První certifikační autorita, a.s.



I.CA RemoteSeal Policy

(Remote Creation of Electronic Seals)

I.CA RemoteSeal Policy (Remote Creation of Electronic Seals) 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 1.04

Copyright © První certifikační autorita, a.s.

CONTENT

1 Introduction 7
1.1 Overview 7
1.2 Document name and identification 8
1.2.1 Seal (signature) creation policy 8
1.2.2 Supported seal formats and classes, their limitations 8
1.2.3 Passing the parameters of the signature 9
1.2.4 Architecture of the Service 9
1.3 PKI Participants 11
1.3.1 Service provider 11
1.3.2 Contact points 11
1.3.3 Relying parties 11
1.3.4 Other participants 11
1.4 Service usage 11
1.4.1 Appropriate Service uses 11
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 17
3.2 Identity validation for service extending 17
3.3 Modification of data 17
3.4 Identification and authentication for revocation request 17

4 Service life cycle requirements 19
4.1 Conclusion of the contract 19
4.2 Establishment of the Service 19
4.2.1 Enrollment process and responsibilities 19
4.3 Activation of the Service 20
4.4 Management of the Service 20
4.5 Extending the validity of the Contract 20
4.6 Contract expiration 21
4.7 Certificate revocation and suspension 21
4.7.1 Circumstances for revocation 21
4.7.2 Who can request revocation 23
4.7.3 Submitting revocation request 24
4.7.4 Revocation request grace period 25
4.8 Use of the Service 25
4.9 Additional security measures 25
5 Facility, management, and operational controls 26
5.1 Physical controls 26
5.1.1 Site location and construction 26
5.1.2 Physical access 26
5.1.3 Power and air conditioning 26
5.1.4 Water exposures 26
5.1.5 Fire prevention and protection 26
5.1.6 Media storage 27
5.1.7 Waste disposal 27
5.1.8 Off-site backup 27
5.2 Procedural controls 27
5.2.1 Trusted roles 27
5.2.2 Number of persons required per task 27
5.2.3 Identification and authentication for each role 27
5.2.4 Roles requiring separation of duties 28
5.3 Personnel controls 28
5.3.1 Qualification, experience, and clearance requirements 28
5.3.2 Background check procedures 28
5.3.3 Training requirements 28
5.3.4 Retraining frequency and requirements 29
5.3.5 Job rotation frequency and sequence 29

5.3.6 Sanctions for unauthorized actions 29
5.3.7 Independent contractor requirements 29
5.3.8 Documentation supplied to personnel 29
5.4 Audit logging procedures 29
5.4.1 Types of events recorded 29
5.4.2 Frequency of processing log 30
5.4.3 Retention period for audit log 30
5.4.4 Protection of audit log 30
5.4.5 Audit log backup procedures 30
5.4.6 Audit collection system (internal vs. external) 30
5.4.7 Notification to event-causing subject 30
5.4.8 Vulnerability assessments 30
5.5 Records archival 30
5.5.1 Types of stored records 30
5.5.2 Retention period for archive 31
5.5.3 Protection of archive 31
5.5.4 Archive backup procedures 31
5.5.5 Requirements for time-stamping of records 31
5.5.6 Archive collection system (internal or external) 31
5.5.7 Procedures to obtain and verify archive information 31
5.6 Compromise and disaster recovery 31
5.6.1 Incident and compromise handling procedures 31
5.6.2 Computing resources, software, and/or data are corrupted 32
5.6.3 Business continuity capabilities after a disaster 32
5.7 Service's provider termination 32
6 Technical security controls 33
6.1 Cryptography, private key and its protection 33
6.2 Computer security controls 33
6.2.1 Specific computer security technical requirements 33
6.2.2 Computer security rating 33
6.3 Life cycle technical controls 35
6.3.1 System development controls 35
6.3.2 Security management controls 35
6.3.3 Life cycle security controls 35
6.4 Network security controls 35
6.5 Protection against fraud and theft of data 35

7 Conformity assessments and other assessments 37
7.1 Frequency or circumstances of assessment 37
7.2 Identity/qualifications of assessor 37
7.3 Assessor's relationship to assessed entity 37
7.4 Topics covered by assessment 37
7.5 Actions taken as a result of deficiency 37
7.6 Communication of results 37
8 Other business and legal matters 39
8.1 Fees 39
8.1.1 Service fees 39
8.1.2 Fees for other services 39
8.1.3 Refund policy 39
8.2 Financial responsibility 39
8.2.1 Insurance coverage 39
8.2.2 Other assets 39
8.2.3 Insurance or warranty coverage for end-entities 39
8.3 Confidentiality of business information 39
8.3.1 Scope of confidential information 39
8.3.2 Information not within the scope of confidential information 40
8.3.3 Responsibility to protect confidential information 40
8.4 Privacy of personal information 40
8.4.1 Privacy plan 40
8.4.2 Information treated as private 40
8.4.3 Information not deemed private 40
8.4.4 Responsibility to protect private information 40
8.4.5 Notice and consent to use private information 40
8.4.6 Disclosure pursuant to judicial or administrative process 41
8.4.7 Other Information disclosure circumstances 41
8.5 Intellectual property rights 41
8.6 Representations and warranties 41
8.6.1 CA Representations and warranties 41
8.6.2 Contact points representations and warranties 41
8.6.3 Representations and warranties of other participants 41
8.7 Disclaimers of warranties 41
8.8 Limitations of liability 42
8.9 Indemnities 42

8.10 Term and termination 43
8.10.1 Term 43
8.10.2 Termination 43
8.10.3 Effect of termination and survival 43
8.11 Individual notices and communications with participants 43
8.12 Amendments 43
8.12.1 Amending procedure 43
8.12.2 Notification mechanism and period 43
8.12.3 Circumstances under which OID must be changed 43
8.13 Disputes resolution provisions 43
8.14 Governing law 44
8.15 Compliance with applicable law 44
8.16 Miscellaneous provisions 44
8.16.1 Entire agreement 44
8.16.2 Assignment 44
8.16.3 Severability 44
8.16.4 Enforcement (attorneys' fees and waiver of rights) 44
8.16.5 Force Majeure 44
8.17 Other provisions 44
9 Final provisions 45

Table 1 – Document history

Version	Date of Release	Approved by	Comments
1.00	19 October 2022	CEO of První certifikační autorita, a.s.	First release.
1.01	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. Revision of text.
1.02	16 August 2025	CEO of První certifikační autorita, a.s.	Updates related to S/MIME BR.
1.03	25 August 2025	CEO of První certifikační autorita, a.s.	Formal errors correction.
1.04	12 September 2025	CEO of První certifikační autorita, a.s.	Error correction in chapter 1.2.

1 INTRODUCTION

This document determines the principles that První certifikační autorita, a.s., (hereinafter also I.CA) applies in accordance with applicable legal regulations and internationally recognized technical standards when providing the service of creating qualified electronic seals remotely (I.CA RemoteSeal, hereafter also the Service). The document also sets out the procedures for users of the Service (hereinafter referred to as the Client) relating to the issuance and management of the relevant qualified certificate (hereinafter referred to as the Certificate). The Client can be a legal person or a government authority.

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

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

The Service is provided to all Clients on the basis of a concluded contractual relationship. I.CA does not restrict potential Clients in any way, the provision of the service is non-discriminatory and the Service is accessible to persons with disabilities.

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 RemoteSeal Policy (Remote Creation of Electronic Seals)** is prepared by I.CA and 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 (seal) 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 aspects;
- 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 RemoteSeal Practice Statement ETSI TS 119 431-1 (also as Statement1) and I.CA RemoteSeal Practice Statement ETSI TS 119 431-2 (also as Statement2).

Note: This is English translation of the Policy, Czech version always takes precedence.

1.2 Document name and identification

Document's title:	I.CA RemoteSeal Policy (Remote Creation of Electronic Seals), version 1.04
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 sealing keys on SCDev; or **0.4.0.19431.1.1.3** (EU SSASC policy) - in case of storing sealing keys on QSCD.

1.2.1 Seal (signature) creation policy

A single signature creation policy is supported at any given time within the Service. It is implemented within the RSeC component located in a Client's environment, which securely communicates with 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 seal 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.

The input will be the choice of signature hash algorithm (SHA256/SHA384/SHA512).

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 seal, it is possible to choose from three variants:

- Text only (which thus fills the entire rectangle for a visible representation of the seal).

- Image only (which thus fills the entire rectangle for a visible representation of the seal).
- 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.

The input will be the choice of signature hash algorithm (SHA256/SHA384/SHA512).

XAdES

XAdES-B and XAdES-T according to the ETSI TS 103 171 standard, in the "enveloped" variant, while the input parameters are:

- An XML document that will be completely used as the input of the sealed data;
- Determination of the ID element to which the Signature element containing the newly created qualified electronic seal will be added as the last child element;
- Definition of required transformations, digest method and mimetype of referenced data for the Reference element with id="xadesReference";
- Choice of signature hash algorithm (SHA256/SHA384/SHA512).

ASiC-E XAdES

ASiC-E XAdES-B a ASiC-E XAdES-T according to the standard ETSI TS 103 174 standard, and:

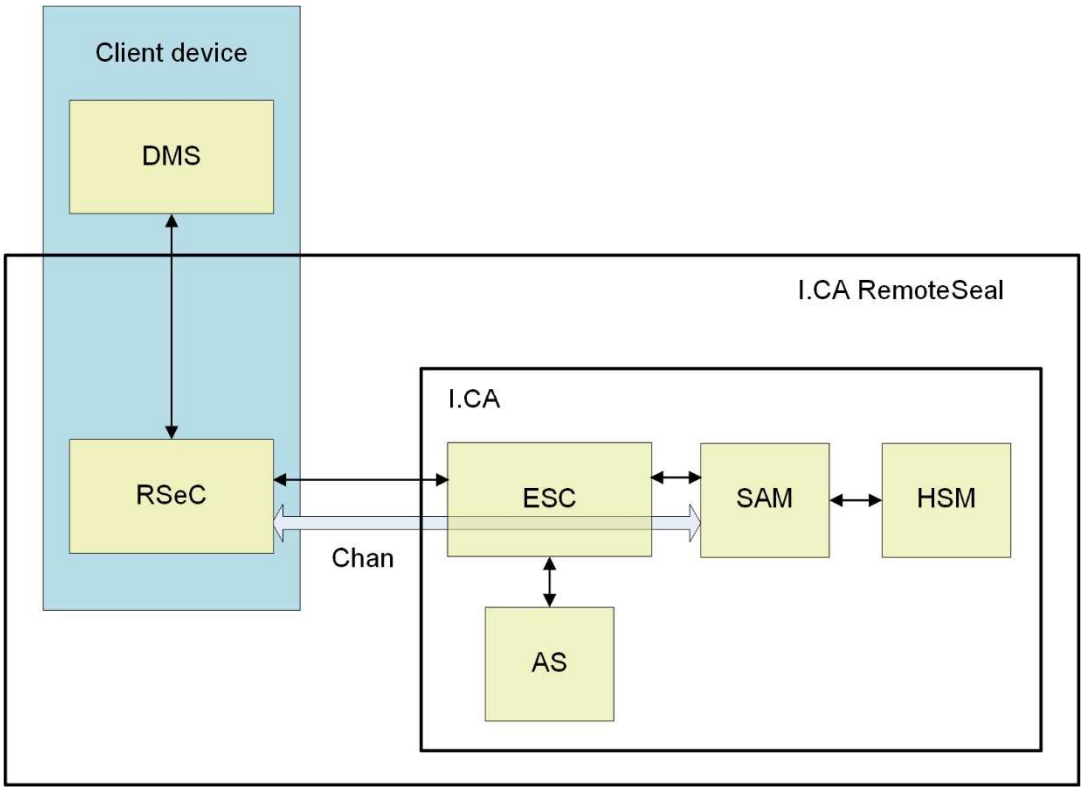
- It is possible to provide exactly one data object with exactly one qualified electronic seal;
- The extension of an existing ASiC-E file with another seal is not supported, nor are several seals within one ASiC-E file;
- For .txt, .pdf, .xml and .png files the appropriate mimetype corresponding to the given file type is added implicitly; this implicit choice can be explicitly reset in the interface to another mimetype, or it is possible to explicitly set the mimetype for other (implicitly unsupported) types of data objects;
- The XAdES seal inside the ASiC-E container contains only the minimum necessary set of signed and unsigned attributes required by the given ETSI standard;
- The input will be the choice of signature hash algorithm (SHA256/SHA384/SHA512).

1.2.3 Passing the parameters of the signature

Defining the signature parameters (PAdES/CAdES/XAdES/ASiC-E XAdES etc.) is a matter of Client's application, usually the document management service, which calls already mentioned RSeC component. This component then completes the electronic seal creation request of one or more documents and sends it to the Service provider.

1.2.4 Architecture of the Service

The architecture of the I.CA RemoteSeal service (remote creation of electronic seals) is shown in the following figure:



The following terms and abbreviations are used in the figure:

Term / Abbreviation	Description
AS	Authorization Server, the application server ensuring authentication of the end user (key owner) and the creation of a data structure for the SAM, which authorizes the use of the corresponding private key for the provision of the corresponding data with an electronic seal
DMS	Document Management System of the Client requiring the provision of document with an electronic seal
ESC	Evolved Signature Core, the basic application server operated by I.CA, through which all communication related to sealing from client components pass
HSM	Hardware Security Module, a mandatory component of the QSCD, a physical device that generates Client key pair, maintains a database of private keys and creates seals after successful identification and authentication of the Client
Chan	channel enabling secure communication of the RSeC application with the SAM module
RSeC	Remote Seal Connector, a client component intended for machine sealing of documents and for integration into a DMS or other system that needs to autonomously create qualified seals; exists in multiple variants for easy integration into different systems a component developed in I.CA, but operated in a third-party environment, used, among other things, for sending seal requests to

	the queue on the ESC server, and vice versa receiving AdES format seals from the ESC
SAM	Signature Activation Module, a mandatory QSCD component for the remote seal that provides access control to private sealing keys

Similar functionality, i.e. creating electronic seals remotely, but directly, not through the RSec component linked to the Client's file service, is also provided by the autonomous RemoteSealProFi application.

1.3 PKI Participants

1.3.1 Service provider

I.CA as the qualified trust service provider.

1.3.2 Contact points

Contact points:

- Accept applications for the Service, provide required information, handle complaints, etc.;
- Establish the Service, including the issuance of a qualified Certificate;
- Provide the necessary information, accept 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 on behalf of I.CA;
- Are authorized to charge for the I.CA services provided through contact point unless otherwise agreed in the Contract.

1.3.3 Relying parties

Any entity relying on qualified electronic seal 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 qualified electronic seal creation process 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.

1.5 Policy administration

1.5.1 Organization administering the document

This Policy and its Statements are administered by I.CA.

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 I.CA is the sole person responsible for making decisions about compliance of the procedures of I.CA as set out in Statements corresponding with this Policy.

1.5.4 Providing statement approval procedures

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

1.6 Definitions and acronyms

Table 2 – Definitions

Term	Explanation
Classified Information Protection Act	act of the Czech Republic no. 412/2005 Coll., on the protection of classified information and security eligibility
electronic seal	qualified electronic seal under trust services legislation
Labor Code	the Czech Republic's Act No. 262/2006 Coll., Labour Code, as amended
private key	unique data to create electronic signature / seal
public key	unique data to verify electronic signature / seal
remote electronic seal	electronic seal created using private key stored in device operated by I.CA; this private key is under sole control of the Client

Signature (seal) creation policy	a set of rules and limitations related to the electronic signatures (seals) being created
secure cryptographic environment	a QSCD type device (consisting of a SAM and an HSM) and a database of private keys encrypted in certified way (the encryption key is managed by the QSCD device), both operated in a physically secure environment
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 concerning trust services
written contract	text of the contract in electronic or paper form

Table 3 – Acronyms

Acronym	Explanation
AdES	Advanced Electronic Signature
ARC	Alarm Receiving Centre
ASiC-E	Associated Signature Container – Extended, container structure for binding signed/sealed data and external signature/seal into one file - container
CAdES	CMS Advanced Electronic Signature
CR	Czech Republic
ČSN	Czech Technical Norm
DMS	Document Management System, computerized system used to store, share, track and manage files or documents
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)
HSM	Hardware Security Module
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
PAdES	PDF Advanced Electronic Signature, type of electronic signature/seal
PDCA	Plan-Do-Check-Act, Deming cycle, management method for control and continuous improvement
QSCD	Qualified Signature/Seal Creation Device
SAM	Secure Access Module,
S/MIME BR	CA/Browser Forum document „Baseline Requirements for the Issuance and Management of Publicly-Trusted S/MIME Certificates"
TS	Technical Specification, type of ETSI standard
UPS	Uninterruptible Power Supply/Source
XAdES	XML Advanced Electronic Signature, type of electronic signature/seal
ZOOÚ	current personal data protection legislation

2 PUBLICATION AND REPOSITORY RESPONSIBILITIES

2.1 Repositories

I.CA 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 I.CA 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 approval and release of a new version;
- Practice statements of the Service – after approval and release of a new version;
- 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

The Service can be used by Clients who have concluded a valid Contract with I.CA. The rules stated in the following subsections also apply to the issuance of a qualified certificate (Certificate), which is an integral part of the Service.

3.1.1 Authentication of organization identity

To authenticate the Client's identity, 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 contact 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

The authorized person of the Client, hereinafter also the Person, is either listed in the Contract, or is equipped with an officially verified power of attorney to represent the Client signed by the Client's statutory representative. This Person is entitled to request the issuance of an initial authentication commercial certificate on a Starcos 3.5 and higher smartcard and automatically becomes the administrator of the sealing service of the given Client.

In the process of Person’s identity authentication, two documents are required, primary and secondary, containing the information listed below in this chapter.

Valid personal identity card or passport must be used as the primary personal document for the citizens of the Czech Republic or 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.

Valid personal identity card or passport must be used as the primary personal document for the citizens of the Czech Republic or 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).

The secondary document must contain a unique identification, such as birth identification 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;
- Photo of the face.

The secondary personal document data clearly identifying the Client must be identical to those in the primary personal document.

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

The extension of the Service takes place automatically in advance of the expiry of the original Certificate and can only be carried out by an authorized person of the Client, i.e. a Person.

3.3 Modification of data

If, due to data modification, it is not possible to extend the Service, an addendum to the contract must be concluded and a new authentication and sealing certificate must be issued.

3.4 Identification and authentication for revocation request

The entities authorized to request for Certificate revocation are listed in 4.8.

If the **Certificate revocation request is submitted to contact point by hand**, the request must be in writing and signed by a person who is either authorized to act on behalf of the Client by law, or is specified in the Contract, or is authorized to act on behalf of the Client by a person authorized to act on behalf of the Client by law. The identity of the person must be properly verified (see chapter 3.1.2).

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

- Using the form on the company's website (and using the Certificate revocation password);
- Using an electronically signed or sealed electronic message where:
  - The electronic signature/seal must be created with the private key belonging to the Certificate to be revoked;
  - Electronic message must be sent to revoke@ica.cz;
- Using an unsigned electronic message:
  - Electronic message must contain the Certificate revocation password; and
  - Electronic message must be sent to revoke@ica.cz;
- Using the data box of I.CA (and using the Certificate revocation password).

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

The data required for Certificate revocation request are listed in 4.9.

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

4 SERVICE LIFE CYCLE REQUIREMENTS

In chapters below the Service life cycle is described.

4.1 Conclusion of the contract

Before the establishment of the Service, the Agreement on the establishment and use of the Service must be signed between I.CA and the Client, the identity of the Client must be authenticated in accordance with the provisions of chapter 3.1.1. Subsequently, the Person can visit the contact point and request the establishment of the Service. The identity of the Person is authorized in accordance with the provisions of chapter 3.1.2.

4.2 Establishment of the Service

The establishment of the Service takes place at contact points, which are selected I.CA registration authorities. A Person with the necessary documents visits the contact point and, after authenticating his identity in accordance with the provisions of chapter 3.1.2, he is issued a personal authentication commercial certificate for a Starcos 3.5 or higher smartcard. The Person thereby automatically becomes the administrator of the sealing service for the given Client.

Subsequently, the contact employee establishes the I.CA RemoteSeal service, including the issuance of a Certificate for the given Client, while the key pair corresponding to this Certificate is generated on the QSCD of the I.CA RemoteSeal service, and the private key is further stored and managed in the relevant secure cryptographic environment.

As part of the issuance of the Certificate, the Person signs the documentation related to the issuance of the Certificate, which may be signed:

- Classically with handwritten signature on a paper document; or
- Paperless/electronically using the Person's personal authentication commercial certificate.

4.2.1 Enrollment process and responsibilities

The Person representing 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 seals (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;
- Inform immediately the Service provider on changes to the data specified in the Contract (and in the Certificate);
- 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);
- In case of a request to terminate the Service, it is the Person's duty to inform I.CA of this fact and, after mutual agreement, terminate the contract in the agreed form.

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.

4.3 Activation of the Service

The Client's organization can activate the Service on multiple devices; an access file and a password are created for each instance (account). The instance is created by the Person through the application (hereinafter also the Application), during the creation it is required to enter the name of the instance (for internal identification within the Client) and set the password. After completion, after selecting the directory, the access file used for authentication to the Service is saved.

4.4 Management of the Service

he management of the client application of the Service is carried out in the Application. Through it, the Person manages the client component for machine sealing of documents, i.e. adds, cancels, blocks, unblocks and renames user accounts, and also manages the issuance of the subsequent sealing certificate.

4.5 Extending the validity of the Contract

In advance of the expiration of the current sealing certificate (thirty, ten and five days), the Person is informed about the approaching end of the Certificate's validity by means of an automatically sent e-mail, the information is also displayed to the Person after logging into the Application. To issue a subsequent certificate, the Person must perform the following steps:

- Log in to the RemoteSealProFi application;

- Go to certificate administration;
- Press the "Renew certificate" button.

The application creates the subsequent certificate application and displays the details of the application. Further:

- The person presses the "Sign" button and enters their password to the Service;
- The Service subsequently ensures the issuance of a subsequent Certificate and, after its issuance, schedules its delayed deployment (fifteen days, or the number of days remaining until the end of validity of the original sealing certificate); Person can change the delay interval in the Application).

After issuing the Certificate, the Person can view information about the new Certificate in the application, save the new Certificate to a file and see the exact time of the planned deployment of the new Certificate.

4.6 Contract expiration

The validity of the Contract ends if the Client revokes the Certificate and this is listed on the CRL. Other possible ways of terminating the contractual relationship are defined by the Contract.

4.7 Certificate revocation and suspension

The Certificate is always revoked when the contract for the provision of the Service is terminated (e.g. the Person does not sign the application for the issuance of a subsequent certificate and it expires).

In addition to that, it is possible to request the revocation of the 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.

4.7.1 Circumstances for revocation

4.7.1.1 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.

4.7.1.2 Reasons to revoke the authority's certificate

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

1. Authority requests revocation in writing;
2. Authority notifies the root certification authority that original Certificate application was not authorized and does not retroactively grant authorization;
3. Root certification authority obtains evidence that the Authority's private key corresponding to the public key in the Certificate suffered a key compromise or no longer

complies with the cryptographic algorithm requirements and the required parameters (quality, see 6.1.5 and 6.1.6);

4. Root certification authority obtains evidence that Authority's certificate was misused;
5. Root certification authority is made aware that Authority's certificate:
   - □ Was not issued in compliance with S/MIME BR, corresponding CP or CPS; or
   - □ Does not meet requirements of S/MIME BR, corresponding CP or CPS;
6. I.CA determines that some information appearing in the Authority's certificate was inaccurate or misleading;
7. Root CA or Authority ceased operation for any reason a did not made arrangement for another CA to provide revocation support for certificates issued by them;
8. Root CA's or Authority's right to issue Certificate under S/MIME BR or 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.

4.7.2 Who can request revocation

Request for revocation may be submitted by:

- Provider of this Service (CEO of I.CA is the person authorized to request for revocation):
  - □ If the Certificate was issued on the basis of false data;
  - □ If establishes that the Certificate was issued in spite of non-compliance 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 went out of business or the data based on which the Certificate was issued are no more valid;
  - □ If the public key in the Certificate application is the same as the public key in a certificate already issued;
  - □ If demonstrably establishes that the private key (or authentication data for it) corresponding to the public key of this Certificate has been compromised;
  - □ If the Contract is terminated.
- Supervisory body and other entities as may be specified in trust services legislation.

Request for revocation may be also submitted by:

- Certificate subscriber (Client) through the Person;
- The subject explicitly specified therefore in the Service (under this Policy) contract;
- Person authorized to act on behalf of the legal successor of the Client;
- Entities permitted by applicable legislation through an authorized person.

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

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 see 4.7.3.

4.7.3 Submitting revocation request

Options for submission the request for revocation by the Client (subscriber) 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 sealed 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.]

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

    Message must be electronically sealed using private key corresponding with public key contained in the Certificate which should be revoked.

    If the request meets the requirements of the 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 requester 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.

I.CA reserves the right to accept other forms of procedures for the identification and authentication of requests for Certificate's revocation, which, however, must not be in conflict with the trusted services legislation.

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.

4.7.4 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.

4.8 Use of the Service

The procedure for providing documents with a qualified electronic seal is as follows:

- The DMS transfers to the RSeC component the access file, the password, the list of documents to be provided with an electronic seal and the required parameters of the seal (visible or invisible, format, with or without a time stamp) - by transferring the Client expresses undeniable consent to the content of the document, which will be provided with an electronic seal;
- The RSeC component prepares data structures according to the requirements of the standards (including hashes of sealed files, complete files are not transferred to the Service provider), authorizes the use of the private key stored in the HSM module;
- The RSeC component retrieves the created sealing structure including a possible time stamp;
- The RSeC component compiles complete document with an electronic seal and sends it back to DMS.

4.9 Additional security measures

For individual instances/accounts, it is possible to set additional security determining from where the given account can contact the Service (restriction to a certain VPN between the Client and I.CA, security of communication with a specific certificate, etc.).

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;
- Restoring these data.

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

I.CA 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 I.CA 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.;
- 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;
- Based on the decision of the supervisory body, the CEO of I.CA, or a person authorized by him, will decide on the next procedure.

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;
- EN 319 142 Electronic Signatures and Infrastructures (ESI); PAdES digital signatures.
- ETSI TS 103 171 Electronic Signatures and Infrastructures (ESI); XAdES Baseline Profile.
- ETSI TS 103 174 Electronic Signatures and Infrastructures (ESI); ASiC Baseline Profile.
- 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.

A report is drawn up on the course and result of the audit, which includes an evaluation of the compliance of the audited procedures with the requirements of the corresponding standards/specifications. In the deficiencies are found their degree of influence on the performance of service quality is quantified and appropriate corrective measures are proposed.

The final audit report is signed by the security manager, who then informs the members of the security committee about the results of the audit at the security committee meeting. In case of finding serious deficiencies (significant non-compliance), the security manager informs the members of the security committee as soon as possible.

8 OTHER BUSINESS AND LEGAL MATTERS

8.1 Fees

8.1.1 Service fees

The fee for using the Service is determined by the number of electronic seals created and the flat rate for the subscription band. Fees for issuing certificates or for issuing the smartcard are not charged separately.

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

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

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

8.2.2 Other assets

I.CA 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 I.CA 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 and from this Policy.

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

I.CA provides only the warranties as given in 8.6.

8.8 Limitations of liability

I.CA 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. I.CA 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 I.CA and the Client. The contract must not be in conflict with current legislation and must always take an electronic or printed form.

I.CA:

- 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 I.CA 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.

I.CA 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:

- Description of the defect that is as accurate as possible;
- 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 in effect no shorter than the Service is provided or this Policy is replaced with a new version.

8.10.2 Termination

CEO of I.CA is the sole person authorized to approve the termination of this Policy.

8.10.3 Effect of termination and survival

After the expiration of this Policy, obligations of I.CA resulting from it shall continue for the duration of the last Contract under which the Service is provided.

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 I.CA 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 and the Czech 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

I.CA 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 RemoteSeal Policy (Remote Creation of Electronic Seals) issued by První certifikační autorita, a.s., takes force and effect on the date mentioned above in Table 1.