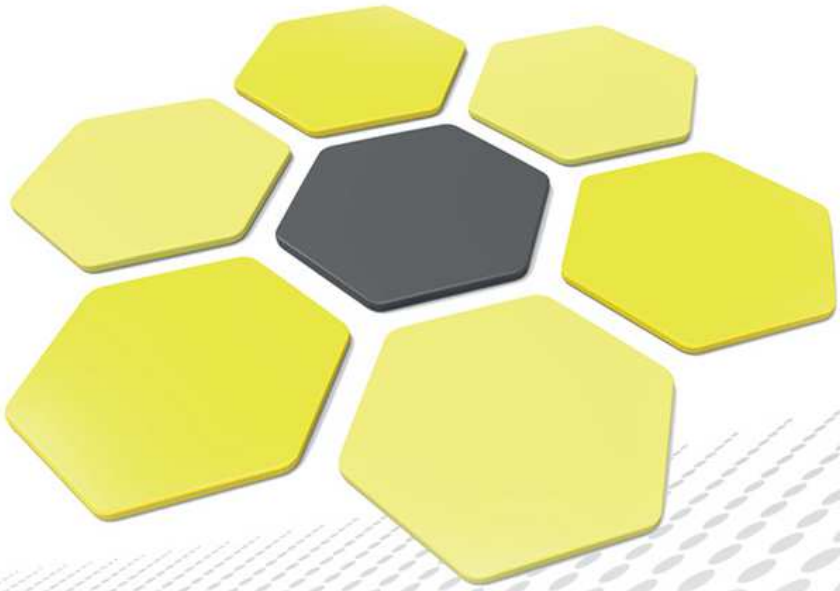
MICROSEC

e-Szignó Certification Authority

eIDAS conform
Qualified Time Stamping
Practice Statement

ver. 2.1

Date of effect: 05/09/2016



OID	1.3.6.1.4.1.21528.2.1.1.69.2.1
Version	2.1
First version date of effect	01/07/2016
Security classification	PUBLIC
Approved by	Gergely Vanczák
Date of approval	05/08/2016
Date of effect	05/09/2016

Microsec Micro Software Engineering & Consulting Private Company Limited by Shares
Hungary, H-1031 Budapest, Záhony u. 7. D

Version	Description	Effect date	Author(s)
2.0	First independent, eIDAS conform time stamping practice statement. OID: 1.3.6.1.4.1.21528.2.1.1.69.2.0	01/07/2016	Sándor Szőke, Dr.
2.1	Changes according to the NMHH comments. OID: 1.3.6.1.4.1.21528.2.1.1.69.2.1	05/09/2016	Melinda Szomolya, Sándor Szőke, Dr.

Table of Contents

1 Introduction

This document contains the *Qualified Time-Stamping Practice Statement* defined by e-Szignó Certification Authority (hereinafter: *Time-Stamping Provider*) operated by Microsec ltd.

The *Qualified Time-Stamping Practice Statement* complies with the requirements set by the eIDAS regulation [1], the service provided according to these regulations is an EU qualified trusted service.

The prerequisites for the qualified trusted service provision and the "EU Trust Mark" indication are:

- the service shall be audited by an independent assessment organization authorized to carry out such an assessment, and it shall issue a conformity assessment certificate for the *Time-Stamping Provider*;
- the *Time-Stamping Provider* shall submit the conformity assessment certificate to the National Media and Infocommunications Authority, as it is the official monitoring body;
- the National Media and Infocommunications Authority shall accept the submitted conformity assessment certificate and it shall publish the service in the national trusted list.

1.1 Overview

The *Qualified Time-Stamping Practice Statement* is a "set of rules that specify the usability of a *Time Stamp* for a community and/or a class of applications with common safety requirements".

This *Qualified Time-Stamping Practice Statement* is only one of several documents issued by the*Time-Stamping Provider* that collectively govern the provided service conditions. Other important documents include General Terms and Conditions, the *Qualified Time-Stamping Policy*, and other customer and partner agreements.

Section 1.6 of this document specifies several terms which are not or not fully used in this sense in other areas. The terms to be used in this sense are indicated by capitalization and italicization throughout this document.

1.2 Document Name and Identification

1.2.1 Document Identification

Issuer	e-Szignó Certification Authority
Document Title	eIDAS conform Qualified Time Stamping Practice Statement
OID	1.3.6.1.4.1.21528.2.1.1.69
Document Version	2.1
Date of Effect	05/09/2016

The current version of the document is available on the website of the the *Time-Stamping Provider*, and the customer service office of the *Time-Stamping Provider*.

1.2.2 Compliance

The *Time Stamp*s issued according to the present *Qualified Time-Stamping Practice Statement* are compliant with the requirements below:

- ETSI EN 319 421 [17]
  BTSP: a best practices policy for time-stamp
  OID: itu-t(0) identified-organization(4) etsi(0)time-stamp-policy(2023)policy-identifiers(1) best-practices-ts-policy (1)

The *Time-Stamping Provider* includes its own OID in the *Time Stamp*s it issues, and it supports the aforementioned ETSI time-stamping policy (i.e. BSTP).

1.2.3 Effect

This *Qualified Time-Stamping Practice Statement* is in effect from the 05/09/2016 date of entry into force to until its withdrawal.

The effect of The *Qualified Time-Stamping Practice Statement* includes each and every one of the participants mentioned in section 1.3.

The geographical scope of the present *Qualified Time-Stamping Practice Statement* is the territory of Hungary. The current Hungarian law shall prevail in relation to the operation of The *Time-Stamping Provider*.

The service provided according to the present *Qualified Time-Stamping Practice Statement* is available worldwide. The validity of the *Time Stamp*s made according to the the *Qualified Time-Stamping Practice Statement* is independent from the geographic location where they were made or from the geographic location where they are used.

1.2.4 Time-Stamping Policy

The present *Qualified Time-Stamping Practice Statement* undertakes the compliance with the requirements of the *Qualified Time-Stamping Policy* below:

- "e-Szignó Certification Authority – eIDAS conform Qualified Time Stamping Policy [31], OID: 1.3.6.1.4.1.21528.2.1.1.86.2.1"

the current version and all previous versions of The *Qualified Time-Stamping Policy* is available at the following URL:

`https://e-szigno.hu/en/pki-services/certificate-policies-general-terms-and-conditions.html`

1.3 PKI Participants

1.3.1 Provider

The *Time-Stamping Service Provider* is a *Trust Service Provider*, that issues *Time Stamp*s within the framework of a *Trust Service*, and performs the related tasks.

The *Time-Stamping Provider* information:

Name	MICROSEC Micro Software Engineering & Consulting Private Limited Company by Shares
Company registry number	01-10-047218 Company Registry Court of Budapest
Head office	1031 Budapest, Záhony street 7. D. building
Telefone number	(+36-1) 505-4444
Telefax number	(+36-1) 505-4445
Internet address	https://www.microsec.hu, https://www.e-szigno.hu

The e-Szignó Certification Authority within the organization of the *Time-Stamping Provider* provides the service related tasks as an autonomous business unit. This autonomous business unit consists of the following two parts:

- customer service office,
- certification unit.

Customer Service Office

The customer service office is responsible for the communication with the *Subscriber*.
The contact information of the office and the consumer protection organization:

The name of the provider unit	e-Szigno Certification Authority
Customer service	1031 Budapest, Záhony str. 7., Graphisoft Park, D building
Office hours of the customer service	on workdays between 8:30-16:30 by prior arrangement
Telephone number of the customer service	(+36-1) 505-4444
E-mail address of the customer service	info@e-szigno.hu
Service related information access	https://www.e-szigno.hu
Place for registering complaints	Microsec zrt. 1031 Budapest, Záhony str. 7., Graphisoft Park, D building
Relevant Consumer Protection Inspectorate	Budapest Capital Authority for Consumer Protection 1052 Budapest, Városház str. 7. 1364 Budapest, Pf. 144.

Main Parts of the Service

The service consists of the following parts:

- reception of the time-stamp request, during which the system of the the *Time-Stamping Provider* identifies the *Subscriber* and receives the request,
- time-stamp generation, during which the system of the *Time-Stamping Provider* generates the time-stamp corresponding to the time-stamp request, containing current, authentic time;
- time-stamp issuance, during which the the *Time-Stamping Provider* sends to the *Subscriber* the time-stamp generated based on the request;

- internal time production system, which provides the accurate time source synchronized to the UTC time to be included in the *Time Stamp*s.

1.3.2 Clients

The *Subscriber* (Client), is who subscribes for the Time-Stamping Service provided by the the *Time-Stamping Provider*, and within the framework of the service requests *Time Stamp*s from the the *Time-Stamping Provider* for a service fee. The *Subscriber* can be a natural or a legal person, or multiple natural persons can request *Time Stamp*s on behalf of the *Subscriber*.

1.3.3 Relying Parties

The *Relying Party* validates and uses the *Time Stamp*s issued by the the *Time-Stamping Provider*. The *Relying Party* is not in a contractual relationship with the the *Time-Stamping Provider*.

1.4 Time-Stamp Usage

The *Time Stamp* credibly certifies that, the electronic document with the *Time Stamp* already existed in the given state before the time indicated in the *Time Stamp*.

1.5 Policy Administration

1.5.1 Organization Administering the Document

The data of the organization administering the present *Qualified Time-Stamping Practice Statement* can be found in the following table:

Organization name	Microsec e-Szignó Certification Authority
Organization address	Hungary, H-1037 Budapest, Záhony street 7. building D
Telephone number	+36 1 505-4444
Fax number	+36 1 505-4445
E-mail address	info@e-szigno.hu

1.5.2 Contact Person

Questions related to the present *Qualified Time-Stamping Practice Statement* can be directly put to the following person:

Contact person	Process management department leader
Organization name	Microsec ltd.
Organization address	Hungary, H-1037 Budapest, Záhony street 7. building D
Telephone number	+36 1 505-4444
Fax number	+36 1 505-4445
E-mail address	info@e-szigno.hu

1.5.3 Person or Organization Responsible for the Suitability of the Practice Statement for the *Qualified Time-Stamping Policy*

The provider that issued the *Qualified Time-Stamping Practice Statement* is responsible for its conformity with the *Qualified Time-Stamping Policy* referenced in it and for the provision of the service according to the regulations contained therein.

The *Qualified Time-Stamping Practice Statement*s and the provision of the services are supervised by the National Media and Infocommunications Authority. The National Media and Infocommunications Authority maintains a register on the *Certificate Policies* and on the *Time-Stamping Provider*s applying these policies.

The register of the National Media and Infocommunications Authority on trust services is available on the below link:

http://webpub-ext.nmhh.hu/esign2016/

1.5.4 Practice Statement Approval Procedures

The writing, the acceptance and the issuance of the new or any modified versions of the *Qualified Time-Stamping Practice Statement* happens according to unified processes – as defined in detail in section 9.12.1.

1.6 Definitions and Acronyms

1.6.1 Definitions

Data Centre	A facility designed for the placement and operation of computer systems and associated components. These components typically include telecommunications systems and communication connections, redundant power supply, data storage, air conditioning, fire protection and safety systems.
Trust Service Supervisory Body	"The National Media and Infocommunications Authority, the supervising authority monitoring the *Trust Service*s." *(Act CCXXII. of 2015. [4] 91.§ 1. paragraph)*

Trust Service	"Means an electronic service normally provided for remuneration which consists of: • the creation, verification, and validation of electronic signatures, electronic seals or electronic time stamps, electronic registered delivery services and certificates related to those services, or • the creation, verification and validation of *Website Authentication Certificate*; or • the preservation of electronic signatures, seals or certificates related to those services; " *(eIDAS [1] 3. article 16. point)*
Trust Service Policy	"A set of rules in which a *Trust Service Provider*, relying party or other person requires conditions for the usage of the *Trust Service* for a community of the relying parties and/or a class of applications with common safety requirements." *(Act CCXXII. of 2015. [4] 1. § 8. point)*
Trust Service Provider	"A natural or a legal person who provides one or more *Trust Service*s either as a qualified or as a non-qualified *Trust Service Provider*." *(eIDAS [1] 3. article 19. point)*
Electronic Time Stamp	"Means data in electronic form which binds other data in electronic form to a particular time establishing evidence that the latter data existed at that time." *(eIDAS [1] 3. article 33. point)*
Subscriber	A person or organization signing the service agreement with the *Time-Stamping Provider* in order to use some of its services.
Relying Party	Recipient of a time-stamp who relies on that time-stamp.
Root Certificate	Also known as top level certificate. Self-signed *Certificate*, which is issued by a specific *Certification Unit* for itself, which is signed with its own private key, so it can be verified with the Signature-Verification Data – indicated on the certificate.
HSM: Hardware Security Module	A hardware-based secure tool that generates, stores and protects cryptographic keys and provides a secure environment for the implementation of cryptographic functions.

Certification Authority	A *Trust Service Provider*, who/which identifies the requester within the confines of the certification service, issues *Certificate*s, keeps a record, receives the *Certificate* related data changes, and publishes the regulations belonging to the *Certificate* and the information on the current state (especially on possible revocation) of the *Certificate*.
Certification Unit	A unit of the *Time-Stamping Provider*'s system that signs the *Certificate*s. Always just one Certificate-Creation Data (signing key, signature-creation data) belongs to a *Certification Unit*. It is possible that a Certification Authority simultaneously operate several *Certification Unit*s.
Time-Stamping Policy	A *Trust Service Policy* in which a *Trust Service Provider*, relying party or other person (organization) requires conditions for the usage of the time-stamping service for a community of the relying parties and/or a class of applications with common safety requirements.
Time-Stamping Service Provider	A *Trust Service Provider*, who issues *Time Stamp*s within the framework of a *Trust Service*, and performs related duties.
Time-Stamping Unit	A system unit of the *Trust Service Provider*, which performs the signature or seal of time-stamps. A time-stamp unit always has one electronic signature or seal creation data. It is possible, that a *Trust Service Provider* operates multiple time-stamping units at the same time.
Compromise	A cryptographic key is compromised, when unauthorized persons might have gained access to it.
Intermediate Certification Unit	A *Certification Unit* whose *Certificate* was issued by another *Certification Unit*.
Cryptographic Key	An individual digital signal series controlling cryptographic transformation, the knowledge of which is required for encryption, decryption, electronic signature creation and verification.
Key Management	The production of cryptographic keys, their delivery to users or its algorithmic implementation, as well as the registration, storage, archival, revocation and termination of keys which are closely linked to the used security method.

Private Key	In the public key infrastructure, the element of an asymmetric cryptographic key pair for an actor that the *Subject* shall keep strictly secret. During the issuance of *Certificate*s, the *Certification Authority* uses the private keys of the *Certification Unit* for placing an electronic signature or seal on the *Certificate* to protect it.
Qualified Trust Service	"A *Trust Service* that meets the applicable requirements laid down in the eIDAS Regulation." *(eIDAS [1] article 3. point 17.)*
Qualified Trust Service Provider	"A *Trust Service Provider* who provides one or more *Qualified Trust Service*s and is granted the qualified status by the supervisory body." *(eIDAS [1] article 3. point 20.)*
Public Key	In the public key infrastructure, the element of an asymmetric cryptographic key pair belonging to an actor, which should be made public. The disclosure is typically in the form of a *Certificate*, which links the name of the actor with its public key. The authenticity of the *Certificate*s can be verified with the public key of the *Certification Unit*.
Public Key Infrastructure, PKI	An infrastructure based on asymmetric cryptography, including the cryptographic algorithms, keys, certificates, the related standards and legislation, the underlying institutional system, a variety of providers and devices.
Extraordinary Operational Situation	An extraordinary situation causing disturbance in the course of the operation of the *Time-Stamping Provider*, when the continuation of the normal operation of the *Time-Stamping Provider* is not possible either temporarily or permanently.
Organization	Legal person.
Trust Service Practice Statement	"The statement of the *Trust Service Provider* of the detailed procedures or other operational requirements used in connection with the provision of particular *Trust Service*s." *(Act CCXXII. of 2015. [4] 1. § point 41.)*
Service Agreement	"The contract between the *Trust Service Provider* and the *Trust Service* client, which includes the conditions for the provision of the *Trust Service* and for using the services." *(Act CCXXII. of 2015. [4] 1. § point 42.)*

Certificate	"The electronic signature certificate, the electronic seal certificate and the *Website Authentication Certificate*, and all those electronic verifications issued within the framework of the *Trust Service* by the service provider, which includes the certificate related verification data and the certificate usage related information, and which as an electronic document is reliably protected against the available counterfeiting technologies at the time of the issuance and during its validity period." *(Act CCXXII. of 2015. [4] 1. § point 44.)*
Certificate Application	The data and statements given by the *Applicant* to the *Time-Stamping Provider* for *Certificate* issuance, in which the *Applicant* reaffirms the authenticity of data to be indicated on the *Certificate*.
Certificate Repository	Data repository containing various *Certificate*s. A Certification Authority has a Certificate Repository in which the issued certificates are disclosed, but the system containing Certificates available to the application on the computer of the *Relying Party* is also called Certificate Repository.
Client	The *Subscriber* other denomination.
Revocation	The termination of the *Certificate*'s validity before the end of the validity period indicated on the *Certificate* too. The *Certificate* revocation is permanent, the revoked *Certificate* cannot be reinstated any more.
Revocation Status Records	The records of the suspended and revoked *Certificate*s which includes the fact of the suspension or revocation and the time of the suspension or revocation maintained by the *Certification Authority*.

1.6.2 Acronyms

CRL	Certificate Revocation List
eIDAS	electronic Identification, Authentication and Signature
GMT	Greenwich Mean Time
IERS	International Earth Rotation and reference System Service
LDAP	Lightweight Directory Access Protocol
NMHH	National Media and Infocommunications Authority
OCSP	Online Certificate Status Protocol

OID	Object Identifier
PKI	Public Key Infrastructure
TAI	International Atomic Time
TSA	Time Stamping Authority
TSP	Trust Service Provider
TSU	Time-Stamping Unit
TDS	TSA Disclosure Statement
UTC	Coordinated Universal Time

2 Publication and Repository Responsibilities

2.1 Repositories

The *Time-Stamping Provider* publishes the *Qualified Time-Stamping Policy*, the *Qualified Time-Stamping Practice Statement* and other documents containing the terms and conditions its operation is based on.

2.2 Publication of Certification Information

The *Time-Stamping Provider* discloses on its webpage its own provider *Certificate*s.

2.2.1 Publication of the *Time-Stamping Provider* Information

The *Time-Stamping Provider* discloses the contractual conditions and policies electronically on its website.

The new documents to be introduced are disclosed on the website 30 days before coming into force.

The documents in force are available on the site in addition to all previous versions of all documents.

The actual version of policies and contractual conditions is readable in printed form at the customer service of the *Time-Stamping Provider*.

The *Time-Stamping Provider* makes available the *Qualified Time-Stamping Policy*, the *Qualified Time-Stamping Practice Statement* and the Service Agreement to the *Client* on a durable medium following the conclusion of the contract.

The *Time-Stamping Provider* notifies its *Client*s about the change of the General Terms and Conditions.

2.3 Time or Frequency of Publication

2.3.1 Frequency of the Publication of Terms and Conditions

The disclosure of the *Qualified Time-Stamping Practice Statement* related new versions is compliant with the methods described in Section 9.12.

The *Time-Stamping Provider* discloses other regulations, contractual conditions and their new versions if necessary.

The *Time-Stamping Provider* publishes extraordinary information without delay in accordance with the legal requirements and in the absence thereof when necessary.

3 The Certificate of the Time-Stamping Unit and Time-Stamping

3.1 Identification of the User

Only the *Subscriber*s of the the *Time-Stamping Provider* can use the service, after the successful identification of the *Subscriber*.

The identification depending on the used service can be done with the authentication certificate or a username-password pair given to the *Subscriber*. Each access methods belong to a different URL as follows:

- Authentication certificate `https://tsa.e-szigno.hu/tsa`
- Username and password: `https://btsa.e-szigno.hu/tsa`

3.2 The Certificate of the Time-Stamping Unit

The *Time-Stamping Provider* publishes the public key of the *Time-Stamping Unit* as a *Certificate* on its website amongst its provider *Certificate*s.

The *Certificate* of the *Time-Stamping Unit* is issued by Microsec e-Szignó Certification Authority, which provides a trust service according to ETSI EN 319 411-1 [11] and the ETSI EN 319 411-2 [12] as a an eIDAS qualified *Trust Service Provider*.

The *Time-Stamping Provider* only begins the issuance of the *Time Stamp*s with the new private key, if:

- the *Certificate* belonging to the given private key was published on the national trust service provider list [30];
- the signature of the *Certificate* was verified through a full certificate chain to a trusted *Certification Authority*;
- it was ascertained that the private key and the public key published in the *Certificate* belong together.

3.3 The Time-Stamp

The *Time Stamp* issued by the the *Time-Stamping Provider* complies with the IETF RFC 3161 [23] and the ETSI EN 319 422 [18] standards;

Accordingly the characteristics of the *Time Stamp* are:

- it includes the hash sent in the message of the requester.

- it includes the OID of the *Time-Stamping Policy*.
- it has a unique identifier.

The *Time-Stamping Unit*s operate in the secure *Data Centre* of the *Time-Stamping Provider*, which guarantees the adequacy of the time value given in the *Time Stamp* (see section 6).

The internal clock of the *Time-Stamping Unit*(s) used for the issuance of the *Time Stamp*s are traceable to the UTC exact time (see section 3.4).

The accuracy of the time indicated in the *Time Stamp*s meets the requirements of the *Time-Stamping Policy* (see section 3.4). The undertaken accuracy is also indicated in the *Time Stamp* itself (see section 3.3.2).

The *Time-Stamping Unit* does not issue a *Time Stamp*as soon as it detects that its internal clock accuracy differs from the current time as UTC more than the specified value (see section 3.4).

The *Time-Stamping Provider* does not use the private keys of the *Time-Stamping Unit*s for other purposes than the certification of the *Time Stamp*s (see section 6.1.2).

After the lifetime of the keys ends, the private keys are deleted according to the details in section 6.3.1, so the *Time-Stamping Unit*s can not issue a *Time Stamp* with an expired private key.

3.3.1 The Time-Stamp Request

The *Time-Stamping Provider* supports the *Time Stamp* requests according to the IETF RFC 3161 [23] section 2.4.1. including the usage of the following fields:

- "reqPolicy"
- "nonce"
- "certReq"

The *Time-Stamping Provider* does not support the usage of the field below:

- "extensions"

The *Time-Stamping Provider* accepts the hashing algorithms in the *Time Stamp* requests specified by ETSI TS 119 312 [19] and the current National Media and Infocommunications Authority algorithmic decree. It takes into account when selecting the hashing algorithms the planned usage time of the *Time Stamp* and the expected duration of the hashing method adequacy.

The currently supported hashing algorithms are:

sha256	{ joint-iso-itu-t(2) country(16) us(840) organization(1) gov(101) csor(3) nistAlgorithm(4) hashAlgs(2) sha256(1) }

The Structure of the Time-Stamp Request

- Version
  The format of the *Time Stamp* request corresponds to version "v1" specified by the IETF RFC 3161 [23], so this field contains the value "1".

- MessageImprint
  The data to be stamped with a *Time Stamp*, which consists of two parts:
  - Hashing algorithm (hashAlgorithm)
    The OID of the hashing algorithm the hash was created with
  - Hash (hashedMessage)
    The hash itself that shall be stamped with the *Time Stamp*. The length of the data shall correspond to the given hashing algorithm.
- *Qualified Time-Stamping Policy* identifier (reqPolicy)
  optional field
  Specifies according to which *Qualified Time-Stamping Policy* the *Time Stamp* is requested to be issued.
- Nonce (nonce)
  optional field
  A maximum 64-bit integer that serves to provide the uniqueness of the *Time Stamp*. In case of the inclusion of the "nonce" in the *Time Stamp* request, the *Time Stamp* response must include the same value.
- Certificate request (certReq)
  by default "FALSE"
  If the request includes a "TRUE" value, the *Certificate* of the *Time-Stamping Unit* referenced in the "SigningCertificate attribute" must be included in the response.
- Extensions (extensions)
  optional field
  The requester may provide extra information in this field. The *Time-Stamping Provider* does not support the usage of this field. If a request which contains this field is received, the *Time-Stamping Provider* does not issue a *Time Stamp*, instead it replies with the "unacceptedExtension" error message.

3.3.2 Time-Stamp Response

The *Time-Stamping Provider* supports the *Time Stamp* responses according to IETF RFC 3161 [23] section 2.4.2 with the following extensions:

- "accuracy";
- "nonce".

In case of the inclusion of the "nonce" in the *Time Stamp* request, the *Time Stamp* response includes the same value.

The *Time-Stamping Provider* uses the cryptographic algorithm sets and key lengths for signing the *Time Stamp*s specified by ETSI TS 119 312 [19] and appointed in the current National Media and Infocommunications Authority algorithmic decree. It takes into account the planned usage time of the *Time Stamp* when selecting the cryptographic algorithm sets and key lengths.

The supported cryptographic algorithm set:

sha256WithRSAEncryption	{ iso(1) member-body(2) us(840) rsadsi(113549) pkcs(1) pkcs-1(1)sha256WithRSAEncryption(11) }

The identifier of the supported ETSI Time-Stamping profile (BTSP):
itu-t(0) identified-organization(4) etsi(0) time-stamp-policy(2023) policy-identifiers(1) baseline-ts-policy (1).

The Structure of the Time-Stamp Response

- Status (PKIStatusInfo)
  The status information about the success of the issuance according to IETF RFC 3161 [23] section 2.4.2.

- *Time Stamp* token (TimeStampToken)
  optional field
  It contains the issued *Time Stamp* in case of status field values "0" or "1", otherwise this field is not included in the response.

The Structure of the Time-Stamp Token

The *Time Stamp* token signed by the *Time-Stamping Unit* according to IETF RFC 3161 [23] section 2.4.2, the fields of which are:

- Version (version)
  The format of the *Time Stamp* token corresponds to version "v1" specified by the IETF RFC 3161 [23], so this field contains the value "1".

- *Qualified Time-Stamping Policy* identifier (policy)
  obligatory field
  Specifies according to which *Qualified Time-Stamping Policy* the *Time Stamp* is requested to be issued. If the request contained the "reqPolicy" field, the *Time Stamp* is issued only in case the OID corresponding to the one in the request is supported, in any other case the request is refused with the "unacceptedpolicy" error message.

- Message hash (messageImprint)
  The data stamped with the *Time Stamp* containing the same value as in the request.

- Serial number (serialNumber)
  obligatory field
  Unique serial number for every *Time Stamp* the *Time-Stamping Unit* issues in the whole life-cycle of the unit. Maximum length is 160 bit.

- Time (genTime)
  obligatory field
  Time of issuance of the *Time Stamp* given in UTC format. The "genTime" in the *Time Stamp*s issued by the *Time-Stamping Provider* is given with a precision of one second according to RFC 2459 [22].

- Accuracy (accuracy)
  optional field

This field specifies up to what extend may the time given in the token deviate from UTC time. The *Time-Stamping Provider* always includes the "Accuracy" in the *Time Stamp*s it issues.

- Ordering (ordering)
  "FALSE" by default
  The value of the field could be "TRUE", if the issued *Time Stamp*s could be ordered clearly based on a given time value. Due to the huge number of *Time Stamp*s the the *Time-Stamping Provider* issues, this condition is not met, so this field is always indicated with a "FALSE" value.

- Nonce (nonce)
  optional field
  A maximum 64-bit integer that serves to provide the uniqueness of the *Time Stamp*. In case of the inclusion of the "nonce" in the *Time Stamp* request, the *Time Stamp* response must include the same value.

- Tsa (tsa)
  optional field
  The name of the *Time-Stamping Unit* can be indicated here. If this field is used, the given name must match with one of the "subject name" values in the the signing *Certificate*.

- Extensions (extensions)
  optional field
  The *Time-Stamping Provider* uses the following extension to indicate the qualified status of the *Time Stamp* according to eIDAS [1]:

  – Qualified Certificate Statements – non critical
    OID: 1.3.6.1.5.5.7.1.3
    The extension contains one statement: "esi4-qtstStatement-1"

3.4 Time-Stamp Accuracy

The *Time-Stamping Provider* guarantees that the deviation of the time indicated in the *Time Stamp*s from the UTC time is at most 1 second.

The *Time-Stamping Unit* clock provider systems are in the strictly protected *Data Centre* of the the *Time-Stamping Provider*, which makes the unnoticed modification of the clock impossible.

The *Time-Stamping Provider* constantly monitors its internal time provider systems. If the internal time deviation from the UTC time exceeds 0.1 second, the the *Time-Stamping Provider* suspends the issuance of *Time Stamp*s.

The accuracy of the internal clock of the *Time-Stamping Provider* is examined every year by the security committee of the *Time-Stamping Provider*.

3.5 Time-Stamp Synchronization

The time indicated in the *Time Stamp* is given by the internal clock of the *Time-Stamping Provider* which is synchronized by the the *Time-Stamping Provider* with two separate Stratum-1 UTC sources:

- one accurate time source uses the satellite-based GPS signal;
- the other accurate time source is based on the longwave time signal service (DCF77).

In order to provide accuracy the the *Time-Stamping Provider* synchronizes its own internal clock with the above Stratum-1 sources within a 0.1 second accuracy, and it performs this synchronization more than 4 times a day.

This way the *Time-Stamping Provider* guarantees that the deviation of the time indicated in the *Time Stamp*s from the UTC time base is at most 1 second.

3.5.1 Leap Second Management

When a leap second occurs the *Time-Stamping Provider* performs the clock synchronization based on the notification of the competent body at the given time according to the specification of the ETSI 319 421 [17] annex C and as defined in the ITU-R TF.460-6 [27] recommendation.

A positive leap second occurs after 23:59:59 UTC the given day, after what 23:59:60 follows, and then UTC time continues with the usual next day 00:00:00.

3.5.2 Daylight Saving Time Management

The *Time-Stamping Provider* writes UTC time into the issued *Time Stamp*s.

The *Time-Stamping Provider* draws the attention of the *Relying Parties* that some applications may display the time given in the *Time Stamp*s in a different way and in different format to the users, usually using local time. Such a display may give rise to misunderstandings to the *Relying Parties* in different time zones, especially near the spring and autumn Daylight Saving Time boundary.

3.6 Time-Stamp Validation

During the verification of the validity of the electronic signature or electronic seal on the *Time Stamp* the *Relying Party* should act as described in the ETSI EN 319 102-1 [8] specification.

During the verification of the *Time Stamp*:

- it shall be verified that the time-stamped document belongs together with the *Time Stamp* and the *Certificate* of the the *Time-Stamping Provider*;
- the signature on the *Time Stamp* shall be verified;
- it shall be verified that the *Time Stamp* meets the specific purpose, among other things that the accuracy, the reliability and the liability of the related Time-Stamping Service Provider is appropriate.

3.7 Time-Stamping Service Availability

The *Time-Stamping Provider* guarantees the continuous availability of the service and the terms and conditions for the use of the *Time Stamp*s the *Time-Stamping Provider* issues with an availability of at least 99.9% per year, while service downtimes do not exceed at most 3 hours in each case.

3.8 Issuing Non-Qualified Time-Stamps

A *Time-Stamping Unit* issuing qualified *Time Stamp*s according to the 910/2014/EU regulation [1] shall not issue non-qualified *Time Stamp*s.

The *Time-Stamping Provider* operated by the e-Szignó Certification Authority only issues qualified *Time Stamp*s.

3.9 Time-Stamping Unit Key Management

The following requirements shall be adhered to within the *Time-Stamping Unit*s:

- the algorithms and key sizes used for the certification of the *Time Stamp*s comply with the following requirements:
  - ETSI TS 119 312 [19];
  - the current National Media and Infocommunications Authority algorithmic decree issued according to the year 2015. act CCXXII [4] 92. § (1) b).
- if possible the signing or seal creation private key shall not be imported into multiple *Hardware Security Module*s at the same time;
- if multiple *Hardware Security Module*s use the same signing or seal creation private key, then those must belong to the same *Certificate*;
- only one *Time Stamp* signing or seal creation private key shall be active in a *Time-Stamping Unit* at a time;
- a hardware-software unit can serve multiple separate *Time-Stamping Unit*s in case of the compliance with the above requirements.

3.10 Time Stamp Transport Protocol

The service can only be used through secure HTTPS protocol. The secure channel consists of the following, based on the *Subscriber* authentication method:

- in case of username and password based authentication, according to the *Certificate* of the *Time-Stamping Unit*.
- in case of authentication *Certificate* based user identification, according to the mutual authentication of the client and the server.

4 Certificate Life-Cycle Operational Requirements

4.1 Key Pair and Certificate Usage

4.1.1 Subscriber Private Key and Certificate Usage

The private key of the *Time-Stamping Unit* shall only be used for the certification of the *Time Stamp*s issued by the *Time-Stamping Unit*, and using the private key for any other purpose is prohibited.

4.1.2 Relying Party Public Key and Certificate Usage

To retain the level of security guaranteed by the *Time-Stamping Provider*, in the course of using the the *Relying Party* is recommended to proceed prudentially particularly regarding to the following:

- the *Relying Party* shall verify the validity and revocation status of the *Certificate*;
- the verifications related to the *Certificate* should be carried out for the entire certificate chain;
- it is recommended to verify that the *Certificate* was issued according to the appropriate Certificate Policy;
- the *Relying Party* shall consider any restrictions indicated in the *Certificate* or in the regulations referenced in the *Certificate*.

5 Facility, Management, and Operational Controls

The *Time-Stamping Provider* applies physical, procedural, and personnel security precautions that comply with acknowledged standards, along with the administrative and governance related procedures that enforce these.

The *Time-Stamping Provider* keeps a record of the system units and resources related to the service provision, and conducts a risk assessment on these. It uses protective measures proportional to the risks related to the individual elements.

The *Time-Stamping Provider* monitors the capacity demands and ensures that the adequate processing power and storage are available for the provision of the service.

5.1 Physical Controls

The *Time-Stamping Provider* takes care that physical access to critical services is controlled, and keeps physical risk of the assets related to critical services at a minimum.

The purpose of physical precautions is to prevent illegitimate access, damage, and unauthorized access to the *Time-Stamping Provider*'s information, and physical zones.

Services that process critical and sensitive information are implemented at secure locations in the system of the *Time-Stamping Provider*.

The provided protection is proportional to the identified threats of the risk analysis that the *Time-Stamping Provider* has performed.

In order to provide adequate security:

- The *Time-Stamping Provider* implements the strongly protected services in its protected computer room. This computer room has been designed and constructed specifically for this purpose, by its design uniform enforcement of various aspects of protection (the placement and structure of the site, physical access (access control and supervision), power supply, air conditioning, protection against water leakage and flooding, fire prevention and protection, media storage etc.) took place.

- The *Time-Stamping Provider* implements every critical service and every necessary tool in a separate security zone. All the devices necessary for this are placed in a protected computer room – forming part of the security zone.

5.1.1 Site Location and Construction

The IT system of the *Time-Stamping Provider* is located and operated within a properly secured *Data Centre* with physical and logical protection that prevents illegitimate access. Defensive solutions – as for example guarding, security locks, intrusion detection systems, video surveillance system, access control system – are applied over the course of locating and establishing the *Data Centre* that are built on each other and interdependent and together they provide a powerful protection system for the IT systems participating in service provision, and for the preservation of the confidential data stored by the provider.

5.1.2 Physical Access

The *Time-Stamping Provider* protects devices and equipment that take part in the service provision from unauthorized physical access in order to prevent tampering with the devices.
Time-Stamping Provider ensures that:

- each entry to the *Data Centre* is registered;
- entry to the *Data Centre* may happen after the simultaneous identification of two authorized staff members with trusted roles – and at least one of the staff members shall be a system administrator;
- persons without independent authorization can only stay in the *Data Centre* in justified cases, for the time required and accompanied by personnel with appropriate rights;
- the entry logs shall be archived continuously and evaluated weekly.

The activation data (passwords, PIN codes) of the devices shall not be stored openly even in the *Data Centre*.
In the presence of unauthorized persons:

- data media containing sensitive information are physically out of reach;
- the logged-in terminals are not left without supervision;
- no work process is carried out during which confidential information may be revealed.

When leaving the computer room the administrator shall verify that:

- every equipment of the *Data Centre* is in an adequately secure operation state;
- there's no terminal left logged-in;
- physical storage devices are locked properly;
- systems, devices providing physical protection operate properly;

- the alarm system has been activated.

There are appointed responsible people to carry out regular physical security assessments. The results of the examinations are recorded in the appropriate log entries.

5.1.3 Power and Air Conditioning

The *Time-Stamping Provider* applies an uninterruptible power supply unit in the *Data Centre* that:

- has adequate capacity to ensure power supply for the *Data Centre*'s IT and subsidiary facility systems;
- protects IT equipment from voltage fluctuations in the external network, power outages, spikes and other;
- in case of lasting power outage has its own power generation equipment, which – by allowing refueling – is able to provide the necessary energy for any period of time.

The air of the outer environment shall not get into the *Data Centre* directly. The *Data Centre* air purity is ensured with adequate filter system to detect a variety of contaminants from the air (dust, pollutants, and corrosive materials, toxic or flammable substances). The ventilation system provides the necessary amount of fresh air with adequate filtration for the safe working conditions of the operators.

The humidity is reduced to the level required by the IT systems.

The *Time-Stamping Provider* uses cooling systems with proper performance to provide the necessary operating temperature, to prevent overheating of IT devices.

5.1.4 Water Exposures

The *Data Centre* of the *Time-Stamping Provider* is adequately protected from water intrusion and flooding. The total area of the security zone is free from sanitary facilities, there is not any drain or water pipe close to it. The total area of water security zone is monitored by an intrusion detection system. In the protected computer room security is further increased by the use of a raised floor.

5.1.5 Fire Prevention and Protection

In the *Data Centre* of the *Time-Stamping Provider*, a fire protection system approved by the competent fire headquarters operates. Smoke and fire detectors automatically alert the fire brigade. Water vapor based, automatic fire extinguishing system has been installed in the computer room, which is not hazardous to human life, and does not damage the IT equipment.

There is the type and quantity of manual fire extinguishers in accordance with the relevant regulations at clearly visible locations in each room.

5.1.6 Media Storage

The *Time-Stamping Provider* protects its media storages from unauthorized access and accidental damage. All audit and archive data is created in duplicate. The two copies are stored separately from each other physically, at locations in a safe distance from each other. The stored media storages are protected from damaging environmental influences such as low or high temperatures, dirt, moisture, sunlight, strong magnetic fields, strong radiation.

The *Time-Stamping Provider* stores the primary media storages in the operational room of the certification organization, a code locked fireproof vault, the secondary copies in a vault in the customer service office.

5.1.7 Waste Disposal

The *Time-Stamping Provider* ensures the environmental standards compliant disposal of the superfluous assets, and media.

The *Time-Stamping Provider* does not use the electronic storage media containing information classified as confidential even for storing data classified as not confidential after deleting their content and devices like that shall not be taken outside of the premises of the *Time-Stamping Provider*. The *Time-Stamping Provider* physically destroys – according to the rules of disposal – the defective for any other reason unusable, redundant media storages containing confidential classified information:

- chops paper documents up in a shredder machine;
- disassembles the hard drives and smashes the critical components;
- destroys the optical disc with a suitable shredder machine.

5.1.8 Off-Site Backup

The *Time-Stamping Provider* creates a backup weekly from which the whole service could be restored in case of a fatal error. The backups – at least including the last full backup – are stored at an external location that's physical and operational protection is identical to the primary site. The secure data transmission from the primary to the reserve locations is resolved.

5.2 Procedural Controls

The *Time-Stamping Provider* takes care that its systems are operated securely, according to the rules, and with a minimal risk of defects.

Procedural precautions have the objective of supplementing, and at the same time intensifying the effectiveness of physical safeguards, along with those applicable to personnel, by means of appointing and isolating trusted roles, documenting the responsibilities of various roles, as well as specifying the personnel headcounts and exclusion roles necessary for the various tasks, moreover identification and authentication expected in the various roles.

The *Time-Stamping Provider*'s internal governance system ensures that its operation complies with legal, as well as its internal regulations. In its system a responsible person shall be clearly assigned for every given system unit and process.

Individuals responsible for a given system element or process are assigned unambiguously to every system element and every process in its system. Development and operations related tasks are sharply segregated in the *Time-Stamping Provider*'s system. The auditing activity of the independent system auditor and the *Time-Stamping Provider*'s internal auditor ensures the system's appropriate operation.

5.2.1 Trusted Roles

The *Time-Stamping Provider* creates trusted roles for the performance of its tasks. The rights and functions are be shared among the various trusted roles in such a way that one user alone shall not be able to bypass the security protection measures.

The *Time-Stamping Provider* defines the following trusted roles, with the following responsibilities:

Manager with overall responsibility for the IT system of the *Time-Stamping Provider*: The individual responsible for the IT system.

Security officer: Senior security associate, the individual with overall responsibility for the security of the service.

System administrator: Infrastructure administrator. The individual with the task to install, configure and maintain the systems of the *Time-Stamping Provider*. Responsible, for the reliable and continuous operation of the assigned system units, and for monitoring the development of technology, and for the detection and proposing of development solutions of the vulnerabilities of each system component.

Operator: System operator, individual performing the IT system's continuous operation, backup and restore.

Independent system auditor: Individual who audits the logged, as well as archived dataset of the *Time-Stamping Provider*, responsible for verifying the enforcement of control measures the service provider implements in the interest of operation that complies with regulations, moreover for the continuous auditing and monitoring of existing procedures.

For the provision of trusted roles the manager responsible for the security of the *Time-Stamping Provider* formally appoints the *Time-Stamping Provider*'s employees.

Only those persons may hold a trusted role who are in employment relationship with the *Time-Stamping Provider*. Trusted roles shall not be hold in the context of a commission contract.

Up to date records are kept of the trusted roles and in case of any change, the National Media and Infocommunications Authority is notified without delay.

5.2.2 Number of Persons Required per Task

The security and operational regulations of the *Time-Stamping Provider* define that the following tasks can be only performed in protected environment, with the contemporaneous presence of two employees holding trusted roles:

- the generation of the *Time-Stamping Provider*'s own service key pair;

- the backup of the provider's private key;
- the activation of the provider's private key;
- the destruction of the provider's private key.

At least one of the persons performing the procedures listed above shall be a system administrator, and the other person shall not be the independent system auditor.

During the implementation of the operations listed, unauthorized person shall not be present in the room.

5.2.3 Identification and Authentication for Each Role

The users managing the IT system of the *Time-Stamping Provider* have unique identification data, enabling secure identification and authentication of the users.

The users can only access the IT systems critical from the aspect of the provision of the certification service after identification and authentication.

The identification and authentication data are revoked without delay in case of the cessation of user rights.

Every user of the IT system and every actor in the administrative process is identified individually.

For the verification of the physical access, the *Time-Stamping Provider* uses an RFID card based access control system, and for the logical access control, it uses VPN Certificates issued on a Secure Signature-Creation Device. Before successful authorization, not even a single safety-critical task can be performed. Every employee of the *Time-Stamping Provider* has exactly as many access rights, as it is absolutely necessary for the assigned role.

5.2.4 Roles Requiring Separation of Duties

Employees of the *Time-Stamping Provider* can hold multiple trusted roles at the same time, but the *Time-Stamping Provider* ensures that:

- the security officer and the registration officer shall not hold the independent system auditor role;
- the system administrator shall not hold the security officer and the independent system auditor role;
- the manager with overall responsibility for the IT system shall not hold the security officer and the independent system auditor role.

In addition to the aforementioned, the *Time-Stamping Provider* seeks the complete separation of trusted roles.

5.3 Personnel Controls

The *Time-Stamping Provider* takes care that its personnel policy, and its practices applicable to employing staff members intensify and support the reliability of the *Time-Stamping Provider*'s

operation. The objective of precautions applicable to personnel is to reduce the risk of human errors, theft, fraud and cases of misuse.

The *Time-Stamping Provider* addresses personnel security already during the hiring stage, including the conclusion of contracts, as well as their validation when they are being employed. In the case of all trusted roles, applicants have valid certificate of no criminal record at the time of the application. Every employee in a trusted role and external parties – who get in contact with the *Time-Stamping Provider*'s services – shall sign a non-disclosure agreement.

At the same time, the *Time-Stamping Provider* ensures for its employees obtaining as well as further developing of common, general know-how along with the specialized professional knowledge necessary for performing the various jobs.

5.3.1 Qualifications, Experience, and Clearance Requirements

As a hiring requirement, the *Time-Stamping Provider* requires at least intermediate education degree, but the *Time-Stamping Provider* continues to takes care that employees receive appropriate training. Immediately after recruitment, the *Time-Stamping Provider* grants a training for its new employees, under the course of which they acquire the knowledge necessary to carry out the job. The *Time-Stamping Provider* usually supports the professional development of the employees, but it also expects employees to independently develop their skills in their respective fields. Some of the employees of the *Time-Stamping Provider* have the role to detect and gather the technical and business innovations and to organize, and share this knowledge with their colleagues.

Trusted roles can be held at the *Time-Stamping Provider* only by persons, who have no external influence and possess the necessary expertise validated by the *Time-Stamping Provider*.

The manager with overall responsibility for the IT system can only be a person who has:

- specialized degree (mathematics, physics college or university degree or a college/university degree acquired at an engineering department belonging to the technical field of science);
- at least three years of expertise in professional working experience related to information security.

5.3.2 Background Check Procedures

The *Time-Stamping Provider* only hires employees for trusted or leading roles, who

- have a clean record and there's no proceeding in progress against them that may affect the impunity.
- are not subject to professional disqualifications prohibiting to exercise electronic signatures related services.

At the time of the appointment, shall the leading role holder *Time-Stamping Provider* employee with a statement, a trusted role holder employee with a certificate of good conduct less than 3 months old justify the clean criminal record.

The *Time-Stamping Provider* verifies the authenticity of the relevant information given in the applicant's CV during the hiring process.

5.3.3 Training Requirements

The *Time-Stamping Provider* trains the newly recruited employees, over the course of which they acquire

- basic PKI knowledge;
- the specifics and the way of handling the *Time-Stamping Provider*'s IT system;
- the necessary special knowledge for fulfilling their scope of activities;
- processes and procedures defined in the public and inner regulations of the *Time-Stamping Provider*;
- the legal consequences of the individual activities;
- the applicable IT security regulations to the extent necessary to the specific scope of activities;
- the data protection rules.

Only employees having passed the training shall gain access to the he production IT system of the *Time-Stamping Provider*.

5.3.4 Retraining Frequency and Requirements

The *Time-Stamping Provider* ensures that the employees have the necessary knowledge continuously, so if needed, further or repeater type of training is held.

Further training is held if there's a change within the processes or the IT system of the *Time-Stamping Provider*.

The training is adequately documented, from what the syllabus and the scope of the participator employees can be clearly determined.

5.3.5 Job Rotation Frequency and Sequence

The *Time-Stamping Provider* does not apply mandatory rotation between individual work schedules.

5.3.6 Sanctions for Unauthorized Actions

The *Time-Stamping Provider* regulates the prosecution possibilities of the employees in an employment contract in case of failures, errors, accidental or intentional damage. If the employee – due to negligence or intentionally – violates their obligations, sanctions could be taken against him by the *Time-Stamping Provider*, which it sets out having regard to the offense and the consequences. The sanctions may include disciplinary proceedings, dismissal, revocation of appointment, criminal liability. Upon appointment every trusted role employee as part of the employment documents:

- gets written information about legal liabilities, rights, certification and management standards for the treatment of personal data,
- gets a job description that includes the concerning security tasks,
- signs a confidentiality agreement in which the related consequences non-compliant with safety measures, (criminal sanctions) can be found too.

All of these include the labor legislation or criminal consequences, that sanction the different discipline – job obligations – violation or breaking the law.

5.3.7 Independent Contractor Requirements

The *Time-Stamping Provider* only assigns trusted roles to its employees.

The *Time-Stamping Provider* chooses persons employed with engagement contract or subcontract to perform the other tasks, chosen if possible, from the list of previously qualified suppliers. The *Time-Stamping Provider* concludes a written contract before working with suppliers.

Each contracting party – before the start of the active work – signs a confidentiality statement in which he agrees that the business / corporate secrets learned later on will not be covered up to unauthorized persons, and will not be exploited in any other way.The confidentiality statement includes sanctions in case of violation. External employees employed under the contract are expected to have appropriate technical skills, and the *Time-Stamping Provider* does not hold any trainings for them.

5.3.8 Documentation Supplied to Personnel

The *Time-Stamping Provider* continuously provides for the employees the availability of the current documentation and regulations necessary to perform their roles.

Each employee in trusted role receives the following documents in writing:

- the organizational security regulations of the *Time-Stamping Provider*,
- the signed confidentiality agreement,
- personal job description,
- educational materials on the occasion of the planned or special training for the specific form of education.

All employees are informed in a written notice about any changes in the organizational safety regulations.

5.4 Audit Logging Procedures

In order to maintain a secure IT environment the *Time-Stamping Provider* implements and operates an event logger and control system covering its full IT system.

5.4.1 Types of Events Recorded

The *Time-Stamping Provider* logs every security-related event that can provide information on events, changes happened in the IT system or in its physical environment according to the generally accepted information security practice. In case of every log entry, it stores the following data:

- the time of the event;
- the type of the event;
- the success or failure of the implementation;
- the identification of the user or the system who/what triggered the event.

All of the essential event logs are available to the independent system auditors, who examine the compliance of the *Time-Stamping Provider*'s operation.
The *Time-Stamping Provider* logs The following events at minimum:

- TIME-STAMPING
  - events related to the issuance of the *Time Stamp*s;
  - the synchronization of the clock to the UTC time, including the operational re-calibrations too;
  - the loss of synchronization;
- LOGGING:
  - the shutdown, restart of the logging system or some of its components;
  - the modification of any parameter of the logging settings, for example the frequency, alert threshold, and the event to be examined;
  - the modification or deletion of the stored logging data;
  - the activities performed because of the logging system's failure.
- SYSTEM LOGINS:
  - successful logins, unsuccessful login attempts for trusted roles;
  - in case of password based authentication:
    - the change of the number of permitted unsuccessful attempts;
    - reaching the limit of the permitted number of the unsuccessful login attempts in case of user login;
    - readmission of the user blocked because of the unsuccessful login attempts;
  - changing the authentication technique (for example from password based to PKI based).
- KEY MANAGEMENT:
  - all events for the entire life cycle of service keys (key generation, loading, saving, etc.);

- CERTIFICATE MANAGEMENT:
  - every event related to the issuance and the status change of the provider *Certificate*s.
  - every event related to the issuance and the status change of the *Time-Stamping Unit*s's *Certificate*s.
- DATA FLOWS:
  - any kind of safety-critical data manually entered into the system;
  - safety-relevant data, messages received by the system;
- CA CONFIGURATION:
  - re-parameterization , any change of the settings of any component, of the CA;
  - user admission, deletion;
  - changing the user roles, rights;
  - changing the Certificate profile;
  - changing the CRL profile;
  - generation of a new CRL list;
  - generation of an OCSP response;
  - *Time Stamp* generation;
  - exceeding the required time accuracy threshold.
- HSM:
  - installing an HSM;
  - removing an HSM;
  - disposing, destructing an HSM;
  - delivering HSM;
  - clearing (resetting) an HSM;
  - uploading keys, certificates to the HSM.
- CONFIGURATION CHANGE:
  - hardware;
  - software;
  - operating system;
  - patch;
- PHYSICAL ACCESS, LOCATION SECURITY:
  - person entry to and exit from the security zone holding the CA components;
  - access to a CA system component;
  - a known or suspected breach of physical security;

  - firewall or router traffic.

- OPERATIONAL ANOMALIES:
  - system crash, hardware failure;
  - software failures;
  - software integrity validation error;
  - incorrect or wrongly addressed messages;
  - network attacks, attack attempts;
  - equipment failure;
  - electric power malfunctions;
  - uninterruptible power supply error;
  - an essential network service access error;
  - violation of the *Qualified Time-Stamping Policy* or the *Qualified Time-Stamping Practice Statement*;
  - deletion of the operating system clock.
- OTHER EVENTS:
  - appointment of a person to a security role;
  - operating system installation;
  - PKI application installation;
  - initiation of a system;
  - entry attempt to the PKI application;
  - password modification, setting attempt;
  - saving the inner database, and restore from a backup;
  - file operations (for example creating, renaming, moving);
  - database access.

5.4.2 Frequency of Audit Log Processing

The independent system auditors of the *Time-Stamping Provider* evaluates the generated log files every working day.

During the evaluation, the authenticity and integrity of the examined logs is ensured, the error messages in the logs are checked and if needed, document the differences and take measures to eliminate the cause of the deviation.

For the IT system evaluation, the *Time-Stamping Provider* uses automated evaluation tools too, that are used to monitor the resulting log entries according to preset criteria and, where necessary, alert the operational staff.

The fact of the investigation, the results of the investigation and the measures undertaken to avert deficiencies found are properly documented.

5.4.3 Retention Period for Audit Log

Before the deletion from the on-line system, the logs are archived and their secure preservation is ensured by the *Time-Stamping Provider* for the amount of time defined in Section 5.5.2.

For that time period, the *Time-Stamping Provider* ensures the readability of archived data, and maintains the necessary software and hardware tools necessary for that.

5.4.4 Protection of Audit Log

The *Time-Stamping Provider* protects the created logs for the required preservation time. During the whole preservation time, the following properties of the logs' data is ensured:

- protection against unauthorized disclosure: only authorized persons – primarily the independent system auditors – access the logs;
- availability: authorized persons are granted access to the logs;
- integrity: any data alteration, deletion in the log files and change in the order of the entries, etc. is prevented.

The *Time-Stamping Provider* provides the log records with qualified *Time Stamp*s, and they are stored in a way excluding the seamless insertion and deletion of the log entries.

The log files are protected against accidental and malicious damage by backups. In case of log entries containing personal data, the *Time-Stamping Provider* makes sure of the confidential storage of the data. Only those individuals are entitled to access to the log entries, who absolutely need it for their work. The *Time-Stamping Provider* verifies the accesses in a secure way. The *Time-Stamping Provider* preserves the log files in a secure environment. Keeps copies of the files at the second operation site.

5.4.5 Audit Log Backup Procedures

Daily log files are created from the continuously generated log entries during the operation in each system.

The daily log files are archived in two copies after the evaluation and stored physically apart from each other, at separate sites for the required time.

The exact process of backups shall be defined in the backup regulations of the *Time-Stamping Provider*.

5.4.6 Audit Collection System (Internal vs External)

Each application automatically collects and sends the records to the logging system.

The logging functions start automatically at the time of the system launch and they are run continuously during the entire period of system operation.

In case of any anomaly in the automatic examiner and logging systems, the operation of the related areas are suspended by the *Time-Stamping Provider* until the incident is resolved.

5.4.7 Notification to Event-causing Subject

The persons, organizations and applications that caused the error event are not always notified, but if necessary the *Time-Stamping Provider* involves them in the investigation of the event. The Clients affected by triggering the event has the duty to cooperate with the *Time-Stamping Provider* to explore the event.

5.4.8 Vulnerability Assessments

Besides processing daily the log entries, the experts of the *Time-Stamping Provider* monthly review extraordinary events and perform analysis of vulnerability, based on which the *Time-Stamping Provider* if necessary, takes measures to increase the security of the system.

Every major event of significant deficiencies detected or in case of external threat, but at least once a year the experts of the *Time-Stamping Provider* perform a comprehensive vulnerability analysis using a mapping of potential internal and external threats that may result in unauthorized access. Based on the results of the analysis, the Certification Authority if necessary, will further develop its processes and systems in order to increase the overall security of the service.

5.5 Records Archival

5.5.1 Types of Records Archived

The *Time-Stamping Provider* is prepared to the proper secure long-term archiving of electronic and paper documents.

The *Time-Stamping Provider* archives the following types of information:

- every document related to the accreditation of the *Time-Stamping Provider*;
- all issued versions of the *Certificate Policies* and *Qualified Time-Stamping Practice Statements*;
- all issued versions of the Terms and Conditions;
- contracts related to the operation of the *Time-Stamping Provider*;
- every electronic and paper based log entry.

5.5.2 Retention Period for Archive

The *Time-Stamping Provider* preserves the archived data for the time periods below:

- *Qualified Time-Stamping Practice Statement*: 10 years after the repeal;
- main data related to the issuance of the *Time Stamp* for at least 10 years after the issuance.

5.5.3 Protection of Archive

The *Time-Stamping Provider* stores all archived data in two copies at locations physically apart from each other. Authentic paper or electronic copy is made in accordance with the applicable law from the only authentic paper based copy of the document available.

Each of the two locations fulfils the requirements for archiving security and other requirements.

During the preservation of the archived data, it is ensured that:

- their integrity is preserved;
- they are protected against unauthorized access ;
- they are available;
- they preserve authenticity.

The archived electronic data is provided with at least an advanced electronic signature or seal and a qualified *Time Stamp*.

5.5.4 Archive Backup Procedures

The *Time-Stamping Provider* stores the paper documents in a single original copy and makes an authentic electronic copy of the original in accordance with the relevant legislation. Electronic copies are stored according to the same rules as other protected electronic documents.

5.5.5 Requirements for Time-stamping of Records

Every electronic log entry is provided with a time sign, on which the system provided time is indicated at least to one second precision.

The *Time-Stamping Provider* ensures that in its service provider systems, the system clock is at maximum different from the reference time with 1 second.

The *Time-Stamping Provider* provides the daily log files with a qualified *Time Stamp*.

During the preservation of the archived data, if necessary (for example algorithm change expiration of the original *Time Stamp*) the authenticity of the data is ensured.

5.5.6 Archive Collection System (Internal or External)

The log entries are generated in the *Time-Stamping Provider*'s protected computer system, and only the log files that are electronically signed and protected with qualified timestamps can leave it.

One original copy of the documents created during the service provision is stored and protected by the *Time-Stamping Provider* in an inner data storage operated by it.

5.5.7 Procedures to Obtain and Verify Archive Information

The *Time-Stamping Provider* creates the log files manually or automatically. In case of an automatic logging system, the certified log files are generated daily.

The archived files are protected from unauthorized access.

Controlled access to the archived data is only available to the eligible persons:

- *Client*s are eligible to see the data stored about them;
- in legal litigation in order to provide evidence the necessary data shall be provided.

5.6 CA Key Changeover

The *Time-Stamping Provider* ensures that the used *Time-Stamping Unit*s are continuously possessing a valid key and Certificate for their operation. For that purpose, sufficient time before the expiration of their Certificates, and the usage expiration of the keys related to them, it generates a new key pair for the *Time-Stamping Unit*s and inform its Clients in time. The new provider key is generated and managed according to this regulation.

If the *Time-Stamping Provider* changes any of its the *Time Stamp* issuer provider Certificate keys, it complies with the following requirements:

- it discloses the affected Certificates and public keys in accordance with the requirements defined in section 2.2 ;
- after the provider re-key the the *Time Stamp* to be issued will only be signed with the new provider keys;
- it preserves its old Certificates and public keys, and makes available the verification until all of the *Time Stamp* with the old provider key validity time expire.

5.7 Compromise and Disaster Recovery

In case of a disaster, the *Time-Stamping Provider* takes all necessary measures in order to minimize the damage resulting from the shortfall of the service, and it restores the services as quickly as possible.

Based on the assessment of the incident that occurred, it takes the necessary amendments, corrective measures to prevent future occurrence of the incident.

Once the problem resolved, the event is reported to the National Media and Infocommunications Authority, as the supervisory authority.

5.7.1 Incident and Compromise Handling Procedures

The *Time-Stamping Provider* has a business continuity plan. The business continuity plan contains the procedures to be followed in case of the signer key compromise, the suspicion of the compromise and the deviation of the *Time-Stamping Unit* clock.

The *Time-Stamping Provider* discloses the information on the event in case of a compromise, the suspicion of a compromise or the deviation of the *Time-Stamping Unit* clock.

The *Time-Stamping Provider* does not issue *Time Stamp*s in case of a compromise, the suspicion of a compromise or the deviation of the *Time-Stamping Unit* clock, until clearing the emergency.

The *Time-Stamping Provider* discloses the information necessary to identify the affected *Time Stamp*s in case of a compromise, the suspicion of a compromise or the deviation of the *Time-Stamping Unit* clock.

The *Time-Stamping Provider* established and maintains a fully functional reserve system, which is at a safe distance from the primary location, geographically located at a different place and is independently capable of supplying the full range of services.

The *Time-Stamping Provider* annually tests the changeover to a reserve system and reviews its business continuity plans.

The *Time-Stamping Provider* has increased security tools and systems in order to minimize the software and hardware failures and data corruptions. The recoverability of services is guaranteed by the underpinning contracts and own backup tools of the *Time-Stamping Provider*.

The *Time-Stamping Provider* constructed its IT system providing the qualified services in such a way that in case of the dropout of any one device, it is able to continue the provision of its qualified services. If multiple units of the *Time-Stamping Provider* fail, the *Time-Stamping Provider* is able to launch its backup system within at most 3 hours, which is able to provide the services related to the continuously operating services – Certificate storage publication, revocation management, publication of revocation status and time stamping – of the *Time-Stamping Provider* for its *Client*s.

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

The IT systems of the *Time-Stamping Provider* are built of reliable hardware and software components. The critical functions are implemented using redundant system elements so that in the event of an item failure they are able to operate further.

The *Time-Stamping Provider* makes a full daily backup of its databases and the generated log events.

The *Time-Stamping Provider* makes full system backups as frequently as necessary to be able to restore the full service in case of a disaster.

The business continuity plan of the *Time-Stamping Provider* includes accurate requirements for the tasks to be performed in case of critical system component failure.

Once the problem resolved and the integrity restored, the *Time-Stamping Provider* restarts its services as soon as possible.

5.7.3 Entity Private Key Compromise Procedures

The emergency response plan of the *Time-Stamping Provider* has an action plan in place in case the provider private keys compromise. The action plan reveals the circumstances of the compromise besides the revocation of the provider public key and the Certificate accompanying, arranges the notification of all concerned parties, takes the necessary steps against the recurrence of the compromise and, if necessary, provides new key to the service unit and the compromise affected end users. The *Time-Stamping Provider* immediately ceases to use that particular key in case of authentication unit key compromise.

The *Time-Stamping Provider* publishes a notice about the provider public key revocation.

5.7.4 Business Continuity Capabilities After a Disaster

The tasks to be performed in case of service failure due to natural or other disaster, are defined in the *Time-Stamping Provider*'s business continuity plan.

In the event of disaster, the regulations come into force, the damage control and the restoration of the services begins.

The secondary services site is placed so far away from the primary site that a probable disaster cannot reach both locations simultaneously.

The *Time-Stamping Provider* is obliged to notify the affected users as quickly as possible in the event of the disaster.

After the restoration of the services, the *Time-Stamping Provider* restores its devices damaged during the disaster and the original service security level as quickly as possible

5.8 Time-Stamping Provider Termination

The *Time-Stamping Provider* notifies the end users and the National Media and Infocommunications Authority at least 60 days before the shutdown in case of the planned discontinuance of any of its services.

At the same time with the notification about the service shutdown, the *Time-Stamping Provider* does not sign new subscriber contracts.

The *Time-Stamping Provider* at least 20 days before the planned termination shuts down the issuance of the new *Time Stamp*s .

At the same time of the termination, the *Time-Stamping Provider* shuts down the information services.

Before a planned discontinuation, the *Time-Stamping Provider* engages in negotiations about the taking over of its services with other Certification Authorities whose rating is identical to its own. Under section 9.3 , it will hand over its records, including confidential user data, to such a Certification Authority or to the National Media and Infocommunications Authority come what may, along with its other services, depending on the outcome of the negotiations or terminates without handover.

The *Time-Stamping Provider* takes measures concerning the revocation of provider *Certificate*s (and destroying private keys) during the 60 day period – depending on the outcome of the negotiations.

The *Time-Stamping Provider* informs the National Media and Infocommunications Authority about the final outcome of the negotiations. The *Time-Stamping Provider* is to inform its *Client*s by electronic mail, and *Relying Parties* by means of a publication on its website.

Upon terminating a service, the *Time-Stamping Provider* produces a full scope backup of its data contained in its IT system, affixing a qualified *Time Stamp* to it.

In order to make the handing over of its data to another service provider possible, the *Time-Stamping Provider* places data on media and in a format which the new service provider can receive or provides the new service provider with the opportunity to process data in the original format, and hands over the appropriate tools, documentation and know-how for this.

6 Technical Security Controls

The *Time-Stamping Provider* uses systems consisting of reliable, and safety technically assessed equipment for the provision of its services. The *Time-Stamping Provider* manages the cryptographic provider keys during their whole life-cycle within a *Hardware Security Module* that has appropriate Certification.

Both the *Time-Stamping Provider* and the system supplier and execution contractors have significant experience with certification service deployment and they use internationally recognized technology.

The *Time-Stamping Provider* continuously monitors the capacity needs, and with setting the trends it estimates the expected future capacity demands. It can arrange if needed an extension of the limited capacity, thereby providing the necessary processing and continuous availability of storage capacities.

6.1 Key Pair Generation and Installation

The *Time-Stamping Provider* makes sure that the generation and management of all the private keys generated by it is secure and complies with the regulatory requirements in force and with industry standards.

6.1.1 Key Pair Generation

The *Time-Stamping Provider* uses key generation algorithms for the key-pair generation, which comply with the requirements set out in the following normatives:

- ETSI TS 119 312 [19];
- the current National Media and Infocommunications Authority algorithmic regulation issued pursuant to the authorization of the year 2015. Act CCXXII [4] 92. § (1) b) .

The *Time-Stamping Provider* in case of the generation of a key pair of its own ensures:

- The creation of the private key of the provider shall be carried out in a protected environment (see section 5.1), with two trusted role holder (see section 5.2.1) authorized person simultaneously, excluding the presence of other unauthorized persons.
- The creation of the provider private key is carried out in a device, that:
  - meets the requirements of ISO/IEC 19790 [21] , or
  - meets the requirements of FIPS 140-2 [28] level 3 or higher, or
  - meets the requirements of CEN 14167-2 [29] workshop agreement,
  - is a reliable system that is evaluated in accordance with MSZ/ISO/IEC 15408 [20] or equal security criteria valued to level 4 or higher guarantee level. The assessment shall be based on a security system design or on safety appropriations meeting the requirements of this document.
- The production of provider private key is performed based on a key generation script.

6.1.2 Key Sizes

The *Time-Stamping Provider* uses algorithms and minimum key sizes, which comply with the requirements set out in the following norms:

- ETSI TS 119 312 [19];
- the current National Media and Infocommunications Authority algorithmic regulation issued pursuant to the authorization of the year 2015. Act CCXXII [4] 92. § (1) b) .

The *Time-Stamping Provider* uses at least 2048 bit RSA keys in every currently active root and intermediate provider *Certificate* and even in the *Certificate*s of the *Time-Stamping Unit*s and the OCSP responders.

6.1.3 Public Key Parameters Generation and Quality Checking

The *Time-Stamping Provider* generates the keys according to the description of the section 6.1.1.

Hardware/Software Key Generation

The generation of the *Time-Stamping Provider* keys used for *Certificate* and *Time Stamp* issuance is done with a *Hardware Security Module*, which has FIPS 140-2 Level 3 certifications. The denomination of each device is in the 8. section.

The other keys – necessary for the internal operation of the certification Authority – keys are generated by the *Time-Stamping Provider* on a *Hardware Security Module* or on a computer operating in a secure environment.

Verification of Compliance of Parameters

The compliance of the key generation parameters is verified by the system from two points of view:

- checking the conformity of the random number generation used for the parameters (whether the generation is sufficiently statistically random),
- checking the fulfilment of the requirements for parameters.

Every *Hardware Security Module* used in the system is able to statistically test the uniformity and independence of the bit sequence it generated. The modules enable the invocation of the tests through a standard interface.

6.1.4 Key Usage Purposes (as per X.509 v3 Key Usage Field)

The private keys of the *Time-Stamping Unit*s may be only used for the certification of the *Time Stamp*s.

6.2 Private Key Protection and Cryptographic Module Engineering Controls

The *Time-Stamping Provider* ensures the secure management of the private keys held by it and prevents the private key disclosure, copy, deletion, modification and unauthorized usage. The *Time-Stamping Provider* may only preserve the private keys as long as the provision of the service definitely requires.

The *Time-Stamping Provider* deletes the signing private keys stored on the *Hardware Security Module*s which are out of order in as defined in the device's manual so that it is virtually impossible to restore the keys.

6.2.1 Cryptographic Module Standards and Controls

The systems of the *Time-Stamping Provider* signing the *Time Stamp*s store the private keys used for the electronic signature creation in such secure hardware devices that are compliant with the following:

- the requirements of ISO/IEC 19790 [21], or
- the requirements of FIPS 140-2 [28] 3, or the requirements of a higher level, or
- the requirements of CEN 14167-2 [29] task force agreement, or
- they are such reliable systems that are evaluated at a guarantee level 4 or higher according to MSZ/ISO/IEC 15408 [20] or an equivalent security criteria system. The assessment either shall be based on the appropriate security system plan that meets the requirements of the present document, or on security appropriations.

The denomination of the used *Hardware Security Module* is described in section 8.

The *Time-Stamping Provider* provider keys are only stored in coded forms outside of the *Hardware Security Module*. For coding only those algorithms and key parameters are used by the current order of the National Media and Infocommunications Authority that was issued according to the year 2015. Act CCXXII [4] 92. § (1) b) that are expected to be able to withstand the cryptographic attacks during the entire lifetime of the keys.

The *Time-Stamping Provider* provider private keys are stored in a physically secure site even in an encrypted form, in the safe of the *Data Centre* , where they are only accessible to authorized people.

In case of the weakening of cryptographic algorithms and key parameters, the *Time-Stamping Provider* destroys the coded keys or recodes them again using algorithm and key parameters that ensure higher protection.

6.2.2 Private Key (N out of M) Multi-Person Control

The *Time-Stamping Provider* implements the "n out of m" at the activation of the private key related key management functions. The parameters are determined so that the simultaneous presence of at least two; trusted role holder employees is needed for the critical operations carried out with its provider private keys.

6.2.3 Private Key Escrow

The *Time-Stamping Provider* does not escrow its own provider private key.

6.2.4 Private Key Backup

The *Time-Stamping Provider* makes security copies of its provider private keys, before putting the private key into service as described in section 6.2.1. in a protected environment, in the simultaneous presence of at least two people holding trusted roles, with the exclusion of other people. During the backup, the private key leaves the module in an encrypted form, and this encrypted key can be loaded into another module. Both the backup and the restore can only be performed by protection mechanisms described in section 6.2.2..

The *Time-Stamping Provider* stores the backup copy in duplicate, and at least one copy of those is stored at a different place from the service provider location.

The same strict safety standards are applied to the management and preservation of backups as for the operation of the production system.

6.2.5 Private Key Archival

The *Time-Stamping Provider* does not archive its private keys.

6.2.6 Private Key Transfer Into or From a Cryptographic Module

All of the provider private keys of the *Time-Stamping Provider* is created in a *Hardware Security Module* that meets the requirements.

The private keys do not exist in an open form outside of the *Hardware Security Module*.

The *Time-Stamping Provider* only exports the private key from the *Hardware Security Module* for the purpose of making a secure copy.

The export and loading of the provider private keys is performed according to section 6.2.2.

6.2.7 Private Key Storage on Cryptographic Module

The *Time-Stamping Provider* keeps its private keys used for service provision in *Hardware Security Module*s according to section 6.2.1.

Private keys are stored and used in the *Hardware Security Module* as specified in the certification of the device with full compliance with the related operating instructions.

6.2.8 Method of Activating Private Key

The *Time-Stamping Provider* keeps its provider private keys in a secure *Hardware Security Module* and complies with its user guide and the requirements outlined in the certification documents. The *Hardware Security Module* can only be activated by the corresponding operator cards and the private keys within the *Hardware Security Module* can not be used before activating the module. The *Time-Stamping Provider* keeps the operator cards in a safe environment and those cards can be only reached by entitled employees of the *Time-Stamping Provider*.

6.2.9 Method of Deactivating Private Key

The private key used by the *Time-Stamping Provider*, and managed by the cryptographic devices becomes deactivated if (in a regular or irregular way) the device is removed from active status. This can happen in the following cases:

- the user deactivates the key,
- the power supply of the device is interrupted (switched off or power supply problem),
- the device enters an error state.

The private key deactivated like this can not be used until the module is in active state again.

6.2.10 Method of Destroying Private Key

The discarded, expired or compromised *Time-Stamping Provider*'s private keys are destroyed in a way that makes further use of the private keys impossible.

The *Time-Stamping Provider* destroys the provider private keys stored in the secure *Hardware Security Module* of the according to the procedures, requirements defined in the user guide and in the certification documents of the used *Hardware Security Module*, in the simultaneous presence of two *Time-Stamping Provider* employees (an infrastructure administrator and a security officer) with the exclusion of other persons.

6.2.11 Cryptographic Module Rating

According to the requirements of Section 6.2.1 every provider private key of the *Time-Stamping Provider* is stored in a cryptographic module that

- has a certification according to ISO/IEC 19790 [21], or
- has a certification according to FIPS 140-2 Level 3 [28], or
- has a Common Criteria based certificate attesting compliance with the requirements of the CEN 14167-2 [29] workshop agreement, or
- has a verification issued for this purpose by an independent certification body eligible for evaluating electronic signature products, registered by the National Media and Infocommunications Authority, or in a member state of the European Union

6.3 Other Aspects of Key Pair Management

6.3.1 Certificate Operational Periods and Key Pair Usage Periods

Certificates of the Time-Stamping Units

The validity period of the *Certificate*s of the *Time-Stamping Unit*s operated by the *Time-Stamping Provider*

- at most 12 years from issuance;

- shall not exceed the amount of time until which the used cryptographic algorithms can be used safely according to the algorithmic decision of the National Media and Infocommunications Authority;
- shall not exceed the expiration date of the provider *Certificate* that issued the *Certificate*.

The *Time-Stamping Provider* issues new private key(s) and *Certificate*(s) valid for 12 years in the first quarter of every year for its *Time-Stamping Unit*s. After beginning the usage of the new *Time-Stamping Unit Certificate*(s) the previous private key(s) are destroyed, so each privet key is used by average for 12 months.

Life-Cycle of the Time-Stamping Keys

The following requirements are met for the private keys used for *Time Stamp* certification:

- the *Time-Stamping Provider* specifies the end of the validity period of the signing keys used in the *Time-Stamping Unit*s, which is 15 months from the issuance;
- the end of the key 15 months validity period shall not be a later time than the end of the *Certificate* 12 year validity period;
- the end of the validity period is not a later date than the end of the implemented cryptographic algorithms and key parameters' validity period;
- the validity period of the *Time-Stamping Unit*s' is given by setting the "PrivateKeyUsagePeriod" value of the *Certificate* (see section 7.1.2.);
- the private key of the *Time-Stamping Unit* is not used past the validity period;
- organizational procedures were established to ensure that, by the end of the *Time-Stamping Unit* key validity period, a new private key is available;
- after the expiry of the validity of a key, the *Time-Stamping Provider* destroys all copies of the private key in such a way that private key recovery is virtually impossible.

Both the service provider and the end-user key validity period is affected, if the National Media and Infocommunications Authority issues a new algorithm decree, according to which the used cryptographic algorithm or key parameter is not secure to the end of the planned usage period.
If this happens, the *Time-Stamping Provider* revokes the related *Certificate*s.

6.4 Activation Data

6.4.1 Activation Data Generation and Installation

The *Time-Stamping Provider*'s private keys are protected in accordance with the procedures, requirements defined in the used *Hardware Security Module* user guide and the certification documents.
In case of password based activation data usage, the passwords are sufficiently complex in order to ensure the required level of protection.

6.4.2 Activation Data Protection

The employees of the *Time-Stamping Provider* manage the private key activation devices and the activation data securely, protect them using technical and organizational measures and passwords are stored in encrypted form only.

6.4.3 Other Aspects of Activation Data

No stipulation.

6.5 Computer Security Controls

6.5.1 Specific Computer Security Technical Requirements

During the configuration and operation of its IT system of the *Time-Stamping Provider* ensures the compliance with the following requirements:

- the user identity is verified with two-factor authentication controls by using VPN certificates stored on the card before granting access to the system or the application;
- roles are assigned to users and it ensures that all users only have permissions appropriate for his or her roles;
- a log entry is created for every transaction, and the log entries are archived;
- for the security-critical processes it is ensured that the internal network domains of the *Time-Stamping Provider* are sufficiently protected from unauthorized access;
- proper procedures are implemented to ensure service recovery after loss of key or system failure.

6.5.2 Computer Security Rating

Microsec lays much emphasis on customer complacency. In order to keep up the high quality services, the *Time-Stamping Provider* operates a quality management system according to the ISO 9001 standard since 23. January 2002. Compliance with this standard is certified by Lloyd's Register Quality Assurance.

Microsec pays close attention to the security of the systems it operates, therefore, in the main areas of its activity it operates a ISO/IEC 27001 compliant information security management system (previously BS 7799) since 19. may 2003. Compliance with this standard is certified by Lloyd's Register Quality Assurance.

6.6 Life Cycle Technical Controls

6.6.1 System Development Controls

The *Time-Stamping Provider* only uses applications and devices in its production IT system that:

- are commercial boxed software, designed and developed by a documented design methodology, or;
- custom hardware and software solutions developed by a reliable party for the *Time-Stamping Provider* during which design structured development methods and controlled development environment were used, or;
- open source software which comply with the security requirements and their adequacy is ensured by software verification and structured development and life-cycle management.

Procurement of IT tools is performed in a way that excludes changes to the hardware and software components using reliable, regularly qualified suppliers.

The hardware and software components applied for the provision of services are not used for other purposes by the *Time-Stamping Provider*.

The *Time-Stamping Provider* prevents the malicious software from entering into the devices used for certification services with appropriate security measures.

The hardware and software components are checked regularly for malicious software prior the first usage, and subsequently.

The *Time-Stamping Provider* acts with the same carefulness in case of program update purchases as at the acquisition of the first version.

The *Time-Stamping Provider* employs reliable, adequately trained staff over the course of installing software and hardware.

The *Time-Stamping Provider* only installs softwares to its service provider IT equipment necessary for the purpose of service provision.

The *Time-Stamping Provider* has a version control system where every change of the IT system is documented.

The *Time-Stamping Provider* operates automatic monitoring system to record all unauthorized changes, which records all changes in every file and in case of changes in the monitored files it generates a log entry or sends an alert to the system operators.

6.6.2 Security Management Controls

The *Time-Stamping Provider* implements processes for documenting, operating, verifying, monitoring and maintaining the systems used in the service including their modification and further development. The version control system detects any kind of unauthorized changes, data entry that affects the system, the firewall, the routers, programs and other components used in the service. Installing the program used in the service the *Time-Stamping Provider* ensures that the program to be installed is the proper version and that it is free from any unauthorized modification. The *Time-Stamping Provider* regularly checks the integrity of the software in its system used in the service.

Each *Hardware Security Module* applied by the *Time-Stamping Provider* has been verified, tested and evaluated. The *Time-Stamping Provider* verifies the integrity of the modules:

- following the acquisition of the devices during the takeover,
- immediately before the first usage,

- regularly during operation.

The *Time-Stamping Provider* deletes the provider keys from the *Hardware Security Module*s permanently or temporarily withdrawn from use.
The *Time-Stamping Provider* stores the unused *Hardware Security Module*s at a physically protected location.

6.6.3 Life Cycle Security Controls

The *Time-Stamping Provider* ensures the protection of the used *Hardware Security Module*s during their whole life cycle.
During the operation of the IT services, devices and operating systems used for the provision of the services the *Time-Stamping Provider* taking into account the safety aspects of the equipment life cycle.

- it uses in its system a *Hardware Security Module* which has the right certification;
- at the reception of the *Hardware Security Module*, during the qualitative takeover it verifies that the protection of the *Hardware Security Module*s against tampering was ensured during transportation;
- it stores the *Hardware Security Module* at a secure location, and the protection of the *Hardware Security Module* against tampering is ensured during storage;
- during the operation it continuously complies with the requirements of the *Hardware Security Module* appropriation of security, user guide and the certification report;
- it deletes the private keys stored in the discarded *Hardware Security Module*s in a way that it is virtually impossible to restore the keys.

6.7 Network Security Controls

The *Time-Stamping Provider* keeps its IT system configuration under strict control, and it documents every change including the smallest modification, development, software update too. The *Time-Stamping Provider* implements proper procedures for the detection of any hardware or software change, system installation, and maintenance occurred on the IT system. The *Time-Stamping Provider* checks the authenticity and integrity of every software component at their first loading.
The *Time-Stamping Provider* applies proper network security measures for example:

- disables unused network ports and services ;
- only runs network applications unconditionally necessary for the proper operation of the IT system .

6.8 Time-stamping

For the protection of the integrity of the log files and other electronic files to be archived the *Time-Stamping Provider* uses qualified electronic *Time Stamp*s issued by the e-Szignó Certification Authority.

7 Certificate, CRL, and OCSP Profiles

7.1 Certificate Profile

The end-user *Certificate*s used by the *Time-Stamping Provider* and the provider certification unit (root and intermediate) *Certificate*s used during the service comply with the following recommendations and requirements:

- ITU X.509 Information technology - Open Systems Interconnection - The Directory: Public-key and attribute certificate frameworks [26]
- RFC 5280 [24]
- RFC 6818 [25]
- ETSI EN 319 412-1 [13]
- ETSI EN 319 412-2 [14] in case of *Certificate*s issued to natural persons
- ETSI EN 319 412-3 [15] in case of *Certificate*s issued to legal persons
- ETSI EN 319 412-5 [16]

7.1.1 Version Number(s)

The provider certification unit (root and intermediate) *Certificate*s used by the *Time-Stamping Provider* and the end-user *Certificate*s used by the *Time-Stamping Provider* are "v3" *Certificate*s according to the X.509 specification [26].

The provider certification unit (root and intermediate) *Certificate*s used by the *Time-Stamping Provider* and the end-user *Certificate*s used by the *Time-Stamping Provider* have the following basic fields:

- Version
  The *Certificate* complies with "v3" *Certificate*s according to the X.509 specification, so the value "2" is in this field. [24]
- Serial Number
  The unique identifier generated by the *Certificate* issuer certification unit.

  In case of the end-user *Certificate*s the "Serial Number" field contains a random number with at least 8 byte entropy.
- Algorithm Identifier
  The identifier (OID) of the algorithm set used for the creation of the electronic seal certifying the *Certificate*.

  The *Time-Stamping Provider* uses the following algorithm:

  – "sha256WithRSAEncryption" (1.2.840.113549.1.1.11),
- Signature
  Electronic seal made by the *Time-Stamping Provider* certifying the *Certificate*, that has been created with an Algorithm set defined in the "Algorithm Identifier" field.

- Issuer
  The unique name of the *Certificate* issuer *Certification Unit* according to the X.501 name format.
- Valid From & Valid To
  The beginning and the end of the validity period of the *Certificate*. The time is recorded according to UTC and compliant with RFC 5280 encoding.
- Subject
  The unique name of the *Subject* according to the X.501 name format. Always filled out.
- *Subject* Public Key Algorithm Identifier

  The *Time-Stamping Provider* supports the RSA algorithm in the end-user *Certificate*s. The length of the public key is at least 1024 bit.

  The value to be included in this field:

  – "rsaEncryption" (1.2.840.113549.1.1.1)
- *Subject* Public Key Value
  The public key of the *Subject*.
- Issuer Unique Identifier
  Not filled out.
- *Subject* Unique Identifier
  Not filled out.

7.1.2 Certificate Extensions

the *Time-Stamping Provider* only uses the following certificate extensions according to the X.509 specification [26]:

Certificate of the Time-Stamping Unit

- Certificate Policies – not critical
  OID: 2.5.29.32
  This field contains the identifier of the valid certification policy at the time of the *Time-Stamping Unit Certificate* issuance and usage, and other information on the other uses of the *Certificate*.

  Filling in is mandatory for this field, and it shall not be critical.

  The reference to the related *Qualified Time-Stamping Practice Statement* can be given in this field.
- Authority Key Identifier – not critical
  OID: 2.5.29.35
  The 40 character long unique identifier of the provider key used for the electronic seal certifying the *Certificate*.

  The field value: the SHA-1 hash of the provider public key.

- Subject Key Identifier – not critical
  OID: 2.5.29.14
  The 40 character long unique identifier of the *Time-Stamping Unit* public key. The field value: the SHA-1 hash of the public key.

- Subject Alternative Names – not critical
  OID: 2.5.29.17
  The central e-mail address of the *Time-Stamping Provider* can be in this field in the *Certificate* of the *Time-Stamping Unit*.

- Basic Constraints – critical
  OID: 2.5.29.19
  The specification whether the *Certificate* has been issued to a certification unit.

  The default value of the extension is: CA = "FALSE", so this field is not present in the *Certificate* issued for the *Time-Stamping Unit*.

  The "pathLenConstraint" field is not present in the *Certificate* issued for the *Time-Stamping Unit*.

- Key Usage – critical
  OID: 2.5.29.15
  The scope definition of the approved key usage.

  In the *Certificate*s issued to the *Time-Stamping Unit* only the following values are present: "nonRepudiation", "digitalSignature".

- Private Key Usage Period – not critical
  OID: 2.5.29.16
  Determination of the permitted private key usage period.

  In the *Certificate*s issued to the *Time-Stamping Unit* the *Time-Stamping Provider* restricts the private key usage time by setting the "notBefore" and "notAfter" values.

- Extended Key Usage – not critical
  The further scope definition of the approved key usage. In the *Certificate*s issued to the *Time-Stamping Unit* only the following values are present:

  "timeStamping" (1.3.6.1.5.5.7.3.8).

- CRL Distribution Points – not critical
  OID: 2.5.29.31
  The field contains the CRL availability through http and/or ldap protocol. Mandatory to fill.

- Authority Information Access – not critical
  OID: 1.3.6.1.5.5.7.1.1 The definition of the other services related to the usage of the time-stamping unit *Certificate* provided by *Certification Authority*.

  Mandatory, and the field contains the following data

  - For the purpose of the fast and reliable verification of the current *Certificate* revocation status, the *Time-Stamping Provider* provides online certificate status service. The availability of this service is indicated here.

  - To facilitate the certificate chain building the *Time-Stamping Provider* gives the access path through http protocol of the *Certificate* of the *Certificate* issuer certification unit.

- Qualified *Certificate* Statements – Critical
  OID: 1.3.6.1.5.5.7.1.3
  The field is intended for the indication of statements related to the qualified *Certificate*s.

  The following statements are present in the *Certificate* of the time-stamping unit:

  - the *Certificate* is an EU qualified *Certificate* – 'id-etsi-qcs 1' (10.4.0.1862.1.1);
  - the transactional limit related to the *Certificate* – also known as the transaction value or financial transaction limit – 'id-etsi-qcs 2' (0.4.0.1862.1.2);
  - that statement that the *Time-Stamping Provider* retains the registration data related to the *Certificate* for 10 years after the expiration of the *Certificate* – 'id-etsi-qcs 3' (0.4.0.1862.1.3);
  - the availability of the document that contains the shortened, extracted version of the Certification Practice Statement concerning the *Time-Stamping Unit Certificate* – 'id-etsi-qcs 5' (0.4.0.1862.1.5);
  - that indication that the *Certificate* was issued for sealing (the value of the field is 'id-etsi-qct-eseal');

The above fields are always filled out according to the given rules. There are no any more *Certificate* extensions.

8 Compliance Audit and Other Assessments

The operation of the *Time-Stamping Provider* is supervised by the National Media and Infocommunications Authority in line with European Union regulations. The National Media and Infocommunications Authority holds site inspections on at least yearly basis at the *Time-Stamping Provider* location. Before the site inspection, the *Time-Stamping Provider* has a screening of its operations by an external auditor and sends the detailed report of the screening to the National Media and Infocommunications Authority within 3 days from its receipt. During the screening it is to be determined whether the operation of the *Time-Stamping Provider* meets the requirements of the eIDAS Regulation [1] and the related Hungarian legislation and the requirements of the applied *Qualified Time-Stamping Policy*(s) and the corresponding *Qualified Time-Stamping Practice Statement*(s).

The subject and methodology of the screening complies with the following normative documents:

- 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 [1];
- ETSI EN 319 403 V2.2.2 (2015-08) Electronic Signatures and Infrastructures (ESI); Trust Service Provider Conformity Assessment - Requirements for conformity assessment bodies assessing Trust Service Providers; [10]

- ETSI EN 319 401 V2.1.1 (2016-02); Electronic Signatures and Infrastructures (ESI); General Policy Requirements for Trust Service Providers [9]
- ETSI EN 319 421 V1.1.1 (2016-03); Electronic Signatures and Infrastructures (ESI); Policy and Security Requirements for Trust Service Providers issuing Time-Stamps. [17]

The result of the screening is a confidential document accessible only to authorized persons.

The conformity certificate issued in accordance with the conformity assessment report shall be published on the webpage of the *Time-Stamping Provider*.

The *Time-Stamping Provider* applies verified and certified elements (electronic signature production IT system elements) in connection with the service.

The *Time-Stamping Provider* uses the following cryptographic modules for the certification of the *Time Stamp*s, and for the provider private key storage:

- nCipher nShield F3 PCI nC4032P-150, firmware version: 2.22.6-3;
- nChipher nShield F3 SCSI nC4032W-150, firmware version: 2.18.15-3;
- nChipher nShield F3 500e PCIe nC4033E-500, firmware versions: 2.50.16-3 and 2.51.10-3.

The above devices have FIPS 140-2 [28] Level 3 certification.

The *Time-Stamping Provider* has rated every one of the system elements used for providing the services into security classes on the basis of its risk assessment system. The *Time-Stamping Provider* keeps records about these system elements and the security ratings associated with them in the scope of its risk management system.

In addition to the external audit, the *Time-Stamping Provider* also has its proprietary internal auditing system, which regularly examines compliance with previous audits, and takes the necessary steps in case of deviations.

The *Time-Stamping Provider* has an ISO 9001 standard compliant quality management system since 2002, moreover an ISO 27001 (formerly BS 7799) compliant information security management system since 2003, which are continuously audited and reviewed by an external auditing organisation.

8.1 Frequency or Circumstances of Assessment

The *Time-Stamping Provider* has the conformance assessment carried out annually on its IT system performing the provision of the services .

8.2 Identity/Qualifications of Assessor

The *Time-Stamping Provider* performs the internal audits with the help of its employees who hold the independent system auditor role.

The eIDAS and ETSI conformity assessment can be performed by an organization, which has a qualifying mandate issued by the national accreditation organization of an EU Member State.

8.3 Assessor's Relationship to Assessed Entity

External audit is performed by a person who:

- is independent from the owners, management and operations of the examined *Time-Stamping Provider*;
- is independent from the examined organization, namely neither himself or herself nor his or her immediate relatives have any employment or business relationship with the *Time-Stamping Provider*.
- remuneration is not dependent on the findings of the activities carried out during the audit.

8.4 Topics Covered by Assessment

The review covers the following areas:

- compliance with the legislation currently in force;
- compliance with technical standards;
- compliance with the Certification Policy and the *Qualified Time-Stamping Practice Statement*;
- adequacy of the employed processes;
- documentation;
- physical security;
- adequacy of the personnel;
- IT security;
- compliance with the data protection rules.

8.5 Actions Taken as a Result of Deficiency

The independent auditor summarizes the result of the screening in a detailed screening report that covers the tested system components, processes, and contains the evidence used in the screening and the auditor statements. The discrepancies revealed during the examination and the deadlines set for correcting them are recorded in a separate chapter of the report.

The independent auditor may record based on their severity the differences and discrepancies revealed during the examination:

- modification suggestions to be optionally taken into consideration;
- derogations to be averted mandatorily.

The independent auditor shall report the revealed serious derogations without delay to the National Media and Infocommunications Authority that is authorized to take the necessary measures.

The *Time-Stamping Provider* shall answer the problems stated by the independent auditor in writing, and to report the measures taken to avert them at the occasion of the next authority review.

The independent auditor shall send the assessment report in each case to the National Media and Infocommunications Authority.

8.6 Communication of Results

The *Time-Stamping Provider* publishes the summary report on the assessment. It does not publish the discrepancies revealed during the independent system assessment, they are treated as confidential information.

9 Other Business and Legal Matters

9.1 Fees

The *Time-Stamping Provider* publishes fees and prices on its webpage, and makes them available for reading at its customer service.

The *Time-Stamping Provider* may unilaterally change the price list. The *Time-Stamping Provider* publishes any modification to the price list 15 days before it becomes effective. Modifications will not affect the price of services paid in advance.

Provisions associated with the payment and refunding of fees are contained in the service contract and its annexes – the general terms of contract in particular.

9.1.1 Refund Policy

See section: 9.1.

9.2 Financial Responsibility

In order to facilitate trust the *Time-Stamping Provider* takes financial responsibility to fulfil all its obligations defined in the present *Qualified Time-Stamping Practice Statement*, the related *Qualified Time-Stamping Policy* and the service agreement concluded with the *Client*.

9.2.1 Insurance Coverage

The *Time-Stamping Provider* has sufficient financial resources for its responsibilities related to the provision of services and for providing the costs related to its termination.

9.2.2 Insurance or Warranty Coverage for End-entities

The *Time-Stamping Provider* has liability insurance to ensure reliability.

9.3 Confidentiality of Business Information

The *Time-Stamping Provider* manages clients' data according to legal regulations. The *Time-Stamping Provider* has a data processing regulation (see section 9.4), which addresses the processing of personal data in particular.

By signing the service agreement, *Client*s consent to the *Time-Stamping Provider* retaining and processing their personal data (in a manner that complies with the data processing regulations). Such consent applies to the forwarding of information specified by law and entered in records to third parties in case the *Time-Stamping Provider*'s services go offline; moreover to forwarding such information to the *Time-Stamping Provider*'s subcontractors – solely for the purpose of performing tasks associated with providing the service.

The *Time-Stamping Provider* uses clients' data solely in connection with the provision of its services. The *Time-Stamping Provider* retains data of which it becomes aware in accordance with statutory requirements, and for the stipulated period of time. In the course of retaining data, the *Time-Stamping Provider* sees to the intactness, confidentiality, and secure storage of information. It only permits accessing information to individuals whose tasks justify this.

The *Time-Stamping Provider* provides for the confidentiality and intactness of information that is not public during the forwarding of *Client*s' data.

9.3.1 Scope of Confidential Information

The *Time-Stamping Provider* treats as confidential:

- all *Client* data, with the exception of those that qualify as information not considered confidential in section 9.3.2;
- besides the *Client* data:
  - transaction related data and log data,
  - non-public regulations,
  - all data whose public disclosure would have an adverse effect on the security of the service.

9.3.2 Information Not Within the Scope of Confidential Information

The *Time-Stamping Provider* considers all data public that can be obtained from a public source, or to the disclosure of which the *Subscriber* gave its consent in writing beforehand.

9.3.3 Responsibility to Protect Confidential Information

The *Time-Stamping Provider* is responsible for the protection of the confidential data it manages.

The *Time-Stamping Provider* shall oblige its employees, subcontractors, affiliated partners to protect all confidential data by signing declaration of confidentiality or by contract.

The *Time-Stamping Provider* processes confidential information it comes to possess according to the provisions of Act CXII of 2011. on the Right to Freedom Of Information, and only discloses it to persons/organizations in the following case:

- **Information provision for authorities**

  For the purpose of investigating or preventing acts of crime committed using the trusted services it provides, as well as in the case of national security related interests, the *Time-Stamping Provider* – if the statutory criteria applicable to data requests are met – discloses the related identity information and the information verified by the *Time-Stamping Provider* according to the section (1) of the Eüt. [4] 90. § to investigating authorities and national security services free of charge.

  The *Time-Stamping Provider* records the fact of data transfers, but does not inform involved clients about it.

- **Disclosure upon owner's request**

  Upon a *Client*'s personal request to do so or on the basis of its authorisation granted officially, in writing, the *Time-Stamping Provider* reveals confidential user information pertaining to the *Client* to third parties.

9.4 Privacy of Personal Information

The *Time-Stamping Provider* takes care of the protection of the personal data it manages, the operation and regulations of the *Time-Stamping Provider* comply with the requirements of the Act CXII of 2011. on the Right to Freedom Of Information [2].

The *Time-Stamping Provider*:

- preserves,
- upon expiry of the obligation to retain – unless the *Client* otherwise indicates – deletes from the client database

the registered personal data and information on the *Client* in accordance with the legal requirements.

The *Time-Stamping Provider* stores identification data, data about the *Subscriber* associated with contact details and data connected to the provision of the service in its records.

The *Time-Stamping Provider* hands over *Client* data to third parties solely in cases where this is stipulated by a legal regulation or if the *Client* has granted its consent to this in writing.

9.4.1 Privacy Plan

The *Time-Stamping Provider* has a Privacy Policy for data processing that contains detailed requirements for the personal data management. The Privacy Policy for data processing is published on the webpage of the e-Szignó Certification Authority on the following URL: `https://e-szigno.hu/letoltesek/dokumentumok-es-szabalyzatok/`

9.4.2 Information Treated as Private

The *Time-Stamping Provider* protects all personal data related to the data subject or containing conclusions on the data subject that cannot be accessed publicly from public data source.

The *Time-Stamping Provider* collects data of the *Subscriber* only with its explicit prior consent and only to that extent which is necessary for the provision of the service.

9.4.3 Information Not Deemed Private

The *Time-Stamping Provider* need not treat as confidential information those personal data that can be accessed from a public source.

9.4.4 Responsibility to Protect Private Information

The *Time-Stamping Provider* stores securely and protects the personal data it manages. The data is protected by appropriate measures in particular against unauthorized access, alteration, and against disclosure.

The *Time-Stamping Provider* is generally responsible to comply with the requirements described in its Privacy policy and its liability extends to activities carried out by the subcontractors too.

9.4.5 Notice and Consent to Use Private Information

The *Time-Stamping Provider* only uses the personal data of the *Client* to the extent required for service provision, to contact the *Client*.

9.4.6 Disclosure Pursuant to Judicial or Administrative Process

In cases defined in the relevant legislation the *Time-Stamping Provider* may disclose the stored personal data about the *Client* without notifying the *Client*.

9.4.7 Other Information Disclosure Circumstances

No stipulation.

9.5 Intellectual Property Rights

During its business operation, the *Time-Stamping Provider* shall not harm any intellectual property rights of a third person.

The present *Qualified Time-Stamping Practice Statement* is the exclusive property of the *Time-Stamping Provider*. The *Client*s, *Subject*s and other *Relying Parties* are only entitled to use the document according to the requirements of the present *Qualified Time-Stamping Practice Statement* and any other use for commercial or other purposes is strictly prohibited.

The present *Qualified Time-Stamping Practice Statement* may be freely distributed in unchanged form, in full length and with the indication of origin.

The rules of the application of the software provided for the use of the service by the *Time-Stamping Provider* is accessible in the description of the software and it is included in the user's guide referenced in the description.

9.6 Representations and Warranties

9.6.1 CA Representations and Warranties

Certification Authority's Responsibility

The responsibility of the *Time-Stamping Provider* is in the *Qualified Time-Stamping Practice Statement*, the related *Certificate Policies*, and the service agreement with the *Client* and its attachments.

- The *Time-Stamping Provider* assumes responsibility for compliance with the procedures described in *Certificate Policies* it supports;
- The *Time-Stamping Provider* assumes responsibility as its own for the damages caused during the provision of the service by its subcontractors;
- The *Time-Stamping Provider* is liable under the rules of liability for breach of contract in the Civil Code of the Republic of Hungary [3] in relation to the *Client*s which are in a contractual relationship with it.
- The *Time-Stamping Provider* is liable under the rules of causing damage outside of contract in the Civil Code of the Republic of Hungary [3] in relation to third parties (such as the *Relying Party*) that are not in a contractual relationship with it.
- The *Time-Stamping Provider* will pay compensation for damages with the limitations specified in its regulations, and the service contracts concluded with Clients for proven damages that occur in the scope of its responsibility (see the section Limitation of Liability 9.8.).
- If the valid claim of several entitled parties related to an insurance event exceeds the amount defined for an insurance event in the liability insurance for the damages, then the compensation of the claims takes place in a relative ratio to the amount determined in the liability contract.

The *Time-Stamping Provider* is not responsible for the regulations issued by the *Relying Parties* or others.

Certification Authority Obligations

The *Time-Stamping Provider* shall fulfil the requirements defined in section (2) of article 24. of the eIDAS regulation [1].

The *Time-Stamping Provider*'s basic obligations is that it shall provide the services in line with the *Qualified Time-Stamping Policy*, this *Qualified Time-Stamping Practice Statement* and other regulations in the public domain, the contractual terms and conditions, furthermore corporate and security related internal regulations. These basic obligations are as follows:

- to establish the legal, regulatory, material, contractual, etc. framework appropriate for the service;

- to provide high standard and secure services in accordance with the applicable regulations;
- to continuously operate and audit organisations associated with the services (certification body, customer service, etc.);
- to abide by the procedures prescribed in the regulations, and to avoid or eliminate any potentially occurring incorrect operation;
- to ensure the Services to every applicant who accepts the terms and conditions specified in the regulations;
- to maintain public and proprietary records, as well as to make them continuously available to anybody over the internet.

9.6.2 Subscriber Representations and Warranties

Subscriber Responsibility

The responsibility of the *Subscriber* is set by the service agreement and its attachments (including the terms and conditions).

Subscriber Obligations

The responsibility of the *Subscriber* is to act in accordance with the contractual terms and regulations of the *Time-Stamping Provider* while using the service .

The obligations of the *Subscriber* are determined by this *Qualified Time-Stamping Practice Statement*, the service agreement and the standard policy conditions and other documents forming an integral part with it, as well as the relevant *Qualified Time-Stamping Policy*s.

Subscriber Rights

- *Subscriber*s have the right to use the services in accordance with this *Qualified Time-Stamping Practice Statement*.

9.6.3 Relying Party Representations and Warranties

The *Relying Parties* decide based on their discretion and/or their policies about the way of accepting and using the *Time Stamp*s. During the verification of the validity for keeping the security level guaranteed by the *Time-Stamping Provider* it is necessary for the *Relying Party* to act with caution, so it is particularly recommended to:

- comply with the requirements, regulations defined in the present *Qualified Time-Stamping Policy* and the corresponding *Qualified Time-Stamping Practice Statement*;
- use reliable IT environment and applications;

- verify the the revocation status of the *Certificate* used for signing the *Time Stamp* based on the current CRL or OCSP response;
- take into consideration every restriction in relation to the *Time Stamp* usage which is included in the *Qualified Time-Stamping Policy* and the *Qualified Time-Stamping Practice Statement*.

9.6.4 Representations and Warranties of Other Participants

No stipulation.

9.7 Disclaimers of Warranties

The *Time-Stamping Provider* excludes its liability if:

- it is unable to provide information or fulfil communication obligations due to the problems of the Internet, or part of it;
- the damage comes from a vulnerability or error of the cryptographic algorithms accepted by the National Media and Infocommunications Authority algorithmic decree.

9.8 Limitations of Liability

The *Time-Stamping Provider* limits the obligation for the loss related to the service, the extent of this limitation is 100 000 HUF per incident.

If the valid claim of several entitled parties related to an insurance event exceeds the amount defined for an insurance event in the liability insurance for the loss, then the compensation of the claims takes place in a relative ratio to the amount determined in the liability contract.

9.9 Indemnities

9.9.1 Indemnification by the *Time-Stamping Provider*

The detailed rules of the indemnities of the *Time-Stamping Provider* are specified in this regulation (see section: 9.8.), the service agreement and the contracts concluded with the *Client*s.

9.9.2 Indemnification by Subscribers

The *Subscriber* and the Subject are liable for damages to the *Time-Stamping Provider* for the loss or damage caused by non-compliance with their obligations and the relevant recommendations.

9.9.3 Indemnification by Relying Parties

See section: 9.8.

9.10 Term and Termination

9.10.1 Term

The effective date of the specific *Qualified Time-Stamping Practice Statement* is specified on the cover of the document.

9.10.2 Termination

The *Qualified Time-Stamping Practice Statement* is valid without a time limit until withdrawal.

9.10.3 Effect of Termination and Survival

In case of the withdrawal of the *Qualified Time-Stamping Practice Statement* the *Time-Stamping Provider* publishes the detailed rules of the withdrawal and the rights and obligations persisting after withdrawal on its webpage.

The *Time-Stamping Provider* guarantees that in case of a the *Qualified Time-Stamping Practice Statement* withdrawal, requirements for the protection of the confidential data remain in effect.

9.11 Individual Notices and Communications with Participants

The *Time-Stamping Provider* maintains a customer service in order to contact with its *Client*s.

The *Client*s may make their legal declarations to the *Time-Stamping Provider* solely in writing, and in executed form. Executing in representation of an organisation shall only be valid together with certification of such right of representation.

The e-Szignó Certification Authority informs its *Client*s by means of publication on its webpage or in electronic mail.

9.12 Amendments

The *Time-Stamping Provider* reserves the right to change the *Qualified Time-Stamping Practice Statement* in a controlled way in case of the change of normative rules, safety requirements, market conditions or other circumstances.

In exceptional cases (for example the need for taking critical security measures) the changes can be put into force with immediate effect.

9.12.1 Procedure for Amendment

The *Time-Stamping Provider* only discloses those of its procedures in its public domain regulations whose knowledge does not jeopardize the security of the services. The *Time-Stamping Provider* has a number of internal security and other regulations, as well as operative level stipulations which it treats in confidence (this certificate practice statement mentions several such). The procedures described in section 8.4. audit these documents as well.

A team responsible for maintaining regulations and documentation operates within the *Time-Stamping Provider*'s certification organization. This team collects change requests, carries out

modifications, and meets any internal and external information provision related obligations. The statement is approved by the director of the e-Szignó Certification Authority.

The team produces internal, non-public working copies of the regulations as it collects changes, and these undergo internal review before being published. The *Time-Stamping Provider* strives to only issue new regulations at the least frequent intervals possible.

The *Time-Stamping Provider* reviews the *Qualified Time-Stamping Practice Statement* annually or in case of exceptional request for change with priority and performs the necessary changes. The document will receive a new version number even after the smallest change and by taking into account the time required by the endorsement process, the planned date of coming into effect will be determined too.

The accepted document will be published on the webpage of the *Time-Stamping Provider* 30 days prior to the planned entry into force date and it will be sent for review to the National Media and Infocommunications Authority .

The *Time-Stamping Provider* will accept remarks connected to new regulations published for 14 days prior to their becoming effective, at the following email address:

`info@e-szigno.hu`

In case of observations that require substantive changes, the document will be amended.

The *Time-Stamping Provider* will close and publish the version of the regulation as amended with remarks on the 7th day prior to its becoming effective.

9.12.2 Notification Mechanism and Period

The *Time-Stamping Provider* notifies the *Relying Parties* of new document version issuances as described in Section 9.12.1..

9.12.3 Circumstances Under Which OID Must Be Changed

The *Time-Stamping Provider* issues a new version number in case of even the smallest change to the *Qualified Time-Stamping Practice Statement*, which is part of the document identifier (OID), so any change to the document will result in an OID change, namely two documents – entered into force – with different content cannot have the same OID.

9.13 Dispute Resolution Provisions

The *Time-Stamping Provider* aims for the peaceful and negotiated settlement of the disputes arising from its operation. The settlement follows the principle of gradual approach.

The *Time-Stamping Provider* and the *Client* mutually agree that in the case of any disputed issue or complaint arising whatsoever, they will attempt amicable consultation through negotiation before taking the dispute to legal channels. The initiating party will be obliged to notify every other affected party promptly and to inform them fully concerning all of the case's implications.

The *Client* in case of a deputation is entitled to appeal to the Arbitration Board of Budapest before incidental judicial proceedings.

Questions, objections, and complaints related to the activity of the *Time-Stamping Provider* shall be addressed to the customer care centre office in written form. The *Time-Stamping Provider*

notifies submitting parties at the address they specify about having received a submission and the time required for investigation, within 3 business days calculated as of receiving a submission. The *Time-Stamping Provider* is obliged to issue a written response to the submitter within the specified time limit. The *Time-Stamping Provider* may request the provision of information required for giving a response from the submitter. The *Time-Stamping Provider* investigates complaints within 30 days, and notifies submitters about the results thereof.

Should a submitter find the response inadequate or if the dispute which had arisen can not be settled based on it without getting the *Time-Stamping Provider* involved, the submitter may initiate consultation with the *Time-Stamping Provider* and the *Relying Parties*. All participants of such consultation shall be given written notice regarding the date of consultation 10 business days in advance thereof; and the submission, the *Time-Stamping Provider*'s response, as well as any documents containing other required information shall be sent to them in writing.

Should consultation fail to achieve a result within 30 business days calculated as of a complaint being submitted, the submitter may file a lawsuit with respect to the issue. The *Relying Parties* shall subject themselves to the sole jurisdiction of the II. and III. District Court of Budapest and/or that of the Municipal Court of Budapest.

9.14 Governing Law

The *Time-Stamping Provider* at all times operates in accordance with the Hungarian legislation in force. The Hungarian law is the proper law of the *Time-Stamping Provider* contracts, regulations, and their execution, and they are to be construed by the Hungarian law.

9.15 Compliance with Applicable Law

The applicable regulations:

- 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 [1];
- (Hungarian) Act CCXXII of 2015 on electronic administration and the general rules of trust services [4];
- (Hungarian) Ministry of Interior Decree 24/2016. (VI. 30.) on the requirements for trust service providers and their services [5];
- (Hungarian) Ministry of Interior Decree 25/2016. (VI. 30.) on the administrative service fees paid to the trust service supervisory body and on fee rates [6];
- (Hungarian) Ministry of Interior Decree 26/2016. (VI. 30.) on the announcement according to trust services and on the content of registers maintained by the trust service supervisory body [7];
- ETSI EN 319 401 V2.1.1 (2016-02); Electronic Signatures and Infrastructures (ESI); General Policy Requirements for Trust Service Providers [9];

- ETSI EN 319 421 V1.1.1 (2016-03); Electronic Signatures and Infrastructures (ESI); Policy and Security Requirements for Trust Service Providers issuing Time-Stamps. (Replaces ETSI TS 102 023) [17];
- ETSI EN 319 422 V1.1.1 (2016-03); Electronic Signatures and Infrastructures (ESI); Time-stamping protocol and time-stamp token profiles (Replaces ETSI TS 101 861) [18];
- (Hungarian) Act CXII of 2011 on the Right to Freedom Of Information [2];
- (Hungarian) Act V of 2013. on the Civil Code. [3].

9.16 Miscellaneous Provisions

9.16.1 Entire Agreement

No stipulation.

9.16.2 Assignment

The providers operating according to this *Qualified Time-Stamping Practice Statement* may only assign their rights and obligations to a third party with the prior written consent of *Time-Stamping Provider*.

9.16.3 Severability

Should some of the provisions of the present *Qualified Time-Stamping Practice Statement* become invalid for any reason, the remaining provisions will remain in effect unchanged.

9.16.4 Enforcement (Attorneys' Fees and Waiver of Rights)

The *Time-Stamping Provider* is entitled to claim payment for damages and attorney fees for reimbursement of the damages, losses, expenses caused by its partners. If in a particular case the *Time-Stamping Provider* does not exercise its claim for damages that does not mean that in similar cases in the future or in case of violation of other provisions of the present *Qualified Time-Stamping Practice Statement*, it would waive the enforcement of claims for damages.

9.16.5 Force Majeure

The *Time-Stamping Provider* is not responsible for the defective or delayed performance of the requirements set out in the *Qualified Time-Stamping Policy* and the *Qualified Time-Stamping Practice Statement* if the reason for failure or delay was a condition that is outside the control of the *Time-Stamping Provider*.

9.17 Other Provisions

No stipulation.

A REFERENCES

[1] 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 .

[2] (Hungarian) Act CXII of 2011 on the Right to Freedom Of Information .

[3] (Hungarian) Act V of 2013. on the Civil Code .

[4] (Hungarian) Act CCXXII of 2015 on the general rules of electronic administration and trust services .

[5] (Hungarian) Ministry of Interior Decree 24/2016. (VI. 30.) on the requirements for trust service providers and their services .

[6] (Hungarian) Ministry of Interior Decree 25/2016. (VI. 30.) on the administrative service fees paid to the trust service supervisory body and on fee rates .

[7] (Hungarian) Ministry of Interior Decree 26/2016. (VI. 30.) on the announcement according to trust services and on the content of registers maintained by the trust service supervisory body .

[8] ETSI EN 319 102-1 V1.1.1 (2016-05); Electronic Signatures and Infrastructures (ESI); Procedures for Creation and Validation of AdES Digital Signatures; Part 1: Creation and Validation.

[9] ETSI EN 319 401 V2.1.1 (2016-02); Electronic Signatures and Infrastructures (ESI); General Policy Requirements for Trust Service Providers.

[10] ETSI EN 319 403 V2.2.2 (2015-08) Electronic Signatures and Infrastructures (ESI); Trust Service Provider Conformity Assessment - Requirements for conformity assessment bodies assessing Trust Service Providers;.

[11] ETSI EN 319 411-1 V1.1.1 (2016-02); Electronic Signatures and Infrastructures (ESI); Policy and security requirements for Trust Service Providers issuing certificates; Part 1: General requirements .

[12] ETSI EN 319 411-2 v2.1.1 (2016-02); 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; (Replaces ETSI TS 101 456).

[13] ETSI EN 319 412-1 V1.1.1 (2016-02); Electronic Signatures and Infrastructures (ESI); Certificate Profiles; Part 1: Overview and common data structures.

[14] ETSI EN 319 412-2 V2.1.1 (2016-02); Electronic Signatures and Infrastructures (ESI); Certificate Profiles; Part 2: Certificate profile for certificates issued to natural persons; (Replaces ETSI TS 102 280).

[15] ETSI EN 319 412-3 V1.1.1 (2016-02); Electronic Signatures and Infrastructures (ESI); Certificate Profiles; Part 3: Certificate profile for certificates issued to legal persons (Replaces ETSI TS 101 861).

[16] ETSI EN 319 412-5 V2.1.1 (2016-02); Electronic Signatures and Infrastructures (ESI); Certificate Profiles; Part 5: QCStatements.

[17] ETSI EN 319 421 V1.1.1 (2016-03); Electronic Signatures and Infrastructures (ESI); Policy and Security Requirements for Trust Service Providers issuing Time-Stamps. (Replaces ETSI TS 102 023).

[18] ETSI EN 319 422 V1.1.1 (2016-03); Electronic Signatures and Infrastructures (ESI); Time-stamping protocol and time-stamp token profiles (Replaces ETSI TS 101 861).

[19] ETSI TS 119 312 V1.1.1 (2014-11); Electronic Signatures and Infrastructures (ESI); Cryptographic Suites.

[20] MSZ/ISO/IEC 15408-2002 "Information Technology - Methods and Means of a Security - Evaluation Criteria for IT Security" .

[21] ISO/IEC 19790:2012: "Information technology – Security techniques – Security requirements for cryptographic modules".

[22] IETF RFC 2459: Internet X.509 Public Key Infrastructure - Certificate and CRL Profile, January 1999.

[23] IETF RFC 3161: Internet X.509 Public Key Infrastructure - Time-Stamp Protocol (TSP), August 2001.

[24] IETF RFC 5280: Internet X.509 Public Key Infrastructure - Certificate and Certificate Revocation List (CRL) Profile, May 2008.

[25] IETF RFC 6818: Updates to the Internet X.509 Public Key Infrastructure - Certificate and Certificate Revocation List (CRL) Profile, January 2013.

[26] ITU X.509 Information technology - Open Systems Interconnection - The Directory: Public-key and attribute certificate frameworks.

[27] Recommendation ITU-R TF.460-6 (2002): Standard-frequency and time-signal emissions.

[28] FIPS PUB 140-2 (2001 May 25): Security Requirements for Cryptographic Modules.

[29] CEN Workgroup Agreement CWA 14167-2: Cryptographic module for CSP signing operations with backup - Protection profile - CMCSOB PP.

[30] Magyarország (Hungary): Trusted List (`http://www.nmhh.hu/tl/pub/HU_TL.pdf`).

[31] e-Szignó Certification Authority - Qualified Signing Certificate Policies .