První certifikační autorita, a.s.

Policy

for Issuing Qualified Electronic Time-Stamp

Tokens by TSA2 System

(RSA algorithm)

Version 2.04

OBSAH

1 Introduction 9
1.1 Overview 9
1.2 Document name and identification 10
1.3 Participants 10
1.3.1 Time stamp authority 10
1.3.2 Time-stamp token requestors 10
1.3.3 Relying parties 10
1.3.4 Other participants 11
1.4 Time-stamp token usage 11
1.4.1 Appropriate certificate uses 11
1.4.2 Prohibited certificate uses 11
1.5 Policy administration 11
1.5.1 Organization administering the document 11
1.5.2 Contact person 11
1.5.3 Person determining Statement suitability for the Policy 11
1.5.4 Statement approval procedures 11
1.6 Definitions and acronyms 11
2 Publication and repository responsibilities 15
2.1 Repositories 15
2.2 Publication of information 15
2.3 Time or frequency of publication 16
2.4 Access controls on repositories 16
3 Identification and authentication 17
3.1 Naming 17
3.1.1 Types of names 17
3.1.2 Need for names to be meaningful 17
3.1.3 Anonymity or pseudonymity of subscribers 17
3.1.4 Rules for interpreting various name forms 17
3.1.5 Uniqueness of names 17
3.1.6 Recognition, authentication, and role of trademarks 17
3.2 Initial identity validation 17
3.2.1 Method to prove possession of private key 17
3.2.2 Authentication of organization identity 17
3.2.3 Authentication of individual identity 17

3.2.4 Non-verified subscriber information 18
3.2.5 Validation of authority 18
3.2.6 Criteria for interoperation 18
3.3 Identification and authentication for routine re-key 18
3.3.1 Identification and authentication for routine re-key 18
3.3.2 Identification and authentication for re-key after revocation 18
3.4 Identification and authentication for revocation request 18
4 Time-stamp tokens life-cycle operational requirements 19
4.1 Entering into the contract 19
4.2 Processing time-stamping request 19
4.2.1 Performing identification and authentication functions 19
4.2.2 Approval or rejection of time-stamping request 19
4.2.3 Time to process time-stamping request 19
4.3 Issuing time-stamp token 20
4.3.1 Time stamp authority actions during time-stamp token issuance 20
4.3.2 Notification to requestor by the TSA of issuance of time-stamp token 20
4.4 Time-stamp token acceptance 20
4.4.1 Time-stamp token requestor's obligations 20
4.4.2 Relying parties' obligations 20
4.5 Time-stamp token issuance termination for specific requestor 20
4.6 TSU pair data and their validity period 20
4.6.1 Key changeover 20
4.6.2 TSU certificate revocation 21
4.7 Time source synchronization with UTC 21
4.7.1 Synchronization 21
4.7.2 Time source security 21
4.7.3 Time source inaccuracy detection 21
4.7.4 Leap second 21
5 Facility, management, and operational controls 22
5.1 Physical controls 22
5.1.1 Site location and construction 22
5.1.2 Physical access 22
5.1.3 Power and air conditioning 22
5.1.4 Water exposures 22
5.1.5 Fire prevention and protection 23
5.1.6 Media storage 23

5.1.7 Waste disposal 23
5.1.8 Off-site backup 23
5.2 Procedural controls 23
5.2.1 Trusted roles 23
5.2.2 Number of persons required per task 23
5.2.3 Identification and authentication for each role 24
5.2.4 Roles requiring separation of duties 24
5.3 Personnel controls 24
5.3.1 Qualifications, experience, and clearance requirements 24
5.3.2 Background check procedures 24
5.3.3 Training requirements 25
5.3.4 Retraining frequency and requirements 25
5.3.5 Job rotation frequency and sequence 25
5.3.6 Sanctions for unauthorized actions 25
5.3.7 Independent contractor requirements 25
5.3.8 Documentation supplied to personnel 25
5.4 Audit logging procedures 25
5.4.1 Types of events recorded 25
5.4.2 Frequency of processing log 26
5.4.3 Retention period for audit log 26
5.4.4 Protection of audit log 26
5.4.5 Audit log backup procedures 26
5.4.6 Audit collection system (internal vs. external) 26
5.4.7 Notification to event-causing subject 26
5.4.8 Vulnerability assessments 26
5.5 Records archival 27
5.5.1 Types of records archived 27
5.5.2 Retention period for archive 27
5.5.3 Protection of archive 27
5.5.4 Archive backup procedures 27
5.5.5 Requirements for time-stamping of records 27
5.5.6 Archive collection system (internal or external) 27
5.5.7 Procedures to obtain and verify archive information 28
5.6 Key changeover 28
5.7 Compromise and disaster recovery 28
5.7.1 Incident and compromise handling procedures 28

5.7.2 Computing resources, software, and/or data are corrupted 28
5.7.3 Entity private key compromise procedures 28
5.7.4 Business continuity capabilities after a disaster 29
5.8 TSA termination 29
6 Techical security controls 30
6.1 Key pair generation and installation....30
6.1.1 Key pair generation 30
6.1.2 Private key delivery to its owner 30
6.1.3 Public key delivery to certificate issuer 30
6.1.4 TSU's public key delivery to relying parties....30
6.1.5 Key sizes....30
6.1.6 Public key parameters generation and quality checking....30
6.1.7 Key usage purposes (as per X.509 v3 key usage field) 31
6.2 Private Key Protection and Cryptographic Module Engineering Controls....31
6.2.1 Cryptographic module standards and controls....31
6.2.2 Private key (n out of m) multi-person control....31
6.2.3 Private key escrow 31
6.2.4 Private key backup 31
6.2.5 Private key archival 31
6.2.6 Private key transfer into or from a cryptographic module 31
6.2.7 Private key storage on cryptographic module 32
6.2.8 Method of activating private key 32
6.2.9 Method of deactivating private key 32
6.2.10 Method of destroying private key 32
6.2.11 Cryptographic module rating....32
6.2.12 Cryptographic module used when time-stamp tokens are created transport....32
6.3 Other aspects of key pair management....32
6.3.1 Public key archival....32
6.3.2 Certificate operational periods and key pair usage periods....32
6.4 Activation data....33
6.4.1 Activation data generation and installation....33
6.4.2 Activation data protection 33
6.4.3 Other aspects of activation data 33
6.5 Computer security controls....33
6.5.1 Specific computer security technical requirements 33
6.5.2 Computer security rating....33

6.6 Life cycle technical controls 34
6.6.1 System development controls 34
6.6.2 Security management controls 34
6.6.3 Life cycle security controls 35
6.7 Network security controls 35
6.8 Time-stamping 35
7 TSU certificate profile, structures of time-stamping request, time-stamping response 4and time-stamp token 36
7.1 Profile and structures 36
7.1.1 Version number(s) 42
7.1.2 Algorithm object identifiers 42
8 Compliance audits and other assessments 43
8.1 Frequency or circumstances of assessment 43
8.2 Identity/qualifications of assessor 43
8.3 Assessor's relationship to assessed entity 43
8.4 Topics covered by assessment 43
8.5 Actions taken as a result of deficiency 43
8.6 Communication of results 43
9 Other business and legal matters 45
9.1 Fees 45
9.1.1 Time-stamp token issuance fees 45
9.1.2 Provider's certificates access fees 45
9.1.3 Revocation or status information access fees 45
9.1.4 Fees for other services 45
9.1.5 Refund policy 45
9.2 Financial responsibility 45
9.2.1 Insurance coverage 45
9.2.2 Other assets 45
9.2.3 Insurance or warranty coverage for end-entities 46
9.3 Confidentiality of business information 46
9.3.1 Scope of confidential information 46
9.3.2 Information not within the scope of confidential information 46
9.3.3 Responsibility to protect confidential information 46
9.4 Privacy of personal information 46
9.4.1 Privacy plan 46
9.4.2 Information treated as private 46
9.4.3 Information not deemed private 46

9.4.4 Responsibility to protect private information....47
9.4.5 Notice and consent to use private information....47
9.4.6 Disclosure pursuant to judicial or administrative process....47
9.4.7 Other information disclosure circumstances....47
9.5 Intellectual property rights....47
9.6 Representations and warranties....47
9.6.1 TSA representations and warranties....47
9.6.2 RA representations and warranties....49
9.6.3 Time-stamp token requestor and owner representations and warranties....49
9.6.4 Relying party representations and warranties....49
9.6.5 Representations and warranties of other participants....49
9.7 Disclaimers of warranties....49
9.8 Limitations of liability....49
9.9 Indemnities....50
9.10 Term and termination....51
9.10.1 Term....51
9.10.2 Termination....51
9.10.3 Effect of termination and survival....51
9.11 Individual notices and communications with participants....51
9.12 Amendments....51
9.12.1 Procedure for amendment....51
9.12.2 Notification mechanism and period....51
9.12.3 Circumstances under which OID must be changed....51
9.13 Dispute resolution provisions....52
9.14 Governing law....52
9.15 Compliance with applicable law....52
9.16 Miscellaneous provisions....52
9.16.1 Entire agreement....52
9.16.2 Assignment....52
9.16.3 Severability....52
9.16.4 Enforcement (attorneys' fees and waiver of rights)....52
9.16.5 Force majeure....52
9.17 Other provisions....53
10 Final provisions....54

Table 1 - Document history

Version	Date of Release	Approved by	Comments
2.00	13 April 2017	CEO of První certifikační autorita, a.s.	First release.
2.01	30 April 2019	CEO of První certifikační autorita, a.s.	Revision, formal errors correction.
2.02	9 December 2019	CEO of První certifikační autorita, a.s.	More specific text.
2.03	1 April 2020	CEO of První certifikační autorita, a.s.	Time-stamp token containing announcement that it is the qualified electronic time-stamp token issued in compliance with eIDAS. SHA1 in time-stamping request no longer supported.
2.04	15 May 2020	CEO of První certifikační autorita, a.s.	Document structured according to RFC 3647.

1 INTRODUCTION

This document **Policy for Issuing Qualified Electronic Time-Stamp Tokens by TSA2 System (RSA algorithm)** - also as Policy - prepared by První certifikační autorita, a.s., in compliance with requirements of relevant legislation deals with the issues related to processes of issuing and utilization of qualified electronic time-stamp tokens (also as Service, time-stamp token) and includes all requirements of BTSP policy (Best practices Time-Stamp Policy) stated in the document EN 319421 Electronic Signatures and Infrastructures (ESI); Policy and Security Requirements for Trust Service Providers issuing Time-Stamps. Legal requirements concerning 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;
- Act of the Czech Republic No. 297/2016 Coll., on trust services for electronic transactions, and
- Act of the Slovak Republic No. 272/2016 Coll. on trust services for electronic transactions in the internal market and on amendments to certain laws (trust services act).

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

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

More details on Time Stamp Authority may be provided in the document Practice Statement for Issuing Qualified Electronic Time-stamp Tokens by TSA2 System (RSA algorithm) - also as Statement.

1.1 Overview

This Policy describes issuing of time-stamp token at a general level, more details are contained in internal documentation. Policy is divided into ten chapters their brief description is as follows:

- Chapter 1 identifies this document, generally describes the entities and individuals taking part in the provision of the Services, and defines the acceptable usage of the certificates available to be issued;
- Chapter 2 deals with the responsibility for the publication and information or documents;
- Chapter 3 describes processes of identification and authentication for TSU certificate applicant, refers to the document Certifikační politika vydávání kvalifikovaných certifikátů pro elektronickou pečeť systému TSA2 (algoritmus RSA)[1] - hereinafter as CP.

[1] CP not translated on the day of this Policy's release.

- Chapter 4 defines life cycle processes of issued time-stamp tokens, i.e. entering into a contract, processing time-stamping request, issuing time-stamp token and termination providing the Service, request for revocation of the TSU certificate and the revocation of this certificate etc.;
- Chapter 5 covers physical, procedural and personal security, including the definition of the set of events subject to logging, the keeping of these records and responses to emergency and compromising situations;
- Chapter 6 focuses on the technical security of generating public and private keys, protection of private keys, including the computer and network protection;
- Chapter 7 defines the basic fields of TSU certificate and structures of time-stamping request, time-stamping response and time-stamp token;
- Chapter 8 focuses on assessing the Service delivered;
- Chapter 9 deals with commercial and legal aspects;
- Chapter 10 contains final provisions.

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

1.2 Document name and identification

This document's title:	Policy for Issuing Qualified Electronic Time-Stamp Tokens by TSA2 System (RSA algorithm), version 2.04
Policy OID:	1.3.6.1.4.1.23624.10.1.50.2.0

1.3 Participants

1.3.1 Time stamp authority

From the perspective of clients TSA2 system is the trustworthy computing and communication infrastructure issuing time-stamp tokens. The company První certifikační autorita, a.s., as the provider is fully responsible for providing trust services in the area of time-stamp tokens.

TSA2 system consists of single servers issuing time-stamp tokens (TSU). Every TSU has the private key and certificate of corresponding public key.

1.3.2 Time-stamp token requestors

Time-stamp token requestor may be, on the basis of contract, individual end user (physical person), legal person or organizational unit of the state.

1.3.3 Relying parties

Any entity relying in their operations on the time-stamp token issued under this Policy 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 Time-stamp token usage

1.4.1 Appropriate certificate uses

This Policy does not set any limitation of usage for time-stamp tokens issued under it.

1.4.2 Prohibited certificate uses

See chapter 1.4.1.

1.5 Policy administration

1.5.1 Organization administering the document

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

1.5.2 Contact person

The contact person of První certifikační autorita, a.s. in respect of this Policy and its Statement is specified on a web page – see chapter 2.2.

1.5.3 Person determining Statement suitability for the Policy

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

1.5.4 Statement approval procedures

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

1.6 Definitions and acronyms

tab. 2 - Definitions

Term	Explanation
Classified Information	the Czech Republic's Act No. 412/2005 Coll., regulating

Protection Act	classified information protection and security competence, as amended
client	time-stamp requestor or relying party
contracting partner	provider of selected certification services contracted by I.CA for certification services or parts thereof – usually, it is a contracted RA
electronic seal	advanced electronic seal or recognized electronic seal or qualified electronic seal under current trust services legislation
hash function	transformation which receives, as an input, a string of characters of arbitrary length, and the result is a string of characters of fixed length (hash)
key pair	a private key and the corresponding public key
Labour Code	the Czech Republic's Act No. 262/2006 Coll., Labour Code, as amended
OCSP responder	server using the OCSP protocol to provide data on public key certificate status
private key	unique data to create electronic signature
public key	unique data to verify electronic signature
relying party	party relying on the time-stamp token issued by I.CA in its operations
supervisory body	the body supervising qualified trust services providers
time-stamp requestor	individual end user (physical person) or legal person or organizational unit of the state (including a number of end users); or the system operated by subjects mentioned above
trust services legislation	current legislation of Czech Republic on trust services and eIDAS regulation
two-factor authentication	authentication employing two of three factors – I know something (the password), I have something (a smart card or a hardware token) or I am something (fingerprint, retina or iris reading)

Table 3 - Acronyms

Acronym	Explanation
ARC	Alarm Receiving Centre
bit	from English *binary digit* – a binary system digit – the fundamental and the smallest unit of information in digital technologies
CA	certification authority
CEN	European Committee for Standardization, an association of national standardization bodies
CEO	Chief Executive Officer

COO	Chief Operating Officer
CR	Czech Republic
CRL	Certificate Revocation List – the list of revoked certificates, which are not held as valid any longer
ČSN	Czech technical standards
DER, PEM	methods of certificate encoding (certificate formats)
eIDAS	REGULATION (EU) no 910/2014 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 23 July 2014 on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC
EN	European Standard, a type of ETSI standard
ESI	Electronic Signatures and Infrastructures
ETSI	European Telecommunications Standards Institute, a European standardization institute for information and communication technologies
FAS	Fire Alarm System
FIPS	Federal Information Processing Standard, standards for information technologies for U.S. non-military state organizations
GDPR	Global Data Protection Regulation, REGULATION (EU) 2016/679 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation)
GPS	Global Positioning System
html	Hypertext Markup Language
http	Hypertext Transfer Protocol
https	Hypertext Transfer Protocol Secure
IAS	Intrusion Alarm System
IEC	International Electrotechnical Commission, the global organization publishing standards for electrical and electronic engineering, communication technologies and related industries
IP	Internet Protocol, principal communications protocol in the Internet protocol suite for relaying packets across network and routing used in the Internet
IPS	Intrusion Prevention System
ISO	International Organization for Standardization, an international organization of national standardization organizations; designation of standards

OCSP	Online Certificate Status Protocol, the protocol to identify public key certificate status
OID	Object Identifier
PDCA	Plan-Do-Check-Act, Deming's cycle, method of permanent improving
PDF	Portable Document Format
PKI	Public Key Infrastructure
RA	registration authority
RFC	Request for Comments, designation for a range of standards and other documents describing web protocols, systems, etc.
RSA	signing and encrypting public key cipher (acronym from the names of the original authors: Rivest, Shamir and Adleman)
sha, SHA	type of hash function
TS	Technical Specification, type of ETSI standard
TSA	Time Stamp Authority
TSU	Time Stamp Unit, server issuing time-stamp tokens
UPS	Uninterruptible Power Supply/Source
USNO	United States Naval Observatory
UTC	Coordinated Universal Time, the standard adopted on 1 January 1972 for the global coordinated time – Bureau International de l'Heure (BIH) plays the role of the 'official keeper' of the atomic time for the whole world
UTC(k)	physical realization of UTC
ZOOÚ	current personal data protection legislation

2 PUBLICATION AND REPOSITORY RESPONSIBILITIES

2.1 Repositories

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

2.2 Publication of information

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

- address of the company's registered office:

  První certifikační autorita, a.s.

  Podvinný mlýn 2178/6

  190 00 Praha 9

  Česká republika
- website: http://www.ica.cz;
- registered offices of the registration authorities.

Electronic address for contact between the public and I.CA are ssl@ica.cz and info@ica.cz, I.CA's data box ID is a69fvfb.

The aforesaid website provides information about:

- Certificates – the following information is published (and more information can be obtained from the Certificate):
  - Certificate number;
  - Content of commonName;
  - Valid from date (specifying the hour, minute and second);
  - Link to where the certificate can be obtained in the specified format (DER, PEM, TXT).
- certificate revocation lists (CRL) – the following information is published (and more information can be obtained from the CRL):
  - Date of CRL release;
  - CRL number;
  - Links to where the CRL can be obtained in the specified formats (DER, PEM and TXT).
- certification and other policies and practice statements, certificates issued or revoked and other public information.

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

Any revocation of a certificate employed in issuing time-stamp tokens because of suspected or actual compromise of a given private key will be announced by I.CA on its web information

address and in a daily newspaper with national distribution – Hospodářské noviny or Mladá fronta Dnes and Hospodárske noviny or Sme,

2.3 Time or frequency of publication

I.CA publishes information concerning time-stamp tokens with the following periodicity:

- Policy - before issuing first time-stamp token under this Policy;
- Statement - immediately (if intended for publication);
- List of issued certificates - updates every time a new certificate is issued;
- Certificate revocation list (CRLs) - see chapter 4.9.7;
- Information about revocation the certificate of the CA issuing certificates for TSUs, stating the reason for revocation - without delay;
- Other public information - not predetermined, but generally this information must reflect the current status of the trust 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, contracting partners or the parties specified by the applicable legislation. Access to such information is governed by the rules defined in internal documentation.

3 IDENTIFICATION AND AUTHENTICATION

3.1 Naming

3.1.1 Types of names

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

3.1.2 Need for names to be meaningful

All attributes of subject field in TSU certificates which can be validated must carry a meaning. See chapter 7 for the attributes supported for these field.

3.1.3 Anonymity or pseudonymity of subscribers

TSU certificates do not support anonymity neither the use of a pseudonym.

3.1.4 Rules for interpreting various name forms

The data specified in a certificate application are carried over to the TSU certificate in the form they are specified in the application.

3.1.5 Uniqueness of names

Uniqueness of subject field in TSU certificate is guaranteed.

3.1.6 Recognition, authentication, and role of trademarks

TSU certificates can contain only trademarks owned by I.CA.

3.2 Initial identity validation

Described in chapter 3.2 of CP.

3.2.1 Method to prove possession of private key

See chapter 3.2.

3.2.2 Authentication of organization identity

See chapter 3.2.

3.2.3 Authentication of individual identity

See chapter 3.2.

3.2.4 Non-verified subscriber information

Not applicable to this document – all information must be duly verified.

3.2.5 Validation of authority

Not applicable to this document.

3.2.6 Criteria for interoperation

Any collaboration between První certifikační autorita, a.s. and other trust service providers is always based on a contract in writing.

3.3 Identification and authentication for routine re-key

Described in chapter 3.3 of CP.

3.3.1 Identification and authentication for routine re-key

See chapter 3.3.

3.3.2 Identification and authentication for re-key after revocation

See chapter 3.3.

3.4 Identification and authentication for revocation request

Described in chapter 3.4 of CP.

4 TIME-STAMP TOKENS LIFE-CYCLE OPERATIONAL REQUIREMENTS

TSA2 system service (Service) operated by První certifikační autorita, a.s., and including processes of creation and issuing time-stamp tokens and implementing identification and authentication of time-stamp tokens requestors are provided in compliance with relevant legislation and technical standards.

4.1 Entering into the contract

Issuing time-stamp tokens by I.CA is the commercially offered service for entities which can be physical persons, legal persons and organizational units of the state. This entity commits to act according to this Policy in the written contract concluded in a manner customary in business.

4.2 Processing time-stamping request

4.2.1 Performing identification and authentication functions

The ways of identification and authentication of time-stamp tokens requestors are:

- Based on non-qualified certificate issued by I.CA; or
- Name and password, or,
- Static IP address.

I.CA reserves the right to use other ways of identification and authentication of time-stamp tokens requestors,

4.2.2 Approval or rejection of time-stamping request

Time-stamp token requestor establishes authenticated connection to TSA2 system's communication server. If establishing has not been successful transaction is terminated and requestor informed in an appropriate manner.

After successful identification and authentication requestor creates time-stamping request (normalized according to RFC 3161) and the data structure is sent to TSA2 system. If the request does not comply with this Policy's requirements it is rejected by TSA2 system.

4.2.3 Time to process time-stamping request

I.CA does not set exact time limit for processing time-stamping request (excluding situation when it is specified in the contract) because it is chronology of actions and some of them are depending only on electronic data transfer form requestor to TSA2 system. Approximate time periods are as follows:

- creating time-stamping request by requestor - seconds;
- creating time-stamp token by TSA2 system - milliseconds.

4.3 Issuing time-stamp token

4.3.1 Time stamp authority actions during time-stamp token issuance

TSA2 system carries out formal data correctness check of time-stamping request and based on the results creates time-stamping response containing status of the response and in case of success also the time-stamp token (see RFC 3631). Time stamp is obtained from trustworthy time source. Time-stamp token is electronically sealed by specific TSU (in the following text "TSU" means "TSU of TSA2 system").

Every time-stamping response is stored in TSA2 system repository.

4.3.2 Notification to requestor by the TSA of issuance of time-stamp token

After taking actions mentioned above in chapter 4.3.1 the time-stamping response (see Table 5) sent by TSA2 system back to the requestor.

4.4 Time-stamp token acceptance

4.4.1 Time-stamp token requestor's obligations

After receiving time-stamping response the requestor is obliged to check its status. If the response has contained the time-stamp token the requestor is obliged to act in compliance with chapter 9.6.3.

4.4.2 Relying parties' obligations

Relying party is obliged to act in compliance with chapter 9.6.4.

4.5 Time-stamp token issuance termination for specific requestor

Time-stamp tokens issuing service for specific user (business relationship) can be terminated by this user, i.e. time-stamp token requestor, or by I.CA if user does not comply with the terms of the written contract.

4.6 TSU pair data and their validity period

4.6.1 Key changeover

TSU certificate's validity is specified in this certificate. Validity of key pair (public and private key) designed for creation and verification of time-stamp tokens electronic seals is limited by validity of the certificate (usually six years).

First year after generating key pair and issuing the certificate the private key us used for time-stamp token's electronic seal creation. Before end of this period new key pair is generated and new certificate issued and newest public key is then used for time-stamp token's electronic seal creation. Newest and all previous public keys are used for verification of time-stamp token's electronic seals created by corresponding private key.

In non-standard situations, for instance such developments in cryptanalytic methods that could compromise the security of issued time-stamp token and the changes to cryptanalytic algorithms or key length are necessary), new key pair generation and new certificate issuance are done as soon as possible.

4.6.2 TSU certificate revocation

TSU certificate can be revoked only in the following circumstances:

- The facts stated in trust services legislation will happen;
- Actual or suspected compromise of private key of certification authority issuing certificates for TSUs and for its OCSP responder;
- Actual or suspected compromise of private key of specific TSU.

Certificate revocation list profile complies with relevant technical standards and norms.

4.7 Time source synchronization with UTC

4.7.1 Synchronization

TSU servers are permanently synchronized with I.CA primary time source (commercial solution). This primary time source obtains time information from GPS system provided by UTC(k) laboratory of USNO. Procedure is described in internal documentation.

4.7.2 Time source security

Time source is placed in the I.CA's premises and ensuring its security is described in internal documentation.

4.7.3 Time source inaccuracy detection

TSU's system time is regularly audited by special application against second independent time source placed in other I.CA's locality. Time information of this time source is also, using internal GPS module, synchronized with UTC.

Successful audit means creation of time limited audit token allowing TSU to issue time-stamp tokens. Before this time limit new successful audit must be done or the TSU terminates time-stamp tokens issuance.

If time inaccuracy greater then maximal acceptable inaccuracy for time-stamp tokens issuing (set in configuration) has been found out, the special application creates invalid token and based on it TSU terminates time-stamp tokens issuance. At the same time alarm is announced to operators (time-stamp tokens issuance termination).

Procedure is described in internal documentation.

4.7.4 Leap second

Leap second is set manually, the procedure is described in internal documentation.

5 FACILITY, MANAGEMENT, AND OPERATIONAL CONTROLS

Facility, management, and operational controls primarily deal with:

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

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

5.1 Physical controls

5.1.1 Site location and construction

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

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

5.1.2 Physical access

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

5.1.3 Power and air conditioning

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

5.1.4 Water exposures

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

5.1.5 Fire prevention and protection

The buildings of the operating sites and the information storage sites have fire alarm system (FAS). Fireproof insulation is installed in the entrance doors to the restricted areas in which the trustworthy systems destined to support the Services 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.

Any paper media required by current trust services legislation to be kept are stored at a site geographically different from the site of the operating office.

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 I.CA employee appointed to a trusted role may be in a conflict of interests that could compromise the impartiality of I.CA's operations.

5.2.2 Number of persons required per task

Processes related to key pair of certifications authorities and OCSP responders are defined as activities which must be carried out with the participation of more than one person. These include in particular:

- Generating key pair of any TSU;
- Destroying key pair of any TSU;
- Backing up and restoring private key of any TSU.

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

5.2.3 Identification and authentication for each role

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

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

5.2.4 Roles requiring separation of duties

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

5.3 Personnel controls

5.3.1 Qualifications, 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.

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 I.CA's employees 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 RA operations is held for RA employees at least once in every three years.

5.3.5 Job rotation frequency and sequence

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

5.3.6 Sanctions for unauthorized actions

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

5.3.7 Independent contractor requirements

I.CA may or must procure some activities from independent contractors, and is fully liable for the job they deliver. These business relations are regulated 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 appropriate certification policies, the relevant parts of internal documentation provided for them, and the required normative documents. Contractual penalties are applied for a breach of the obligations or duties specified in the said documents, or the contract with the contractor in breach is terminated immediately.

5.3.8 Documentation supplied to personnel

In addition to the certification policy, the certificate practice statement and the security and operating 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 current trust services legislation or the relevant technical and other standards.

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 in case 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, with each copy kept in a different room of the operating site. These audit records are saved on a medium each month or more frequently and this medium is kept outside the operating premises of I.CA.

Printed audit records are kept outside the operating premises of I.CA.

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

5.4.5 Audit log backup procedures

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

5.4.6 Audit collection system (internal vs. external)

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

5.4.7 Notification to event-causing subject

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

5.4.8 Vulnerability assessments

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

5.5 Records archival

The storage of records, i.e. information and documentation, performs První certifikační autorita, a.s. according to internal documentation.

5.5.1 Types of records archived

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

- Service contracts;
- Life cycle records for TSU certificates including certificates issued and the certificates related thereto;
- Video recording, if any, of the generation of key pair of CA issuing TSU certificates;
- Other records concerning operation of CA issuing TSU certificates;
- Issued time-stamp tokens including corresponding time-stamping requests;
- Records concerning operation of all TSUs;
- Information handling records, such as takeover, handover, saving, check, conversion from printed to electronic, etc.;
- Application software, operating and security documentation.

5.5.2 Retention period for archive

All records pertaining to the certificates of all I.CA certification authorities and their respective OCSP responders, except the pertinent private keys, are stored throughout the existence of I.CA. The same applies for TSU certificates. Other records are stored in accordance with chapter 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 in 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 located in designated locations and are accessible to:

- I.CA employees if they need to have such an access for their job;
- Authorized supervising and inspection entities and the investigative, prosecuting and adjudicating bodies if required by legislation.

A written record is made of any such permitted access.

5.6 Key changeover

See chapter 4.6.1.

5.7 Compromise and disaster recovery

5.7.1 Incident and compromise handling procedures

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

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

See chapter 5.7.1.

5.7.3 Entity private key compromise procedures

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

- Stops using the private key, revokes immediately and demonstrably the pertinent TSU certificate and destroys the corresponding private key - about this fact, including the reason of revocation, informs on its web pages, the relevant certificate revocation list shall also be used for making this information available;
- Informs, if possible, all clients of the Service via sending e-mails to addresses specified in contracts, e-mail contains information about the reason of revocation;
- Notifies the supervisory body of that the pertinent TSU certificate has been revoked and why it has been revoked;
- Issues new certificate for this TSU - the procedure is the same as when issuing primary certificate.

5.7.4 Business continuity capabilities after a disaster

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

5.8 TSA termination

The following rules apply to termination of TSA2 system's operations:

- Termination must be notified in writing to the supervisory body and to all subjects having a contract with I.CA that directly concerns Service provision;
- Termination must be published on I.CA's web page;
- TSU's private keys must be demonstrably destroyed, destruction must be recorded in writings and the record must be kept in accordance with this CP.
- Termination of operations is a controlled process following a pre-defined scenario.

Issue of withdrawal of the qualified trust services provider status is described in internal documentation.

6 TECHICAL SECURITY CONTROLS

6.1 Key pair generation and installation

6.1.1 Key pair generation

The generation of TSU's key pairs is done in secured reserved areas of operating sites and is carried out in a cryptographic module assessed under FIPS PUB 140-2, level 3.

Key pairs of the employees taking part in the issuance of Certificates to end users are generated on chip cards that meet the QSCD requirements. The private keys of these key pairs of data are saved on the chip card in non-exportable form and PIN needs to be entered to use the keys.

All requirements concerning key pair generation are described are described in internal documentation.

6.1.2 Private key delivery to its owner

Not applicable to this document, private keys of TSU are stored in cryptographic module.

6.1.3 Public key delivery to certificate issuer

The TSU's public key is delivered to the certification authority in the certificate application (the PKCS#10 format).

6.1.4 TSU's public key delivery to relying parties

TSU’s public keys intended to verify advanced electronic seals of issued time-stamp tokens are included in specific TSU’s certificates. These certificates can be obtained:

- Via I.CA’s web pages;
- Via supervisory body's web pages.

6.1.5 Key sizes

TSA2 system uses RSA asymmetric algorithm. The size of the keys (or the given algorithm’s parameters) used for creation of advanced electronic seals of issued time-stamp tokens is 2048 bits at a minimum.

6.1.6 Public key parameters generation and quality checking

The parameters of the algorithms used in generating TSU's public keys meet the requirements listed in current trust services legislation and the technical and other standards referred to therein.

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

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

6.2 Private Key Protection and Cryptographic Module Engineering Controls

6.2.1 Cryptographic module standards and controls

Key pairs used for electronic seals of issued time-stamp tokens creation are stored in cryptographic modules which meet the requirements of the current trust services legislation, that is, the FIPS PUB 140-2 standard, level 3.

6.2.2 Private key (n out of m) multi-person control

If cryptographic module related operations require the presence of two I.CA management members, then each member only has knowledge of some part of the code required for these operations.

6.2.3 Private key escrow

Not applicable to this document; the private key escrow is not provided.

6.2.4 Private key backup

TSU's private key is backed-up as a part of securely encrypted directory tree, the encryption is certified.

6.2.5 Private key archival

When private keys used for creation of electronic seals of issued time-stamp token expire, they and their backup copies are destroyed. Because storing these private keys is a security risk, it is prohibited at I.CA.

6.2.6 Private key transfer into or from a cryptographic module

TSU's private keys used for creation of electronic seals of issued time-stamp tokens are generated in cryptographic module of specific TSU.

Not relevant for TSUs private keys transfer from cryptographic module, it is a normal backup of securely encrypted directory tree, the encryption is certified

TSU's private keys transfer to cryptographic module is done with the use of administrator's smart cards of this cryptographic module.

Every actual transfer is documented in a written record.

6.2.7 Private key storage on cryptographic module

TSUs private keys are stored in the cryptographic module which meets the requirements of current trust services legislation, that is, the FIPS PUB 140-2 standard, level 3. Out of cryptographic module they are securely encrypted, the encryption is certified.

6.2.8 Method of activating private key

TSU's private key generated in cryptographic module is activated by Security Officer(1) trusted role employee choosing corresponding profile. Activation is documented in a written record.

6.2.9 Method of deactivating private key

Preceding TSU's private key is deactivated when new profile is chosen.

6.2.10 Method of destroying private key

TSU's private keys are stored cryptographic module. The destruction means secure deletion of securely encrypted directory tree, the encryption is certified.

6.2.11 Cryptographic module rating

The cryptographic module used for storage and management of TSU's private key meets the requirements of the FIPS PUB 140-2 standard, level 3.

6.2.12 Cryptographic module used when time-stamp tokens are created transport

Cryptographic module (Hardware Security Module - HSM) is delivered (by trusted carrier) to the head quarter if I.CA or to its operating site. When the delivery is receipted intactness and integrity of the seals are checked. After that the module is saved in a safe place with controlled access.

6.3 Other aspects of key pair management

6.3.1 Public key archival

The public keys for verification of issued time-stamp tokens are as part of certificates of specific TSUs stored throughout the existence of I.CA.

6.3.2 Certificate operational periods and key pair usage periods

The maximum period of validity of each TSU certificate is specified in this certificate. After this period the data for verification of electronic seals can be used without guaranties.

6.4 Activation data

6.4.1 Activation data generation and installation

TSU's activation data are created during initialization of the corresponding cryptographic module.

6.4.2 Activation data protection

TSU's activation data are protected by a method described in internal documentation.

6.4.3 Other aspects of activation data

TSU's activation data must not be transferred or kept in an open form. All aspects are described in internal documentation.

6.5 Computer security controls

6.5.1 Specific computer security technical requirements

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

6.5.2 Computer security rating

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

- CEN/TS 419261 Security requirements for trustworthy systems managing certificates and time-stamps.
- ČSN ETSI EN 319 421 Electronic Signatures and Infrastructures (ESI); Policy and Security Requirements for Trust Service Providers issuing Time-Stamps.
- ETSI EN 319 421 Electronic Signatures and Infrastructures (ESI); Policy and Security Requirements for Trust Service Providers issuing Time-Stamps.
- ČSN ETSI EN 319 422 Electronic Signatures and Infrastructures (ESI); Time-stamping protocol and time-stamp token profiles.
- ETSI EN 319 422 Electronic Signatures and Infrastructures (ESI); Time-stamping protocol and time-stamp token profiles.
- 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 Electronic Signatures and Infrastructures (ESI); Trust Service Provider Conformity Assessment - Requirements for conformity assessment bodies assessing Trust Service Providers.
- ETSI EN 319 403 Electronic Signatures and Infrastructures (ESI); Trust Service Provider Conformity Assessment - Requirements for conformity assessment bodies assessing Trust Service Providers.
- ČSN ETSI EN 319 411-1 Electronic Signatures and Infrastructures (ESI); Policy and security requirements for Trust Service Providers issuing certificates; Part 1: General requirements.
- ETSI EN 319 411-1 Electronic Signatures and Infrastructures (ESI); Policy and security requirements for Trust Service Providers issuing certificates; Part 1: General requirements.
- ČSN ETSI EN 319 411-2 Electronic Signatures and Infrastructures (ESI); Policy and security requirements for Trust Service Providers issuing certificates; Part 2: Requirements for trust service providers issuing EU qualified certificates.
- ETSI EN 319 411-2 Electronic Signatures and Infrastructures (ESI); Policy and security requirements for Trust Service Providers issuing certificates; Part 2: Requirements for trust service providers issuing EU qualified certificates.
- ETSI TS 119 312 Electronic Signatures and Infrastructures (ESI); Cryptographic Suites.
- ČSN 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.
- EN 301 549 Accessibility requirements for ICT products and services.
- RFC 3161 Internet X.509 Public Key Infrastructure Time-Stamp Protocol (TSP).

6.6 Life cycle technical controls

6.6.1 System development controls

System development is carried out in accordance with internal documentation.

6.6.2 Security management controls

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

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

- ČSN ISO/IEC 27000 Information Technology – Security Techniques – Information Security Management Systems – Overview and Vocabulary;

- ČSN ISO/IEC 27001 Information Technology – Security Techniques – Information Security Management Systems – Requirements;
- ČSN ISO/IEC 27002 Information Technology – Security Techniques – Information Security Management Systems – Code of Practice for Information Security Controls.

6.6.3 Life cycle security controls

I.CA takes the Plan-Do-Check-Act (PDCA) procedural approach to life cycle security management; the PDCA approach consists of the following consecutive processes:

- Establishing – defining the scope and the boundaries for information security management, determining a security policy and plans, and choosing security controls depending on the risks identified, all this in accordance with the corporate security policy;
- Implementing and operating – effective and systematic enforcement of the selected security controls;
- Monitoring and reviewing – providing feedback, regular monitoring and evaluation of the successful and the poor aspects of information security management, providing the knowledge gained for the company management for assessment;
- Maintenance and improvement – implementing corrective and improvement measures as decided by the company management.

6.7 Network security controls

In the I.CA environment the trustworthy systems destined for supporting the Service and situated at I.CA's operating sites are not directly accessible from the Internet. These systems are protected with a firewall-type commercial product with an integrated intrusion prevention system (IPS).

6.8 Time-stamping

See chapter 5.5.5 for the time-stamping solution.

7 TSU CERTIFICATE PROFILE, STRUCTURES OF TIME-STAMPING REQUEST, TIME-STAMPING RESPONSE AND TIME-STAMP TOKEN

7.1 Profile and structures

Table 4 - Basic fields of TSU certificate

Field	Content	Comments
version	v3 (0x2)	
serialNumber	unique serial number of the Certificate	
signatureAlgorithm	sha256WithRSAEncryption at minimum	
issuer	issuer of the certificate	
validity		
notBefore	start of the Certificate's validity (UTC)	UTC
notAfter	end of the Certificate's validity (UTC)	UTC
subject[2]		
commonName	I.CA Time Stamping Authority TSU *X MM/RRRR**	
organizationName	První certifikační autorita, a.s.	
countryName	CZ	
organizationIdentifier	NTRCZ-26439395	
subjectPublicKeyInfo		
algorithm	rsaEncryption	
subjectPublicKey	2048 at minimum	
extensions	extensions to the certificate	
signature	certificate issuer's advanced electronic seal	

* *X* – number of TSU; *MM/RRRR* – month and year of certificate's issuance; there is just one space between *X* and *MM/RRRR*

Table 5 – Time-stamping request structure

Request item	Content, comments
TimeStampReq ::= SEQUENCE **{**	
version INTEGER { v1(1) },	v1 When anything else is stated in the request, it will be

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

	rejected.
messageImprint MessageImprint	
MessageImprint ::= SEQUENCE {	
hashAlgorithm AlgorithmIdentifier,	Acceptable algorithms are SHA256, SHA512, when anything else is stated in the request, it will be rejected.
hashedMessage OCTET STRING }	Hash of data for which issuing the time-stamp token is requested (length of this string must meet length requirements of specific algorithm).
reqPolicy TSAPolicyId ::= OBJECT IDENTIFIER OPTIONAL,	Identifier of policy under which the client wants the time-stamp token should be issued: ▪ optional, server must be able to process it; ▪ if contained this must be OID of the policy under which the time-stamp tokens are issued.
nonce INTEGER OPTIONAL,	Random number (optional, server must be able to process it).
certReqBOOLEAN DEFAULT FALSE,	Request for inserting TSU certificate into SignedData structure in the response (optional, server must be able to process it): ▪ TRUE - response must contain TSU certificate; ▪ FALSE or certReq not contained - response must not contain TSU certificate.
extensions [0] IMPLICIT Extensions OPTIONAL	I.CA does not process any extension, if the field is contained in the request it will be rejected (in compliance with RFC 3631).
}	

Note 1: Request created by client, I.CA is not able to affect the content.

Note 2: When the progression in cryptoanalysis can endanger some algorithm used when creating timestamp request I.CA reserves in this case the right not to support this algorithm. Information which algorithms are no longer supported is available on I.CA's web pages.

Table 6 – Time-stamping response request structure

Response item	Content, comments
TimeStampResp ::= SEQUENCE **{**	
status PKIStatusInfo ::= SEQUENCE {	
status PKIStatus ::= INTEGER	Result of time-stamping request processing. If the time-stamp token has been contained in time-stamping response the value MUST be 0 or 1. In any other case the time-stamp token MUST NOT be contained in time-stamping response).

	Results: *0* - issued, timeStampToken contained; *1* - issued, modified, timeStampToken contained; *2* - request rejected; *3* - waiting; *4* - risk of immediate TSU certificate's revocation; *5* - TSU certificate revoked.
statusString PKIFreeText OPTIONAL,	Description of error may be contained.
failInfo PKIFailureInfo OPTIONAL ::= BIT STRING }	If the time-stamp token has not been contained in time-stamping response this item indicates the reason: *(0)* - *BadAlg* - algorithm not known or not supported; *(2)* - *BadRequest* - transaction not allowed or not supported; *(5)* - *BadDataFormat* - bad sent data format; *(14)* - *TimeNotAvailable* - time source not available; *(15)* - *UnacceptedPolicy* - policy not supported by TSA2 system; *(16)* - *UnacceptedExtension* - extension not supported by TSA2 system; *(17)* - *AddInfoNotAvailable* - requested additional information not undestood or not available; *(25)* - *SystemFailure* - request not processed because of system failure.
timeStampToken OPTIONAL	
TimeStampToken ::= ContentInfo	ContentInfo = SignedData type CMS message, see time-stamp token structure below (Table 7).
}	

Note: Time-stamping response contains always the status of the response and in case of success also the time-stamp token.

Table 7 – Time-stamp token structure

Time-stams token item	**Content, comments**
ContentInfo ::= SEQUENCE **{**	
contentType ::= OBJECT IDENTIFIER	id-signedData (CMS).
content [0] EXPLICIT ANY DEFINED BY contentType	SignedData structure.
SignedData ::= SEQUENCE {	
version CMSVersion,	v3
digestAlgorithms DigestAlgorithmIdentifiers,	
DigestAlgorithmIdentifiers ::= SET OF DigestAlgorithmIdentifier,	Hash algorithm used for creation of advanced electronic seal of time-stamp token (CMS message).
encapContentInfo	

EncapsulatedContentInfo ::= SEQUENCE {	
eContentType ContentType ::= OBJECT IDENTIFIER	id-ct-TSTInfo
eContent [0] EXPLICIT OCTET STRING OPTIONAL	TstInfo, see also TstInfo structure (Table 9).
certificates [0] IMPLICIT CertificateSet OPTIONAL	
CertificateSet ::= SET OF CertificateChoices	

CertificateChoices ::= CHOICE {
certificate Certificate,
extendedCertificate [0] IMPLICIT
 	
ExtendedCertificate,
attrCert [1] IMPLICIT AttributeCertificate
}
	If time-stamping request has contained certReq=true then TSU certificate in the format Certificate = X.509v3 is inserted, other formats are not used.

crls [1] IMPLICIT CertificateRevocationLists OPTIONAL,	Not contained.
signerInfos SignerInfos ::= SET OF SignerInfo	
SignerInfo ::= SEQUENCE {	
version CMSVersion,	v1
sid SignerIdentifier ::= CHOICE	
{ issuerAndSerialNumber IssuerAndSerialNumber, subjectKeyIdentifier [0] SubjectKeyIdentifier },	issuerAndSerialNumber of TSU certificate.
digestAlgorithm DigestAlgorithmIdentifier,	sha256, mandatory.
signedAttrs [0] IMPLICIT SignedAttributes OPTIONAL	
SignedAttributes ::= SET SIZE (1..MAX) OF Attribute	Added attributes: ▪ id-aa-signingCertificateV2: ▪ mandatory according to EN 319 422 and supervisory body of SR supports only this option; ▪ see signingCertificateV2 attribute below (Table 8); ▪ contentType ::= OBJECT IDENTIFIER= id-ct-

	TSTInfo; ▪ messageDigest ::= OCTET STRING; ▪ signingTime ::= UTCTime format.
signatureAlgorithm SignatureAlgorithmIdentifier,	
signature SignatureValue ::= OCTET STRING,	
unsignedAttrs [1] IMPLICIT UnsignedAttributes ::= SET SIZE (1..MAX) OF Attribute OPTIONAL	No unsigned attributes added.
}	
}	

Table 8 - signingCertificateV2 attribute

signingCertificateV2 items	**Content, comments**
Attribute ::= SEQUENCE **{**	
attrType OBJECT IDENTIFIER,	id-aa-signingCertificateV2: ▪ mandatory according to EN 319 422 and supervisory body of SR supports only this option; ▪ defined in RFC 5816.
attrValues SET OF AttributeValue	
AttributeValue ::= SEQUENCE {	
certs SEQUENCE OF ESSCertIDv2	
ESSCertIDv2 ::= SEQUENCE {	
hashAlghoritm ::= default SHA256	hashAlghoritm = sha256.
certHash Hash ::= OCTET STRING,	certHash = hash of TSU certificate.
issuerSerial IssuerSerial OPTIONAL	Not contained.

IssuerSerial ::= SEQUENCE
{
issuer GeneralNames,
serialNumber CertificateSerialNumber
}	

}	
policies SEQUENCE OF PolicyInformation OPTIONAL	Not contained.
}	
}	

Table 9 - TstInfo structure

TstInfo items	Content, comments
TSTInfo ::= SEQUENCE **{**	
version INTEGER { v1(1) },	v1
policy TSAPolicyId,	Identifier of I.CA's policy under which the time-stamp token is issued.
messageImprint MessageImprint,	

MessageImprint ::= SEQUENCE {
hashAlgorithm AlgorithmIdentifier,
hashedMessage OCTET STRING
}
	Same values as in time-stamping request.

serialNumber INTEGER,	Unique number (up to 160 bits) assigned by TSU to issued time-stamp token.
genTime GeneralizedTime	UTC time of time-stamp token creation including fractions-of-second, i.e. in the format YYYYMMDDhhmmss.sssZ (three decimal places used).
accuracy Accuracy OPTIONAL	Time stamp in time-stamp token accuracy.
Accuracy ::= SEQUENCE {	
seconds INTEGER OPTIONAL,	Not contained.
millis [0] INTEGER (1..999) OPTIONAL,	Contained = 500 ms.
micros [1] INTEGER (1..999) OPTIONAL }	Not contained.
ordering BOOLEAN DEFAULT FALSE,	Nor contained (i.e. taken as FALSE). (EN 319 422 - must not be contained).
nonce INTEGER OPTIONAL,	When nonce has been contained in time-stamping request then time-stamping response contains nonce with the same value (mandatory RFC 3161).
tsa [0] GeneralName OPTIONAL,	TSU's distinguished name, content of subject field in TSU certificate.
extensions [1] IMPLICIT Extensions OPTIONAL }	
Extensions ::= SEQUENCE SIZE (1..MAX) OF Extension	esi4-qtstStatement-1 (qualified electronic time-stamp token): ▪ see also qcStatements.esi4-qtstStatement-1 extension below (Table 10); ▪ optional, recommended.
}	

Table 10 - qcStatements.esi4-qtstStatement-1 extension

qcStatement items	Content, comments
Extension ::= SEQUENCE **{**	
extnID OBJECT IDENTIFIER,	qcStatements (id-pe-qcStatements = { id-pe 3 })
critical BOOLEAN DEFAULT FALSE,	False
extnValue OCTET STRING	
extnValue ::= SEQUENCE OF **QCStatement**	
QCStatement ::= SEQUENCE {	
statementId OBJECT IDENTIFIER,	id-etsi-tsts-EuQCompliance ▪ { id-etsi-tsts 1 } = 0.4.0.19422.1.1, ▪ mnemonic designation esi4-qtstStatement-1; ▪ Qualified electronic time-stamp token issued in compliance with eIDAS.
statementInfo ANY DEFINED BY statementId OPTIONAL }	Not included.
}	

7.1.1 Version number(s)

TSU certificate's profile complies with X.509, version 3 standard.

7.1.2 Algorithm object identifiers

The algorithms used in providing qualified electronic time-stamp tokens issuing are in accordance with the relevant technical standards.

8 COMPLIANCE AUDITS AND OTHER ASSESSMENTS

8.1 Frequency or circumstances of assessment

The assessment interval and circumstances are defined in current 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.

8.2 Identity/qualifications of assessor

The identity (accredited conformity assessment entity) and the qualification of the assessor carrying out the assessment pursuant to current 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.

8.3 Assessor's relationship to assessed entity

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

External assessor is an assessor without any property or personal relation to I.CA.

8.4 Topics covered by assessment

In the case of the assessment required by current trust services legislation, the assessed areas are specified by this legislation. Assessed areas for other assessment are specified by the technical standards and standards under which the evaluation is performed.

8.5 Actions taken as a result of deficiency

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

8.6 Communication of results

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

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

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

9 OTHER BUSINESS AND LEGAL MATTERS

9.1 Fees

9.1.1 Time-stamp token issuance fees

Time-stamp token issuance fees can be got on tsa@ica.cz.

9.1.2 Provider's certificates access fees

No fee is charged by I.CA for electronic access to the certificates related to TSA2 system.

9.1.3 Revocation or status information access fees

No fee is charged by I.CA for electronic access to revocation information (CRL) and status information about the certificates issued by I.CA.

9.1.4 Fees for other services

Fees for services above standard are agreed contractually.

9.1.5 Refund policy

I.CA reserves the right to agree contractually different time-stamp token issuance fees.

9.2 Financial responsibility

9.2.1 Insurance coverage

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

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

9.2.2 Other assets

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

Please refer to the Annual Report of První certifikační autorita, a.s., disclosed in business register for detailed information on the company's assets.

9.2.3 Insurance or warranty coverage for end-entities

Not applicable to this document; the service is not provided.

9.3 Confidentiality of business information

9.3.1 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 private keys, which are employed in providing the Services;
- I.CA's business information;
- Any internal information and documentation;
- Any personal data.

9.3.2 Information not within the scope of confidential information

Public information is only the information designated as public and that published in the manner pursuant to 2.2.

9.3.3 Responsibility to protect confidential information

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

9.4 Privacy of personal information

9.4.1 Privacy plan

I.CA protects personal data and other non-public information in accordance with the relevant legislation, which means ZOOU and GDPR in particular.

9.4.2 Information treated as private

Any personal data subject to protection under applicable legislation are treated as private.

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

9.4.3 Information not deemed private

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

9.4.4 Responsibility to protect private information

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

9.4.5 Notice and consent to use private information

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

9.4.6 Disclosure pursuant to judicial or administrative process

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

9.4.7 Other information disclosure circumstances

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

9.5 Intellectual property rights

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

9.6 Representations and warranties

9.6.1 TSA representations and warranties

9.6.1.1 General TSA representations and warranties

První certifikační autorita a.s., warrants in particular:

- Access to the Service;
  - Continuous, excluding planned (announced in advance) interruptions caused by technical interventions;
  - Under the conditions defined by contract;
- Authenticated access to the Service based on the contract;
- Strict application of current legislation concerning time-stamp tokens issuance including respect to copyrights and intellectual property rights;
- To provide the Service by persons:
  - With necessary knowledge and qualification;
  - Familiar with relevant security procedures;
- To use trustworthy systems and security tools, provide sufficient security of procedures supporting systems and tools mentioned above including cryptographical security of this tools;

- Throughout of its existence it has enough financial and other sources to provide the Service in compliance with trust services legislation requirements and taking into account the risk of damage liability;
- To inform before entering the contract the time-stamp tokens requestors in writing about terms and conditions of the Service, about possible limitations of use, about claims and complaints and about the fact that it is or is not the qualified provider of the Service;
- I.CA employees or other physical persons who come into contact with personal data must maintain confidentiality of these data and the security controls the disclosure of which would put the security of these data at risk (the confidentiality duty survives the termination of employment or other similar relationship, or the completion of pertinent work).

9.6.1.2 TSA representations and warranties related to time-stamp token requestors and owners

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

- Issued time-stamp tokens meet the statutory trust services legislation requirements;
- Will use the private keys of certification authorities issuing certificates to TSUs solely for issuing certificates to TSUs, certificates to their OCSP responders and releasing certification revocation lists;
- Will use the private keys of certification authorities' OCSP responders solely in the processes of providing responses to certificate status requests;
- Will use the private keys corresponding with TSU certificates only for electronic sealing of issued time-stamp tokens;
- Implemented adequate measures to prevent time-stamp tokens forgery;
- Will issue the time-stamp token immediately after obtaining correct and valid time-stamping request;
- Does not verify in any way the hash which should be time-stamped (excluding the check of its length);
- Uses trustworthy time synchronization;
- Issued time-stamping response contains at minimum:
  - Serial number of issued time-stamp token which is unique for specific TSU of TSA2 system;
  - Identifier of policy under which the time-stamp token is issued;
  - Time information corresponding with UTC at the moment of time-stamp token issuance, accuracy of time information meets the requirements of relevant technical standards (time deviation less than 1 second, usually less than 500 milliseconds;
  - Electronic data contained in time-stamping request (time-stamped document hash)
  - electronic seal of TSU.

9.6.2 RA representations and warranties

Not applicable to this document.

9.6.3 Time-stamp token requestor and owner representations and warranties

Time-stamp token requestor or owner guarantees correctness of information in the time-stamp tokens issuance contract and acts in compliance with trust services legislation, this Policy and contract mentioned above.

Time-stamp token requestors are, after receiving time-stamping response, obliged to check the status of the response. In case of an error time-stamp token is not included in the response and the requestor is obliged to check up corresponding error message. In an opposite case the requestor is obliged in particular:

- To verify validity of electronic seal of issued time-stamp token and also validity of all certificates related to TSU which created this time-stamp token;
- To check whether the hash in issued time-stamp token is the same as in time-stamping request;
- To check, if items “nonce“ or “reqPolicy“ has been included in time-stamping request, that the value of this items in issued time-stamp token is the same.

9.6.4 Relying party representations and warranties

Relying parties are acting in accordance with this Policy. Their obligation is especially:

- Verify validity of time-stamp token's electronic seal including verification of all certificates in certification path;
- Consider possible limited usability of time-stamp tokens stated in this Policy;
- Consider other measures agreed by contract.

9.6.5 Representations and warranties of other participants

Not applicable to this document.

9.7 Disclaimers of warranties

První certifikační autorita, a.s. only provides the warranties as given in 9.6.

9.8 Limitations of liability

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

9.9 Indemnities

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

První certifikační autorita, a.s.:

- Undertakes to discharge all the duties defined in valid legislation (including the trust services legislation) and those in the relevant policies;
- Gives the aforesaid warranties throughout the term of the contract of the Service;
- Agrees that the application software suppliers with a valid contract with První certifikační autorita, a.s., for the distribution of the root certificate assume no obligation or liability, except for where damage or loss is directly attributable to the software of that supplier;
- Does not provide any other warranties than those mentioned above.

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

- Any defect in the services rendered which is due to incorrect or unauthorized use of the services rendered under the contract of the Service by time-stamp token owner, particularly for any use contrary to the terms and conditions specified in this Policy,
- Any defect due to force majeure, including a temporary telecommunication failure.

Claims and complaints may be made and delivered by:

- E-mail to reklamace@ica.cz;
- Message to I.CA's data box;
- 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 (time-stamp token owner or the relying party) must provide:

- Description of the defect that is as accurate as possible;
- Serial number of the product complained about;
- 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 to a different method.

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 compensation may be determined by court.

9.10 Term and termination

9.10.1 Term

This Policy takes force on the date specified in chapter 10 and remains valid until further notice.

9.10.2 Termination

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

9.10.3 Effect of termination and survival

Terminating the Service does not mean invalidity of time-stamp token issued when this Policy was valid.

9.11 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 them, or negotiations in person.

Communication with I.CA is also possible through the channels specified on the web Information Address.

9.12 Amendments

9.12.1 Procedure for amendment

This procedure is a controlled process described in internal documentation.

9.12.2 Notification mechanism and period

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

9.12.3 Circumstances under which OID must be changed

The Policy's OID must be changed when the changes of the Policy materially reduce the assurance that the time-stamp token is trusted and have a significant effect on the acceptability of the time-stamp token in compliance with trust services legislation.

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

9.13 Dispute resolution provisions

If the time-stamp token owner or the relying party disagrees with the proposed way of resolving the dispute, they may use the following levels of appeal:

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

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

9.14 Governing law

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

9.15 Compliance with applicable law

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

9.16 Miscellaneous provisions

9.16.1 Entire agreement

Not applicable to this document.

9.16.2 Assignment

Not applicable to this document.

9.16.3 Severability

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

9.16.4 Enforcement (attorneys' fees and waiver of rights)

Not applicable to this document.

9.16.5 Force majeure

První certifikační autorita, a.s. may not be held liable for breaching its obligations resulting from client's contract if it is the result of force majeure, such as major natural disaster, major disaster caused by human activity, strike or civil unrest always followed by the declaration of

a situation of emergency, or the declaration of a state of threat to state or a state of war, or communication failure.

9.17 Other provisions

Not applicable to this document.

10 FINAL PROVISIONS

This Policy issued by První certifikační autorita, a.s., takes force and effect on the date mentioned in Table 1 above.