První certifikační autorita, a.s.
(accredited provider of certification services)

POLICY FOR THE ISSUANCE

OF QUALIFIED TIMESTAMPS

Classification: public document

Version 3.0

Table 1 - Document History

Version	Date of Release	Approved by	Comments
3.0	Dec 22, 2009	CEO of První certifikační autorita, a.s.	The issuance of certificates with parameters meeting the requirements of the applicable legislation concerning the matters of hash functions (use of SHA-2 family algorithms) and the minimum length of an encryption key for the RSA algorithm (2048 bits). Acceptance of requirements resulting from the statement of the Ministry of the Interior of the Czech Republic regarding algorithms used in the field of timestamps.

Contents

1 Introduction

This document has been prepared to meet the requirements of the applicable legislation (referring to the recommendations of technical specifications ETSI[1] TS 102 176-1) concerning the matters of use of encryption algorithms in the process of creation of electronic signatures and algorithms used to create a hash in the generation of an application for a timestamp.

The document Policy for the Issuance of Qualified Timestamps, prepared by První certifikační autorita, a.s., deals with the issues relating to the processes of the issuance and use of qualified timestamps and is in accordance with:

- Act of the Czech Republic No. 227/2000 Coll. on electronic signatures and on the amendment to certain other acts (Electronic Signatures Act), as amended by Act No. 226/2002 Coll., Act No. 517/2002 Coll. and Act No. 440/2004 Coll., and related rules and regulations,
- Regulation of the Czech Republic No. 378/2006 Coll. on procedures of qualified providers of certification services, on requirements for electronic signature tools, and on requirements for the protection of data used to create electronic marks (Regulation on Procedures of Qualified Certification Service Providers),
- the current version of Act of the Slovak Republic No. 215/2002 Coll. on electronic signature and related implementing regulations,
- the recommendations ETSI TS 102 023 (Electronic Signatures and Infrastructures (ESI); Policy requirements for time-stamping authorities), RFC 3647 (internet X.509 Public Key Infrastructure, Certificate Policy and Certification Practices Framework) and ETSI TS 101861 (Time Stamping Profile) with regard to the recommendations of EU authorities and to the law order of the Czech Republic and of the Slovak Republic in the relevant field.

Read this document to make sure that the qualified timestamps issued by První certifikační autorita, a.s., meet your needs.

[1] European Telecommunications Standards Institute

2 Overview

Among other things, this document may be used by independent institutions as a basis for the confirmation of the fact that it is possible to regard the certification services provided by První certifikační autorita, a.s., as trustworthy.

První certifikační autorita, a.s., became:

- on March 18, 2002 – the first accredited provider of certification services in the Czech Republic for the field of issuance of **qualified certificates** under Act No. 227/2000 Coll. on electronic signatures and on the amendment to certain other acts (Electronic Signatures Act)), as amended by Act No. 226/2002 Coll., Act No. 517/2002 Coll. and Act No. 440/2004 Coll.,
- on February 1, 2006 – an accredited provider of certification services in the Czech Republic for the field of issuance of **qualified system certificates and qualified timestamps** under Act No. 227/2000 Coll. on electronic signatures and on the amendment to certain other acts (Electronic Signatures Act),), as amended by Act No. 226/2002 Coll., Act No. 517/2002 Coll. and Act No. 440/2004 Coll.,
- on September 21, 2006 – the first foreign qualified provider of certification services in the Slovak Republic, who has been given an accreditation for issuing of **qualified certificates and qualified timestamps** under the current version of Act No. 215/2002 Coll. (of the Slovak Republic) on electronic signature on the amendment to certain acts, as amended, and related implementing regulations.

The detailed description of the processes of a time-stamping authority is specified in other documents, which are generally non-public. Non-public documents, including reports, results of tests and internal inspections, form a documentation set that is available solely to the authorized personnel and auditors. Table 2 lists important security documents relating to certification services.

Table 2 - Security Documents

Number	Document Title	Status
1.	Policy for the Issuance of Qualified Timestamps	Public
2.	Certification Practice Statement for the Issuance of Qualified Timestamps	Non-public
3.	Report and Consent of the I.CA Management on the TSA Risk Assessment (including a risk analysis)	Non-public
4.	Statement of Applicability	Non-public
5.	TSA System Security Policy	Non-public
6.	Crisis Management Plan and Recovery Plan	Non-public
7.	TSA Disclosure Statement	Public
8.	set of security standards and guidelines	Non-public
9.	Corporate Security Policy	Non-public

The document Policy for the Issuance of Qualified Timestamps has been prepared at a general level. Technical details of the data communication system, company structure, operational procedures or technical protection are specified in relevant internal documents.

The issuance and administration of root certificates and TSU server certificates are governed by internal documents, the administration of which is governed by special documents in První certifikační autorita, a.s.

In the process of provision of certification services, První certifikační autorita, a.s., operates a single time-stamping authority, the basis of which is a set of qualitatively identical TSUs.

Information on other providers of certification services can be found at the website specified in Chapter 7.4.13.3.2.

2.1 Document Name and Identification

Title of this document:	Policy for the Issuance of Qualified Timestamps
OID:	1.3.6.1.4.1. 23624.1.1.50.3.0

3 Definitions and Abbreviations

The below glossary of definitions and abbreviations applies to this document. The abbreviations are of an alternative nature, i.e. both the full text and its abbreviation may be used in the text, and both of them shall be deemed to convey the same information.

3.1 Definitions

Table 3 - Definitions

Definition	Explanation
electronic signature, advanced electronic signature or electronic mark	data or information meeting the requirements of the applicable legislation[2]
qualified certificate, qualified system certificate	a certificate that meets the requirements defined by the applicable legislation
hash (fingerprint, …)	a transformation which receives, as an input, a string of characters of any length, and the result is a string of characters of fixed length
client	an applicant for a timestamp and/or relying party
qualified timestamp or timestamp	a data message issued by a qualified provider of certification service, which connects, in a trustworthy way, data in an electronic form to a moment of time and guarantees, that the data in the electronic form existed prior to that moment of time
key pair	unique data for the creation of an electronic signature or an electronic mark along with the corresponding data for the verification of an electronic signature or an electronic mark
private key	unique data for the creation of an electronic signature or electronic mark
relying party	an individual or legal entity relying, in its activities on a qualified certificate, qualified system certificate or a qualified timestamp issued by I.CA
public key	unique data for the verification of an electronic signature or an electronic mark
applicant for a timestamp, subscriber	an individual end user (individual), legal entity or government authority (comprising several end users) or a system operated by the above parties

3.2 Abbreviations

Table 4 - Abbreviations

Abbreviation	Explanation
CRL	**C**ertificate **R**evocation **L**ist
FAS	**Fire A**larm **S**ystem
HSM	**H**ardware **S**ecurity **M**odule (secure private key repository)
I.CA	První certifikační autorita, a.s. – accredited provider of certification services
MICR	**M**inistry of **I**nterior of the **C**zech **R**epublic
NIST	**N**ational **I**nstitute of **S**tandards and **T**echnology
NSASR	National Security Authority of the Slovak Republic
OID	Object Identifier (numerical identification of an object within the harmonized classification of objects under ISO/ITU)
PKI	**P**ublic **K**ey **I**nfrastructure
TSA	**T**ime **S**tamping **A**uthority
TSS	**T**ime **S**tamp **S**ervice

[2] See ESA.

Abbreviation	Explanation
TSU	**T**ime **S**tamp **U**nit
UTC	**C**oordinated **U**niversal **T**ime, a standard accepted on January 1, 1972 for the Coordinated Universal Time (UTC). The function of the "official timekeeper" of the atomic time for the whole world is performed by Bureau International de l'Heure (BIPM)
ESR	• Regulation of the Czech Republic No. 378/2006 Coll. on procedures of qualified providers of certification services, on requirements for electronic signature tools, and on requirements for the protection of data used to create electronic marks (Regulation on Procedures of Qualified Certification Service Providers • a set of Regulations of the Slovak Republic concerning the matters of the current version of Act of the Slovak Republic No. 215/2002 Coll. on electronic signature and on the amendment to certain other acts
ESA	• the current version of Act of the Czech Republic No. 227/2000 Coll. on electronic signatures and on the amendment to certain other acts (Electronic Signatures Act), as amended by Act No. 226/2002 Coll., Act No. 517/2002 Coll. and Act No. 440/2004 Coll. • the current version of Act of the Slovak Republic No. 215/2002 Coll. on electronic signature and on the amendment to certain acts

4 General Concepts

4.1 Time-Stamping Services

The services of the time-stamping authority operated by První certifikační autorita, a.s., include the fields of creation of qualified timestamps and implementation of authentication of applicants for timestamps, and are provided in accordance with ESA and ESR.

4.2 Time-Stamping Authority

From the point of view of the clients, a time-stamping authority is a trustworthy communication infrastructure issuing timestamps. První certifikační autorita, a.s., as the operator of the timestamping authority bears the overall responsibility for the provision of certification services.

4.3 Subscribers

An applicant for a timestamp may be an individual end user (individual), legal entity or government authority (comprising several end users) or a system operated by the above parties, acting under a written contract entered into with I.CA.

In the event that the applicant for a timestamp is an individual end user, this user shall be directly responsible for the performance of obligations to I.CA.

In the event that the applicant for a timestamp is a legal entity or government authority, its obligations to I.CA shall apply also to its end users, and the legal entity or government authority shall always be responsible for ensuring that its end users will perform its obligations to I.CA. The legal entity or government authority must therefore inform its own end users in an appropriate manner.

4.4 Relying Party

A relying party is any entity relying on the timestamp issued by I.CA.

5 Time-Stamp Policies

5.1 Use of Qualified Timestamps

This document does not define any restrictions on the use of timestamps issued in accordance with its content[3]. Timestamps may be used for example in the fields of:

- electronic signatures/marks, where it is necessary to verify that that they were created at the time when the certificate of the public key of the signing/marking entity was valid,
- protection of an executable code,
- transactions carried out on a network.

5.2 Compliance Audit and Other Assessment

I.CA performs assessments of security in the fields specified in Chapter 5.2.4. The assessments also include the monitoring of whether the standards specified in Chapter 7.4.7.2 are fully complied with. The areas of assessment are defined by an I.CA internal guideline.

5.2.1 Frequency or Circumstances of Assessment

With regard to the fact that První certifikační autorita, a.s., is an accredited provider of certification services, the frequencies of assessments, including the circumstances for the performance of assessments, are strictly defined by the requirements of ESA and ESR – this concerns in particular an audit of the information security management system, which is performed every two years, an inspection of security conformity performed every four years (overall inspection) or annually (partial inspection), and an audit of the security of the provision of certification activities (every year).

První certifikační autorita, a.s., reserves the right to perform other forms of assessment as well.

5.2.2 Identity / Qualification of the Assessor

The identity and qualification of the assessor performing an assessment required by ESA and ESR shall be defined by the applicable legislation, and in other cases the assessor shall be required to be certified for the relevant activities.

5.2.3 Assessor's Relationship to Assessed Entity

In the case of performance of an assessment required by ESA and ESR, the relation of the assessor to the provider of certification services is specified by the applicable legislation, and in other cases it shall be an external assessor.

5.2.4 Topics Covered by Assessment

In the event of performance of an assessment required by ESA and ESR, the assessed areas are defined by the applicable legislation, and in other cases the assessed areas shall be those specified in the standards under which the assessment is performed.

5.2.5 Actions Taken as a Result of Deficiency

The findings of all types of performed assessments shall be notified to the security manager, who shall ensure that any discovered deficiencies are corrected.

[3] Timestamps issued under this Policy may be used both in open systems of public services (for example in the state administration) and in closed systems of private businesses.

5.2.6 Communication of Results

The announcement of assessment results shall be performed in the form of a written final report, which shall be handed over by the assessor to the Chief Executive Officer or to the security manager of the company.

The security manager shall convene a meeting of the security committee as soon as possible. In addition to the company management, the meeting shall be attended by the heads of individual departments, and the security manager shall inform them of the results of the assessment.

The announcement of assessment results shall be also governed by the requirements of ESA and ESR.

6 Obligations and Liability

6.1 TSA Obligations

6.1.1 General

With regard to the service provided, První certifikační autorita, a.s., shall guarantee in particular:

- an access to TSA services:
  - continuous, with the exception of planned (notified in advance) or unplanned breakdowns (the circumstances are specified in the relevant internal documents) relating to technical procedures or
  - under the conditions agreed upon in a written contract,
- an authenticated access to the services of issuance of timestamps under a written contract,
- strict observance of the applicable legislation (ESA) governing the entire process of issuance of timestamps, including non-infringement of any copyright or license rights by the activities of the company,
- provision of certification services by persons having the proficiency and qualifications necessary for the provision of such certification services and being familiar with the relevant security procedures,
- use of secure systems and secure tools, safeguarding of sufficient security of the procedures that are supported by such systems and tools, including sufficient cryptographic security of such tools,
- sufficiency of financial resources or other financing methods for operation in accordance with the requirements defined by ESA and with regard to the risk of liability for damage during the whole time of its activities,
- written notification of an applicant for the issuance of timestamps of the exact conditions for the use of the service prior to the execution of the contract, including any restrictions on its use, and on the conditions for complaints and settlement of disputes, and on whether it is accredited or not,
- obligation of its own employees or other individuals being in contact with personal data to maintain the confidentiality of such information and the confidentiality of any data and security measures the disclosure of which would endanger the security of such information and data (the confidentiality obligation shall survive the termination of employment or any other similar relationship, as well as the completion of the relevant work.

6.1.2 TSA Obligations Towards Subscribers

První certifikační autorita, a.s., in particular guarantees that:

- the timestamps issued by it comply with all the requirements of ESA and ESR,
- it will use the private keys, corresponding to TSU certificates, only for the purposes of signing/marking issued timestamps,
- the data in the electronic form which are the subject of an application for the issuance of a timestamp clearly correspond to the data in the electronic form contained in the issued timestamp,
- it has implemented appropriate measures against the forgery of timestamps,
- it will issue a timestamp immediately after receiving a valid request,
- it does not verify, in any way, the hash to which the timestamp is to be allocated (with the exception of its length),
- it uses a trustworthy time synchronization,
- its response to an application for a timestamp contains at least:

- a serial number that is unique for the particular TSU of the TSA system,
- the identifier of the Policy under which the timestamp has been issued,
- a time specification corresponding to the value of the Coordinated Universal Time (UTC) at the time of the creation of the qualified timestamp with an accuracy of 1 second,
- the data in the electronic form contained in a timestamp corresponding to the data in the electronic form contained in the application for the issuance of the timestamp,
- an electronic signature/mark of TSU.

6.2 Subscriber Obligations

After the receipt of a response to an application for a timestamps, applicants are obligated to ascertain the status of the response. In the case of an error, the timestamp is not included in the response and the applicant must check the relevant error message. Otherwise the applicant must in particular:

- verify the validity of the electronic signature/mark of the timestamp and subsequently of all the certificates relating to the TSU which created the electronic signature/mark,
- verify that the returned hash is identical to that sent in the application,
- in the event, that the application contained the field “nonce” and/or the field “reqPolicy”, verify that its value is identical in the response.

6.3 Relying Parties Obligations

Relying parties are in particular obligated to verify:

- the issued timestamp – this concerns in particular the hash of the verified data, the validity of the electronic signature/mark (at the time of the creation of the electronic signature/mark) and whether the policy under which the timestamp was issued is acceptable for their needs or the needs of the applications operated by them,
- the security of the timestamp creation process with emphasis on the cryptographic functions for the creation of a hash, the length of an encryption key, and the algorithm for the creation of an electronic signature/mark.

6.4 Liability

Any warranties and performances thereunder may be recognized only if the applicant/subscriber or the relying party has not violated any obligation under this Policy. The warranties shall not apply to any timestamps not issued by I.CA.

7 Requirements on TSA Practices

7.1 Policy Administration

7.1.1 Organization Administering the Document

This Certification Policy and the relevant TSA Practice Statement are administered by První certifikační autorita, a.s.

7.1.2 Contact Person

The Chief Executive Officer of První certifikační autorita, a.s., shall specify the person, whose contact data are available at the Internet address (see Chapter 7.4.13.3.2).

7.1.3 Person Responsible for Decisions on Consistence of the Provider's Procedures with the Procedures of Other Providers of Certification Services

The only person that is responsible for decisions on consistence of the procedures of První certifikační autorita, a.s., with the procedures of other providers of certification services is the Chief Executive Officer of První certifikační autorita, a.s.

7.1.4 Procedure for the Approval of Compliance with Section 7.1.3

If it is necessary to amend this Policy and or to create a new version thereof, the Chief Executive Officer of První certifikační autorita, a.s., shall appoint a person authorized to perform such changes. Any new version of the Policy (specified in Chapter 8) must be, prior to its effective date, approved by the Chief Executive Officer of První certifikační autorita, a.s.

7.2 Key Management Life Cycle

The following chapters describe the comprehensive issue of the life cycle of key pair (public and private key) of a TSU. Specific technological procedures are described in the relevant internal documents of I.CA.

7.2.1 TSU Key Generation

7.2.1.1 Key Pair Generation

The generation of key pair, which takes place in a secured area in accordance with the TSA System Security Policy and the course of which is recorded in a written report, shall be carried out in an encryption module complying with ESA and ESR.

7.2.1.2 Public Key Delivery

The public keys used to verify electronic signatures/marks of issued timestamps are contained in a certificate of the relevant TSU. The certificate may be obtained via at least two independent channels:

- via the website of I.CA,
- via the website of MICR.

7.2.1.3 Key Sizes

I.CA uses exclusively the most credible classical asymmetric encryption algorithm – RSA. The size of the keys (or the parameters of the relevant algorithm) used for the signing/marking of issued timestamps is 2048 bits.

7.2.2 TSU Private Key Protection

The following chapters describe TSU issues. Specific technological procedure of the generation of TSU key pair and subsequent issuance of a TSU certificate, protection of private keys and procedures in the administration of TSU are described in the relevant internal documents of I.CA.

7.2.2.1 Cryptographic Module Standards and Controls

The private keys used to create electronic signatures/marks of issued timestamps are stored in an encryption module meeting the requirements of the FIPS PUB 140-2 Level 3 standard and of the applicable legislation.

7.2.2.2 Private Key (n out of m) Multi-Person Control

The protection by secret sharing is performed by the means of an encryption module. During the performance of individual sensitive activities related to the fundamental activities of I.CA, the presence of three authorized I.CA employees in trusted roles, two of whom know a part of the code necessary to perform such activities, is required.

7.2.2.3 Private Key Backup

The cryptographic module used for the administration and use of private keys for the creation of electronic signatures/marks of issued timestamps also allows their backups in an encrypted form.

7.2.2.4 Private Key Archival

Upon expiry of the term of the private keys designed for the electronic signing/marking of issued timestamps, the private keys and all their backups shall be destroyed. The archiving of the private keys is a security risk, and it is therefore prohibited in I.CA.

7.2.2.5 Private Key Transfer into or from a Cryptographic Module

The private keys used for the creation of electronic signatures/marks of issued timestamps are generated directly in the cryptographic module of the relevant TSU.

In the event of restoring the private keys from an encrypted backup, the insertion of the private keys used for the creation of electronic signatures/marks of issued timestamps into the cryptographic module of the relevant TSU shall take place in the direct personal presence of at least two designated employees of I.CA, and a written report shall be made with respect to the insertion of the private keys and signed by the designated employees of I.CA. At the time of the insertion, the TSU must be disconnected from the computer network.

7.2.2.6 Private Key Storage on Cryptographic Module

The private key used for the creation of electronic signatures/marks shall be stored in a secure manner in the cryptographic module meeting the requirements of the applicable legislation.

7.2.2.7 Activation Data

The activation data are created during the process of installation, when key pair used for the electronic signing/marking of issued timestamps is generated. They are designed exclusively for the processes of the provision of certification services and must not be transferred or archived in a clear form.

7.2.2.8 Method of Activating Private Key

The activation of the private keys used for the creation of electronic signatures/marks of issued timestamps, generated in the cryptographic module of the relevant TSU, shall be performed by the designated employees of I.CA through the activation of the cryptographic module itself and of an activation smart card in accordance with a specific procedure. A written report on the performance of the activation of the private keys shall be executed and signed by the designated employees of I.CA.

7.2.2.9 Method of Deactivating Private Key

The deactivation of the private keys used for the creation of electronic signatures/marks of issued timestamps shall be performed by the designated employees of I.CA through the cryptographic module and the activation smart card in accordance with a specific procedure. A written report on the performance of the deactivation shall be executed and signed by the designated employees of I.CA.

7.2.2.10 Method of Destroying Private Key

The private keys used for the electronic signing/marking of issued timestamps shall be stored in the cryptographic module. The destruction of the private keys shall be performed through the means of the cryptographic module. Private key backups, stored in an encrypted form on external media, shall also be destroyed. The destruction shall consist in the physical destruction of said media.

7.2.2.11 Public Key Archival

Public keys, used to verify the electronic signatures/marks of issued timestamps, are necessary for the trustworthiness and verification of the validity of issued timestamps. These keys are contained in the certificates of the relevant TSU. Unlike the corresponding private keys, it is important to archive public keys for the purposes of subsequent verification of issued timestamps.

7.2.3 Profile of a Certificate

The minimum length of key used for electronic signing/marking of issued timestamps is 2048 bits.

Table 5 - TSU Certificate Basic Fields

Field	Content
Version	v3
serialNumber	unique serial number of the issued certificate
SignatureAlgorithm	identifier of the algorithm used by I.CA for the electronic signature/mark of the issued certificate to the particular TSU (sha256WithRSAEncryption)
Issuer	identification of the issuer of the certificate (see Table 6)
Validity • NotBefore • NotAfter	 beginning of the term of the issued certificate (UTC) end of the term of the issued certificate (UTC)
Subject	identification of the subscriber (see Table 7)
SubjectPublicKeyInfo • Algorithm • SubjectPublicKey	 identifier of the algorithm used by the public key indicated in the issued certificate public key in the issued certificate (2048 bits)
Extensions	certificate extensions (see Table 8)

Table 6 - Issuer

Field	Content
Organization (O)	První certifikační autorita, a.s.
OrganizationUnitName(OU)	I.CA – Accredited Provider of Certification Services
CommonName (CN)	I.CA – Qualified Certification Authority, MM/YYYY
Country (C)	CZ

Note: MM/YYYY – the month and year of the issuance of the certificate.

Table 7 - Subject

Field	Content
Organization (O)	První certifikační autorita, a.s.
OrganizationUnitName (OU)	I.CA - Accredited Provider of Certification Services
CommonName (CN)	I.CA - Time Stamping Authority, TSS/TSU X, MM/YYYY
Country (C)	CZ

Note: X – TSU number; MM/YYYY – the month and year of the issuance of the certificate.

Table 8 - TSU Certificate Extensions

Field	Content	Critical
AutorityKeyIdentifier		NO

• KeyIdentifier	hash of public key of certificate issuer	
Subject Key Identifier	hash of public key of issued certificate	NO
[1] Certificate Policy • Policy • Explicit Text [2] Certificate Policy • Policy • Explicit Text	 see Chapter 7.2.3.1 see Chapter 7.2.3.2 see Chapter 7.2.3.1 see Chapter 7.2.3.2	NO
CRL Distribution Points	list of CRL distribution points accessible via http protocol	NO
Key Usage (critical)	Digital Sign, Non Repudiation	YES
ExtendedKeyUsage (critical)	id-kp-timeStamping	YES
Qualified Certificate Statements : 0.4.0.1862.1.1	esi4-QCStatement-1: Compliance with Annex I and II of EU Directive 1999/93/EC	NO
AuthorïtyInfoAccess	if the particular TSU issues timestamps complying both with legislation of the Czech Republic and legislation of the Slovak Republic this field shall contain http address of the file containing the certificates of NSASR, which can be used for verification of TSU certificate in accordance with the legislation of the Slovak Republic	NO

7.2.3.1 Certificate OID

[1] Certificate Policy.Policy : 1.3.6.1.4.1.23624.1.1.10.3.1

If the particular TSU issues qualified timestamps complying both with the legislation of the Czech Republic and the legislation of the Slovak Republic, the field **Certificate Policy** shall be extended by adding a mandatory attribute **Policy Identifier** with the value:

[2] Certificate Policy.Policy : 1.3.158.36061701.0.0.0.1.2.2

7.2.3.2 Policy Qualifiers Syntax and Semantics

The text of the user notice of the mandatory “Policy Qualifiers” extending field shall be as follows:

[1] Certificate Policy.Explicit Text: Tento certifikat je vydan jako kvalifikovany systemovy certifikat podle zakona c. 227/2000 Sb. v platnem zneni/This is qualified system certificate according to Czech Act No. 227/2000 Coll.

If the particular TSU issues qualified timestamps complying both with the legislation of the Czech Republic and the legislation of the Slovak Republic, the field **Certificate Policy** containing PolicyIdentifier for the Slovak Republic shall be extended by adding an optional attribute, this announcement:

[2] Certificate Policy.Explicit Text[4]: Tento kvalifikovany certifikat je vydan podle zakona Slovenske republiky c. 215/2002 Z.z. v platnem zneni./This is qualified certificate according to Slovak Act No. 215/2002 Coll.

7.2.4 Rekeying TSU's Key

In standard situations (expiry of the term of a certificate of the relevant TSU), the replacement of data for the verification of electronic signatures/marks in issued timestamps shall be sufficiently in advance prior to the expiry of the term of the certificate performed in the form of issuance of a new certificate of the relevant TSU. In the event of non-standard situations (for example in the event of a development of cryptanalytic methods that may endanger the security of the process of creation of electronic signatures/marks, i.e. a change in encryption algorithms, key length, etc.), the replacement shall be performed at the adequate time.

[4] Chief Executive Officer of I.CA shall, if needed, determine the use of this text.

Both in the event of standard and non-standard situations, the replacement of data for the verification of electronic signatures/marks in a certificate of the relevant TSU shall be notified to the general public in advance (if possible) and in an appropriate manner.

7.2.5 End of TSU Key Life Cycle

The term of the key pair (with the key size of 2048 bits) to be used for the electronic signing/marking of generated timestamps shall be at least 5 years.

The term of the data to be used for the verification of signed/marked timestamps shall be determined by the terms of the issued certificates of the relevant TSU. After the expiry of such term, the data for the verification of electronic signatures/marks may be used without any warranty.

In the event of a development of cryptanalytic methods that may endanger the security of the process of issuance of timestamps, the term of the key pair shall be shortened. In such a case, a procedure analogous to the procedure defined in Chapter 7.4.10.4 shall apply.

7.2.5.1 Certificate Revocation and Suspension

I.CA does not provide the service of certificate suspension.

7.2.5.1.1 Certificate Revocation List

The profile of a certificate revocation list shall be in accordance with the internationally recognized standards and regulations.

7.2.5.1.2 Circumstances for Revocation

A TSU certificate may be revoked only under the following circumstances:

- the situation defined in ESA and ESR occurs,
- the data for the creation of electronic signatures/marks used to sign/mark qualified certificates, qualified system certificates and certificate revocation lists have been compromised or there is a reasonable suspicion that the data have been compromised,
- the data for the creation of electronic signatures/marks of this particular TSU have been compromised or there is a reasonable suspicion that the data have been compromised

I.CA shall revoke the certificate of particular TSU on the initiative of:

- entities defined by applicable legislation,
- Chief Executive Officer of I.CA.

7.2.6 Life Cycle Management of the Cryptographic Module used to Sign Time-Stamps

The hardware of the relevant TSU (containing cryptographic module), which is connected to the infrastructure of trustworthy synchronization time, shall be delivered by the manufacturer (with the use of trustworthy freight forwarders) to the registered address of První certifikační autorita, a.s. In the process of receipt of the delivery, the correctness and integrity of the seals of the manufacturer's shipping container shall be inspected. After the receipt of the delivery, it shall be moved to the operational office, where another inspection of the seals of the shipping container shall be carried out, including the seals of the hardware itself. The TSU shall be stored in a safe place with a controlled access, and the basic installation including tests, synchronization and inspection shall follow. Each of the above activities shall be recorded in writing. The installation, initialization, inspection and synchronization of the TSU shall be performed by persons in credible roles and in the presence of witnesses. In the event of having the TSU hardware repaired or in the event of termination of the provision of certification services or in the event of termination of the activities of I.CA, the data for the creation of electronic signatures/marks of generated timestamps shall be destroyed as recommended by the manufacturer. Specific procedures of the TSU administration are described in the relevant internal documents of I.CA.

7.2.6.1 Cryptographic Module Rating

The cryptographic module used for the electronic signing/marking of issued timestamps meets the requirements for cryptographic modules defined in the document "Standard for the Assessment of Security of Encryption Modules Issued by the NIST in USA – FIPS PUB 140-2, Level 3".

7.3 Time-Stamping

7.3.1 Conclusion of a Contract

The issuance of qualified timestamps is a service commercially offered by I.CA to an individual, legal entity or government authority that has undertaken to act in accordance with this Policy under a written contract entered into in a manner that is usual in business relations.

7.3.2 Processing of an Application for a Qualified Timestamp

7.3.2.1 Identification and Authentication

With regard to the commercial basis and above-standard services in the process of issuance of timestamps, the process of identification and authentication of an applicant for a timestamp if carried out on the basis of a "commercial" certificate issued by I.CA.

I.CA reserves the right to use another method of identification and authentication of an applicant for a timestamp.

7.3.2.2 Acceptance or Rejection of an Application for a Qualified Timestamp

An applicant for the issuance of a timestamp shall create an authenticated connection with the communication server of the TSA system. In the event of unsuccessful connection, the transaction shall be terminated and the applicant shall be notified in an appropriate manner.

After the successful identification and authentication, the applicant shall generate an application for a timestamp (in the standard format according to RFC 3161). The generated data structure shall be handed over to the TSA system.

7.3.2.3 Time of Processing of an Application for a Qualified Timestamp

Unless otherwise agreed in a written contract, I.CA shall not define any fixed time limit within which an application for a timestamp is to be processed, since it is a sequence of the following activities, some of which depend only on the electronic transfer of an application from an applicant for a timestamp to the TSA system. Approximate time information is specified in the following list:

- generation of an application for the issuance of a timestamp on the part of the applicant – within seconds,
- generation of a timestamp on the part of the TSA system – within milliseconds.

7.3.3 Issuance of a Qualified Timestamp

7.3.3.1 Activities Performed by TSA during the Process of Issuance of a Qualified Timestamp

The TSA system shall perform all inspections of formal correctness of the application for a timestamp and use the result thereof to create a particular TSU response containing, if the result of the inspections is positive, a timestamp (see RFC 3161). The time information (UTC), the accuracy of which is 1 second during the creation of a timestamp, shall be obtained from a trustworthy clock. The response shall be electronically signed/marked with the data for the creation of an electronic signature/mark of the particular TSU (by this, the servers will guarantee beyond any doubt that the information indicated in the generated timestamp is correct).

Every response to an application for a timestamp containing, in addition to the above data, other required information (including information on the trustworthy clock) shall be located in the relevant repository of the TSA system.

7.3.3.2 Notification of Issuance of a Qualified Timestamp to the Applicant

After the activities specified in Chapter 7.3.3.1 have been carried out, the above data structure (with an accompanying report, if any) shall be sent back to the applicant by the TSA system.

7.3.4 Acceptance of a Qualified Timestamp

7.3.4.1 Applicant for a Timestamp

After the receipt of the above data structure, the applicant shall be obligated to ascertain the status of the response. If the response contains a timestamp, the applicant shall proceed in accordance with Chapter 6.2.

7.3.4.2 Relying Party

The verification of a timestamp by a relying party shall be carried out in the following steps:

- creation of the value hash_1 from the electronic data (message, document, transaction, etc.), which shall be compared against the value hash_2 contained in the timestamp,
- selection of the timestamp containing the value hash_2,
- comparison of the values hash_1 and hash_2.

In the event of discrepancy, the electronic data corresponding to the value hash_1 were modified. The relying party shall then proceed in accordance with Chapter 6.3.

7.3.5 Termination of the Provision of Services to an Applicant for a Qualified Timestamp

The provided certification service of the issuance of timestamps (business relationship) shall be terminated either by the applicant for a timestamp or by I.CA (if the applicant has failed to meet the conditions of the contract).

7.3.6 Structure of the Application, Response and Timestamp

The timestamps shall be generated by the relevant TSU upon receipt of an application.

7.3.6.1 Application

Table 9 - Application Format

Field	Description/Value	Note
Version	Version/1	mandatory field
messageImprint • HashAlgorithm • HashedMessage	 OID of hash algorithm/SHA1, SHA-256, SHA-512. Hash of the data for which a timestamp is requested (the length of this string must meet the requirements for the length of the selected algorithm.	mandatory field
reqPolicy	Policy identifier/ see Chapter 2.1.	optional field
Nonce	Random number/(64 bits) which is expected to be generated only once by the applicant.	optional field
certReq	Requirement for a TSU certificate: • TRUE – the response must contain a TSU certificate, • FALSE, or not specified - the response must not contain a TSU certificate.	mandatory field, in the event of issuing the timestamps in accordance with the legislation of the Slovak Republic the value must be TRUE

In the event of a development of cryptanalytic methods that may endanger the security of the creation of a hash in an application for a timestamp (see HashAlgorithm in Table 9), I.CA reserves the right

not to support the algorithm and to reject the application. Information on unsupported algorithms shall be published by I.CA on its website (see Chapter 7.4.13.3.2).

7.3.6.2 Response

The response to an application for a timestamp shall contain the status and, in the event of successful issuance, also a timestamp (see RFC 3161).

Table 10 – Responce Status

Field	Description	Value
PKIStatus	Number (integer), specifying the status of the response to an application for a timestamp. If the timestamp is included in the response, the value MUST be 0 or 1, and in the event of any other status value, the response MUST NOT contain a timestamp.	• 0 – issued • 1 – issued modified • 2 – application rejected • 3 – pending • 4 – threat of immediate revocation of the TSU certificate • 5 – TSU certificate revoked
PKIFailureInfo ::= BIT STRING {	BIT STRING – if the timestamp is not contained in the response, this field specifies the reason for the rejection of the application	• BadAlg (0) – unknown or unsupported algorithm • BadRequest (2) – unauthorized or unsupported transaction • BadDataFormat (5) – incorrect format of sent data • TimeNotAvailable (14) – unavailable source of time • UnacceptedPolicy (15) – TSA does not support the requested policy • UnacceptedExtension (16) – TSA does not support the requested extension • AddInfoNotAvailable (17) – the requested additional information have not been understood or are unavailable • SystemFailure (25) – the request could not be processed due to a system failure

Table 11 – Timestamp

Field	Description/Value
Version	version/1
Policy	policy identifier/see Chapter 2.1
messageImprint • HashAlgorithm • HashedMessage	the relevant field of the application for a qualified timestamp (see Table 9)/must have the same value as the corresponding field in the application
serialNumber	integer number under 160 bits/unique number assigned by the particular TSU
genTime	generalizedTime/time information corresponding to the UTC value at the time of the creation of the timestamp
Accuracy	accuracy/accuracy of the time information contained in the issued

	timestamp
Ordering	definition of the relation between two qualified timestamps/TRUE
Nonce	see Table 9/if it appears in the application, it must also appear in the response and must have the same value as the corresponding field in the application

7.3.7 Clock Synchronization with UTC

7.3.7.1 Synchronization

The synchronization of the clock with a trustworthy synchronization source of UTC shall be performed once a day. For the synchronization and verification of the time information included in generated timestamps, a commercial solution, which was already operated in EU (European Union), has been used. This solution is based on a model of trustworthy synchronization time infrastructure. This secure and irrefutable synchronization time service of a master clock provides valid and controllable information for the purposes of disputes between a provider of timestamps and his clients. The matters of synchronization are dealt with in internal documents.

7.3.7.2 Clock Security

The clock is located in secured premises of I.CA and its comprehensive security is dealt with in internal documents.

7.3.7.3 Clock Deviation Detection

The matters of deviation of the clock from the synchronization source of UTC are dealt with within the above commercial solution.

7.3.7.4 Leap Second

The matters of the occurrence of a leap second of the clock are dealt with within the above commercial solution.

7.4 TSA Management and Operation

7.4.1 Security Management

The structure of the security management in První certifikační autorita, a.s., is described in company's internal documents.

7.4.2 Risk Assessment and Management

The following activities have been carried out in I.CA:

- identification of assets (software, technical equipment, data) and their relations,
- evaluation of the information system assets,
- identification of threats and vulnerabilities,
- assessment of threats and vulnerabilities,
- calculation of the measure of risk for each combination of asset (group of assets), threat and vulnerability.

7.4.3 Vulnerability Assessment

The assessment of vulnerability is performed in První certifikační autorita, a.s., both on a regular basis and immediately (in the event of an incident having an impact on the security of the provided services).

7.4.4 Notification to Event-Causing Subject

In case of unauthorized attempts, the party shall not be informed about the inclusion of the event in an audit record.

7.4.5 Personnel Security

7.4.5.1 Trusted Roles

Trusted roles have been defined for certain activities carried out in I.CA. The roles are defined in internal documents together with the relevant activities and responsibilities.

7.4.5.2 Number of Persons Required per Task

For the activities specified below, the presence of at least three employees of I.CA is required:

- generation of TSU key pair,
- destruction of data for the creation of electronic signatures/marks of issued timestamps.

For the activities specified below, the presence of at least two employees of I.CA is required:

- backup/restore of data for the creation of the electronic signature/mark of each TSU issuing timestamps,
- activation of each TSU issuing timestamps,
- physical inspection of the operation of each TSU issuing timestamps.

The number of persons required to be present during the performance of other activities is not specified, but they must only be authorized employees.

7.4.5.3 Identification and Authentication for each Role

The employees of each role are given means for proper identification (name, certificate) and authentication (password, private key) for the components which are necessary for their activities.

7.4.5.4 Roles Requiring Separation of Duties

The roles requiring separation of duties in the process of the provision of certification services are defined in the internal security documentation.

7.4.5.5 Qualifications, Experience, and Clearances Requirements

I.CA's employees for trusted roles are selected and hired according to the staffing criteria described below:

- absolutely no criminal records – proven by a statement of criminal records or by an affirmation,
- university degree achieved in an accredited bachelor or master study program and at least three years experience in the field of information and communications technologies, or secondary education and at least five years' experience in the field of information and communications technologies, of which at least one year in the field of the provision of certification services,
- proficiency of the area of public key infrastructure and information security,
- in individual cases, the time period of the experience may be reduced by up to one third of the required length if the employee has passed an examination and proven sufficient knowledge required for his/her position.

Other I.CA's employees are hired according to the following criteria:

- university degree achieved in an accredited bachelor or master study program, or secondary education,
- basic knowledge of public key infrastructure and information security.

7.4.5.6 Background Check Procedures

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

- the employees themselves,

- persons who know the employees,
- public information sources.

Employees provide the initial information during a personal interview at the time of the hiring, and the information is updated in regular interviews with their superior employees taking place during the course of the employment.

7.4.5.7 Training Requirements

I.CA's employees are professionally trained in the use of the relevant software and of special devices. The training is carried out by the combination of the method of self-preparation and methodological leadership by a previously trained employee. The regular period of the training is one month.

7.4.5.8 Retraining Frequency and Requirements

At least once a year, I.CA organizes an internal learning seminar focusing on the issue of information security for its own employees.

7.4.5.9 Job Rotation Frequency and Sequence

Due to possibility of deputizing in exceptional cases, I.CA's employees are motivated to acquire knowledge required for the performance of a different role within I.CA.

7.4.5.10 Sanctions for Unauthorized Actions

In the event of discovery of an unauthorized activity, the relevant employee shall be treated in the manner defined in the company's internal documents and in accordance with the Labor Code (this procedure shall be without prejudice to any criminal proceedings, if initiated, if the seriousness of the discovered unauthorized activities substantiates this).

7.4.5.11 Independent Contractor Requirements

I.CA may or must ensure certain activities contractually. These business relationships are governed by bilateral commercial contracts. They include for example contractual registration authorities, creators of application software, hardware suppliers, system software suppliers, external auditors, etc. These parties are obligated to abide by the relevant public policies, by the relevant parts of I.CA's internal documents that have been provided to them, and by the relevant normative documents. In the event of violation of any obligation defined in said documents, contractual penalties shall be imposed or the contract entered into with the contractor shall be terminated with immediate effect.

7.4.5.12 Documentation Supplied to Personnel

In addition to the policy, the TSA practice statement and security and operational documents, I.CA's own employees shall be provided with any and all other standards, guidelines, manuals and instructions required for the performance of their duties and responsibilities.

7.4.6 Physical and Environmental Security

7.4.6.1 Site Location and Construction

Location of the operational office is geographically different from the location of the company head office, commercial and development offices, registration authority offices and business points.

Devices providing certification services are located in the restricted areas of the operational office. These areas are secured similarly to the secured areas of the "Confidential" security clearance.

7.4.6.2 Physical Access

The requirements for the physical access to restricted areas (protected by mechanical and electronic means) of the operational office are specified in the company's internal regulations. The structure is protected by an electronic security system (ESS), by connection to a centralized protection panel (CPP)

and by a special system for the monitoring, transmission and display of the movement of persons and vehicles.

7.4.6.3 Power and Air-Conditioning

In the areas dedicated for the performance of the certification services, there is sufficiently dimensioned active air-conditioning, which keeps the temperature at 20℃ ± 5℃ all year round. The pow er supply is backed-up by UPS (Uninterruptible Power Supply) or a diesel unit.

7.4.6.4 Water Exposures

All the critical systems of the operational office are located so as not to be flooded with a 100-year flood.

7.4.6.5 Fire Prevention and Protection

There is an automatic fire alarm system installed in the building of the operational office. The entrance door of the restricted areas, in which the devices providing certification services are located, is equipped with fireproof insulation. In the areas themselves, there is a fire extinguisher.

7.4.6.6 Media Storage

Storage media containing operational backups and records in an electronic form are stored in metal boxes or in the safe of Chief Executive Officer of I.CA.

Paper media which must be archived under ESA and ESR are stored in a location that is geographically different from the location of the operational office.

7.4.6.7 Waste Disposal

All office paper waste is shredded before leaving the premises of I.CA.

7.4.6.8 Off-Site Backup

Copies of operational and working backups are stored at a place specified by the Chief Executive Officer of I.CA.

7.4.7 Operations Management

7.4.7.1 Specific Computer Security Technical Requirements

The level of security of components used for the provision of certification services is defined by ESA and ESR.

A detailed solution of the specific technical requirements for computer security is described in the relevant internal documents.

7.4.7.2 Computer Security Rating

The security evaluation of I.CA is based on national and international standards:

- ETSI TS 102 023 – Electronic Signatures and Infrastructures - Policy Requirements for Time-Stamping Authorities.
- CWA 14167-1 - Security Requirements for Trustworthy Systems Managing Certificates for Electronic Signatures - Part 1: System Security Requirements.
- ETSI TS 101 456 - Electronic Signatures and Infrastructures (ESI); Policy Requirements for Certification Authorities Issuing Qualified Certificates.
- ČSN ISO/IEC 17799 - Information Technology – Code of Practice for Information Security Management.
- ČSN ISO/IEC 27001 – Information Technology – Security Techniques – Information Security Management Systems – Requirements.

- ČSN ISO/IEC TR 13335 – Information Technology – Guidelines for the Management of IT Security 1–3.
- ČSN EN ISO 19011 – Guidelines for Quality and/or Environmental Management Systems Auditing.

7.4.8 System Access Management

The internal subsystems of the TSA system are available only to authorized employees of I.CA, contractual partners and parties specified in the applicable legislation. The access to such information is governed by the rules defined in internal documents.

7.4.9 Trustworthy Systems Deployment and Maintenance

7.4.9.1 System Development Controls

The system development shall be governed by the relevant internal documents.

7.4.9.2 Security Management Controls

The process of inspections of security management is verified by regular audits of the information security management system and by inspections of the security of provided certification services.

7.4.9.3 Life Cycle Security Controls

The management of life cycle security is performed in I.CA by the procedural approach of "Plan-Do-Check-Act", which consists of several consecutive processes:

- establishing – definition of the security policy, plans, objectives, processes and procedures with regard to the risk management and security of information so as to make sure that they are consistent with the corporate security policy,
- implementation and operation – of the security policy, plans, objectives, processes and procedures,
- monitoring and reconsidering – evaluation of the process with regard to the security policy and handover of the findings to the company management for assessment,
- application – performance of remedial measures resulting from the decision of the company management.

7.4.10 Compromise of TSA Services

7.4.10.1 Incident and Compromise Handling Procedures

The procedures are defined in the internal document Crisis Management Plan and Recovery Plan.

7.4.10.2 Computing Resources, Software, and/or Data are Corrupted

In the event of damage to computer equipment, software or data, I.CA shall proceed in accordance with the internal document Crisis Management Plan and Recovery Plan and with any documents to which the Plan refers so as to assure the business continuity in the required time limit.

7.4.10.3 Clock Deviation

The synchronization of the clock is described in Chapter 7.3.7.1. If the discovered deviation from UTC is outside the interval defined at the time of the initialization of the TSU server, its activity shall be immediately terminated and the service of issuance of qualified timestamps shall not be provided until its new initialization. These matters are dealt with in I.CA's internal documents.

7.4.10.4 Entity Private Key Compromise Procedures

In the event of compromising of or in the event of occurrence of a reasonable concern regarding the compromising of the data for the creation of electronic signatures/marks for the signing/marking of qualified timestamps, I.CA shall:

- terminate the use thereof and provably revoke the certificate of the relevant TSU – it shall announce this, including the reason, at its website and a certificate revocation list shall also be used to make this information available,
- if possible, notify the relevant TSU subscribers of this TSU certificate revocation by sending them an e-mail message to the electronic addresses indicated by them in their applications for the issuance of a qualified timestamp – the notification shall also mention the reason for the revocation of the certificate of the relevant TSU,
- notify the relevant authority of the relevant TSU certificate revocation with specification of the reason for revocation,
- issue a new certificate to the relevant TSU.

7.4.10.5 Business Continuity Capabilities after a Disaster

In the event of a disaster, I.CA shall proceed in accordance with the internal document Crisis Management Plan and Recovery Plan and with any documents to which the Plan refers.

7.4.11 TSA Termination

In the event of planned termination of the activities of I.CA as a qualified provider of certification services, i.e. on grounds other than extraordinary events, such as strikes, civil unrests, war, natural disasters of a national scale or other results of force majeure, I.CA shall ensure that the following activities are carried out in accordance with the relevant legislations:

- in the event of the Czech Republic:
  - notify the relevant authority of its intention to terminate the activities of provision of certification services at least 3 months prior to the planned termination of the activities,
  - put forth maximum effort to ensure that the records kept under the applicable legislation are taken over by another qualified provider of certification services, and if it has not succeeded to hand the records over to another qualified provider of certification services, notify this at least 30 days prior to the planned date of termination of the activities to the relevant authority, and ensure that the records are handed over to the relevant authority – include this information in a message sent to all its clients that are holders of effective contracts on the provision of certification services, if this is known at least 2 months prior to the planned termination of the activities,
  - inform about the termination of I.CA's activities in the field of issuance of timestamps at its website at least 2 months prior to the planned termination of activities,
  - terminate the provision of certification services,
  - destruct its data for the creation of electronic signatures/marks used to sign/mark issued timestamps in a provable manner,
- in the event of the Slovak Republic:
  - notify the relevant authority of its intention to terminate the activities of provision of certification services at least 6 months prior to the planned termination of the activities,
  - notify each subscriber of its intention to terminate the activities of provision of certification services at least 6 months prior to the planned termination of the activities,
  - may agree with another qualified provider of certification services to take over the records on issued timestamps and the operational documentation – if no qualified provider of certification services takes over the records, the records shall be taken over by the authority.

The matters of planned termination of I.CA's activities as a qualified provider of certification services are specified in detail in I.CA's internal documents.

7.4.12 Compliance with Legal Requirements

TSA is operated in compliance with the applicable legislation, in particular ESA and ESR.

7.4.13 Recording of Information Concerning Operation of Time-Stamping Services

7.4.13.1 Audit Logging Procedures

The principles of creation, processing and storage or audit logs are described in the fundamental documents (see Table 2) and elaborated on in detail in specific internal security standards and guidelines.

7.4.13.1.1 Types of Events Recorded

With regard to the fact that I.CA is an accredited provider of certification services, all the events required by ESA and ESR are recorded in the process of the provision of such services.

All audit records shall be, to the necessary extent, created, stored and processed while maintaining the provability of the origin, integrity, availability, confidentiality and time authenticity thereof.

The audit system has been designed and operated in a way that guarantees the storage of audit data, reservation of sufficient space for audit data, automatic non-rewriting of the audit file, presentation of audit records to users in a suitable manner, and access to the audit file restricted only to defined users.

7.4.13.1.2 Frequency of Processing Log

Audit records are checked and assessed in the intervals defined in internal security documents, or immediately in the event of a security incident.

7.4.13.1.3 Retention Period for Audit Log

Unless the relevant legislation enacts otherwise, audit records shall be archived for at least 10 years after the creation thereof.

7.4.13.1.4 Protection of Audit Log

Audit records in an electronic and paper form are stored in a manner ensuring protection against any modification, theft or destruction thereof (whether intentional or unintentional).

Electronic audit records are stored in two copies. Each copy is located in a different room of I.CA's operational premises. At least once a month, the audit records are stored in a medium that is stored outside I.CA's operational premises.

Audit records in a paper form are stored outside I.CA's operational premises.

The protection of the above types of audit records is defined in internal security documents.

7.4.13.1.5 Audit Log Back Up Procedures

The backup of audit records is performed in a similar method as the backup of other electronic information. The backup of audit records in a paper form is not performed.

7.4.13.1.6 Audit Collection System (Internal vs. External)

The system of collection of audit records is internal in relation to I.CA, and external in relation to contractual partners.

7.4.13.2 Records Archival

The storage of information and documents is carried out by I.CA in accordance with the requirements of ESA. The principles of the storage of information and documents are described in the fundamental documents (see Table 2) and elaborated on in detail in specific internal security standards and guidelines.

7.4.13.2.1 Types of Records Archived

I.CA stores the following types of information and documents (in an electronic or paper form) relating to the provision of certification services, and in particular:

- subscriber agreements on the provision of certification service,
- audit records defined in Chapter 7.4.13.1.1 hereof,

- application software and all the company's documents that are necessary for the performance of inspections,
- issued timestamps, including applications for the issuance thereof,
- electronic or paper information required by ESA and ESR,
- all TSU certificates and certificate revocation lists,
- any and all information relating to TSU certificates, with the exception of the relevant data for the creation of an electronic signature/mark.

7.4.13.2.2 Retention Period for Archive

I.CA shall ensure that the information and documents specified in Chapter 7.4.13.2.2 are stored at least for 10 years since the creation thereof (unless otherwise provided).

7.4.13.2.3 Protection of Archive

Stored information and documents contain also the personal data of clients, and therefore because of the applicable legislation, the data are protected to a greater extent. The premises within which the stored information and documents are located are secured in the form of measured based on the requirements for structural and physical security.

Stored information and documents may only be used for I.CA's internal needs, and shall be available to:

- I.CA's employees in trusted roles,
- authorized supervisory authorities, authorities engaged in criminal proceedings and courts, if this is required by the applicable legislation.

A written record shall be made of each such authorized access.

The procedures for the protection of repositories of stored information and documents are defined in I.CA's internal documents.

7.4.13.2.4 Archive Backup Procedures

The procedures for the backup of stored information and documents are defined in I.CA's internal documents.

7.4.13.2.5 Requirements for Time-Stamping of Records

In the event that timestamps are used, these are qualified timestamps issued by I.CA.

7.4.13.2.6 Archive Collection System (Internal or External)

The issue of preparation and the method of storage of information and documents in an electronic or paper form are described in internal standards and regulations (see Chapter 7.4.13.2.4). The collection of stored information is filed.

7.4.13.2.7 Procedures to Obtain and Verify Archive Information

The workplaces where information and documents are stored keep a list thereof including the dates of their storage.

7.4.13.3 Publication and Repository Responsibilities

7.4.13.3.1 Repositories

With regard to the requirements of ESA, První certifikační autorita, a.s., establishes and operates repositories of information and documents, for which it is also responsible as a provider of certification services.

7.4.13.3.2 Publication of Certification Information

The primary addresses (hereinafter also referred to as "information addresses"), at which it is possible to find public information on První certifikační autorita, a.s. (certification policies, TSA disclosure

statements, other information specified in ESA and ESR, other public and up-to-date information and documents, etc.) or links to other sources of information, are as follows:

a) the registered address of the company:
První certifikační autorita, a.s.
Podvinný mlýn 2178/6
190 00 Prague 9
Czech Republic

b) the website http://www.ica.cz,

c) the registered addresses of registration authorities.

The contact address, used for the contact between clients or the general public and I.CA, is the electronic mail address tsa@ica.cz (clients and the general public may also send inquiries, comments or suggestions for improvement of the provided service to this electronic address).

I.CA publishes the contact addresses at its website. Designated employees of I.CA are also obligated to provide such information upon request to all potential clients. The same applies in the event of a change in the contact addresses.

The possibility of obtaining a certificate of a certification authority and TSU is guaranteed via the Internet address of I.CA and MICR or NSASR.

Information on CRL is available at the address http://www.ica.cz/. The following information is published directly (other information can be seen in the CRL):

- date of issuance of the CRL,
- CRL number,
- links to the locations where the CRL is available in the designated formats (DER, PEM, TXT).

The supported protocols for the access to the public information are HTTP, HTTPS and FTP. No other protocols are allowed. I.CA may terminate or suspend the access via any of the above protocols without giving reasons – in doing so, I.CA must abide by the relevant provisions of ESA and ESR. I.CA shall publish any such changes at its information addresses. Detailed information on the features and relevant specifications of the above protocols are published by I.CA at the same addresses.

In the event of termination of accreditation or in the event of a reasonable concern regarding the misuse of the data used for the creation of electronic signatures/marks of the issued timestamps, I.CA shall announce this at its on-line information address and through the nationally distributed daily newspaper.

7.4.13.3.3 Time or Frequency of Publication

With regard to the field of timestamps, I.CA shall publish information with the following frequency:

- policies – prior to the issuance of a first timestamp under the relevant policy,
- TSA disclosure statements – at the launching or modification of the provided certification service,
- acquisition or termination of accreditation – immediately,
- information on the revocation of the I.CA and TSU root certificate along with the reasons for the revocation (in the event of misuse or a reasonable concern that the data for the creation of electronic signatures/marks designed for the signing/marking of issued timestamps, certificates and certificate revocation lists might have been misuses) – immediately,
- other public information – not specified in advance, but in general, such information must reflect the current state of the provided certification services.

7.4.13.3.4 Access Controls on Repositories

All public information shall be made available by I.CA without any restrictions. Non-public information is available only to authorized employees of I.CA, contractual partners or the parties specified by

the applicable legislation. The access to such information is governed by the rules defined in internal regulations.

7.5 Other Business and Legal Matters

7.5.1 Fees

7.5.1.1 Qualified Timestamps Issuance Fees

Information on the fees for the issuance of qualified timestamps is available at the address tsa@ica.cz.

7.5.1.2 Provider's Certificates Access Fees

I.CA does not charge any fees for the access to the provider's certificates in an electronic way.

7.5.1.3 Revocation or Status Information Access Fees

I.CA does not charge any fees for the access to information about revoked certificates or about certificate statuses in an electronic way.

7.5.1.4 Fees for Other Services

Certificate revocation and downloading the electronic versions of policies (in the PDF format) is provided for free.

Fees for above-standard services are defined contractually.

7.5.1.5 Refund Policy

I.CA reserves the right to change the fee for the issuance of qualified timestamp. I.CA shall also have the right to determine different fees in individually concluded contracts.

7.5.2 Financial Responsibility

7.5.2.1 Insurance Coverage

První certifikační autorita, a.s., declares that it has an insurance policy covering business risks to such an extent so as to cover financial losses, if any.

7.5.2.2 Other Assets

První certifikační autorita, a.s., declares that it has sufficient financial resources and other assets ensuring the operation of the certification services in accordance with the requirements of ESA and corresponding to the risk of liability for damage.

Detailed information on the assets of První certifikační autorita, a.s., is available in the Annual Report of I.CA.

7.5.2.3 Insurance or Warranty Coverage for End-Entities

The service is not provided.

7.5.3 Confidentiality of Business Information

7.5.3.1 Scope of Confidential Information

Sensitive or confidential information of I.CA shall be in particular:

- data for the creation of electronic signatures/marks, corresponding to the data for the verification of electronic signatures/marks, contained in I.CA root certificates and in TSU certificates,
- data for the creation of electronic signatures/marks, corresponding to the data for the verification of electronic signatures/marks, contained in I.CA purpose certificates,

- other cryptographically significant information used for the operation of I.CA,
- selected business information of I.CA,
- any and all internal information and documents concerning the provision of certification services under ESA,
- any and all personal data.

7.5.3.2 Information not within the Scope of Confidential Information

Public information shall be in particular those types of information that do not belong to any of the groups specified in Chapter 7.5.3.1.

7.5.3.3 Responsibilities to Protect Confidential Information

Each employee being in contact with the information specified in Chapter 7.5.3.1 must not disclose them to any third party without the consent of the Chief Executive Officer of I.CA.

I.CA's employees or any other individuals who are in contact with personal data shall be obligated to maintain the confidentiality of such information and the confidentiality of any data and security measures the disclosure of which would endanger the security of such information and data. The confidentiality obligation shall survive the termination of employment or any other similar relationship, as well as the completion of the relevant work.

7.5.4 Privacy of Personal Information

7.5.4.1 Privacy Plan

The protection of personal data and other non-public information is dealt with in I.CA in accordance with the requirements of the applicable legislation.

7.5.4.2 Information Treated as Private

Private information shall be any and all personal data that are protected under the applicable legislation.

7.5.4.3 Information not Deemed Private

In general, non-confidential data shall be the data published in the manner specified in Chapter 7.4.13.3.2.

7.5.4.4 Responsibility to Protect Private Information

The protection of personal data and other non-public information is the responsibility of I.CA.

7.5.4.5 Notice and Consent to Use Private Information

The issues of notification of the use of confidential information and of the consent to the use of sensitive information are dealt with in I.CA in accordance with the requirements of the applicable legislation.

7.5.4.6 Disclosure Pursuant to Judicial or Administrative Process

The provision of sensitive information for judicial or administrative purposes is dealt with in I.CA in accordance with the requirements of the applicable legislation.

7.5.4.7 Other Information Disclosure Circumstances

In the event of disclosure of personal data, I.CA shall strictly abide by the requirements of the applicable legislation.

The persons specified in Chapter 7.5.3.3 may be relieved of the confidentiality obligation by the party in the interest of which they are so obligated or by a court of law.

7.5.5 Intellectual Property Rights

This document, all related documents, the content of websites, CA certificates, I.CA keys and the procedures ensuring the operation of the system providing the certification services are protected by the copyright of První certifikační autorita, a.s., and represent its significant know-how.

7.5.6 Representations and Warranties

7.5.6.1 I.CA Representations and Warranties

I.CA above all represents and warrants that:

- it shall use the private keys corresponding to I.CA signing certificates only for the purposes of the signing/marking of the issued certificates and certificate revocation lists,
- it shall use the private keys corresponding to TSU certificates only for the purposes of the signing/marking of the issued timestamps,
- the issued certificates and timestamps meet the requirements defined in ESA and ESR, under which the accreditation was granted.

Any representations and warranties and performances thereunder may be recognized only if:

- subscriber has not violated any obligation under the contract subscriber agreement on the provision of certification services and under this document,

the relying party has not violated any obligation under this document.

7.5.6.2 Subscriber Representations and Warranties

Subscriber for a qualified timestamp shall guarantee the correctness of the information provided by them in the contract subscriber agreement on the provision of qualified timestamps and shall act in accordance with the applicable legislation and this Policy

7.5.6.3 Relying Parties Representations and Warranties

The relying parties shall act in accordance with the applicable legislation and this Policy, in particular the provisions of Chapter 6.2.

7.5.6.4 Representations and Warranties of Other Participants

The service is not provided.

7.5.7 Disclaimers of Warranties

První certifikační autorita, a.s., strictly abides by ESA and cannot disclaim the representations and warranties defined therein.

7.5.8 Indemnities

In the process of the provision of certification services, the representations and warranties agreed between První certifikační autorita, a.s., and the applicant for a particular service shall apply. The contract must not be contrary to the applicable legislation and must always be in writing.

První certifikační autorita, a.s.:

- undertakes that it will perform all the obligations defined both in the applicable legislation and in the relevant certification policies of I.CA reflecting the issues of the issuance of qualified timestamps,
- grants the above representations and warranties for the entire term of the contract subscriber agreement on the provision of certification services entered into with the customer,
- does not grant any representations and warranties other than those above.

Other possible damages shall result from the provisions of the applicable legislation and their amounts may be determined by a court

První certifikační autorita, a.s., **shall not be liable for**:

- any shortcomings in the provided services occurred as the result of incorrect or unauthorized use of the services provided as part of the performance of the contract on the provision of certification services by subscriber, in particular for the operation contrary to the terms and conditions specified in the certification policy, as well as for any shortcomings occurred as a result of force majeure, including a temporary downtime of telecommunications connection, etc.

A justified complaint may be filed in the following ways:

- by e-mail to the address reklamace@ica.cz,
- by a registered letter sent to the registered address:
  - První certifikační autorita, a.s., Podvinný mlýn 2178/6, 190 00 Prague 9, Czech Republic.

The person filing a complaint must provide:

- the contract number,
- the receipt number,
- an in-depth description of the shortcomings and their implications.

Obligations of I.CA:

I.CA shall decide a complaint at the latest within three business days after the delivery of the complaint, and shall notify the complainant of the decision (in the form of an electronic mail or a registered letter), unless otherwise agreed between the parties

A complaint, including defects and errors, shall be disposed of without unreasonable delay, but no later than one month after the filing of the complaint, unless otherwise agreed between the parties.

7.5.9 Term and Termination

7.5.9.1 Term

This document shall enter into force on the date indicated in Chapter 8 and shall continue in force until the termination thereof.

7.5.9.2 Termination

The only person entitled to approve amendments to this Policy and to determine its conformity with the relevant TSA practice statement shall be the Chief Executive Officer of První certifikační autorita, a.s.

7.5.9.3 Effects of Termination and Survival

Specified in Chapter 7.5.9.1.

7.5.10 Individual Notices and Communications with Participants

For the individual notifications and communication with the clients, I.CA may use the e-mail addresses, mail addresses or telephone numbers provided by them, or discuss in person.

Subscribers, relying parties and the general public may communicate with I.CA in the methods specified at http://www.ica.cz/.

7.5.11 Amendments

7.5.11.1 Procedure for Amendment

The procedure is implemented in a controlled process, specified in an internal document of I.CA.

7.5.11.2 Notification Mechanism and Period

The procedure is implemented in a controlled process, specified in an internal document of I.CA.

7.5.11.3 Circumstances under which OID Must Be Changed

A new OID shall be assigned in the event of a release of a new version of this document.

7.5.12 Dispute Resolution Provisions

This document and the relevant TSA practice statement and the interpretation and application thereof shall be governed by ESA and ESR.

In the event that a subscriber and/or a relying party do not agree to the presented interpretation, they may use the following levels of appeal:

- the responsible employee of I.CA (a submission in writing is mandatory),
- the Chief Executive Officer of I.CA (a submission in writing and payment of a financial security, which will be returned in the event of a positive disposal of the complaint, is mandatory).

The above procedure gives a disagreeing party an opportunity to have their opinion heard in a way that is quicker than legal proceeding.

7.5.13 Governing Law

The business activities of První certifikační autorita, a.s., are governed by the laws of the Czech Republic.

7.5.14 Compliance with Legal Requirements

The system of provision of certification services is carried out in compliance with the requirements of ESA.

7.5.15 Miscellaneous Provisions

7.5.15.1 Entire Agreement

These matters are irrelevant for the application of the release of this document.

7.5.15.2 Assignment

These matters are irrelevant for the application of the release of this document.

7.5.15.3 Severability

These matters are irrelevant for the application of the release of this document.

7.5.15.4 Waiver of Rights

These matters are irrelevant for the application of the release of this document.

7.5.15.5 Force Majeure

The contract on the provision of certification services may contain provisions concerning force majeure.

7.5.16 Other Provisions

These matters are irrelevant for the application of the release of this document.

8 Final Provisions

This document, issued by První certifikační autorita, a.s., shall enter into force and effect on December 22, 2009.