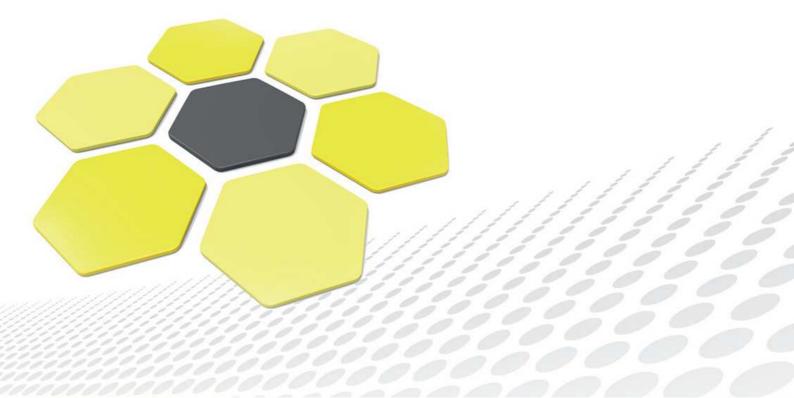**MICROSEC**

e-Szignó Certification Authority

eIDAS conform
Qualified Long-Term Preservation Service
Long-Term Preservation Policy

ver. 2.1

Date of effect:    05/09/2016

| OID | 1.3.6.1.4.1.21528.2.1.1.87.2.1 |
|---|---|
| Version | 2.1 |
| First version date of effect | 15/12/2006 |
| 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.<br>OID: 1.3.6.1.4.1.21528.2.1.1.19 | 15/12/2006 | István Zsolt Berta, Dr. |
| 1.1 | Changes according to the feedback of the National Telecommunications Authority.<br>OID: 1.3.6.1.4.1.21528.2.1.1.19.1.1 | 08/01/2007 | István Zsolt Berta, Dr. |
| 1.2 | Change in the contact data of the consumer protection.<br>OID: 1.3.6.1.4.1.21528.2.1.1.19.1.2 | 01/01/2008 | István Zsolt Berta, Dr. |
| 1.3 | Not issued.<br>OID: 1.3.6.1.4.1.21528.2.1.1.19.1.3 | 01/10/2008 | István Zsolt Berta, Dr. |
| 1.4 | Conforming to the new requirements of the NHH.<br>OID: 1.3.6.1.4.1.21528.2.1.1.19.1.4 | 20/12/2008 | István Zsolt Berta, Dr. |
| 2.0 | Change in the company form.<br>Change related to the encryption of the archived e-dossiers.<br>OID: 1.3.6.1.4.1.21528.2.1.1.19.2.0 | 01/05/2012 | István Zsolt Berta, Dr. |
| 2.0 | New, eIDAS conform preservation policy with new OID.<br>OID: 1.3.6.1.4.1.21528.2.1.1.87.2.0 | 01/07/2016 | Sándor Szőke, Dr. |
| 2.1 | Changes according to the NMHH comments.<br>OID: 1.3.6.1.4.1.21528.2.1.1.87.2.1 | 05/09/2016 | Melinda Szomolya,<br>Sándor Szőke, Dr. |

# Table of Contents

# 1   Introduction

This document contains the *Qualified Long-Term Preservation Policy* defined by e-Szignó Certification Authority operated by Microsec ltd. (hereinafter: Microsec or *Long-Term Preservation Provider*) concerning the qualified preservation service.

The *Qualified Long-Term Preservation Policy*  complies with the requirements set by the eIDAS Regulation [1], the service provided according to these regulations is an EU qualified trust service.

Microsec asked for its registration as a trust service proider at the National Media and Infocommunications Authority on the 1st of July 2016.

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

- the service shall be audited by an independent assessment body accredited under eIDAS Regulation, it shall issue a conformity assessment report and a certificate for the *Long-Term Preservation Provider* about the successful assessment;

- the *Long-Term Preservation Provider* shall submit the conformity assessment certificate to the National Media and Infocommunications Authority, as it is the official supervisory 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 Long-Term Preservation Policy* is a set of rules that specify the qualified preservation service usability for a community and/or a class of applications with common safety requirements.

The *Qualified Long-Term Preservation Policy* sets out basic requirements for the *Long-Term Preservation Provider* related to the qualified preservation to be established.

The *Qualified Long-Term Preservation Policy* is one of several documents issued by the *Long-Term Preservation Provider* that collectively govern conditions of the services provided by the *Long-Term Preservation Provider*. Other important documents include General Terms and Conditions, *Long-Term Preservation Practice Statement*s, and other customer and partner agreements.

Section 1.5 of this document specifies several terms, which are not or not fully in this sense used 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

| | |
|---|---|
| Issuer | e-Szignó Certification Authority |

| Document name | eIDAS conform |
| | Qualified Long-Term Preservation Service |
| | Long-Term Preservation Policy |
| OID | 1.3.6.1.4.1.21528.2.1.1.87 |
| Document version | 2.1 |
| Date of effect | 05/09/2016 |

### 1.2.1    Long-term preservation policy

The first seven numbers of the *Qualified Long-Term Preservation Policy* identifier OID is the unique identifier of Microsec as follows:

| (1) | International Organization for Standardization (ISO) |
| (3) | Organization identification schemes registered according to ISO/IEC 6523-2 |
| (6) | United States Department of Defense (DoD) |
| (1) | Internet |
| (4) | Private projects |
| (1) | Private enterprises |
| (21528) | MICROSEC Ltd. |

The system of the following numbers was allocated within Microsec own competence, interpretation as follows:

| (1.3.6.1.4.1.21528) | MICROSEC Ltd. |
| (2) | e-Szignó Certification Authority |
| (1) | documents |
| (1) | public documents |
| (x) | unique identifier number of the document |
| (y) | document version |
| (z) | document subversion |

The present document defines the following *Certificate Policies*:

| OID | DENOMINATION | SHORT NAME |
|---|---|---|
| 1.3.6.1.4.1.21528.2.1.1.87.2.1 | qualified long-term preservation policy according to eIDAS regulation. | MAR |

### 1.2.2   Effect

This *Qualified Long-Term Preservation Policy* is in effect from the 05/09/2016 date of entry into force to withdrawal.

The present *Qualified Long-Term Preservation Policy* and the *Long-Term Preservation Practice Statement*s based on these policies should be reviewed at least annually and their amendment to the potentially changed requirements and prerequisites shall be ensured.

The effect of the *Qualified Long-Term Preservation Policy* extends each of the participants mentioned in section 1.3.

Present *Qualified Long-Term Preservation Policy* include specific requirements for services primarily provided for Hungarian *Client*s, operating by the Hungarian law in Hungary in Hungarian language. The *Long-Term Preservation Provider* can extend the geographical scope of the service; in this case, it shall use not less stringent requirements than those applicable to Hungarian conditions. The details shall be recorded in the the *Long-Term Preservation Practice Statement*.

## 1.3      PKI Participants

### 1.3.1      Certification Authorities

The long term service provider is a *Trust Service Provider*, within the framework of which *Trust Service* deals with validity preservation of the electronic signatures, electronic seals, *Time Stamp*s and their creator *Certificate*s, optionally including the signed and sealed electronic document preservation too.

The requirements of the present document apply to every *Long-Term Preservation Provider* who undertake in their the *Long-Term Preservation Practice Statement* the compliance with any of the *Qualified Long-Term Preservation Policy*(s) described in the present document.

### 1.3.2      Subscribers

*Subscriber*s define the scope of  users using the service, and *Subscriber*s also cover the service fees related to the usage of these services.

### 1.3.3      Relying Parties

The *Relying Party* is not necessarily in a contractual relationship with the *Long-Term Preservation Provider*. The *Long-Term Preservation Practice Statement* and the other policies mentioned in it

contain the recommendations related to its operation.

## 1.4     Policy Administration

### 1.4.1     Organization Administering the Document

The data of the organization administering the present *Qualified Long-Term Preservation 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 |

### 1.4.2     Contact Person

Questions related to the present *Qualified Long-Term Preservation 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 |

### 1.4.3     Person or Organization Responsible for the Suitability of the Practice Statement for the *Qualified Long-Term Preservation Policy*

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

The *Long-Term Preservation 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 *Long-Term Preservation 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/

### 1.4.4    Practice Statement Approval Procedures

The *Long-Term Preservation Provider* shall describe the acceptance procedure of the *Long-Term Preservation Practice Statement* that announces its conformity with the present *Qualified Long-Term Preservation Policy* in the given *Long-Term Preservation Practice Statement*.

## 1.5    Definitions and Acronyms

### 1.5.1   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: <br><br> • 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 <br><br> • the creation, verification and validation of *Website Authentication Certificate*; or <br><br> • the preservation of electronic signatures, seals or certificates related to those services; <br><br> " *(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)* |
| E-dossier | The electronic file (e-dossier) is a container format electronic signature. An e-dossier may contain documents, or the related profiles (metadata), signatures, countersignatures and time-stamps. |
| Electronic Document | "Means any content stored in electronic form, in particular text or sound, visual or audiovisual recording" *(eIDAS [1] 3. article 35. 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 *Long-Term Preservation Provider* in order to use some of its services. |

| File | In a general sense of logically related data file, which is stored and which is interpreted in a particular format with a specific meaning (typically text, images, sound, video…) is an electronic document. The definition of file in the present *Qualified Long-Term Preservation Policy*  a narrower sense, we use only for electronic documents placed in e-dossiers files. |
|---|---|
| Suspension | The temporary termination of the *Certificate*'s validity before the end of the validity period indicated on the *Certificate*. The *Certificate* suspension is not definitive; the suspended *Certificate*'s validity can be restored. |
| 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 *Long-Term Preservation 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. |

| | |
|---|---|
| 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. <br><br> 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. <br><br> 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. |
| Unencrypted e-dossier | An e-dossier, which includes unencrypted files and electronic signatures or electronic seals on them. In the unencrypted e-dossier the signed, stamped files and signatures, seals are included unencrypted. |
| Extraordinary Operational Situation | An extraordinary situation causing disturbance in the course of the operation of the *Long-Term Preservation Provider*, when the continuation of the normal operation of the *Long-Term Preservation 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 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. |
| --- | --- |
| Encrypted e-dossier | This e-dossier is an XML file that contains another (unencrypted or encrypted) e-dossier (too) – encrypted according to the S/MIME specification. |
| Client | The *Subscriber* and the service users, for whom the *Subscriber* grants user rights. |
| 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*. |

### 1.5.2   Acronyms

| | |
| --- | --- |
| CRL | Certificate Revocation List |
| eIDAS | electronic Identification, Authentication and Signature |
| LDAP | Lightweight Directory Access Protocol |
| NMHH | National Media and Infocommunications Authority |
| OCSP | Online Certificate Status Protocol |
| OID | Object Identifier |
| PKI | Public Key Infrastructure |
| TSP | Trust Service Provider |

# 2   Publication and Repository Responsibilities

## 2.1   Repositories

The *Long-Term Preservation Provider* shall publish the *Qualified Long-Term Preservation Policy*, the *Long-Term Preservation Practice Statement* and other documents containing the terms and conditions its operation is based on.

## 2.2   Publication of Certification Information

### 2.2.1   Publication of the *Long-Term Preservation Provider* Information

The *Long-Term Preservation 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 *Long-Term Preservation Provider*.

The *Long-Term Preservation Provider* shall make  available the *Qualified Long-Term Preservation Policy*, the *Long-Term Preservation Practice Statement* and the Service Agreement to the *Client* on a durable medium following the conclusion of the contract.

The *Long-Term Preservation 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 Long-Term Preservation Policy*   related new versions is compliant with the methods described in Section 8.12.

The *Long-Term Preservation Provider* discloses other regulations, contractual conditions and their new versions if necessary.

The *Long-Term Preservation Provider* shall publish  extraordinary information without delay in accordance with the legal requirements and in the absence thereof when necessary.

## 3 Electronic Long-Term Preservation Service

Under the electronic long-term preservation service the following tasks must be provided:

- The *Subscriber* can upload electronically signed electronic documents included into the electronic dossier (e-dossier) to the archive operated by the *Long-Term Preservation Provider*. At the reception of the e-dossier the *Long-Term Preservation Provider* checks the electronic signature(s) or seal(s) on the e-dossier, or on the files included into the e-dossiers, completes or compiles the long-term validation material, places electronic archive *Time Stamp* on the long-term validation material, and saves the accepted e-dossier. (see section 3.2).

- The *Long-Term Preservation Provider* securely preserves the accepted e-dossiers – the included files and long-term validation material – and ensures during the whole preservation period that:

  - only authorized persons have access to the preserved data;
  - the entitled *Subscriber* has continuous access to the preserved data;
  - the preserved data can not be modified or deleted without authorization.

- The *Long-Term Preservation Provider* ensures the long term validity provision of the electronic signatures and seals placed on the e-dossiers and on the files preserved in the e-dossiers. The *Long-Term Preservation Provider* ensures the long-term readability of the files in the e-dossiers and in case of specified file formats during the preservation period. The preservation period is 50 years, except if the validity of the service agreement ceases before the end of this period (for details see section 4).

- The *Subscriber* has access continuously to the e-dossiers, electronic documents, signatures and seals placed by them in the archive of the *Long-Term Preservation Provider* and to the corresponding long-term validation material, and they can download them (see section: 3.3).

- At the request of the *Subscriber* the *Long-Term Preservation Provider* issues an authentic acknowledgement that it preserves the e-dossiers, and that at the time of the acceptance to the archive the electronic signatures or seals on the documents stored in the e-dossiers were valid (see section: 3.4).

- At the request of the *Subscriber* the *Long-Term Preservation Provider* deletes the e-dossiers from its archive (see section: 3.6).

The primary task of the long-term preservation service is the preservation of the validity of the electronic signature or seal placed on the electronic document.

The *Long-Term Preservation Provider* can provide other services to the *Subscriber* besides the provision of the basic task, for example:

- preservation of the electronic documents with an electronic signature or seal,

- ensuring the readability and human interpretability of the electronic documents uploaded to the archive,

- performing the file format conversions that become necessary.

The present *Qualified Long-Term Preservation Policy* defines the requirements for the long-term validity assurance of electronic signatures and seals, so it does not enable the acceptance and preservation of documents without any electronic signature or seal.

The *Long-Term Preservation Provider* may specify and restrict in the *Long-Term Preservation Practice Statement* the format of the accepted electronic signatures or seals, the accepted Certification Authorities and any other parameter.

## 3.1   Concluding a Service Agreement

Before using the service the *Subscriber* shall conclude a service agreement with the the *Long-Term Preservation Provider*.

The *Long-Term Preservation Practice Statement* and the other regulations cited therein shall clearly specify the details of the service to be provided, and the tools needed for using the service.

## 3.2   Uploading the Document

1. The *Long-Term Preservation Provider* shall only accept the e-dossiers to be archived after the identification of the *Subscriber* within the framework of a secure procedure.

2. It shall be clearly specified in the *Long-Term Preservation Practice Statement* which signature and file format the *Long-Term Preservation Provider* accepts in the e-dossier, how it verifies the electronic signatures and seals and under what conditions it accepts the e-dossiers.

3. The validity of the electronic signature(s) or seal(s) on the received e-dossier shall be verified using the full long-term validation material. The verification may be based on the partial or full long-term validation material attached to the electronic signature(s) or seal(s). Any still necessary information for the validation shall be collected by the *Long-Term Preservation Provider* and it shall preserve that linked to the e-dossier. After compiling the long-term validation materials the *Long-Term Preservation Provider* shall place a qualified archive *Time Stamp* on each long-term validation material.

4. The *Long-Term Preservation Provider* shall preserve the accepted e-dossier encrypted. The encryption shall ensure that unauthorized personnel cannot ascertain its content. The decryption of the encrypted e-dossier shall only happen in cases related to the provision of the electronic long-term preservation service, for example downloading (3.3), certification (4.4), and re-encryption (4.5).

5. The *Long-Term Preservation Provider* shall send confirmation to the *Subscriber* as soon as possible, but no later than 3 days from admission that the long-term validation material has been compiled successfully, and it accepted the e-dossier. If the process is interrupted somewhere, the *Long-Term Preservation Provider* shall notify the *Subscriber* in an error message. Based on the error message it must be clearly identifiable that which e-dossier is involved and what was the reason for rejection.

   If the verification on the acceptance of the e-dossier does not arrive to the *Subscriber* within the stated deadline, it shall be considered that the *Long-Term Preservation Provider* did not accept the e-dossier. The *Long-Term Preservation Provider* is solely responsible for the preservation of the e-dossier and for ensuring the long-term credibility of the included electronic signatures and seals in case of sending positive confirmation.

## 3.3   Provision of the Long-Term Validation Material Availability – E-Dossier Download

The *Long-Term Preservation Provider* shall ensure that the *Subscriber* can download his e-dossiers preserved in the archive and the corresponding long-term validation material during the validity period of the service agreement.

1. The *Subscriber* only has access to the e-dossiers and the long-term validation material preserved in the archive of the *Long-Term Preservation Provider* through a secure channel.

2. The *Long-Term Preservation Provider* shall ensure that every *Subscriber* only have access to the e-dossiers and the long-term validation material to which he is really entitled to access.

## 3.4   Issuance of the Acknowledgement

At the request of the *Subscriber* the *Long-Term Preservation Provider* issues an acknowledgement in connection with the e-dossier. The acknowledgement consists of the following:

1. The statement that the frame signature or in the absence of the frame signature on the e-dossier the advanced or qualified electronic signatures, seals, *Time Stamp*s on the files and the corresponding *Certificate*s in the e-dossier were valid at the time of the time stamping and the validation after their upload.

2. The statement that the given e-dossier has the given hash, so it is identical to the e-dossier with the same hash presented by the *Subscriber*.

3. The statement that the specified person or organization placed valid electronic signatures or seals as frame signatures or in the absence of a frame signature on the e-dossier as signatures or seals on the files included into the e-dossier.

4. The statement that *Time Stamp*s valid at the given date were placed as frame *Time Stamp*s or in the absence of a frame signature on the e-dossier as *Time Stamp*s on the files included into the e-dossier.

The *Long-Term Preservation Provider* issues the acknowledgement on paper or in an e-dossier with a qualified electronic signature. The acknowledgement is created by an official responsible for issuing the archive acknowledgement, and in case of an electronic acknowledgement places his qualified electronic signature and a qualified *Time Stamp*, in case of a paper based acknowledgement he authenticates the printed acknowledgement with his handwritten signature.

Knowledge of the archived e-dossier is not needed for the issuance of the acknowledgement, it is issued based on the hash of the unencrypted e-dossier preserved in cleartext. No information can be obtained from the hash value in relation to the content of the preserved e-dossier. The applied solution ensures that the officials responsible for issuing the archive acknowledgement do not get to know the contents of the unencrypted e-dossier in connection with the issuance of the acknowledgement.

The issuance of the acknowledgement may happen in a way that the *Subscriber* presents the *Long-Term Preservation Provider* the unencrypted archived e-dossier. Then, provided that the archive of the *Long-Term Preservation Provider* contains an e-dossier with the same hash as the presented unencrypted e-dossier, the employee of the *Long-Term Preservation Provider* issues the acknowledgement in relation to the presented e-dossier.

The *Subscriber* can request the issuance of the acknowledgement from the *Long-Term Preservation Provider* with a paper based hand signed request submitted by any delivery manner or by filing an electronic request certified with at least an advanced electronic signature or seal.

The issuance of the acknowledgement may be requested by the authorized representative of the *Subscriber* if he presented the authorization of the *Subscriber* contained in a fully conclusive private document beforehand.

## 3.5   Document Display

The *Long-Term Preservation Provider* shall make available to the *Subscriber*, that by using the software and hardware devices of the *Long-Term Preservation Provider* at a pre-agreed date and venue they may view their documents stored in the archive of the *Long-Term Preservation Provider*.

## 3.6   Deletion of the Document and the Long-Term Validation Material

The *Long-Term Preservation Provider* shall make available the selective deletion of the e-dossiers and all the corresponding long-term validation materials preserved in the archive to the request of the *Subscriber*. The deletion means the physical deletion of the preserved e-dossier and its overwriting in such a way that it can not be restored (or only with unrealistically high financial expenditure) from the data medium later. The deletion shall be performed on the whole system of the *Long-Term Preservation Provider*, and during the deletion it shall destroy every preserved copy of the e-dossier.

The *Long-Term Preservation Provider* shall specify in the *Long-Term Preservation Practice Statement* the manner and conditions of the admission and processing of the deletion request.

## 3.7   Termination of the Service Agreement

In case of the termination of the contract the *Long-Term Preservation Provider* shall make available the e-dossiers and the long-term validation material commissioned by the *Subscriber* to be preserved for download to the *Subscriber* or to another entitled person.

After the termination of the contract the *Long-Term Preservation Provider* shall delete the e-dossiers and the long-term validation material corresponding to the *Subscriber*.

# 4   Technical Security Measures

## 4.1   Security Guarantees

The *Long-Term Preservation Provider* uses reliable systems and products protected against modification. It uses a uniform IT system consisting of reliable, technically evaluated and certified security products for the provision of its services. The *Long-Term Preservation Provider* uses reliable systems and products that are protected against unauthorized modification. Both the *Long-Term Preservation Provider*, and the system supplier and installer contractors have significant experience in building certification services and use internationally recognized technology.

If the *Long-Term Preservation Provider* uses a trusted service of a third party, it shall verify whether that third party complies with every necessary requirement. The *Long-Term Preservation Provider* stores the archived e-dossiers in a physically protected environment, according to the physical and procedural requirements described in section 5, the safety of which is guaranteed by the internal security policies and the regular internal and external security audits. The *Long-Term Preservation Provider* ensures that the stored e-dossiers can not be read even by its employees. The *Long-Term Preservation Provider* only submits the e-dossiers to a third party (e.g. authority) if the *Subscriber* authorizes it or when it is required by law.

The integrity of the stored e-dossiers is ensured by the physical protection of the e-dossiers, as well as by technologies related to electronic signatures. The availability of the e-dossiers is ensured by the high quality system of the *Long-Term Preservation Provider* and the internal regulations governing the system, the business continuity and emergency management procedures and other procedures for managing emergency situations. The *Long-Term Preservation Provider* avoids errors arising during operation and maintenance using these processes, and their continuous internal and external monitoring and testing. The *Long-Term Preservation Provider* stores the archived e-dossiers at two physical locations far from each other.

The *Long-Term Preservation Provider* destroys the archived e-dossiers – at the request of the *Subscriber* or in case of the termination of the contract – under the conditions described in section 3.6. The *Long-Term Preservation Provider* creates the signing keys used in the confirmations, the keys used to encrypt/decrypt archived e-dossiers and infrastructure and system control keys in a cryptographic hardware device. The *Long-Term Preservation Provider* periodically replaces these keys. The *Long-Term Preservation Provider* monitors the development of technology and if it detects that a key is no longer secure or the algorithm is no longer usable according to the decision of the National Media and Infocommunications Authority, it immediately replaces the affected key or keys.

The *Long-Term Preservation Provider* stores the e-dossiers encrypted. The *Long-Term Preservation Provider* encrypts e-dossiers always using an algorithm which is considered safe at the given the state of technology. If the security of this algorithm is compromised during the development of technology, the *Long-Term Preservation Provider* ensures the re-encryption of the e-dossier with a secure algorithm based on its own internal regulations.

## 4.2   Computer Security Precautions

The *Long-Term Preservation Provider* uses reliable IT systems and solutions, technologies and developed a redundant system. Two instances operate for all critical service provider system components, and in case of a failure of any of those units, the other unit takes over the operation.

The IT system of the *Long-Term Preservation Provider* is protected by a multi-stage firewall system. Each firewall has two copies, in case of the failure of a unit another instance of the same unit takes over its function by using a cluster.

## 4.3   Life-Cycle Related Technical Precautions

In order to meet the high level of security requirements in all the system development projects of the *Long-Term Preservation Provider*, the elevated requirements shall be taken into account in the overall development process (even in the planning and requirement definition phase).

Products used for the provision of services are applied by taking into account the life cycle related security considerations.

## 4.4   Regular Certification

The *Long-Term Preservation Provider* places a qualified electronic signature or seal and a qualified *Time Stamp* on the long-term validation material:

- at least once annually;

- if any of the algorithms used for electronic signatures, seals and time-stamping (including the hashing algorithm) lose confidence;

- if the National Media and Infocommunications Authority makes such a decision.

The *Long-Term Preservation Provider* creates the qualified electronic signature or seal and the qualified *Time Stamp* using secure algorithms according to the current version of the decision of the National Media and Infocommunications Authority related to the algorithms (at the time of the publication of  the *Qualified Long-Term Preservation Policy*  [8]).

## 4.5   Re-Encrypting the Archive

The archived e-dossiers shall be stored encrypted in the archive. It shall be ensured that the archived e-dossiers are encrypted with an encryption algorithm that is secure at all times.

The e-dossiers shall be re-encrypted, if:

- an algorithm used for encryption loses confidence – in this case they should be re-encrypted with an algorithm considered safe at the time of encryption;

- the confidentiality of the decoding key of the *Long-Term Preservation Provider* is compromised;

- the *Long-Term Preservation Practice Statement* or the contract concluded with the *Subscriber* requires so.

After the re-encryption of archived e-dossiers the former copies encrypted in a manner deemed not sufficiently secure shall be destroyed.

## 4.6   Continuous Monitoring of Technology

The *Long-Term Preservation Provider* shall continuously monitor the development of the electronic signature and cryptography related technology. If the *Long-Term Preservation Provider* learns that a cryptographic algorithm with a given parameter which is accepted by the decision of the National Media and Infocommunications Authority is no longer secure, it shall notify the National Media and Infocommunications Authority and request the revision of the decision related to the cryptographic algorithms.

The *Long-Term Preservation Provider* is free to decide at any time to change the used cryptographic algorithm sets and their parameters in case of an algorithm and parameter accepted by the decision of the National Media and Infocommunications Authority.

## 4.7   Acceptance of the Certification and Time-Stamping Providers

The *Long-Term Preservation Provider* may specify under what conditions it accepts the *Certificate*s of a given Certification Authority and what Certification Authorities it accepts, along with the criteria for the Certification Authorities to be included in this list or to be excluded from it within the framework of the long term preservation service.

## 4.8   The Maintenance of the Readability and Interpretability of the e-Dossiers and the Files Within Them

The *Long-Term Preservation Provider* shall clearly determine in the *Long-Term Preservation Practice Statement* or in an other document referenced in the *Long-Term Preservation Practice Statement*, that which file format and document readability it ensures within the framework of the long term preservation service.

## 4.9   The Availability of Certain Elements of the Electronic Long-Term Preservation Service

The annual availability of the following electronic long term preservation service elements is 99% and the occasional service interruptions shall not exceed 3 days:

- the electronic download of the archived e-dossiers and validity chains;

- search of archived e-dossiers;

- receiving deletion requests;

- receiving timed deletion requests (with the help of which the *Subscriber* can specify how long a given e-dossier is archived by the *Long-Term Preservation Provider*), and the modification of former timed deletion requests;

- requesting information on the status of previously sent requests.

The *Long-Term Preservation Provider* is entitled to suspend the document (e-dossier) upload service  .

The issuance of the verifications is ensured by the *Long-Term Preservation Provider* continuously as described in the *Long-Term Preservation Practice Statement*, and the issuance of the verifications service interruption shall not exceed 3 days.

# 5    Facility, Management, and Operational Controls

The *Long-Term Preservation 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 *Long-Term Preservation 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 *Long-Term Preservation 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 *Long-Term Preservation 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 *Long-Term Preservation 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 *Long-Term Preservation Provider* performed.

### 5.1.1    Site Location and Construction

The IT system of the *Long-Term Preservation 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 *Long-Term Preservation 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.

*Long-Term Preservation 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 *Long-Term Preservation 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 *Long-Term Preservation 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 *Long-Term Preservation 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 *Long-Term Preservation 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 *Long-Term Preservation 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 *Long-Term Preservation Provider*.

### 5.1.8    Off-Site Backup

The *Long-Term Preservation 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 *Long-Term Preservation 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 *Long-Term Preservation 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 *Long-Term Preservation Provider*'s system. The auditing activity of the independent system auditor and the *Long-Term Preservation Provider*'s internal auditor ensures the system's appropriate operation.

### 5.2.1    Trusted Roles

The *Long-Term Preservation 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.

- long term preservation officer: it is possible to decrypt an e-dossier with the co-operation of two long term preservation officer. The long term preservation officers are responsible for the secure management of the decrypted e-dossier, and for its destruction after use.

- officer responsible for long term preservation statement issuance: his duty is the issuance and certification of the long term preservation statements.

For the provision of trusted roles the manager responsible for the security of the *Long-Term Preservation Provider* shall formally appoint the *Long-Term Preservation Provider*'s employees.

Only those persons may hold a trusted role who are in employment relationship with the *Long-Term Preservation 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 *Long-Term Preservation 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 *Long-Term Preservation 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.

The co-operation of two long term preservation officer is necessary to decrypt an encrypted e-dossier stored in the archive. The long term preservation officers are responsible for the secure management of the decrypted e-dossier, and for its destruction after use.

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 *Long-Term Preservation 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 *Long-Term Preservation Provider* can hold multiple trusted roles at the same time, but the *Long-Term Preservation 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 *Long-Term Preservation Provider* shall take care that its personnel policy, and its practices applicable to employing staff members intensify and support the reliability of the *Long-Term Preservation 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 *Long-Term Preservation 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 *Long-Term Preservation Provider*'s services shall sign a non-disclosure agreement.

At the same time, the *Long-Term Preservation 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 *Long-Term Preservation 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 *Long-Term Preservation Provider* only by persons, who have no external influence and possess the necessary expertise validated by the *Long-Term Preservation 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 *Long-Term Preservation 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 *Long-Term Preservation 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 *Long-Term Preservation 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 *Long-Term Preservation 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 *Long-Term Preservation 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 *Long-Term Preservation 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 *Long-Term Preservation Provider*.

### 5.3.4    Retraining Frequency and Requirements

The *Long-Term Preservation 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 *Long-Term Preservation 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 *Long-Term Preservation 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 *Long-Term Preservation 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 *Long-Term Preservation Provider*.

### 5.3.8    Documentation Supplied to Personnel

The *Long-Term Preservation 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 *Long-Term Preservation Provider* shall implement and operate an event logger and control system covering its full IT system.

### 5.4.1    Types of Events Recorded

The *Long-Term Preservation 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 *Long-Term Preservation Provider*'s operation.

The following events shall be logged at minimum:

- LONG TERM PRESERVATION

    - information related to the upload of the e-dossiers and the validation of the electronic signatures within them;

    - information related to the availability of data, integrity preservation, authenticity and non-repudiation preservation, maintenance of the information readability and deletion;

    - information related to the e-dossier download, statement request fulfilment, and the handover of the archive to another provider;

- 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.

- 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 Long-Term Preservation Policy* or the *Long-Term Preservation 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 *Long-Term Preservation 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 *Long-Term Preservation 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 *Long-Term Preservation 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 *Long-Term Preservation Practice Statement*.

### 5.4.6    Audit Collection System (Internal vs External)

The *Long-Term Preservation Provider* specifies the operation of its logging processes in its *Long-Term Preservation Practice Statement*.

The *Long-Term Preservation 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 *Long-Term Preservation Provider* shall be suspended until the incident is resolved.

### 5.4.7    Notification to Event-causing Subject

In case of the detected errors, the *Long-Term Preservation 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 *Long-Term Preservation 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 *Long-Term Preservation Provider* shall be prepared to the proper secure long-term archiving of electronic and paper documents.

The *Long-Term Preservation Provider* shall archive the following types of information:

- every document related to the accreditation of the *Long-Term Preservation Provider*;

- all issued versions of the *Certificate Policies* and *Long-Term Preservation Practice Statement*s;

- all issued versions of the Terms and Conditions;

- contracts related to the operation of the *Long-Term Preservation Provider*;

- every electronic and paper based log entry.

### 5.5.2    Retention Period for Archive

The *Long-Term Preservation Provider* is bound to preserve the archived data for the time periods below:

- *Long-Term Preservation Practice Statement*: 10 years after the repeal;

### 5.5.3    Protection of Archive

The *Long-Term Preservation 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 *Long-Term Preservation 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 *Long-Term Preservation 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 *Long-Term Preservation 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 *Long-Term Preservation 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    Compromise and Disaster Recovery

In case of a disaster, the *Long-Term Preservation 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.

### 5.6.1    Incident and Compromise Handling Procedures

The *Long-Term Preservation Provider* shall have a business continuity plan.

The *Long-Term Preservation 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 *Long-Term Preservation 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.

### 5.6.2    Computing Resources, Software, and/or Data are Corrupted

The IT systems of the *Long-Term Preservation 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 *Long-Term Preservation Provider* shall make a full daily backup of its databases and the generated log events.

The *Long-Term Preservation 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 *Long-Term Preservation 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 *Long-Term Preservation Provider* shall restart its services as soon as possible.

### 5.6.3    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 *Long-Term Preservation 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 *Long-Term Preservation 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 *Long-Term Preservation Provider* shall restore its devices damaged during the disaster and the original service security level as quickly as possible.

## 5.7    Long-Term Preservation Service  Termination

The *Long-Term Preservation 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 *Long-Term Preservation Provider* shall make every effort to ensure that at the latest by the service termination another provider takes over the records and service obligations;

- 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 *Long-Term Preservation 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    Private Key Protection and Cryptographic Module Engineering Controls

The *Long-Term Preservation 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 *Long-Term Preservation 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.

### 6.1.1    Cryptographic Module Standards and Controls

The systems of the *Long-Term Preservation Provider*    store the private keys  in such secure
hardware devices that are compliant with the following:

- the requirements of ISO/IEC 19790 [12], or

- the requirements of FIPS 140-2 [13] 3, or the requirements of a higher level, or

- the requirements of CEN 14167-2 [14] 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 [11] 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.

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

The *Long-Term Preservation 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.

### 6.1.3    Private Key Escrow

The *Long-Term Preservation Provider* shall not escrow its own provider private keys.

### 6.1.4    Private Key Backup

The *Long-Term Preservation 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.

### 6.1.5    Private Key Archival

The *Long-Term Preservation Provider* shall not archive   its private keys.

### 6.1.6    Private Key Transfer Into or From a Cryptographic Module

All of the provider private keys of the *Long-Term Preservation 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 *Long-Term Preservation 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.

### 6.1.7    Private Key Storage on Cryptographic Module

The *Long-Term Preservation 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*.

### 6.1.8    Method of Activating Private Key

The *Long-Term Preservation 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.

### 6.1.9    Method of Deactivating Private Key

The *Long-Term Preservation 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.

### 6.1.10    Method of Destroying Private Key

The discarded, expired or compromised *Long-Term Preservation 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 *Long-Term Preservation Provider* employees (an infrastructure administrator and a security officer) with the exclusion of other persons.

### 6.1.11    Cryptographic Module Rating

According to the requirements of Section 6.1.1 every provider private key of the *Long-Term Preservation Provider* shall be stored in a cryptographic module that

- has a certification according to ISO/IEC 19790 [12], or

- has a certification according to FIPS 140-2 Level 3 [13], or

- has a Common Criteria based certificate attesting compliance with the requirements of the CEN 14167-2 [14] 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

## 6.2    Activation Data

### 6.2.1    Activation Data Generation and Installation

The *Long-Term Preservation 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.

### 6.2.2    Activation Data Protection

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

### 6.2.3    Other Aspects of Activation Data

No stipulation.

## 6.3    Computer Security Controls

### 6.3.1    Specific Computer Security Technical Requirements

During the configuration and operation of the IT system of the *Long-Term Preservation 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 *Long-Term Preservation Provider* are sufficiently protected from unauthorized access;

- proper procedures are implemented to ensure service recovery after loss of key or system failure.

### 6.3.2    Computer Security Rating

In order to provide IT security and service quality the *Long-Term Preservation 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.

## 6.4    Life Cycle Technical Controls

### 6.4.1    System Development Controls

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

The *Long-Term Preservation Provider* shall have a version control system where every change shall be documented.

The *Long-Term Preservation Provider* shall implement procedures for unauthorized change detection.

### 6.4.2    Security Management Controls

The *Long-Term Preservation 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 *Long-Term Preservation Provider* shall ensure that the program to be installed is the proper version and that it is free from any unauthorized modification. The *Long-Term Preservation Provider* shall regularly check the integrity of the software in its system used in the service.

### 6.4.3    Life Cycle Security Controls

The *Long-Term Preservation 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.

## 6.5    Network Security Controls

The *Long-Term Preservation 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 *Long-Term Preservation Provider* shall implement proper procedures for the detection of any hardware or software change, system installation, and maintenance occurred on the IT system. The *Long-Term Preservation Provider* shall check the authenticity and integrity of every software component at their first loading.

The *Long-Term Preservation 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 .

## 6.6    Time-stamping

The *Long-Term Preservation 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    Compliance Audit and Other Assessments

The operation of the *Long-Term Preservation 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 *Long-Term Preservation Provider* location. Before the site inspection, the *Long-Term Preservation 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 *Long-Term Preservation Provider* meets the requirements of the eIDAS Regulation [1] and the related

Hungarian legislation and the requirements of the applied *Qualified Long-Term Preservation Policy*(s) and the corresponding *Long-Term Preservation 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]

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 *Long-Term Preservation Provider*.

The *Long-Term Preservation 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 Long-Term Preservation Policy*(s) in order to verify compliance with the requirements.

## 7.1    Frequency or Circumstances of Assessment

The *Long-Term Preservation Provider* shall have the conformance assessment carried out annually.

## 7.2    Identity/Qualifications of Assessor

The *Long-Term Preservation 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.

## 7.3    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 *Long-Term Preservation 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 *Long-Term Preservation Provider*.

## 7.4    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 *Long-Term Preservation Practice Statement*;

- adequacy of the employed processes;

- documentation;

- physical security;

- adequacy of the personnel;

- IT security;

- compliance with the data protection rules.

## 7.5    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 *Long-Term Preservation 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.

## 7.6    Communication of Results

The *Long-Term Preservation 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.

# 8    Other Business and Legal Matters

## 8.1    Fees

The fees applied by the *Long-Term Preservation Provider* shall be publicly disclosed in accordance with the applicable regulations.

### 8.1.1    Refund Policy

No stipulation.

## 8.2    Financial Responsibility

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

### 8.2.1    Insurance Coverage

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

- The *Long-Term Preservation Provider* has at least an amount of 25 million HUF as an unconditional and irrevocable bank warranty.

- The *Long-Term Preservation 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 *Long-Term Preservation Provider* covering the costs. The amount of this financial guarantee shall be at least 25 million HUF.

### 8.2.2    Insurance or Warranty Coverage for End-entities

The *Long-Term Preservation Provider* shall have liability insurance to ensure reliability.

## 8.3    Confidentiality of Business Information

The *Long-Term Preservation Provider* shall manage the data of the Clients in accordance with the respective regulations.

### 8.3.1    Scope of Confidential Information

The *Long-Term Preservation Provider* shall specify the scope of data that are considered confidential information in its *Long-Term Preservation Practice Statement*.

### 8.3.2    Information Not Within the Scope of Confidential Information

The *Long-Term Preservation Provider* may consider all data public that are not specified as confidential in the *Long-Term Preservation Practice Statement*.

### 8.3.3    Responsibility to Protect Confidential Information

The *Long-Term Preservation Provider* is responsible for the protection of the confidential data it manages.

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

Circumstances when the *Long-Term Preservation Provider* may disclose the confidential data shall be determined case-by-case in the *Long-Term Preservation Practice Statement*.

## 8.4    Privacy of Personal Information

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

The *Long-Term Preservation 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.

### 8.4.1    Privacy Plan

The *Long-Term Preservation 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 *Long-Term Preservation Provider*.

### 8.4.2    Information Treated as Private

The *Long-Term Preservation 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 *Long-Term Preservation 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.

### 8.4.3    Information Not Deemed Private

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

### 8.4.4    Responsibility to Protect Private Information

The *Long-Term Preservation 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 *Long-Term Preservation 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.

### 8.4.5    Notice and Consent to Use Private Information

The *Long-Term Preservation Provider* shall only use  the personal data of the *Client* to the extent required for service provision, to contact the *Client*.

### 8.4.6    Disclosure Pursuant to Judicial or Administrative Process

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

### 8.4.7    Other Information Disclosure Circumstances

No stipulation.

## 8.5    Intellectual Property Rights

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

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

The present *Qualified Long-Term Preservation 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 *Long-Term Preservation Provider* shall be determined in the *Long-Term Preservation Practice Statement*.

## 8.6    Representations and Warranties

### 8.6.1    CA Representations and Warranties

**Certification Authority's Responsibility**

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

- The *Long-Term Preservation Provider* assumes responsibility for compliance with the procedures described in *Certificate Policies* it supports;

- The *Long-Term Preservation Provider* assumes responsibility as its own for the damages caused during the provision of the service by its subcontractors;

- The *Long-Term Preservation 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 *Long-Term Preservation 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 *Long-Term Preservation 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 8.8.).

**Certification Authority Obligations**

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

The *Long-Term Preservation Provider*'s basic obligations is that it shall provide the services in line with the *Qualified Long-Term Preservation Policy*, this *Long-Term Preservation 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.

### 8.6.2    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 *Long-Term Preservation Provider* while using the service .

The obligations of the *Subscriber* are determined by this *Qualified Long-Term Preservation Policy*, the service agreement and its attachments – in particular the general terms and conditions –– and the *Long-Term Preservation Practice Statement*.

### 8.6.3    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 *Certificate* and *Time Stamp*s. During the verification of the validity for keeping the security level guaranteed by the *Long-Term Preservation 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 Long-Term Preservation Policy* and the corresponding *Long-Term Preservation Practice Statement*;

- use reliable IT environment and applications;

- verify the   based on the current CRL or OCSP response;

- take into consideration every restriction in relation to the   usage which is included  in the *Qualified Long-Term Preservation Policy* and the *Long-Term Preservation Practice Statement*.

### 8.6.4    Representations and Warranties of Other Participants

No stipulation.

### 8.7    Disclaimers of Warranties

The *Long-Term Preservation 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.

## 8.8    Limitations of Liability

No stipulation.

## 8.9    Indemnities

### 8.9.1    Indemnification by the *Long-Term Preservation Provider*

The detailed rules of the indemnities of the *Long-Term Preservation Provider* are specified in the *Long-Term Preservation Practice Statement*, the service agreement, or the contracts concluded with the *Client*s.

### 8.9.2    Indemnification by Subscribers

The *Long-Term Preservation Provider* sets the term of claim for damages from *Subscriber*s in the *Long-Term Preservation Practice Statement* and the service agreement.

### 8.9.3    Indemnification by Relying Parties

The *Long-Term Preservation Provider* sets the term of its claim for damages from Relying parties in the *Long-Term Preservation Practice Statement*.

## 8.10    Term and Termination

### 8.10.1    Term

The effective date of the specific *Qualified Long-Term Preservation Policy*  is specified on the cover of the document.

### 8.10.2    Termination

The *Qualified Long-Term Preservation Policy*  is valid without a time limit until withdrawal.

### 8.10.3    Effect of Termination and Survival

In case of the withdrawal of the *Qualified Long-Term Preservation Policy*  the *Long-Term Preservation Provider* publishes the detailed rules of the withdrawal and the rights and obligations persisting after withdrawal on its webpage.

## 8.11    Individual Notices and Communications with Participants

The *Long-Term Preservation Provider* shall operate a customer service in order to maintain contact with its *Client*s.

## 8.12   Amendments

The *Long-Term Preservation Provider* reserves the right to change the *Qualified Long-Term Preservation 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.

### 8.12.1   Procedure for Amendment

The *Long-Term Preservation Provider* reviews  the *Qualified Long-Term Preservation 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 *Long-Term Preservation 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 *Long-Term Preservation 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 *Long-Term Preservation Provider* will close and publish the version of the regulation as amended with remarks on the 7th day prior to its becoming effective.

### 8.12.2   Notification Mechanism and Period

The *Long-Term Preservation Provider* notifies the *Relying Parties* of new document version issuances as described in Section 8.12.1..

### 8.12.3   Circumstances Under Which OID Must Be Changed

The *Long-Term Preservation Provider* issues a new version number in case of even the smallest change to the *Qualified Long-Term Preservation 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.

## 8.13    Dispute Resolution Provisions

The *Long-Term Preservation 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.

## 8.14    Governing Law

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

## 8.15    Compliance with Applicable Law

The present *Qualified Long-Term Preservation 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];

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

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

## 8.16    Miscellaneous Provisions

### 8.16.1    Entire Agreement

No stipulation.

### 8.16.2    Assignment

The providers operating according to this *Qualified Long-Term Preservation Policy* may only assign their rights and obligations to a third party with the prior written consent of the *Long-Term Preservation Provider*.

### 8.16.3    Severability

Should some of the provisions of the present *Qualified Long-Term Preservation Policy*  become invalid for any reason, the remaining provisions will remain in effect unchanged.

### 8.16.4    Enforcement (Attorneys' Fees and Waiver of Rights)

The *Long-Term Preservation 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 *Long-Term Preservation Provider* does not exercise its claim for damages that does not mean that in similar cases in the future or in case of violation of other provisions of the present *Qualified Long-Term Preservation Policy* , it would waive the enforcement of claims for damages.

### 8.16.5    Force Majeure

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

## 8.17    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] (Hungarian) Number EF/26838-10/2011 decree of the National Media and Infocommunications Authority dated on the 27th of September 2011 on the applicable secure crypthographic algorithms and their parameters during the provision of services in relation to electronic signatures. .

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

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

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

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