MICROSEC

e-Szignó Certification Authority

eIDAS conform
Qualified Time Stamping Policy

ver. 2.1

Date of effect: 05/09/2016

OID	1.3.6.1.4.1.21528.2.1.1.86.2.1
Version	2.1
First version date of effect	01/04/2005
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)
1.0	First version. OID: 1.3.6.1.4.1.21528.2.1.1.3	01/04/2005	István Zsolt Berta, Dr. Csilla Endrődi Internal auditor: Elemér Tóth
2.0	Rewritten based on the suggestions of the internal auditor. (Identical to the version 1.1)	15/04/2005	István Zsolt Berta, Dr. Internal auditor: Elemér Tóth
3.0	Smaller corrections	02/05/2005	István Zsolt Berta, Dr. Internal auditor: Elemér Tóth
3.2	Corrections based on the supervisory audit	08/08/2005	István Zsolt Berta, Dr. Internal auditor: Elemér Tóth
4.0	Correction due to the change od the General Terms and Conditions	19/11/2006	István Zsolt Berta, Dr.
4.1	Assigning new OID OID: 1.3.6.1.4.1.21528.2.1.1.3.4.1	04/12/2006	István Zsolt Berta, Dr.
4.2	Change in the contact data of the consumer protection. OID: 1.3.6.1.4.1.21528.2.1.1.3.4.2	28/10/2007	István Zsolt Berta, Dr.
4.3	Change in the contact data of the consumer protection again. OID: 1.3.6.1.4.1.21528.2.1.1.3.4.3	01/01/2008	István Zsolt Berta, Dr.
4.4	Not issued. OID: 1.3.6.1.4.1.21528.2.1.1.3.4.4	01/10/2008	István Zsolt Berta, Dr.
4.5	Stop the audit logging of the time stamps. OID: 1.3.6.1.4.1.21528.2.1.1.3.4.5	20/12/2008	István Zsolt Berta, Dr.
5.0	Change in the company form. OID: 1.3.6.1.4.1.21528.2.1.1.3.5.0	01/05/2012	István Zsolt Berta, Dr.
5.1	Smaller changes. OID: 1.3.6.1.4.1.21528.2.1.1.3.5.1	01/08/2013	Sándor Szőke, Dr.
2.0	New, eIDAS conform policy with new OID. OID: 1.3.6.1.4.1.21528.2.1.1.86.2.0	01/07/2016	Sándor Szőke, Dr.
2.1	Changes according to the NMHH comments. OID: 1.3.6.1.4.1.21528.2.1.1.86.2.1	05/09/2016	Melinda Szomolya, Sándor Szőke, Dr.

Table of Contents

1 Introduction

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

The *Time-Stamping Policy* 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 Policy* 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".

The *Qualified Time-Stamping Policy* sets out basic requirements related to *Time Stamp*s in particular for the *Time Stamp* issuer *Time-Stamping Provider*. The manner these requirements are met, and a detailed description of the methods mentioned here shall be included in the *Qualified Time-Stamping Practice Statement* issued by the *Time-Stamping Provider* .

The *Qualified Time-Stamping Policy* 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, *Qualified Time-Stamping Practice Statement*, 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 Policy
OID	1.3.6.1.4.1.21528.2.1.1.86
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 *Time-Stamping Policy* 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)

To ensure compliance revelation the the *Time-Stamping Provider* can choose from the following two solutions:

- it can include the aforementioned OID in the *Time Stamp*s it issues;
- if the the *Time-Stamping Provider* uses its own OID in the *Time Stamp*s it issues, it shall indicate in its *Qualified Time-Stamping Practice Statement* and in its TSA disclosure statement, the support of the aforementioned ETSI time-stamping policy (i.e. BSTP).

1.2.3 Effect

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

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

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

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 requirements of the present document are applicable to the *Time-Stamping Provider*s that in their *Qualified Time-Stamping Practice Statement* undertake the compliance with the *Time-Stamping Policy* defined in this document.

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 *Time-Stamping Policy* 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 Policy* 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 *Time-Stamping Provider* shall describe the acceptance procedure of the *Qualified Time-Stamping Practice Statement* that announces its conformity with the present *Qualified Time-Stamping Policy* in the given *Qualified Time-Stamping Practice Statement*.

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* shall publish 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* shall disclose on its webpage its own provider *Certificate*s.

2.2.1 Publication of the *Time-Stamping Provider* Information

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

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

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

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

The *Time-Stamping Provider* shall make 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* shall notify 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 Policy* 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* shall publish 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

The *Time-Stamping Provider* can require the prior identification of the users for the issuance of the *Time Stamp*s. The identification method shall be described in the *Qualified Time-Stamping*

Practice Statement.

3.2 The Certificate of the Time-Stamping Unit

In order to ensure the integrity and authenticity of the public key of the *Time-Stamping Unit*:

- the public key of the *Time-Stamping Unit* shall be published as a *Certificate*;
- the *Certificate* of the *Time-Stamping Unit* shall be issued by a *Certification Authority* which provides its services according to ETSI EN 319 411-1 [11];
- the *Certificate* of the *Time-Stamping Unit* issuing *Time Stamp*s which are qualified according to the 910/2014/EU regulation [1] shall be issued by a *Certification Authority* that provides its services according to ETSI EN 319 411-2 [12] ;
- the *Time-Stamping Unit* may issue *Time Stamp*s only when it already has a *Certificate* for the verification of the *Time Stamp*s, and its signature was verified through a full certificate chain to a trusted *Certification Authority*.

3.3 The Time-Stamp

The requirements for the *Time Stamp*:

- the *Time Stamp* shall comply with the IETF RFC 3161 [22] and the ETSI EN 319 422 [18] standards;
- the *Time Stamp* shall be issued within a secure environment and it shall contain the correct time;
- the internal clock of the *Time-Stamping Unit*(s) used for the issuance of the *Time Stamp* must be traceable to at least one accurate time provided by a UTC laboratory;
- the time given in the *Time Stamp*s shall conform to the time value provided by UTC, and the difference shall not exceed the accuracy indicated in the *Time-Stamping Policy* and in the *Time Stamp* itself;
- the *Time-Stamping Unit* shall 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;
- the private keys used for the certification of the *Time Stamp*s shall not be used for other purposes;
- the *Time-Stamping Unit* shall refuse every attempt for *Time Stamp* issuance after the lifetime of the keys ends.

3.3.1 The Time-Stamp Request

The time-stamping client shall support the *Time Stamp* requests according to the IETF RFC 3161 [22] section 2.4.1. It is recommended to support the following fields:

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

The *Time-Stamping Provider* shall support the use of every extension.

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

3.3.2 Time-Stamp Response

The *Time-Stamping Provider* shall support the *Time Stamp* responses according to IETF RFC 3161 [22] section 2.4.2 with the following additional requirements:

- it is obligatory to support the usage of the "accuracy" field;
- it is recommended to support the "nonce" field.

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

The *Time-Stamping Provider* shall use 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. When selecting the cryptographic algorithm sets and key lengths the planned usage time of the *Time Stamp* shall be taken into account.

3.4 Time-Stamp Accuracy

The time accuracy of the issued *Time Stamp*s shall be within 1 second.

- the clock of the *Time-Stamping Unit* shall be protected from threats which could enable the unnoticed modification of the clock to an accuracy outside the undertaken range;
- the *Time-Stamping Provider* shall notice if the internal time to be indicated in the *Time Stamp*s falls outside the undertaken accuracy range;
- as soon as the *Time-Stamping Provider* notices that the the internal time to be indicated in the *Time Stamp*s falls outside the undertaken accuracy range, it shall pause the issuance of *Time Stamp*s;

3.5 Time-Stamp Synchronization

The *Time-Stamping Unit* clock shall be synchronized to the UTC time within the undertaken accuracy. The calibration of the *Time-Stamping Unit* shall be performed so that the clock can not slip out of the undertaken accuracy.

3.5.1 Leap Second Management

The *Time-Stamping Provider* has to perform the clock synchronization based on the notification of the competent body at the leap second occurrence. The change shall take place at the last minute of the appointed day according to the specification of the ETSI 319 421 [17] annex C and as defined in the ITU-R TF.460-6 [26] recommendation.

3.5.2 Daylight Saving Time Management

The time given in UTC format in the *Time Stamp*s can be displayed by the application to the user in a different way and format, 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.

Potential problems related to the interpretation of dates shall be brought to the attention of the *Relying Parties* in the *Qualified Time-Stamping Practice Statement*.

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* shall guarantee 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 may 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 separate *Time-Stamping Unit* does not necessarily mean different hardware and software, but for the separation of the services with different safety levels at least:

- a different *Certificate* shall be used;
- different access points shall be provided.

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 shall 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 and to meet the requirements described in the *Qualified Time-Stamping Practice Statement*, particularly regarding to the following:

- the *Relying Party* shall verify the validity and revocation status of the *Certificate*;
- 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* shall apply 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* shall keep a record of the system units and resources related to the service provision, and conduct a risk assessment on these. It shall use protective measures proportional to the risks related to the individual elements.

The *Time-Stamping Provider* shall monitor the capacity demands, and shall ensure that the adequate processing power and storage are available for the provision of the service.

5.1 Physical Controls

The *Time-Stamping Provider* shall take care that physical access to critical services is controlled, and shall keep 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 shall be implemented at secure locations.

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

5.1.1 Site Location and Construction

The IT system of the *Time-Stamping Provider* shall be 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 – shall be 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 that take part in service provision, and for the preservation of the confidential data stored by the provider.

5.1.2 Physical Access

The *Time-Stamping Provider* shall protect 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 shall ensure 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 should be physically out of reach;
- the logged-in terminals shall not be left without supervision;
- no work process should be 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 should be appointed responsible people to carry out regular physical security assessments. The results of the examinations shall be recorded in the appropriate log entries.

5.1.3 Power and Air Conditioning

The *Time-Stamping Provider* shall apply 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 shall be 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 should provide the necessary amount of fresh air with adequate filtration for the safe working conditions of the operators.

The humidity should be reduced to the level required by the IT systems.

Cooling systems with proper performance should be used 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* shall be adequately protected from water intrusion and flooding.

5.1.5 Fire Prevention and Protection

Smoke and fire detectors shall be installed in the *Data Centre* of the *Time-Stamping Provider* that automatically alert the fire brigade. Manual fire extinguishers of the appropriate type and amount compliant with the relevant regulations should be placed in a visible place in each room.

Automatic fire extinguishers shall be applied in the *Data Centre*.

5.1.6 Media Storage

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

5.1.7 Waste Disposal

The *Time-Stamping Provider* shall take care of the destruction of its devices, media storages becoming superfluous in compliance with environmental regulations.

Such devices and media storages shall be permanently deleted or made unusable in accordance with the widely accepted methods under the personal supervision of employees of the *Time-Stamping Provider*.

5.1.8 Off-Site Backup

The *Time-Stamping Provider* shall create 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 – shall be 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 shall be resolved.

5.2 Procedural Controls

The *Time-Stamping Provider* shall take 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 shall be 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* shall create trusted roles for the performance of its tasks. The rights and functions shall 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.

Trusted roles to be implemented:

- manager with overall responsibility for the provider's IT system;
- security officer: individual with overall responsibility for the security of the service;
- system administrator: individual performing the IT system installation, configuration and maintenance;
- 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 provider , responsible for verifying the enforcement of control measures the 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* shall formally appoint 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 shall be kept of the trusted roles and in case of any change, the National Media and Infocommunications Authority shall be notified without delay.

5.2.2 Number of Persons Required per Task

It shall be defined in the *Time-Stamping Provider*'s security and operational regulations 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* shall 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 shall be revoked without delay in case of the cessation of user rights.

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* is bound to ensure 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.

5.3 Personnel Controls

The *Time-Stamping Provider* shall take 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* shall address 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 shall 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* shall ensure 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

Each employee of the *Time-Stamping Provider* shall have the necessary education, practice and professional experience for the provision of his scope of activities. Even during recruitment, particular emphasis shall be given to the personality traits when selecting potential employees and only reliable persons can be hired for trusted roles.

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* shall only hire 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* shall verify 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* shall train 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* shall ensure that the employees have the necessary knowledge continuously, so if needed, further or repeater type of training shall be held.

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

The training shall be 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

No stipulation.

5.3.6 Sanctions for Unauthorized Actions

The *Time-Stamping Provider* shall regulate 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.

5.3.7 Independent Contractor Requirements

The same rules shall be applied to workers employed with a contractual relationship as to employees.

The trusted role holder person shall be in an employment relationship with the *Time-Stamping Provider*.

5.3.8 Documentation Supplied to Personnel

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

5.4 Audit Logging Procedures

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

5.4.1 Types of Events Recorded

The *Time-Stamping Provider* shall log 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, the following data shall be stored:

- 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 shall be available to the independent system auditors, who examine the compliance of the *Time-Stamping Provider*'s operation.

The following events shall be logged 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 *Time-Stamping Provider* shall ensure the regular evaluation of the created logs.

The created daily log files shall be evaluated in the next working day if possible, but not later than 1 week.

The evaluation of the log files shall be performed by an independent system auditor with the right expertise, system privileges and appointment.

The *Time-Stamping Provider* can use automatized tools to assist the evaluation of the electronic logs.

During the evaluation, the authenticity and integrity of the examined logs shall be ensured. During the evaluation, the system generated error messages shall be analysed.

The significant changes in the traffic should be analysed with statistical methods.

The fact of the audit, the audit results and the measures taken in order to remove any deficiencies found shall be properly documented.

5.4.3 Retention Period for Audit Log

Before the deletion from the on-line system, the logs shall be archived and their secure preservation shall be ensured for the amount of time defined in Section 5.5.2.

5.4.4 Protection of Audit Log

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

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

5.4.5 Audit Log Backup Procedures

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

The daily log files shall be 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 *Qualified Time-Stamping Practice Statement*.

5.4.6 Audit Collection System (Internal vs External)

The *Time-Stamping Provider* specifies the operation of its logging processes in its *Qualified Time-Stamping Practice Statement*.

The *Time-Stamping Provider* can use automatic audit and logging systems if it can ensure that they are active at the time of the system launch and they operate continuously until the system's shutdown.

If there's any anomaly in the automatic audit and logging systems, the operation of the *Time-Stamping Provider* shall be suspended until the incident is resolved.

5.4.7 Notification to Event-causing Subject

In case of the detected errors, the *Time-Stamping Provider* at its discretion can decide whether it notifies the person, role, device or application of the error that caused it.

5.4.8 Vulnerability Assessments

Vulnerability assessment shall be carried out each year by the *Time-Stamping Provider* to help discover potential internal and external threats, which may lead to unauthorized access.

The occurrence probability of the event and the expected damage shall be mapped too.

It shall regularly assess the implemented processes, safety measures, information systems, so that they are able to correctly withstand the threats detected.

After evaluation of the detected errors, if necessary the defence systems shall be amended to prevent similar mistakes in the future.

5.5 Records Archival

5.5.1 Types of Records Archived

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

The *Time-Stamping Provider* shall archive 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* is bound to preserve 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* is bound to store every archived data in two copies at locations physically apart from each other. Authentic paper or electronic copy can be made in accordance with the applicable law from the only authentic paper based copy of the document available.

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

During the preservation of the archived data, it shall be ensured that:

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

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

5.5.4 Archive Backup Procedures

The duplicate of the archived data shall be stored at a physically separate location from the *Time-Stamping Provider*'s site according to the requirements of Section 5.1.8.

5.5.5 Requirements for Time-stamping of Records

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

The *Time-Stamping Provider* shall ensure that in its service provider systems, the system clock is at maximum different from the reference time with 1 second. The system time used for generating the time signal shall be synchronized to the UTC time at least once a day.

The daily log files shall be provided with a *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 shall be ensured.

5.5.6 Archive Collection System (Internal or External)

The log entries shall be 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.

5.5.7 Procedures to Obtain and Verify Archive Information

The *Time-Stamping Provider* can create the log files manually or automatically. In case of automatic logging system, the certified log files shall be generated daily.

The archived files shall be protected from unauthorized access.

Controlled access to the archived data shall be 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* shall ensure that the used *Time-Stamping Unit*s are continuously having the 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 shall generate a new key pair for the *Time-Stamping Unit*s , and inform its Clients in time. The new provider key shall be generated and managed according to this regulation.

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

- it shall disclose 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 can only be signed with the new provider keys;
- it shall preserve its old Certificates and public keys.

5.7 Compromise and Disaster Recovery

In case of a disaster, the *Time-Stamping Provider* is obliged to take 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 shall take the necessary amendments, corrective measures to prevent future occurrence of the incident.

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

5.7.1 Incident and Compromise Handling Procedures

The *Time-Stamping Provider* shall have a business continuity plan. The business continuity plan shall contain 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* shall disclose 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* shall 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* shall disclose 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* shall establish and maintain 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* shall continually test the operation of the reserve system and shall review its business continuity plans annually.

In case of a disaster, the availability of the services shall be restored as quickly as possible.

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

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

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

The *Time-Stamping Provider* shall make full 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* shall include 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* shall restart its services as soon as possible.

5.7.3 Entity Private Key Compromise Procedures

In case of the *Time-Stamping Provider*'s private key compromise, the following steps should be taken without delay:

- all of the affected Certificates of the *Time-Stamping Provider* shall be revoked;
- new provider private key shall be generated for the restoration of the services;
- the revoked provider Certificates' data shall be disclosed according to the regulated method in Section 2.2 ;
- the information related to the compromise shall be disclosed for every *Subscriber* and *Relying Party*;
- in case of a severe compromise, the information shall be made available to the *Subscriber*s and the *Relying Parties* with which it can be determined unambiguously the scope of the affected *Time Stamp*s.

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 shall be defined in the *Time-Stamping Provider*'s business continuity plan.

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

The secondary services site shall be 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* shall restore 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* shall comply with the requirements laid down in in the legislation in case of service termination.

During the termination the priority tasks are:

- the Relying parties and the *Subscriber*s shall be notified about the planned termination in time;
- the *Time-Stamping Provider* shall make every effort to ensure that at the latest by the service termination another provider takes over the records and service obligations;
- new *Time Stamp* issuance shall be terminated;
- after the termination of the service, a full system backup and archiving shall be carried out;
- the archived data shall be handled over to the provider that takes over the services, or to the National Media and Infocommunications Authority.

6 Technical Security Controls

The *Time-Stamping Provider* shall use reliable systems and equipment protected against modification for the management of the cryptographic keys and activation data for the whole life-cycle.

The capacity demands shall be continuously monitored and the future capacity demands shall be estimated, so that the necessary availability of processing and storage needs are ensured.

6.1 Key Pair Generation and Installation

The *Time-Stamping Provider* shall ensure the secure production and management of its generated private keys corresponding to the industry standards and regulatory requirements in force corresponding production and management.

6.1.1 Key Pair Generation

The *Time-Stamping Provider* may only use 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 shall ensure:

- 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 [27] level 3 or higher, or
  - meets the requirements of CEN 14167-2 [28] 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* shall only use 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) .

6.1.3 Public Key Parameters Generation and Quality Checking

The requirements for the key parameter generation are in Section 6.1.1.

Devices with appropriate device certificates used in the creation of keys shall be operated with strict compliance with the requirements set out in the certification to ensure the quality of the generated key parameters.

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* shall ensure the secure management of the private keys held by it and shall prevent 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.

During the management of the *Hardware Security Module*s the signing private keys stored on the *Hardware Security Module*s which are out of order shall be deleted so that it is practically 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 [27] 3, or the requirements of a higher level, or
- the requirements of CEN 14167-2 [28] 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 provider keys may only be stored in coded forms outside of the *Hardware Security Module*. For coding only those algorithms and key parameters shall be 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 provider private keys shall be stored in a physically secure site even in an encrypted form, where they are only accessible to authorized people.

In case of the weakening of cryptographic algorithms and key parameters, the coded keys shall be destroyed or they shall be recoded using algorithm and key parameters that ensure greater protection.

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

The *Time-Stamping Provider* shall to ensure 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* shall not escrow its own provider private keys.

6.2.4 Private Key Backup

The *Time-Stamping Provider* shall make security copies of its provider private keys, and at least one copy of those shall be stored at a different place from the service provider location.

Making backups may only be done in protected environment, in the simultaneous presence of at least two people holding trusted roles, with the exclusion of other people.

At least the same strict safety standards shall be 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* shall 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* shall be created in a cryptographic module that meets the requirements.

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

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

The private key transport between the *Hardware Security Module*s is only permitted in the form of a secure copy.

6.2.7 Private Key Storage on Cryptographic Module

The *Time-Stamping Provider* shall store the private keys used for the provision of the service according to the present *Certificate Policies* in a *Hardware Security Module*.

There is no restrictive term applied for the storage form in the *Hardware Security Module*.

6.2.8 Method of Activating Private Key

The *Time-Stamping Provider*'s private keys shall be activated in accordance with the procedures and requirements defined in the used cryptographic module user guide and the certification documents.

6.2.9 Method of Deactivating Private Key

The *Time-Stamping Provider*'s private keys shall be deactivated in accordance with the procedures, requirements defined in the used *Hardware Security Module*'s user guide and the certification documents.

6.2.10 Method of Destroying Private Key

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

The provider private keys shall be destroyed 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* shall be 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 [27], or
- has a Common Criteria based certificate attesting compliance with the requirements of the CEN 14167-2 [28] 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* shall issue new private key(s) and *Certificate*(s) 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) shall be destroyed.

Life-Cycle of the Time-Stamping Keys

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

- the *Time-Stamping Provider* shall specify the end of the validity period of the signing keys used in the *Time-Stamping Unit*s;
- the end of the key validity period shall not be a later time than the end of the *Certificate* validity period;
- the end of the validity period shall not be 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' key can be given at the parametrization of the used *Hardware Security Module*, or by setting the "private key usage period" value of the *Certificate*;
- the private key of the *Time-Stamping Unit* shall not be used past the validity period;

- organizational or technical procedures shall be 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, all copies of the private key shall be destroyed 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 shall be 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 need to be sufficiently complex in order to ensure the required level of protection.

6.4.2 Activation Data Protection

The devices, activation data necessary for the private key activation shall be stored securely by the employees of the *Time-Stamping Provider*, the passwords may only be stored encoded.

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 the IT system of the *Time-Stamping Provider* the compliance with the following requirements shall be ensured:

- the user identity is verified before granting access to the system or the application;
- roles are assigned to users and it shall be ensured that all users only have permissions appropriate for its roles;
- a log entry is created for every transaction, and the log entries shall be 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

In order to provide IT security and service quality the *Time-Stamping Provider* shall implement a control system by internationally accepted methodologies, and the adequacy of those shall be certified by a certificate issued by an independent certification body.

6.6 Life Cycle Technical Controls

6.6.1 System Development Controls

The *Time-Stamping Provider* shall only use 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.

The procurement shall be conducted in a way that excludes the modification of the hardware and software components.

The hardware and software components applied for the provision of services may not be used for other purposes.

The *Time-Stamping Provider* with proper protection measures shall prevent malicious software to enter the devices used in the certification service.

Prior to the first use and later on the hardware and software components shall be regularly checked searching for malicious codes.

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

Reliable, adequately trained staff shall be employed over the course of installing software and hardware.

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

The *Time-Stamping Provider* shall have a version control system where every change shall be documented.

The *Time-Stamping Provider* shall implement procedures for unauthorized change detection.

6.6.2 Security Management Controls

The *Time-Stamping Provider* shall implement processes for documenting, operating, verifying, monitoring and maintaining the systems used in the service including their modification and further development. The version control system shall detect 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* shall ensure that the program to be installed is the proper version and that it is free from any unauthorized modification. The *Time-Stamping Provider* shall regularly check the integrity of the software in its system used in the service.

6.6.3 Life Cycle Security Controls

The *Time-Stamping Provider* shall ensure the protection of the used *Hardware Security Module*s during their whole life cycle.

- the *Hardware Security Module* used shall have the right certification;
- at the reception of the *Hardware Security Module*, it shall be verified that the protection of the *Hardware Security Module*s against tampering was ensured during transportation;
- the protection of the *Hardware Security Module* against tampering shall be ensured during storage;
- during the operation the requirements of the *Hardware Security Module* appropriation of security, user guide and the certification report shall be continuously observed;
- the private keys stored in the discarded *Hardware Security Module*s shall be deleted in a way that it is practically impossible to restore the keys.

6.7 Network Security Controls

The *Time-Stamping Provider* shall keep its IT system configuration under strict control, and it shall document every change including the smallest modification, development, software update too. The *Time-Stamping Provider* shall implement proper procedures for the detection of any hardware or software change, system installation, and maintenance occurred on the IT system. The *Time-Stamping Provider* shall check the authenticity and integrity of every software component at their first loading.

The *Time-Stamping Provider* shall apply proper network security measures for example:

- shall disable unused network ports and services ;
- shall only run network applications unconditionally necessary for the proper operation of the IT system .

6.8 Time-stamping

The *Time-Stamping Provider* shall use *Time Stamp*s provided by a qualified time-stamp provider listed on the trusted list of one of the European Union member states for the protection of the integrity of the log files and other electronic files to be archived.

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 shall comply with the following recommendations and requirements:

- ITU X.509 Information technology - Open Systems Interconnection - The Directory: Public-key and attribute certificate frameworks [25]
- RFC 5280 [23]
- RFC 6818 [24]
- 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* shall be "v3" *Certificate*s according to the X.509 specification [25].

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. [23]
- Serial Number
  The unique identifier generated by the *Certificate* issuer certification unit.

  In case of the end-user *Certificate*s the "Serial Number" field shall contain 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 signature or seal certifying the *Certificate*.
- Signature
  Electronic signature or 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 Identifier of the *Subject* Public Key Algorithm.
- *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* may only use certificate extensions according to the X.509 specification [25] , the usage of self-defined critical extensions is not allowed.
Specific requirements concerning certificates extension:

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 signature or seal certifying the *Certificate*. Filling in is mandatory.

  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.

  Filling in is mandatory.

- Subject Alternative Names – not critical
  OID: 2.5.29.17
  Filling in is optional.

- 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 shall not be present in the *Certificate* issued for the *Time-Stamping Unit*.

  The "pathLenConstraint" field shall not be 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* this field shall be mandatory and exclusively set to: "nonRepudiation", "digitalSignature".

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

  Usage is optional. If it is implemented, than both "notBefore" and "notAfter" values shall be set.

- Extended Key Usage – not critical
  The further scope definition of the approved key usage. In the *Certificate*s issued to the *Time-Stamping Unit* this field shall be mandatory and exclusively set to:

  "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* shall provide online certificate status service. The availability of this service shall be indicated here.

  - To the facilitation of the certificate chain building the *Time-Stamping Provider* shall give 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 shall be 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');

There shall not be any more *Certificate* extension.

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* shall have a screening of its operations by an external auditor and shall send 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 shall comply 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* reserves the right to inspect at any time involving an independent expert the operation of the providers who operate according to the present *Qualified Time-Stamping Policy*(s) in order to verify compliance with the requirements.

8.1 Frequency or Circumstances of Assessment

The *Time-Stamping Provider* shall have the conformance assessment carried out annually.

8.2 Identity/Qualifications of Assessor

The *Time-Stamping Provider* can perform 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 can be performed only 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*.

8.4 Topics Covered by Assessment

The review shall cover at least 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 shall summarize 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 shall be 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* shall publish the summary report on the assessment. It is not needed to disclose the discrepancies revealed during the independent system assessment, they can be treated as confidential information.

9 Other Business and Legal Matters

9.1 Fees

The fees applied by the *Time-Stamping Provider* shall be publicly disclosed in accordance with the applicable regulations.

9.1.1 Refund Policy

No stipulation.

9.2 Financial Responsibility

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

9.2.1 Insurance Coverage

In order to cover the costs associated with the termination of the service activity and to sustain reliability the *Time-Stamping Provider* shall meet at least one of the following requirements:

- The *Time-Stamping Provider* has at least an amount of 25 million HUF as an unconditional and irrevocable bank warranty.
- The *Time-Stamping Provider* provides deposit for the National Media and Infocommunications Authority as beneficiary at a financial institution to guarantee the payment of costs. The sum of the deposit shall be at least 25 million HUF.
- An EU company with at least 100 million HUF registered capital provides financial guarantee to the *Time-Stamping Provider* covering the costs. The amount of this financial guarantee shall be at least 25 million HUF.

9.2.2 Insurance or Warranty Coverage for End-entities

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

9.3 Confidentiality of Business Information

The *Time-Stamping Provider* shall manage the data of the Clients in accordance with the respective regulations.

9.3.1 Scope of Confidential Information

The *Time-Stamping Provider* shall specify the scope of data that are considered confidential information in its *Qualified Time-Stamping Practice Statement*.

9.3.2 Information Not Within the Scope of Confidential Information

The *Time-Stamping Provider* may consider all data public that are not specified as confidential in the *Qualified Time-Stamping Practice Statement*.

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.

Circumstances when the *Time-Stamping Provider* may disclose the confidential data shall be determined case-by-case in the *Qualified Time-Stamping Practice Statement*.

9.4 Privacy of Personal Information

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

The *Time-Stamping Provider* shall:

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

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

9.4.1 Privacy Plan

The *Time-Stamping Provider* shall have a Privacy Policy for data processing that contains detailed requirements for the personal data management. The Privacy Policy for data processing shall be published on the webpage of the *Time-Stamping Provider*.

9.4.2 Information Treated as Private

The *Time-Stamping Provider* shall protect 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* shall only collect data of the *Subscriber* 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* shall store securely and protect the personal data it manages. The data shall be 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* shall only use 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 *Time-Stamping Policy* 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 *Time-Stamping Policy* and any other use for commercial or other purposes is strictly prohibited.

The present *Time-Stamping Policy* 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* shall be determined in the *Qualified Time-Stamping Practice Statement*.

9.6 Representations and Warranties

9.6.1 CA Representations and Warranties

Certification Authority's Responsibility

The *Time-Stamping Provider* is responsible for the obligations set by the terms of this *Qualified Time-Stamping Policy*, in the related *Qualified Time-Stamping Practice Statement* and in the service agreement concluded with the *Client*.

- 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.).

Obligations of Certification Authority to the Subscriber

The *Time-Stamping Provider* is oblidged to:

- issue a ETSI EN 319 422 [18] compliant *Time Stamp* to the request of the *Subscriber* which corresponds to the hash included in the application and contains the unique serial number included in the application;
- keep the accuracy of the *Time Stamp* within 1 second (deviation from UTC shall be at most 1 second);
- ensure the reliability and safety of the service according to the requirements concerning qualified time-stamping providers;
- log every important event in relation with the service and retain these log files according to legal requirements.

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 Policy*, the service agreement and its attachments – in particular the general terms and conditions -– and the *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* can limit its liability for loss.

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 the *Qualified Time-Stamping Practice Statement*, the service agreement, or the contracts concluded with the *Client*s.

9.9.2 Indemnification by Subscribers

The *Time-Stamping Provider* sets the term of claim for damages from *Subscriber*s in the *Qualified Time-Stamping Practice Statement* and the service agreement.

9.9.3 Indemnification by Relying Parties

The *Time-Stamping Provider* sets the term of its claim for damages from Relying parties in the *Qualified Time-Stamping Practice Statement*.

9.10 Term and Termination

9.10.1 Term

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

9.10.2 Termination

The *Time-Stamping Policy* is valid without a time limit until withdrawal.

9.10.3 Effect of Termination and Survival

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

9.11 Individual Notices and Communications with Participants

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

9.12 Amendments

The *Time-Stamping Provider* reserves the right to change the *Qualified Time-Stamping Policy* 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* reviews the *Qualified Time-Stamping Policy* 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 *Time-Stamping Policy* , 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* shall aim for the peaceful and negotiated settlement of the disputes arising from its operation. The settlement shall follow the principle of gradual approach.

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 present *Qualified Time-Stamping Policy* is compliant with the following 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 Policy* may only assign their rights and obligations to a third party with the prior written consent of the *Time-Stamping Provider*.

9.16.3 Severability

Should some of the provisions of the present *Time-Stamping Policy* 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 *Time-Stamping Policy* , 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 3161: Internet X.509 Public Key Infrastructure - Time-Stamp Protocol (TSP), August 2001.

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

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

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

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

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

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