management Systems;
- ISO/IEC 17021 Conformity assessment -- Requirements for bodies providing audit and certification of management systems;
- ISO/IEC 17065 Conformity assessment -- Requirements for bodies certifying products, processes and services.

6.3 Life cycle technical controls

6.3.1 System development controls

System development is carried out in accordance with internal documentation.

6.3.2 Security management controls

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

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

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

6.3.3 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.

6.4 Network security controls

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

6.5 Protection against fraud and theft of data

Protection against fraud and theft of data is part of complete information security management system i.e., not only of systems supporting the Service, but all systems of I.CA. Involved are top management, senior staff and also employees in trusted roles having appropriate authorizations.

7 CONFORMITY ASSESSMENTS AND OTHER ASSESSMENTS

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

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

7.3 Assessor's relationship to assessed entity

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

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

7.4 Topics covered by assessment

The areas to be assessed in an assessment required under trust services legislation are those as specified in that legislation, in any other assessment are specified in the technical standards under which the assessment is made.

7.5 Actions taken as a result of deficiency

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

7.6 Communication of results

Assessment result notification is subject to the requirements of trust services legislation and the relevant technical standards.

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

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

8 OTHER BUSINESS AND LEGAL MATTERS

8.1 Fees

8.1.1 Service fees

The fees of the Service are given by contract concluded between I.CA and specific third party (can be flat fee per time period, paying for successful creation of electronic signature etc.).

8.1.2 Fees for other services

Not applicable for this document.

8.1.3 Refund policy

Not applicable for this document.

8.2 Financial responsibility

8.2.1 Insurance coverage

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

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

8.2.2 Other assets

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

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

8.2.3 Insurance or warranty coverage for end-entities

Not applicable for this document.

8.3 Confidentiality of business information

8.3.1 Scope of confidential information

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

- All cryptographic pieces of information used in providing the Service;
- I.CA's business information;
- Any internal information and documentation;
- Any personal data.

8.3.2 Information not within the scope of confidential information

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

8.3.3 Responsibility to protect confidential information

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

8.4 Privacy of personal information

8.4.1 Privacy plan

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

8.4.2 Information treated as private

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

I.CA employees or the entities defined by relevant legislation that come into contact with personal data must maintain confidentiality of 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.

8.4.3 Information not deemed private

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

8.4.4 Responsibility to protect private information

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

8.4.5 Notice and consent to use private information

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

8.4.6 Disclosure pursuant to judicial or administrative process

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

8.4.7 Other Information disclosure circumstances

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

8.5 Intellectual property rights

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

8.6 Representations and warranties

8.6.1 CA Representations and warranties

I.CA warrants that:

- Technical support of Service operations, dealing with non-standard situations and Service operational consultancy through contacts provided at www.ica.cz;
- The Service is all the time legislatively and technically actual and in compliance with relevant legislation and technical standards and norms.

All warranties and the performance resulting therefrom may only be recognized on condition that Client did not violate obligations arising from the Contract.

8.6.2 Contact points representations and warranties

Contact point:

- Assumes the obligation that the services it provides are correct;
- Does not accept the application if the Client refuses to provide the necessary data or is not authorized to submit the application;
- Is responsible for handling objections and complaints.

8.6.3 Representations and warranties of other participants

Not applicable for this document.

8.7 Disclaimers of warranties

První certifikační autorita, a.s., provides only the warranties as given in 8.6.

8.8 Limitations of liability

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

8.9 Indemnities

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

První certifikační autorita, a.s.:

- Undertakes to discharge all the obligations defined in relevant legislation and specific policies;
- Provides all warranties during the term of the Contract;
- Agrees that the application software suppliers with a valid contract with První certifikační autorita, a.s., for the distribution of the root certificate assume no obligation or liability, except for where damage or loss is directly attributable to the software of that supplier.

První certifikační autorita, a.s., may not be held liable for any defect in the services rendered which is due to incorrect or unauthorized use of the services rendered under the Contract, particularly for any use contrary to the terms and conditions specified in this Policy, and for any defect due to force majeure, including a temporary telecommunication connection failure.

Claims and complaints may be made by:

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

The party making the claim or complaint must provide:

- Most concise description of the defect and its symptoms;
- Suggestion how the claim/complaint should be resolved.

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

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

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

8.10 Term and termination

8.10.1 Term

This Policy takes effect on the date specified in Table 1 and remains ii effect no shorter than the Service is provided or this Policy is replaced with a new version.

8.10.2 Termination

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

8.10.3 Effect of termination and survival

The obligations of I.CA out of this Policy survive until the last Contract is terminated.

8.11 Individual notices and communications with participants

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

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

8.12 Amendments

8.12.1 Amending procedure

This procedure is a controlled process described in an internal documentation.

8.12.2 Notification mechanism and period

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

8.12.3 Circumstances under which OID must be changed

No OID is assigned to this Policy, it covers OIDs as defined in chapter 1.2. Any change to this Policy results in a new version of the document.

8.13 Disputes resolution provisions

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

- Contact point employee in charge;
- I.CA employee in charge (electronic or written filing is required);

- CEO of I.CA (electronic or written filing is required).

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

8.14 Governing law

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

8.15 Compliance with applicable law

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

8.16 Miscellaneous provisions

8.16.1 Entire agreement

Not applicable for this document.

8.16.2 Assignment

Not applicable for this document.

8.16.3 Severability

If a court or a public authority with jurisdiction over the activities covered by this Policy establishes that the implementation of a mandatory requirement is unlawful, the scope of that requirement will be so limited as to ensure the requirement is lawful and complies with relevant legislation.

8.16.4 Enforcement (attorneys' fees and waiver of rights)

Not applicable for this document.

8.16.5 Force Majeure

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

8.17 Other provisions

Not applicable for this document.

9 FINAL PROVISIONS

This I.CA RemoteSign Policy (Remote Creation of Electronic Signatures) issued by První certifikační autorita, a.s., takes force and effect on the date mentioned above in

Table 1. The use of the newly added procedures for authentication of individual identity described in chapters 3.1.2.1.1.2 and 3.1.2.1.1.3 is subject to their approval by the supervisory body.