e-Szignó Certification Authority

eIDAS conform
Qualified Long-Term Preservation Service
Preservation Practice Statement

ver. 2.11

Date of effect: 25/09/2019

OID	1.3.6.1.4.1.21528.2.1.1.188.2.11
Version	2.11
First version date of effect	15/12/2006
Security classification	PUBLIC
Approved by	Gergely Vanczák
Date of approval	23/09/2019
Date of effect	25/09/2019

Microsec Micro Software Engineering & Consulting Private Company Limited by Shares
Hungary, H-1033 Budapest, Ángel Sanz Briz str. 13. Building C

Version	Description	Effect date	Author(s)
1.0	First version. OID: 1.3.6.1.4.1.21528.2.1.1.18	15/12/2006	István Zsolt Berta, Dr.
1.1	Changes according to the feedback of the National Telecommunications Authority. OID: 1.3.6.1.4.1.21528.2.1.1.18.1.1	08/01/2007	István Zsolt Berta, Dr.
1.2	Change in the contact data of the consumer protection. OID: 1.3.6.1.4.1.21528.2.1.1.18.1.2	01/01/2008	István Zsolt Berta, Dr.
1.3	Not issued. OID: 1.3.6.1.4.1.21528.2.1.1.18.1.3	01/10/2008	István Zsolt Berta, Dr.
1.4	Conforming to the new requirements of the NHH. OID: 1.3.6.1.4.1.21528.2.1.1.18.1.4	20/12/2008	István Zsolt Berta, Dr.
2.0	Change in the company form. Change related to the encryption of the archived e-dossiers. OID: 1.3.6.1.4.1.21528.2.1.1.18.2.0	01/05/2012	István Zsolt Berta, Dr.
2.0	New, eIDAS conform preservation policy with new OID. OID: 1.3.6.1.4.1.21528.2.1.1.88.2.0	01/07/2016	Sándor Szőke, Dr.
2.1	Changes according to the NMHH comments.	05/09/2016	Melinda Szomolya, Sándor Szőke, Dr.
2.2	Changes according to the auditor comments.	30/10/2016	Sándor Szőke, Dr.
2.4	Yearly revision.	30/09/2017	Sándor Szőke, Dr.
2.6	Global revision. Smaller improvements.	24/03/2018	Sándor Szőke, Dr.
2.7	Yearly revision.	15/09/2018	Sándor Szőke, Dr.
2.8	Changes based on the suggestions of the auditor.	14/12/2018	Sándor Szőke, Dr.
2.11	Yearly revision.	25/09/2019	Sándor Szőke, Dr.

Table of Contents

1 Introduction **9**
1.1 Overview . . . 9
1.2 Document Name and Identification . . . 9
1.2.1 Long-term preservation policy . . . 10
1.2.2 Effect . . . 11
1.3 PKI Participants . . . 11
1.3.1 Certification Authorities . . . 11
1.3.2 Subscribers . . . 14
1.3.3 Relying Parties . . . 14
1.4 Policy Administration . . . 14
1.4.1 Organization Administering the Document . . . 14
1.4.2 Contact Person . . . 15
1.4.3 Person or Organization Responsible for the Suitability of the Practice Statement for the *Qualified Long-Term Preservation Policy* . . . 15
1.4.4 Practice Statement Approval Procedures . . . 15
1.5 Definitions and Acronyms . . . 15
1.5.1 Definitions . . . 15
1.5.2 Acronyms . . . 19

2 Publication and Repository Responsibilities **20**
2.1 Repositories . . . 20
2.2 Publication of Certification Information . . . 20
2.2.1 Publication of the *Long-Term Preservation Provider* Information . . . 20
2.3 Time or Frequency of Publication . . . 20
2.3.1 Frequency of the Publication of Terms and Conditions . . . 20

3 Electronic Long-Term Preservation Service **21**
3.1 Concluding a Service Agreement . . . 22
3.2 Uploading the Document . . . 23
3.3 Provision of the Long-Term Validation Material Availability – E-Document Download . . . 26
3.4 Issuance of the Acknowledgement . . . 27
3.5 Document Display . . . 29
3.6 Deletion of the Document and the Long-Term Validation Material . . . 29
3.7 Termination of the Service Agreement . . . 29

4 Technical Security Measures 29
4.1 Security Guarantees . . . 29
4.2 Computer Security Precautions . . . 30
4.3 Life-Cycle Related Technical Precautions . . . 31
4.4 Regular Certification . . . 31
4.5 Re-Encrypting the Archive . . . 31
4.6 Continuous Monitoring of Technology . . . 31
4.7 Acceptance of the Certification and Time-Stamping Providers . . . 32
4.8 The Maintenance of the Readability and Interpretability of the Electronic Documents 32
4.9 The Availability of Certain Elements of the Electronic Long-Term Preservation Service . . . 35

5 Facility, Management, and Operational Controls 36
5.1 Physical Controls . . . 36
5.1.1 Site Location and Construction . . . 36
5.1.2 Physical Access . . . 37
5.1.3 Power and Air Conditioning . . . 37
5.1.4 Water Exposures . . . 38
5.1.5 Fire Prevention and Protection . . . 38
5.1.6 Media Storage . . . 38
5.1.7 Waste Disposal . . . 38
5.1.8 Off-Site Backup . . . 39
5.2 Procedural Controls . . . 39
5.2.1 Trusted Roles . . . 39
5.2.2 Number of Persons Required per Task . . . 40
5.2.3 Identification and Authentication for Each Role . . . 41
5.2.4 Roles Requiring Separation of Duties . . . 41
5.3 Personnel Controls . . . 41
5.3.1 Qualifications, Experience, and Clearance Requirements . . . 42
5.3.2 Background Check Procedures . . . 42
5.3.3 Training Requirements . . . 43
5.3.4 Retraining Frequency and Requirements . . . 43
5.3.5 Job Rotation Frequency and Sequence . . . 43
5.3.6 Sanctions for Unauthorized Actions . . . 44
5.3.7 Independent Contractor Requirements . . . 44
5.3.8 Documentation Supplied to Personnel . . . 44
5.4 Audit Logging Procedures . . . 45
5.4.1 Types of Events Recorded . . . 45
5.4.2 Frequency of Audit Log Processing . . . 47

5.4.3 Retention Period for Audit Log . . . 48
5.4.4 Protection of Audit Log . . . 48
5.4.5 Audit Log Backup Procedures . . . 48
5.4.6 Audit Collection System (Internal vs External) . . . 48
5.4.7 Notification to Event-causing Subject . . . 49
5.4.8 Vulnerability Assessments . . . 49
5.5 Records Archival . . . 49
5.5.1 Types of Records Archived . . . 49
5.5.2 Retention Period for Archive . . . 50
5.5.3 Protection of Archive . . . 50
5.5.4 Archive Backup Procedures . . . 50
5.5.5 Requirements for Time-stamping of Records . . . 50
5.5.6 Archive Collection System (Internal or External) . . . 51
5.5.7 Procedures to Obtain and Verify Archive Information . . . 51
5.6 Compromise and Disaster Recovery . . . 51
5.6.1 Incident and Compromise Handling Procedures . . . 51
5.6.2 Computing Resources, Software, and/or Data are Corrupted . . . 52
5.6.3 Business Continuity Capabilities After a Disaster . . . 52
5.7 Long-Term Preservation Service Termination . . . 52

6 Technical Security Controls 53
6.1 Private Key Protection and Cryptographic Module Engineering Controls . . . 54
6.1.1 Cryptographic Module Standards and Controls . . . 54
6.1.2 Private Key (N out of M) Multi-Person Control . . . 54
6.1.3 Private Key Escrow . . . 54
6.1.4 Private Key Backup . . . 55
6.1.5 Private Key Archival . . . 55
6.1.6 Private Key Transfer Into or From a Cryptographic Module . . . 55
6.1.7 Private Key Storage on Cryptographic Module . . . 55
6.1.8 Method of Activating Private Key . . . 55
6.1.9 Method of Deactivating Private Key . . . 56
6.1.10 Method of Destroying Private Key . . . 56
6.1.11 Cryptographic Module Rating . . . 56
6.2 Activation Data . . . 56
6.2.1 Activation Data Generation and Installation . . . 56
6.2.2 Activation Data Protection . . . 57
6.2.3 Other Aspects of Activation Data . . . 57
6.3 Computer Security Controls . . . 57
6.3.1 Specific Computer Security Technical Requirements . . . 57

6.3.2 Computer Security Rating . . . 57
6.4 Life Cycle Technical Controls . . . 58
6.4.1 System Development Controls . . . 58
6.4.2 Security Management Controls . . . 59
6.4.3 Life Cycle Security Controls . . . 59
6.5 Network Security Controls . . . 60
6.6 Time-stamping . . . 61

7 Compliance Audit and Other Assessments 61
7.1 Frequency or Circumstances of Assessment . . . 62
7.2 Identity/Qualifications of Assessor . . . 62
7.3 Assessor's Relationship to Assessed Entity . . . 62
7.4 Topics Covered by Assessment . . . 62
7.5 Actions Taken as a Result of Deficiency . . . 63
7.6 Communication of Results . . . 63

8 Other Business and Legal Matters 63
8.1 Fees . . . 63
8.1.1 Refund Policy . . . 63
8.2 Financial Responsibility . . . 64
8.2.1 Insurance Coverage . . . 64
8.2.2 Insurance or Warranty Coverage for End-entities . . . 64
8.3 Confidentiality of Business Information . . . 64
8.3.1 Scope of Confidential Information . . . 65
8.3.2 Information Not Within the Scope of Confidential Information . . . 65
8.3.3 Responsibility to Protect Confidential Information . . . 65
8.4 Privacy of Personal Information . . . 66
8.4.1 Privacy Plan . . . 66
8.4.2 Information Treated as Private . . . 67
8.4.3 Information Not Deemed Private . . . 67
8.4.4 Responsibility to Protect Private Information . . . 67
8.4.5 Notice and Consent to Use Private Information . . . 67
8.4.6 Disclosure Pursuant to Judicial or Administrative Process . . . 67
8.4.7 Other Information Disclosure Circumstances . . . 67
8.5 Intellectual Property Rights . . . 67
8.6 Representations and Warranties . . . 68
8.6.1 CA Representations and Warranties . . . 68
8.6.2 Subscriber Representations and Warranties . . . 69
8.6.3 Relying Party Representations and Warranties . . . 70

8.6.4 Representations and Warranties of Other Participants 70
8.7 Disclaimers of Warranties 70
8.8 Limitations of Liability 70
8.9 Indemnities 70
8.9.1 Indemnification by the *Long-Term Preservation Provider* 70
8.9.2 Indemnification by Subscribers 70
8.9.3 Indemnification by Relying Parties 71
8.10 Term and Termination 71
8.10.1 Term 71
8.10.2 Termination 71
8.10.3 Effect of Termination and Survival 71
8.11 Individual Notices and Communications with Participants 71
8.12 Amendments 71
8.12.1 Procedure for Amendment 71
8.12.2 Notification Mechanism and Period 72
8.12.3 Circumstances Under Which OID Must Be Changed 72
8.13 Dispute Resolution Provisions 72
8.14 Governing Law 73
8.15 Compliance with Applicable Law 73
8.16 Miscellaneous Provisions 74
8.16.1 Entire Agreement 74
8.16.2 Assignment 74
8.16.3 Severability 74
8.16.4 Enforcement (Attorneys' Fees and Waiver of Rights) 74
8.16.5 Force Majeure 74
8.17 Other Provisions 74

A REFERENCES **75**

1 Introduction

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

The *Long-Term Preservation Provider* provides its services for its *Client*s with whom it has contractual relationship.

The present *Qualified Long-Term Preservation Practice Statement* describes the framework of the provision of the aforementioned services and includes the detailed procedures and miscellaneous operating rules.

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

The *Long-Term Preservation Provider* asked for its registration as a trust service provider at the National Media and Infocommunications Authority on the 1st of July 2016.

The conformity assessment audit of the trust services was carried out by the independent auditor TÜV Informationstechnik GmbH (hereinafter: TÜViT).

Based on the successful audit the National Media and Infocommunications Authority registered the qualified trust service and published it in the national Trust List on the 20th of December 2016.

1.1 Overview

The aim of the present *Qualified Long-Term Preservation Practice Statement* is to summarize all the information that the *Client*s coming into contact with the *Long-Term Preservation Provider* should know. This aims to foster that its *Client*s and future *Client*s:

- get better acquainted with the details and requirements of the services provided by the *Long-Term Preservation Provider*, and the practical background of the service provision;
- be able to see through the operation of the *Long-Term Preservation Provider*, and thus more easily decide whether the services comply or which type of services meet their individual needs and expectations.

Considering the end user activity related to the services used, besides the present *Qualified Long-Term Preservation Practice Statement* further requirements may be found in the *Qualified Long-Term Preservation Policy* [50], the General Terms and Conditions and the service agreement concluded with the provider, the *Certificate Policies* applied by the *Long-Term Preservation Provider* (see section 1.2.1) and other regulation or document independent from the *Long-Term Preservation Provider* as well.

1.2 Document Name and Identification

Issuer	e-Szignó Certification Authority
Document name	eIDAS conform Qualified Long-Term Preservation Service Preservation Practice Statement

OID	1.3.6.1.4.1.21528.2.1.1.188
Document version	2.11
Date of effect	25/09/2019

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 further numbers were allocated within Microsec's own scope of authority, the interpretation of it is 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 service provided according to the present *Qualified Long-Term Preservation Practice Statement* complies with the requirements of the *Qualified Long-Term Preservation Policy* below:

OID	DENOMINATION	SHORT NAME
1.3.6.1.4.1.21528.2.1.1.187.2.11	qualified long-term preservation policy according to eIDAS Regulation.	MAR

The detailed requirements can be found in " e-Szignó Certification Authority – eIDAS Qualified Long-Term Preservation Service – Long-Term Preservation Policy ver.2.11." [48]

1.2.2 Effect

Subject Scope

The *Qualified Long-Term Preservation Practice Statement* is related to the provision and usage of the services described in section 1.3.1.

Temporal Scope

The present version of the *Qualified Long-Term Preservation Practice Statement* is effective from the 25/09/2019
date of effect, until withdrawal. The effect automatically terminates at the cessation of services or issuance of the newer version of the *Qualified Long-Term Preservation Practice Statement*.

Personal Scope

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

Geographical Scope

The present *Qualified Long-Term Preservation Practice Statement* includes specific requirements for services operating under the Hungarian law in Hungary.

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 in the *Qualified Long-Term Preservation Practice Statement*. At services provided to foreign *Client*s, detailed conditions that differ from the *Qualified Long-Term Preservation Practice Statement* may be regulated in a specific service agreement.

The service provided according to the present *Qualified Long-Term Preservation Practice Statement* is available worldwide. The validity of the documents, the long-term validation material and the related issued statements archived according to the present *Qualified Long-Term Preservation Practice Statement* is independent of the location where they were sent into the archive from, and where they where queried from.

The service provided according to the present *Qualified Long-Term Preservation Practice Statement* can be only used as described in the present document and in the *Long-Term Preservation Policy*.

1.3 PKI Participants

1.3.1 Certification Authorities

Data of the *Long-Term Preservation Provider*

Name:	MICROSEC Micro Software Engineering & Consulting Private Limited Company by Shares
Company registry number:	01-10-047218 Company Registry Court of Budapest
Head office:	Hungary, H-1033 Budapest, Ángel Sanz Briz str. 13. Building C

Telephone number:	(+36-1) 505-4444
Fax number:	(+36-1) 505-4445
Internet address:	`https://www.microsec.hu`, `https://www.e-szigno.hu`

Contact information of the customer service:

The name of the provider unit:	e-Szignó Certification Authority
Customer service:	Hungary, H-1033 Budapest, Ángel Sanz Briz str. 13., Graphisoft Park South Area, Building C
Office hours of the customer service:	on workdays between 8:30-16:30 by prior arrangement
Telephone number of the customer service:	(+36-1) 505-4444
Email address of the customer service:	`info@e-szigno.hu`
Send revocation request to:	`revocation@e-szigno.hu`
Service related information access:	`https://www.e-szigno.hu`
Place for registering complaints:	Microsec ltd. Hungary, H-1033 Budapest, Ángel Sanz Briz str. 13., Graphisoft Park South Area, Building C
Relevant Consumer Protection Inspectorate:	Budapest Capital Authority for Consumer Protection 1052 Budapest, Városház str. 7. 1364 Budapest, Pf. 144.
Relevant Arbitration Board:	Arbitration Board of Budapest 1016 Budapest, Krisztina krt. 99. III. em. 310. Mailing address: 1253 Budapest, Pf.: 10.

Introduction of the *Long-Term Preservation Provider*

Microsec ltd. is an EU qualified trust service provider according to the 910/2014/EU Regulation [1] (hereinafter: eIDAS).

Microsec ltd. (its predecessor) started the provision of its services related to electronic signatures under the effect of Act XXXV. of 2001. [3] (hereinafter: Eat.):

- provides non-qualified electronic signature certification services, time stamping, and placement of signature-creation data on signature creation devices services according to Eat. since May 30, 2002 (registration number: MH 6834 1/2002.);
- provides qualified electronic signature certification services, time stamping, and device services according to Eat. since May 15, 2005;
- provides qualified long term preservation service according to Eat. since February 1, 2007. (reference number of the decision on the registration: HL-3549-2/2007).

On the 1st of July, 2016. the whole system of services related to electronic signatures changed uniformly on a European basis with eIDAS and its complement Act CCXXII of 2015. [6] coming into force.

Microsec provides its non-qualified trust services conformant to eIDAS furthermore started the issuance of eIDAS qualified signing certificates for natural persons from the 1st of July 2016.

Microsec provides the following qualified trust services conformant to eIDAS form the 20th of December 2016:

- qualified certificates for electronic seals
- qualified time stamping
- qualified archiving (preservation of digital signatures).

Microsec provides the following qualified trust servic conformant to eIDAS form the 2nd of January 2019:

- qualified certificates for website authentication.

Quality and Information Security

Microsec highlights the importance of *Client* experience. In order to maintain a high level of services, the *Long-Term Preservation Provider* has been operating a quality control system compliant with the ISO 9001 standard since January 23, 2002. Compliance with the standard has been verified by Lloyd's Register Quality Assurance.

Microsec assigns high priority to the security of the systems it operates, and has therefore been operating an information security management system that is compliant with ISO/IEC 27001 (formerly known as BS 7799) in its main areas of activity since May 19, 2003. Compliance with the standard has been verified by Lloyd's Register Quality Assurance.

The scope of both the quality control system and the information security management system cover the trust services provided by Microsec.

Microsec has two level risk assessment which covers beyond the information technology risks the whole organization including also the business risks. The risk assessment is updated at least yearly. Based on the results of the risk assessment the *Long-Term Preservation Provider*

- sets up new measures to eliminate the vulnerabilities, or/and
- accepts the identified residual risks by stating the reason of the decision.

The *Long-Term Preservation Provider* makes available for all interested parties its Information Security Policy on its web page on the following link:

`https://www.microsec.hu/hu/biztonsagi-garanciak`

Any change to the Information Security Policy is communicated to third parties through this web page.

Due to their confidential nature the *Long-Term Preservation Provider* dosen't disclose its internal Security Rules. The *Long-Term Preservation Provider* informs its subcontractors, contractors and

other interested parties concerned of the security rules applicable to them when concluding the contract.

Changes to the information security policy is communicated to third parties, where applicable. This includes subscribers, relying parties, assessment bodies, supervisory or other regulatory bodies.

Services

The *Long-Term Preservation Provider* provides the following trust services defined by the eIDAS Regulation [1] to the *Subscriber* within the framework of the present *Qualified Long-Term Preservation Practice Statement*:

- Qualified Long Term Preservation Service

The *Long-Term Preservation Provider* provides its services within the framework of the present *Qualified Long-Term Preservation Practice Statement* as a qualified trust service provider.

1.3.2 Subscribers

The *Client*s of the services provided by the *Long-Term Preservation Provider*:

- *Subscriber*
  - signs the service agreement with the *Long-Term Preservation Provider* ,
  - accepts the General Terms and Conditions ,
  - defines the scope of the users,
  - may appoint *Organizational Administrator*s,
  - responsible for the payment of the fees arising from the usage of the service.

1.3.3 Relying Parties

The *Relying Party* is not necessarily in a contractual relationship with the *Long-Term Preservation Provider*. The *Qualified Long-Term Preservation Practice Statement* sections 8.6.3 and 8.9.3 and the other policies mentioned in it contain the recommendations related to its operation.

The party who accepts and uses the statements issued during the long term preservation service.

1.4 Policy Administration

1.4.1 Organization Administering the Document

The data of the organization administering the present *Qualified Long-Term Preservation Practice Statement* can be found in the following table:

Organization name	Microsec e-Szignó Certification Authority
Organization address	Hungary, H-1033 Budapest, Ángel Sanz Briz str. 13. Building C
Telephone number	+36 1 505-4444
Fax number	+36 1 505-4445
Email address	info@e-szigno.hu

1.4.2 Contact Person

Questions related to the present *Qualified Long-Term Preservation Practice Statement* can be directly put to the following person:

Contact person	Process management department leader
Organization name	Microsec ltd.
Organization address	Hungary, H-1033 Budapest, Ángel Sanz Briz str. 13. Building C
Telephone number	+36 1 505-4444
Fax number	+36 1 505-4445
Email 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 *Qualified Long-Term Preservation Practice Statement* is responsible for its compliance with the *Qualified Long-Term Preservation Policy* referenced in it and for the provision of the service in harmony with the regulations contained therein.

The *Qualified 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.

1.4.4 Practice Statement Approval Procedures

Preparing, modifying, acceptance and issuance of a new version of the *Qualified Long-Term Preservation Practice Statement* is implemeted according to unified processes as described in detail in section 8.12.1.

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 security systems.
Trust Service Supervisory Body	"The National Media and Infocommunications Authority, the supervising authority monitoring the *Trust Service*s." *(Act CCXXII. of 2015. [6] 91.§ 1. paragraph)*

Trust Service	"Means an electronic service normally provided for remuneration which consists of: • the creation, verification, and validation of electronic signatures, electronic seals or electronic time stamps, electronic registered delivery services and certificates related to those services, or • the creation, verification and validation of *Website Authentication Certificate*; or • the preservation of electronic signatures, seals or certificates related to those services; " *(eIDAS [1] 3. article 16. point)*
Trust Service Policy	"A set of rules in which a *Trust Service Provider*, relying party or other person requires conditions for the usage of the *Trust Service* for a community of the relying parties and/or a class of applications with common security requirements." *(Act CCXXII. of 2015. [6] 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, a type of e-document. An e-dossier may contain documents, or the related profiles (metadata), signatures, countersignatures and time-stamps.
E-document	An e-document is such an electronic document that contains at least one eIDAS Regulation conformant electronic signature or seal. Depending on the type of the e-document it may contain further electronic documents and the corresponding 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.

Suspension	A temporary pause 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 its own public key – indicated on the certificate.
HSM: Hardware Security Module	A hardware-based secure device 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 considered as compromised, when it can be assumed, that unauthorized person has access to it.
Intermediate Certification Unit	A *Certification Unit* whose *Certificate* was issued by another *Certification Unit*.
Cryptographic Key	A unique digital data string controlling a cryptographic transformation, the knowledge of which is required for encryption, decryption and the creation and verification of digital signatures.
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 belonging to the key-pair owner that the *Subject* shall keep strictly secret. During the issuance of *Certificate*s, the *Certification Authority* uses the private keys of the *Certification Unit* for placing an electronic signature or seal on the *Certificate* to protect it.
Qualified Trust Service	"A *Trust Service* that meets the applicable requirements laid down in the eIDAS Regulation." *(eIDAS [1] article 3. point 17.)*
Qualified Trust Service Provider	"A *Trust Service Provider* who provides one or more *Qualified Trust Service*s and is granted the qualified status by the supervisory body." *(eIDAS [1] article 3. point 20.)*
Public Key	In the public key infrastructure, the element of an asymmetric cryptographic key pair belonging to key-pair owner, which should be made public. The disclosure is typically in the form of a *Certificate*, which links the name of the actor with its public key. The authenticity of the *Certificate*s can be verified with the public key of the *Certification Unit*.
Public Key Infrastructure, PKI	An infrastructure based on asymmetric cryptography, including the cryptographic algorithms, keys, certificates, the related standards and legislation, the underlying institutional system, a variety of providers and devices.
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. [6] 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. [6] 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. [6] 1. § point 44.)*
Certificate Repository	Data repository containing various *Certificate*s. A Certification Authority has a Certificate Repository in which the issued *Certificate*s are disclosed, but the system containing *Certificate*s 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 internal 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 given in seconds maintained by the *Certification Authority*.

1.5.2 Acronyms

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* publishes the *Qualified Long-Term Preservation Policy*, the *Qualified 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* discloses the contractual conditions and policies electronically on its website on the following link:

`https://e-szigno.hu/en/terms-and-informations/`

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

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

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

The *Long-Term Preservation Provider* makes available the *Qualified Long-Term Preservation Policy*, the *Qualified 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* notifies its *Client*s about the change of the General Terms and Conditions.

2.3 Time or Frequency of Publication

2.3.1 Frequency of the Publication of Terms and Conditions

The disclosure of the *Qualified Long-Term Preservation Practice Statement* 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* publishes extraordinary information without delay in accordance with the legal requirements and in the absence thereof when necessary.

3 Electronic Long-Term Preservation Service

The *Long-Term Preservation Provider* provides the electronic long-term preservation service to the *Subscriber* as an eIDAS qualified trust service provider within the framework of the Service Agreement. The service contains the following main service units:

- The *Subscriber* can upload electronically signed e-documents to the archive operated by the *Long-Term Preservation Provider*. At the reception of the e-document the *Long-Term Preservation Provider* checks the electronic signature(s) or seal(s) on the e-document, or on the files included into the e-documents, completes or compiles the long-term validation material, places electronic archive *Time Stamp* on the long-term validation material, and saves the accepted e-document. (see section 3.2).
- The *Long-Term Preservation Provider* securely preserves the accepted e-documents – 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-documents and on the files preserved in the e-documents. The *Long-Term Preservation Provider* ensures the long-term readability of the files in the e-documents 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-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-documents, and that at the time of the acceptance to the archive the electronic signatures or seals on the e-document and on the documents stored in the e-documents were valid (see section: 3.4).
- At the request of the *Subscriber* the *Long-Term Preservation Provider* deletes the e-documents from its archive (see section: 3.6).

In each case the *Long-Term Preservation Provider* also preserves the electronically signed electronic document, and does not provide the archival service without the preservation of the document. This certainly does not exclude that the *Subscriber* make themselves a reasonably secure hash from the electronic document that they do not want to hand over to the *Long-Term Preservation Provider* for some reason and upload that into the archive as a electronic document inserted into an e-document. In this case the *Subscriber* shall undertake the renewal of the preservation, for example in case of the weakening of the hash algorithm.

The *Long-Term Preservation Provider* in case of some specified file formats undertakes the support of interpretability and display of the electronic documents preserved in the archive.

The *Long-Term Preservation Provider* within the framework of this service provides long-term preservation of the validity of electronic signatures and seals, so only accepts e-documents with a valid electronic signature or seal at the time of admission.

The *Long-Term Preservation Provider* only accepts e-documents with an electronic signature or seal, when

- all the electronic signatures and seals are equipped with an *Time Stamp*
- the format of the electronic signatures and seals complies with the requirements of one of the following
  - XAdES ETSI TS 101 903 [22] [23] [24] [25]
  - PAdES PDF/A format (ISO 19005) [40]
  - ASiC (Associated Signature Containers) ETSI TS 102 918 [30]
  - CAdES ETSI EN 319 122 [10], [11]
  - XAdES ETSI EN 319 132 [12], [13]
  - PAdES ETSI EN 319 142 [14], [15]
  - ASiC ETSI EN 319 162 [16], [17]

The *Certificate* of the issuer unit of the *Time Stamp* and the *Certificate* used for the creation of the electronic signature or seal shall be traced back to a root or intermediate provider *Certificate* considered to be trusted by the *Long-Term Preservation Provider*.

The archival period is specified by the service agreement concluded between the *Subscriber* and the the *Long-Term Preservation Provider*. The *Long-Term Preservation Provider* undertakes orders for long retention periods up to 50-100 years.

The *Long-Term Preservation Provider* ensures the long-term readability of the file formats listed in section 4.8 in the manner specified therein, subject to the conditions described there.

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

The service agreement conclusion process:

1. The *Subscriber* contacts with the customer service of the *Long-Term Preservation Provider*.
2. The *Long-Term Preservation Provider* customer service provides information on the features of the electronic long-term preservation service and the steps needed to order the service. The *Subscriber* can get more information from the website of the *Long-Term Preservation Provider* on the usage, security level, terms and conditions, service agreement conditions and the applicable data protection regulations of the electronic long-term preservation service. They are able to do so on the basis of the General Terms and Conditions [51], *Qualified Long-Term Preservation Policy* [48], this *Qualified Long-Term Preservation Practice Statement* [49] and the customer information document made by the *Long-Term Preservation Provider* available on the website of the *Long-Term Preservation Provider*.

3. The *Long-Term Preservation Provider* informs the *Subscriber* before concluding the contract on the availability and content of the *Qualified Long-Term Preservation Practice Statement*.

4. The service agreement can be concluded in writing on paper or electronically, validated by at least an advanced electronic signature or seal with a qualified *Time Stamp*.

5. For using the service the *Subscriber* needs an encryption and an authentication *Certificate* which can be provided by the e-Szignó Certification Authority for them within the framework of a separate service agreement. The *Long-Term Preservation Provider* may require that under what conditions it provides the service in case of encryption and authentication *Certificate*s issued by another provider.

3.2 Uploading the Document

The *Long-Term Preservation Provider* only accepts the e-documents to be archived after the identification of the *Subscriber* within the framework of a secure procedure. The procedure ensures the integrity, confidentiality of the e-documents.

The uploading typically takes place via the Internet by using the interface provided by the *Long-Term Preservation Provider* as follows:

1. The *Subscriber* creates a TLS connection with the *Long-Term Preservation Provider* based on mutual authentication using their client authentication *Certificate*. The *Long-Term Preservation Provider* identifies the *Subscriber* based on the client authentication *Certificate* used for establishing the TLS connection. The *Subscriber* can upload e-documents through the TLS connection to the archive of the *Long-Term Preservation Provider*. The *Subscriber* can provide metadata according to Dublin Core [41] in connection with the electronic documents. The metadata can be inserted into the e-document or provided upon uploading.

2. The *Long-Term Preservation Provider* verifies the compliance of the e-document based on the uploaded e-document type according to the following:

   - in case of e-dossier The *Long-Term Preservation Provider* verifies that the uploaded e-dossier is in the right format, so it complies with the e-document specification published on the website of the *Long-Term Preservation Provider* [42]. The uploaded e-dossier may also contain one or more electronic documents. The e-dossier may contain electronic signatures or seals on the electronic documents, but it can contain a frame signature too, which provides the integrity of every electronic document and every signature, seal and *Time Stamp* on the electronic document in the e-document. If the e-dossier contains a frame signature, then the *Long-Term Preservation Provider* only verifies the frame signatures (the inner signatures and seals are not verified). If the e-dossier does not contain a frame signature, then the *Long-Term Preservation Provider* verifies each electronic signature and seal on the electronic documents included into the e-dossier. If the *Subscriber* needs to ensure the validity of the frame signatures and the inner signatures and seals then they have to submit the e-dossier with and also without the frame signatures.

     Without a frame signature, at least one valid electronic signature or seal shall be placed on every electronic document included into the e-dossier.

The *Long-Term Preservation Provider* rejects those e-dossiers on which an electronic signature or seal verified according to any of the above is invalid or those which contain unsigned electronic documents.

- in case of PAdES formatted e-document the *Long-Term Preservation Provider* verifies that the uploaded PADES formatted e-document format complies with any of the supported formats. The PAdES formatted e-document may contain further electronic documents too. The *Long-Term Preservation Provider* verifies the validity of all of the signatures and seals, but preserves the validity only of the last, outer signature or seal. The *Long-Term Preservation Provider* requires that there is a valid electronic signature or seal and internal *Time Stamp* on the uploaded PDF formatted e-document. The *Long-Term Preservation Provider* does not accept into its archive the e-document without a *Time Stamp* or with an external *Time Stamp*.
- in case of ASiC formatted e-document the *Long-Term Preservation Provider* verifies that the uploaded e-document format complies with any of the supported formats. The uploaded e-document may contain one or more electronic document. The e-document may contain further e-documents too, but the *Long-Term Preservation Provider* does not verify the validity of the electronic signatures, seals in those. The *Long-Term Preservation Provider* verifies every extrenal electronic signature, seal associated with the e-document. Every electronic document stored in the e-document shall have valid electronic signature or seal and *Time Stamp*. The *Long-Term Preservation Provider* rejects the acceptance of the e-document that does not meet any of the conditions.

3. During the verification of the validity of each electronic signature or seal the *Long-Term Preservation Provider* checks that the signature or seal corresponds to the given document. After that it attempts to trace back the given signature or seal to a trusted root *Certificate* (see section: 1.3.1), and it verifies the revocation status of every element of the certificate chain based on OCSP. The acceptance procedure continues only if every electronic signature, seal and *Time Stamp* in the e-document is proved to be valid.

   The *Long-Term Preservation Provider* uses the e-Szignó signature creator and validator application for signature validation. The signer module of the 3rd version of the e-Szignó software is a qualified signature-creation application according to the certification of the MATRIX Ltd. which verifies the signatures according to CWA 14171 [46] and creates a format according to ETSI TS 101 903 [22] [23] [24] [25] .

   The *Long-Term Preservation Provider* only provides the long-term preservation service in respect of those data – namely it accepts such e-documents – on which at least an advanced electronic signature or seal can be found. During the verification of the electronic signature, seal or *Time Stamp Long-Term Preservation Provider* traces back the certificate chain to a trusted root certificate of an accepted Certification (or Time-Stamping) Authority. It may occur that a Certification Authority issues a test *Certificate* that can be verified by its trusted root certificate. The *Long-Term Preservation Provider* cannot distinguish a *Certificate* like that from a real *Certificate* – appropriate for the creation of advanced or qualified electronic signatures or seals –, and it is not responsible for any resulting damage.

   In case the *Long-Term Preservation Provider* does not accept the e-document it preserves for 3 days the information which may help ascertain the cause of rejection. Such information among others are the electronic signature, seal, signing *Certificate* and their certificate chains,

and the time-stamp certificates and their certificate chains and the corresponding incidental metadata included in the e-document.

4. The *Long-Term Preservation Provider* collects the missing revocation status information using an OCSP service. If the OCSP grace period for every provider in the certificate chain is 0, then the revocation information is available – in as short as seconds. If there is a grace period longer than 0, then the *Long-Term Preservation Provider* performs the necessary verifications after the grace period is over according to the related standards and international recommendations. The *Long-Term Preservation Provider* rejects the e-document if it can not perform the verification under 3 days.

   The *Long-Term Preservation Provider* compiles the long-term validation materials corresponding to the electronic signatures and seals in the e-document and places a qualified archive electronic *Time Stamp* on them. It places the resulting long-term validation material in ETSI TS 101 903 [22] [23] [24] [25] format, namely as an archive signature into the e-document.

5. The *Long-Term Preservation Provider* preserves the unencrypted e-document to be archived encrypted in an e-dossier with a provider key using a cryptographic algorithm and key parameter deemed secure in the long run. The unencrypted copies of the accepted e-document are destroyed by the *Long-Term Preservation Provider* by using such a procedure which ensures that the e-document can not be restored (or only with unrealistically high financial expenditure).

6. The *Long-Term Preservation Provider* sends a confirmation to the *Subscriber* that it successfully accepted the e-document as soon as possible, but at most within 3 days from the upload. If the process is interrupted somewhere the *Long-Term Preservation Provider* also notifies the *Subscriber*. In this case the *Subscriber* receives an error message that informs him that the *Long-Term Preservation Provider* could not accept the electronic document (for example because it was not able to build the certificate chain). The *Long-Term Preservation Provider* sends the confirmations and error messages in an electronic mail or through a channel previously agreed on with the *Subscriber*.

   The confirmation contains the hash of the e-document submitted to the archive and whether the archive accepted the electronic document. Besides that in case of a successful reception it includes:

   - the hash of the e-document accepted into the archive – already containing archival electronic signatures, seals –, which serves as a unique identifier hereinafter,
   - the identifier of the *Qualified Long-Term Preservation Policy*,
   - the clear identification that the service is an eIDAS compliant long-term preservation service subject to the Electronic Administration Act,
   - the time period of the archival,
   - whether the *Long-Term Preservation Provider* undertakes the support of the readability and interpretability of each e-document in the electronic document.

   The confirmation may contain other information as well. The successful acceptance confirmation is authenticated by a qualified electronic seal and a qualified *Time Stamp*. The *Subscriber* shall make sure that the confirmation indeed corresponds to the uploaded

e-document (namely whether it contains the hash of the uploaded e-document), and the electronic seal on the confirmation is valid. The confirmation is an electronically sealed document, so if the *Subscriber* needs to preserve the authenticity of the confirmation in the long run then he shall act according to the normatives related to the validity preservation of electronically sealed documents.

If the *Subscriber* does not receive a positive confirmation within the given deadline, that shall be considered that the *Long-Term Preservation Provider* did not accept the e-document. The *Long-Term Preservation Provider* is solely responsible for the preservation of the e-document and for ensuring the long-term credibility of the included electronic signatures and seals in case of having sent a positive confirmation.

The *Long-Term Preservation Provider* provides multiple possibilities for uploading via internet, for example

- web interface for uploading at the `https://archivmail.e-szigno.hu/arupload` URL;
- the e-Szignó Archive client uploader software;
- archive uploader functionality built into the e-Szigno client at the `https://archivmail.e-szigno.hu/submit` URL;
- automatic archiver function integrated into other services.

The *Long-Term Preservation Provider* may provide uploading possibility to the *Subscriber* through other secure channels as well. In this case, the confidentiality of the uploaded e-documents is not ensured by the SSL connection, but by these channels – such as leased lines. Apart from this, the process will still take place in accordance with the above principles.

In individual cases the *Subscriber* can send documents to the the *Long-Term Preservation Provider* not only through the network, but on a data medium for example on an optical disk. The contents of the data medium received this way are processed according to the inner regulations of the *Long-Term Preservation Provider* also according to the aforementioned principles. The *Long-Term Preservation Provider* does not preserve the received data medium, it returns the data medium as requested by the *Subscriber* or destroys it in a secure manner after processing the data obtained from the data medium.

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

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

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

The download is typically done via internet by using the interface provided by the the *Long-Term Preservation Provider* according to the following:

1. The *Subscriber* establishes a mutual identification based SSL connection with the server of the *Long-Term Preservation Provider* using his client authentication *Certificate*. The *Long-Term Preservation Provider* identifies the *Subscriber* based on the client authentication *Certificate* used for establishing the SSL connection.

2. The *Subscriber* selects the e-document he wishes to access. For choosing the right e-document he has opportunity to search for the e-documents on the web interface by the Dublin Core [41] compliant metadata corresponding to the e-document. The selection is done according to the identifier based on the hash clearly identifying the e-document.

3. The *Long-Term Preservation Provider* determines whether the *Subscriber* is entitled to access the selected electronic document.

4. In case of appropriate access rights the *Long-Term Preservation Provider* searches for the e-document preserved in the encrypted e-dossier in the archive based on the specified hash based identifier, and sends it to the *Subscriber* depending on the e-document type as follows:

   - in case of an e-dossier encodes it with the public key corresponding to the *Subscriber* encryption *Certificate*, and sends through protected SSL connection the thus re-encrypted e-dossier to the *Subscriber*.
   - in case of a PAdES formatted e-document it sends the decoded e-document unencrypted trough a protected SSl connection to the *Subscriber*.
   - in case of an ASiC formatted e-document it sends the decoded e-document unencrypted trough a protected SSl connection to the *Subscriber*.

   The *Long-Term Preservation Provider* refuses the download of the electronic document if it received a deletion request previously taken effect in relation to the e-document.

5. In case of the e-dossier based preservation the *Subscriber* possesses the private key corresponding to his encryption *Certificate* applied for using the long-term preservation service. He decodes the e-dossier with this key so gaining access to the long-term validation material and the electronic documents stored in the e-dossier.

In case previously agreed on with the *Long-Term Preservation Provider* the *Subscriber* may receive the e-documents and the long-term validation material preserved in the archive of the *Long-Term Preservation Provider* on a data medium, for example on an optical disk. The access also takes place by the aforementioned principles, but this time the *Subscriber* (or his representative authorized in writing) identifies himself not based on his authentication *Certificate*, but with a document appropriate for personal identification.

The handover of the data medium may happen during the face to face meeting with the employee of the *Long-Term Preservation Provider* having the proper security role or based on the formerly received written request of the *Subscriber* by using a trusted third party.

The uploaded e-documents are the property of the *Subscriber* (see section: 1.3.2), so the *Subscriber* also plays the role of data administrator. If a third party has access to the e-document, then he acts on behalf of the *Subscriber*.

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-document. The acknowledgement consists of the following:

1. The statement that the advanced or qualified electronic signatures, seals, *Time Stamp*s on the given e-documents and the corresponding *Certificate*s were valid at the time of the time stamping and the validation after their upload.
2. The hash of the e-document, the name and identifier of the *Subscriber*.
3. The statement that the given e-document has the given hash, so it is identical to the e-document with the same hash presented by the *Subscriber*, or created with the help of the *Long-Term Preservation Provider*.
4. The time of the e-document acceptance into the archive.

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-document is not needed for the issuance of the acknowledgement, it is issued based on the hash of the unencrypted e-document preserved in cleartext. No information can be obtained from the hash value in relation to the content of the preserved electronic document. The applied solution ensures that the officials responsible for issuing the archive acknowledgement do not get to know the contents of the unencrypted electronic document 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-document. Then, provided that the archive of the *Long-Term Preservation Provider* contains an e-document with the same hash as the presented unencrypted e-document, an official of the *Long-Term Preservation Provider* issues the acknowledgement in relation to the presented e-document.

The *Subscriber* may 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 which is based on qualified certificate.

The issuance of the acknowledgement may be requested by the authorized representative of the *Subscriber* if he presented the authorization of the *Subscriber* in a document containing also his signature beforehand.

For requesting the acknowledgement the *Subscriber* (or his representative) shall provide the hash of the e-document related to which he requests the acknowledgement. This information can be acquired from the searching interface described in section 3.3. The acknowledgement is issued by the *Long-Term Preservation Provider* to the *Subscriber* who the given e-document corresponds to according to the IT system of the *Long-Term Preservation Provider*. The *Long-Term Preservation Provider* only issues the acknowledgement to a third party in case of presenting the aforementioned authorization.

The issuance of the acknowledgement is performed in an e-dossier format, in the "format specified in the technical specification developed by the Ministry for Information Technology and Communications concerning the electronic signature formats applicable in public administration". At the request of the *Subscriber* the acknowledgement may be issued in another format. The *Long-Term Preservation Provider* uses a signing application which has a certificate issued by an independent certification organization for the issuance of the acknowledgement.

3.5 Document Display

At a date pre-agreed with the the *Long-Term Preservation Provider* the *Subscriber*s may view their e-documents stored in the archive of the *Long-Term Preservation Provider* at the customer service of the *Long-Term Preservation Provider* using the software and hardware devices of the *Long-Term Preservation Provider*.

For viewing the e-dossiers preserved in the archive the *Subscriber* shall bring with themselves their private key corresponding to their encryption *Certificate* necessary for using the long-term preservation service and the intelligent card that stores the key.

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

The *Long-Term Preservation Provider* deletes the e-documents and all the corresponding long-term validation material preserved in the archive at the request of the *Subscriber*. The deletion means the physical deletion of the preserved e-document 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 is performed on the whole system of the *Long-Term Preservation Provider*, and during the deletion it destroys every preserved copy of the e-document.

The deletion request shall be submitted to the customer service of the *Long-Term Preservation Provider* in writing signed on paper or by an electronically signed application. The *Long-Term Preservation Provider* assesses and performs the deletion within one working day. The deletion request may be submitted in a way that the *Long-Term Preservation Provider* shall not perform the deletion immediately, but on a specified date.

The *Long-Term Preservation Provider* sends a confirmation to the *Subscriber* about the deletion.

3.7 Termination of the Service Agreement

The *Long-Term Preservation Provider* makes available the e-documents and the long-term validation material corresponding to the *Subscriber* for download to the *Subscriber* or to another entitled person for 60 days after the termination of the service agreement.

After the deadline the *Long-Term Preservation Provider* deletes the e-documents and the long-term validation material corresponding to the *Subscriber*.

Even in case of the deletion occurring at the termination of contract the *Long-Term Preservation Provider* provides the deletion as described in section 3.6 so the the deleted e-documents can not be restored.

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-documents 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-documents can not be read even by its employees. The *Long-Term Preservation Provider* only submits the e-documents 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-documents 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-documents at two physical locations far from each other.

The *Long-Term Preservation Provider* destroys the archived e-documents – 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-documents 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-documents in encrypted e-dossiers. The *Long-Term Preservation Provider* encrypts e-documents 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-document with a secure algorithm based on its own internal regulations. It only restores the unencrypted e-documents for the fulfilment of the legal requirements relating to the provision of the long term preservation service, namely in the cases described in sections 3.3, 4.4 and 4.5.

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 confirmation signing keys, the keys required to encrypt/decrypt archived data and the infrastructure and system control keys are generated in a cryptographic hardware device.

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* is bound to place a time stamp issued by a qualified provider or have a time stamp placed on the long-term validation material in the following cases:

- if the National Media and Infocommunications Authority makes such a decision;
- following the obligatory submission of the notification to the National Media and Infocommunications Authority about the initiation of the dissolution proceeding or the imposition of liquidation against the *Long-Term Preservation Provider*.

4.5 Re-Encrypting the Archive

The *Long-Term Preservation Provider* stores the archived e-documents encrypted in an e-dossier in the archive. It ensures that the archived e-documents are encrypted with an encryption algorithm that is secure at all times.

The *Long-Term Preservation Provider* ensures that the e-documents are 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 *Qualified Long-Term Preservation Practice Statement* or the contract concluded with the *Subscriber* requires so.

After the *Long-Term Preservation Provider* re-encrypted the archived e-documents in a secure way, it destroys the former copies encrypted in a manner deemed not sufficiently secure.

4.6 Continuous Monitoring of Technology

The *Long-Term Preservation Provider* continuously monitors 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 notifies the National Media and Infocommunications Authority and requests 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* publishes on its website which *Certification Authorities* and *Time-Stamping Service Provider*s it accepts *Certificate*s and *Time Stamp*s of. The list of the accepted providers is available at the following URL:

`https://e-szigno.hu/hitelesites-szolgaltatas/archivalas-szolgaltatas/elfogadott-szolgaltatok.html`

The *Long-Term Preservation Provider* has documented procedures, according to which it accepts or declines the *Certificate*s and *Time Stamp*s of the particular *Certification Authorities* and *Time-Stamping Service Provider*s. These procedures specify among others what measures the *Long-Term Preservation Provider* executes in case of a private key compromise of a previously accepted *Certification Authority* or *Time-Stamping Service Provider*.

4.8 The Maintenance of the Readability and Interpretability of the Electronic Documents

The *Long-Term Preservation Provider* ensures, that during the archival period certain file format displayer necessary software and hardware devices are made available continuously. The *Long-Term Preservation Provider* for this purpose developed regulated and audited internal processes. The *Long-Term Preservation Provider*'s internal regulations cover at all times the availability provision of the hardware and software environment used to display files, the regular review of the environment and keeping it up to date.

The *Long-Term Preservation Provider* ensures the readability of the original signed bit sequence, so the *Long-Term Preservation Provider* does not transform the signed file to another format.

The *Long-Term Preservation Provider* ensures the technical readability of the file and is not responsible for the meaningful content of the file (for example a technically correct PDF file which contains an empty page due to a faulty scanning).

The *Long-Term Preservation Provider* accepts e-documents into its archive containing files with such a format, in respect of which it does not ensure readability and interpretability. The *Long-Term Preservation Provider* undertakes the preservation of documents, therefore the document legibility maintenance until the end of the validity period of the service contract agreement. At the termination of the service the *Long-Term Preservation Provider* hands over the service to another service provider as described in section 5.7. Then, in addition to the archived e-documents the

Long-Term Preservation Provider hands over the knowledge to ensure the long-term view required for the software and hardware devices necessary to display the above supported file formats too.

The *Long-Term Preservation Provider* ensures legibility and interpretability with regard to the following file formats:

- ISO/IEC 646:1991 (7 bit character sets to ensure information exchange, ASCII) [32],
- ISO 8859-1:1998 (Latin-1, 8 bit graphic character set) [33],
- ISO 8859-2:1999 (Latin-2) [34], for the Hungarian reference set, the MSZ 7795-3:1992 [37] derogation under ASCII and ASCII/PC codes,
- Microsoft Rich Text Format 1.7. [43],
- Portable Document Format (PDF) 1.3. [47],
- PDF/A format (ISO 19005) [40],
- every version of the Microsec e-dossier format [42],
- XAdES ETSI TS 101 903 v1.2.2 [22], v1.3.2 [23], v1.4.1 [24] and v1.4.2 [25], format XAdES signatures (if an XML file contains XAdES signature, the *Long-Term Preservation Provider* ensures the interpretability of the signature),
- XAdES Baseline Profile ETSI TS 103 171 v2.1.1 [31],
- CAdES ETSI TS 101 733 v1.8.1 [20],
- CAdES Baseline Profile ETSI TS 101 733 v2.1.1 [21],
- ASiC ETSI TS 102 918 v1.3.1 [30],
- PAdES ETSI TS 102 778 -1 v1.1.1 [26], -2 v1.2.1 [27], -3 v1.1.2 [28], -4 v1.1.2 [29],
- ETSI EN 319 122-1 [10] format CAdES signatures
- ETSI EN 319 122-2 [11] format CAdES signatures
- ETSI EN 319 132-1 [12] format XAdES signatures
- ETSI EN 319 132-2 [13] format XAdES signatures
- ETSI EN 319 142-1 [14] format PAdES signatures
- ETSI EN 319 142-2 [15] format PAdES signatures
- ETSI EN 319 162-1 [16] format ASiC signatures
- ETSI EN 319 162-2 [17] format ASiC signatures
- IETF RFC 2822 (Internet Message Format) [39],
- IETF RFC 2045 (Multipurpose Internet Mail Extensions, MIME) [38],

- XML formats used in the electronic company procedures [1],
- Such XML formats, for which the *Subscriber* submits to the *Long-Term Preservation Provider* the XSD schema definition and XSLT stylesheet used for the given XML format display in advance, and makes a statement about the manner in which the XML with the specific namespaces shall be displayed.

If a *Subscriber* requires the *Long-Term Preservation Provider* for a format not included in the above list to ensure the given format readability and interpretability, and indicates this demand to the *Long-Term Preservation Provider*, the *Long-Term Preservation Provider* shall examine the format according to the relevant procedural rules if this is feasible and under what conditions. If the *Long-Term Preservation Provider* includes the format requested by the *Subscriber* to the formats supported in respect of readability and legibility, that means the modification of the present *Qualified Long-Term Preservation Practice Statement*.

The *Long-Term Preservation Provider* only supports versions of the aforementioned formats cited in the above specifications, the readability and display of files with different (or later) versions is not guaranteed. The *Long-Term Preservation Provider* undertakes the readability and interpretability of the formats, so if an application creates or displays files incorrectly, or differently from the above specifications, the *Long-Term Preservation Provider* is not responsible for any resulting damages.

The *Long-Term Preservation Provider* undertakes the display of the formats only to the extend described in the above cited specifications. If a format can contain embedded objects, the *Long-Term Preservation Provider* does not undertake the provision of the display of these embedded objects. Since the e-mail format (RFC 2822 [39]) does not specify the character coding of the e-mail, the *Long-Term Preservation Provider* only undertakes the display of such e-mails that has one of the aforementioned character coding. In case of "attachments" encoded according to the MIME specification (RFC 2045 [38]) the *Long-Term Preservation Provider* only undertakes the display of only those attachments which has one of the aforementioned formats.

The *Long-Term Preservation Provider* undertakes the readability and display of files according to the definition of the files described in section 1.5. This means that the *Long-Term Preservation Provider* only ensures the interpretability and display of a file (in an aforementioned format) if it is inserted into an e-document. The *Long-Term Preservation Provider* does not undertake the readability of files encoded with other (further) transformations, particularly the encrypted files. Besides the files the *Long-Term Preservation Provider* ensures the readability and display of the e-dossiers too. This extends to the verifiability of signatures, seals and *Time Stamp*s, and the extraction of files placed in e-dossiers.

The determination of the file formats is performed based on the "mimeType" value in the e-document, without which the *Long-Term Preservation Provider* considers the given electronic document format unrecognized and does not ensures the interpretability of the electronic document. The *Long-Term Preservation Provider* supports the usage of the "mimeType" values in the following list:

- text/txt
- application/xml

[1] The format which is available at the `http://www.e-cegjegyzek.hu/e-cegeljaras/cegnyomtatvany.htm` url.

- text/xml
- text/plain
- application/pdf
- application/eszigno3
- application/vnd.eszigno3+xml
- application/octet-stream(dosszie)
- application/octet-stream(es3)
- application/nldossier2
- application/octet-stream(xml)
- application/octet-stream(pdf)

The *Long-Term Preservation Provider* draws *Client*s' attention to that if they enable the usage of active elements (particularly in case of some non-character formats) in some formats, then it may happen that the file formatted such way might display differently at different times even according to the aforementioned specifications. The *Long-Term Preservation Provider* recommends its *Client*s that if it is possible, they should not place a signature on files containing active elements. The *Long-Term Preservation Provider* displays the active elements according to the aforementioned specifications, but it does not undertake responsibility for damages resulting from the various displayability – but compliant with the aforementioned specifications – of files.

The *Long-Term Preservation Provider* doesn't perform any checks on whether the uploaded e-document contain any active code, which may result in a change in display of the document.

At the time of the reception of an e-dossier the *Long-Term Preservation Provider* checks with an automation that whether the files in the e-dossier have any of the supported formats. For those, which does not have a supported format, it refuses the maintenance of readability. The verification described in section 3.2. contains that the format of which file is unknown – the readability of such files is not guaranteed by the *Long-Term Preservation Provider*. The check carried out at the reception is not complete, the *Long-Term Preservation Provider* assumes no responsibility that the file format not considered unknown have supported format and correct syntax.

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-documents and validity chains;
- search of archived e-documents;
- receiving deletion requests;

- receiving timed deletion requests (with the help of which the *Subscriber* can specify how long a given e-document 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 e-document upload service .

The customer service of the *Long-Term Preservation Provider* accepts applications for issuance of a verification every working day during office hours; the issuance of verifications takes place under 3 days.

The office hours of the customer service of the *Long-Term Preservation Provider* is in section 1.3.1.

5 Facility, Management, and Operational Controls

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

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

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

5.1 Physical Controls

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

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

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

The provided protection is proportional to the identified threats of the risk analysis that the *Long-Term Preservation Provider* has performed.

In order to provide adequate security:

- The *Long-Term Preservation Provider* implements the strongly protected services in its protected computer room. This computer room has been designed and constructed specifically for this purpose, by its design uniform enforcement of various aspects of protection (the placement and structure of the site, physical access (access control and supervision), power supply, air conditioning, protection against water leakage and flooding, fire prevention and protection, media storage etc.) took place.
- The *Long-Term Preservation Provider* implements every critical service and every necessary tool in a separate security zone. All the devices necessary for this are placed in a protected computer room – forming part of the security zone.

5.1.1 Site Location and Construction

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

5.1.2 Physical Access

The *Long-Term Preservation Provider* protects 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 ensures that:

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

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

In the presence of unauthorized persons:

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

When leaving the computer room the administrator shall verify that:

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

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

5.1.3 Power and Air Conditioning

The *Long-Term Preservation Provider* applies an uninterruptible power supply unit in the *Data Centre* that:

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

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

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

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

5.1.4 Water Exposures

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

5.1.5 Fire Prevention and Protection

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

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

5.1.6 Media Storage

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

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

5.1.7 Waste Disposal

The *Long-Term Preservation Provider* ensures the environmental standards compliant disposal of the superfluous assets, and media.

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

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

5.1.8 Off-Site Backup

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

Based on the randomly selected backup data a restoration test is made at least yearly. The main circumstances and results of the restoration test is recorded in an audit report.

5.2 Procedural Controls

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

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

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

The *Long-Term Preservation Provider* defines the following trusted roles, with the following responsibilities:

Manager with overall responsibility for the IT system of the *Long-Term Preservation Provider*: The individual responsible for the IT system.

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

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

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

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

Long term preservation officer: It is possible to decrypt an electronic document with the co-operation of two long term preservation officer. The long term preservation officers are responsible for the secure management of the decrypted electronic document, 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* formally appoints 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 are kept of the trusted roles and in case of any change, the National Media and Infocommunications Authority is notified without delay.

5.2.2 Number of Persons Required per Task

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

- the generation of the *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 electronic document stored in the archive. The long term preservation officers are responsible for the secure management of the decrypted electronic document, 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* have unique identification data, enabling secure identification and authentication of the users.

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

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

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

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

5.2.4 Roles Requiring Separation of Duties

Employees of the *Long-Term Preservation Provider* can hold multiple trusted roles at the same time, but the *Long-Term Preservation Provider* ensures that:

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

In addition to the aforementioned, the *Long-Term Preservation Provider* seeks the complete separation of trusted roles.

5.3 Personnel Controls

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

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

5.3.1 Qualifications, Experience, and Clearance Requirements

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

Trusted roles can be held at the *Long-Term Preservation Provider* only by persons, who have no external influence and possess the necessary expertise validated by the *Long-Term Preservation Provider*. All personnel in trusted roles shall be free from conflict of interest that might prejudice the impartiality of the the *Long-Term Preservation Provider*'s operations.

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* only hires employees for trusted or leading roles, who

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

At the time of the appointment, shall the leading role holder *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* verifies the authenticity of the relevant information given in the applicant's CV during the hiring process, like previous employment, professional references, most relevant educational qualifications.

5.3.3 Training Requirements

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

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

The training material is updated at least in every 12 months and contains the new threats and actual security practices.

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

5.3.5 Job Rotation Frequency and Sequence

The *Long-Term Preservation Provider* does not apply mandatory rotation between individual work schedules.

5.3.6 Sanctions for Unauthorized Actions

The *Long-Term Preservation Provider* regulates the prosecution possibilities of the employees in an employment contract in case of failures, errors, accidental or intentional damage. If the employee – due to negligence or intentionally – violates their obligations, sanctions could be taken against him by the *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. Upon appointment every trusted role employee as part of the employment documents:

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

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

5.3.7 Independent Contractor Requirements

The *Long-Term Preservation Provider* only assigns trusted roles to its employees.

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

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

5.3.8 Documentation Supplied to Personnel

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

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

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

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

5.4 Audit Logging Procedures

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

5.4.1 Types of Events Recorded

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

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

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

- INTERNAL CLOCK
  - the synchronization of the internal clock to the UTC time, including the operational re-calibrations too;
  - the loss of synchronization;
- 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:

- DATA FLOWS:
  - any kind of security-critical data manually entered into the system;
  - security-relevant data, messages received by the system;

- 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 *Qualified 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 independent system auditors of the *Long-Term Preservation Provider* evaluates the generated log files every working day.

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

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

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

5.4.3 Retention Period for Audit Log

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

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

5.4.4 Protection of Audit Log

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

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

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

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

5.4.5 Audit Log Backup Procedures

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

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

The exact process of backups shall be defined in the backup regulations of the *Long-Term Preservation Provider*.

5.4.6 Audit Collection System (Internal vs External)

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

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

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

5.4.7 Notification to Event-causing Subject

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

5.4.8 Vulnerability Assessments

Besides processing daily the log entries, the experts of the *Long-Term Preservation Provider* monitor the publicly available information about possible vulnerabilities and the new software patches. They analise the information, classify the vulnerability and if necessary inform the management about the result and propose an action plan to increase the security of the system.

Every major event of significant deficiencies detected or in case of external threat within a period of 48 hours after its discovery, but at least once a year the experts of the *Long-Term Preservation Provider* perform a comprehensive vulnerability analysis using a mapping of potential internal and external threats that may result in unauthorized access.

Based on the results of the analysis the *Long-Term Preservation Provider*

- creates and implements a plan to mitigate the vulnerability; or
- documents the factual basis for the decision that the residual risk is accepted and the vulnerability does not require remediation.

At first the new software versions and software patches are installed on the test system of the *Long-Term Preservation Provider* and only after the successfully finished test are installed on the live system which is used to provide the services.

The new software patches are not installed on the live system if they introduce additional vulnerabilities or instabilities that outweigh the benefits of applying them. The reasons for not applying any security patches are documented.

5.5 Records Archival

5.5.1 Types of Records Archived

The *Long-Term Preservation Provider* is prepared to the proper secure long-term archiving of electronic and paper documents.

The *Long-Term Preservation Provider* archives 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 *Qualified Long-Term Preservation Practice Statements*;
- 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* preserves the archived data for the time periods below:

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

5.5.3 Protection of Archive

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

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

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

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

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

5.5.4 Archive Backup Procedures

The *Long-Term Preservation Provider* makes an authentic electronic copy of the original paper documents in accordance with the relevant legislation. Electronic copies are stored according to the same rules as other protected electronic documents.

After archiving the authentic electronic copies the *Long-Term Preservation Provider* may destroy the original paper documents.

5.5.5 Requirements for Time-stamping of Records

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

The time value is given by the internal clock of the *Long-Term Preservation Provider* which is synchronized to two separate Stratum-1 UTC time sources:

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

In order to provide accuracy the *Long-Term Preservation Provider* synchronizes its own internal time with the above Stratum-1 sources within a 0.1 second accuracy, and it performs this synchronization at least 4 times a day.

This way the *Long-Term Preservation Provider* guarantees that the deviation of the time indicated in the time marks from the UTC time base is at most 1 second.

The *Long-Term Preservation Provider* provides the daily log files with a qualified *Time Stamp*.

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

5.5.6 Archive Collection System (Internal or External)

The log entries are generated in the *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.

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

5.5.7 Procedures to Obtain and Verify Archive Information

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

The archived files are protected from unauthorized access.

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

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

5.6 Compromise and Disaster Recovery

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

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

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

5.6.1 Incident and Compromise Handling Procedures

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

The *Long-Term Preservation Provider* established and maintains a fully functional backup 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* annually tests the changeover to a backup system and reviews its business continuity plans.

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

The *Long-Term Preservation Provider* constructed its IT system providing the qualified services in such a way that in case of the dropout of any one device, it is able to continue the provision of its qualified services.

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

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

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

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

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

Once the problem resolved and the integrity restored, the *Long-Term Preservation Provider* restarts 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, are defined in the *Long-Term Preservation Provider*'s business continuity plan.

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

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

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

At the same time with the notification about the service shutdown, the *Long-Term Preservation Provider* shuts down the following services:

- new electronic document acceptance into the archive

The *Long-Term Preservation Provider* terminates the service agreements at least 30 days before the planned termination and calls the *Subscriber*s to download their electronic documents stored in the archive.
The *Long-Term Preservation Provider* at least 20 days before the planned termination shuts down the following services:

- issuance of the statements on the stored electronic documents

At the same time of the termination, the *Long-Term Preservation Provider* shuts down the following services:

- information provision,
- the download of the electronic documents stored in the archive

Before a planned discontinuation, the *Long-Term Preservation Provider* engages in negotiations about the taking over of its services with other Certification Authorities whose rating is identical to its own. Under section 8.3 , it will hand over its records, including confidential user data, to such a Certification Authority or to the National Media and Infocommunications Authority come what may, along with its other services, depending on the outcome of the negotiations or terminates without handover.
The *Long-Term Preservation Provider* informs the National Media and Infocommunications Authority about the final outcome of the negotiations. The *Long-Term Preservation Provider* is to inform its *Client*s by electronic mail, and *Relying Parties* by means of a publication on its website.
Upon terminating a service, the *Long-Term Preservation Provider* produces a full scope backup of its data contained in its IT system, affixing a qualified *Time Stamp* to it.
In order to make the handing over of its data to another service provider possible, the *Long-Term Preservation Provider* places data on media and in a format which the new service provider can receive or provides the new service provider with the opportunity to process data in the original format, and hands over the appropriate tools, documentation and know-how for this.
After the termination of the service the *Long-Term Preservation Provider* hand over the archived files, signatures, seals or certification chains to the *Subscriber* in a format agreed upon with the *Subscriber* and deletes them from its archive in an unrecoverable way described in section 3.6.

6 Technical Security Controls

The *Long-Term Preservation Provider* uses systems consisting of reliable, and safety technically assessed equipment for the provision of its services. The *Long-Term Preservation Provider* manages the cryptographic provider keys during their whole life-cycle within a *Hardware Security Module* that has appropriate Certification.
Both the *Long-Term Preservation Provider* and the system supplier and execution contractors have significant experience with certification service deployment and they use internationally recognized technology.
The *Long-Term Preservation Provider* continuously monitors the capacity needs, and with setting the trends it estimates the expected future capacity demands. It can arrange if needed an extension of the limited capacity, thereby providing the necessary processing and continuous availability of storage capacities.

6.1 Private Key Protection and Cryptographic Module Engineering Controls

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

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 [36], or
- the requirements of FIPS 140-2 [44] 3, or the requirements of a higher level, or
- the requirements of CEN 14167-2 [45] 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 [35] 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 *Long-Term Preservation Provider* provider keys are only stored in encrypted forms outside of the *Hardware Security Module*. For coding only those algorithms and key parameters are used by the current order of the National Media and Infocommunications Authority that was issued according to the year 2015. Act CCXXII [6] 92. § (1) b) that are expected to be able to withstand the cryptographic attacks during the entire lifetime of the keys.

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

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

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

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

6.1.3 Private Key Escrow

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

6.1.4 Private Key Backup

The *Long-Term Preservation Provider* makes security copies of its provider private keys, before putting the private key into service as described in section 6.1.1. in a protected environment, in the simultaneous presence of at least two people holding trusted roles, with the exclusion of other people. During the backup, the private key leaves the module in an encrypted form, and this encrypted key can be loaded into another module. Both the backup and the restore can only be performed by protection mechanisms described in section 6.1.2..

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

The same strict security standards are 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* does 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* is created in a *Hardware Security Module* that meets the requirements.

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

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

The export and loading of the provider private keys is performed according to section 6.1.2.

6.1.7 Private Key Storage on Cryptographic Module

The *Long-Term Preservation Provider* keeps its private keys used for service provision in *Hardware Security Module*s according to section 6.1.1.

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

6.1.8 Method of Activating Private Key

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

6.1.9 Method of Deactivating Private Key

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

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

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

6.1.10 Method of Destroying Private Key

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

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

The *Long-Term Preservation Provider* destroys each backup copy of the private key in a documented way in such a way that its restoration and usage becomes impossible.

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* is stored in a cryptographic module that

- has a certification according to ISO/IEC 19790 [36], or
- has a certification according to FIPS 140-2 Level 3 [44], or
- has a Common Criteria based certificate attesting compliance with the requirements of the CEN 14167-2 [45] 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 are protected in accordance with the procedures, requirements defined in the used *Hardware Security Module* user guide and the certification documents.

In case of password based activation data usage, the passwords are sufficiently complex in order to ensure the required level of protection.

6.2.2 Activation Data Protection

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

6.2.3 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 its IT system of the *Long-Term Preservation Provider* ensures the compliance with the following requirements:

- the user identity is verified with two-factor authentication controls by using VPN certificates stored on the card before granting access to the system or the application;
- roles are assigned to users and it ensures that all users only have permissions appropriate for his or her roles;
- a log entry is created for every transaction, and the log entries are archived;
- for the security-critical processes it is ensured that the internal network domains of the *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

Microsec highlights the importance of *Client* experience. In order to maintain a high level of services, the *Long-Term Preservation Provider* has been operating a quality control system compliant with the ISO 9001 standard since January 23, 2002. Compliance with the standard has been verified by Lloyd's Register Quality Assurance.

Microsec assigns high priority to the security of the systems it operates, and has therefore been operating an information security management system that is compliant with ISO/IEC 27001 (formerly known as BS 7799) in its main areas of activity since May 19, 2003. Compliance with the standard has been verified by Lloyd's Register Quality Assurance.

The scope of both the quality control system and the information security management system cover the trust services provided by Microsec.

Microsec has two level risk assessment which covers beyond the information technology risks the whole organization including also the business risks. The risk assessment is updated at least yearly. Based on the results of the risk assessment the *Long-Term Preservation Provider*

- sets up new measures to eliminate the vulnerabilities, or/and

- accepts the identified residual risks by stating the reason of the decision.

6.4 Life Cycle Technical Controls

6.4.1 System Development Controls

The *Long-Term Preservation Provider* only uses applications and devices in its production IT system that are:

- commercial boxed software, designed and developed by a documented design methodology, or;
- custom hardware and software solutions developed by the *Long-Term Preservation Provider* itself during which design structured development methods and controlled development environment were used, 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.

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

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

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

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

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

The *Long-Term Preservation Provider* employs reliable, adequately trained staff over the course of installing software and hardware.

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

The *Long-Term Preservation Provider* has a version control system where every change of the IT system is documented.

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

6.4.2 Security Management Controls

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

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

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

The *Long-Term Preservation Provider* deletes the provider keys from the *Hardware Security Module*s permanently or temporarily withdrawn from use.

The *Long-Term Preservation Provider* stores the unused *Hardware Security Module*s at a physically protected location.

6.4.3 Life Cycle Security Controls

The *Long-Term Preservation Provider* ensures the protection of the used *Hardware Security Module*s during their whole life cycle.

During the operation of the IT services, devices and operating systems used for the provision of the services the *Long-Term Preservation Provider* taking into account the security aspects of the equipment life cycle.

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

6.5 Network Security Controls

The *Long-Term Preservation Provider* keeps its IT system configuration under strict control, and it documents every change including the smallest modification, development, software update too. The *Long-Term Preservation Provider* implements 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* checks the authenticity and integrity of every software component at their first loading.

The *Long-Term Preservation Provider* applies proper network security measures for example:

- divides its IT system into well separated security zones;
- separates dedicated network for administration of IT systems and the *Long-Term Preservation Provider*'s operational network;
- separates the production systems for the TSP services from systems used in development and testing;
- establishes communication between distinct trustworthy systems only through trusted channels that are logically distinct from other communication channels and provide assured identification of its end points and protection of the channel data from modification or disclosure;
- operates the IT systems used for the live operational network in secure network zones;
- restricts access and communications between zones to those necessary for the operation of the service;
- disables the not used protocols and user accounts;
- disables unused network ports and services ;
- only runs network applications unconditionally necessary for the proper operation of the IT system .
- reviewes the established rule set on a regular basis.

The *Long-Term Preservation Provider* undergoes or performs a vulnerability scan on public and private IP addresses:

- within one week of receiving a request from the CA/Browser Forum;
- after any system or network changes that the CA determines are significant;
- at least every three (3) months.

The *Long-Term Preservation Provider* checks the compliance of the local network components (e.g. routers) configuration with the requirements specified by the *Long-Term Preservation Provider* at least every three months.

The *Long-Term Preservation Provider* orders a penetration test from an external independent expert who has the necessary skills, tools, proficiency and code of ethics to provide a reliable report yearly and in case of a significant change in the IT network.

6.6 Time-stamping

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

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* has a screening of its operations by an external auditor and sends the detailed report of the screening to the National Media and Infocommunications Authority within 3 days from its receipt. During the screening it is to be determined whether the operation of the *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 *Qualified Long-Term Preservation Practice Statement*(s).

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

- REGULATION (EU) No 910/2014 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 23 July 2014 on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC [1];
- ETSI EN 319 403 V2.2.2 (2015-08) Electronic Signatures and Infrastructures (ESI); Trust Service Provider Conformity Assessment - Requirements for conformity assessment bodies assessing Trust Service Providers; [19]
- ETSI EN 319 401 V2.2.1 (2018-04); Electronic Signatures and Infrastructures (ESI); General Policy Requirements for Trust Service Providers [18]

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 is published on the webpage of the *Long-Term Preservation Provider*.

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

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

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

The *Long-Term Preservation Provider* has an ISO 9001 standard compliant quality management system since 2002, moreover an ISO 27001 (formerly BS 7799) compliant information security management system since 2003, which are continuously audited and reviewed by an external auditing organisation. (see section: 1.3.1.)

7.1 Frequency or Circumstances of Assessment

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

7.2 Identity/Qualifications of Assessor

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

The eIDAS and ETSI conformity assessment is 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 is performed 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*.
- remuneration is not dependent on the findings of the activities carried out during the audit.

7.4 Topics Covered by Assessment

The review covers the following areas:

- compliance with the legislation currently in force;
- compliance with technical standards;
- compliance with the Certification Policy and the *Qualified 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 summarizes the result of the screening in a detailed screening report that covers the tested system components, processes, and contains the evidence used in the screening and the auditor statements. The discrepancies revealed during the examination and the deadlines set for correcting them are recorded in a separate chapter of the report.

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

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

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

The *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* publishes the summary report of the assessment on its web page on the following url:

`https://e-szigno.hu/en/eidas/`

The *Long-Term Preservation Provider* doesn't publish the detailes of the findings, they are treated as confidential information.

8 Other Business and Legal Matters

8.1 Fees

The *Long-Term Preservation Provider* publishes fees and prices on its webpage, and makes them available for reading in printed form at its customer service.

The *Long-Term Preservation Provider* may unilaterally change the price list. The *Long-Term Preservation Provider* publishes any modification to the price list 30 days before it comes into force. The changes favorable for the *Client* may come into force with shorter deadline than 30 days. Modifications will not affect the price of services paid in advance.

Provisions associated with the payment and refunding of fees are contained in the service agreement and its annexes – the General Terms and Conditions in particular.

8.1.1 Refund Policy

See section: 8.1.

8.2 Financial Responsibility

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

8.2.1 Insurance Coverage

To ensure financial reliability, as well as to cover the costs related to the termination of service the *Long-Term Preservation Provider* has a deposit.

8.2.2 Insurance or Warranty Coverage for End-entities

- The *Long-Term Preservation Provider* has liability insurance to ensure reliability.
- The liability insurance covers the following damages caused by the *Long-Term Preservation Provider* in connection with the provision of services:
  - damages caused by the breach of the service agreement to the trust service *Client*s;
  - damages caused out of contract to the trust service *Client*s or third parties;
  - damages caused to the National Media and Infocommunications Authority by the *Long-Term Preservation Provider* terminating the provision of the trust service;
  - under the eIDAS Regulation [1] 17. article (4) e) point, the legal costs of conformity assessment bodies to perform a conformity assessment by the request of the National Media and Infocommunications Authority if it enforces the costs as legal costs.
- The liability insurance policy shall cover at least for 3.000.000 Hungarian forints. Coincidental damages occurred for the same reason constitute a single insurance event.
- The liability insurance provides coverage for the full damage of the aggrieved party – up to the liability limit – arising in context of the harmful behaviour of the *Long-Term Preservation Provider* regardless of whether the damage was caused by breach of contract or outside the contract.
- If the valid claim of several entitled parties related to an insurance event exceeds the liability limit defined for an insurance event in the liability insurance, then the compensation of the claims takes place in the proportion of the liability limit to the total sum of the claims.

8.3 Confidentiality of Business Information

The *Long-Term Preservation Provider* manages clients' data according to legal regulations. The *Long-Term Preservation Provider* has a data processing regulation (see section 8.4), which addresses the processing of personal data in particular.

By signing the service agreement, *Client*s consent to the *Long-Term Preservation Provider* retaining and processing their personal data (in a manner that complies with the data processing regulations). Such consent applies to the forwarding of information specified by law and entered in

records to third parties in case the *Long-Term Preservation Provider*'s services go offline; moreover to forwarding such information to the *Long-Term Preservation Provider*'s subcontractors – solely for the purpose of performing tasks associated with providing the service.

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

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

8.3.1 Scope of Confidential Information

The *Long-Term Preservation Provider* treats as confidential:

- all *Client* data, with the exception of those that qualify as information not considered confidential in section 8.3.2;
- besides the *Client* data:
  - the electronic documents of the *Subscriber*s are stored in the archive, with the related certificate chains and other metadata;
  - transaction related data and log data,
  - non-public regulations,
  - all data whose public disclosure would have an adverse effect on the security of the service.

8.3.2 Information Not Within the Scope of Confidential Information

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

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.

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

- **Information provision for authorities**

  For the purpose of investigating or preventing acts of crime committed using the trusted services it provides, as well as in the case of national security related interests, the *Long-Term Preservation Provider* – if the statutory criteria applicable to data requests are met – discloses the related identity information and the information verified by the *Long-Term Preservation Provider* according to the section (1) of the Eüt. [6] 90. § to investigating authorities and national security services free of charge.

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

- **Disclosure upon owner's request**

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

8.4 Privacy of Personal Information

The *Long-Term Preservation Provider* takes care of the protection of the personal data it manages, the operation and regulations of the *Long-Term Preservation Provider* comply with the requirements of the Act CXII of 2011. on the Right to Freedom Of Information [4] and the 2016/679 EU General Data Protection Regulation [2].
The *Long-Term Preservation Provider*:

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

the registered personal data and information on the *Client* in accordance with the legal requirements.
The *Long-Term Preservation Provider* stores identification data, data about the *Subscriber* associated with contact details and data connected to the provision of the service in its records.
The *Long-Term Preservation Provider* hands over *Client* data to third parties solely in cases where this is stipulated by a legal regulation or if the *Client* has granted its consent to this in writing.

8.4.1 Privacy Plan

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

8.4.2 Information Treated as Private

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

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

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

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

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

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

8.6 Representations and Warranties

8.6.1 CA Representations and Warranties

Certification Authority's Responsibility

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

- 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 [5] 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 [5] 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.).
- If the valid claim of several entitled parties related to an insurance event exceeds the amount defined for an insurance event in the liability insurance for the damages, then the compensation of the claims takes place in a relative ratio to the amount determined in the liability contract.

The *Long-Term Preservation Provider* is not responsible:

- for the certificate verification and usage activities of the *Relying Parties*;
- for the regulations issued by the *Relying Parties* or others.

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 *Qualified 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 Practice Statement*, the service agreement and the standard policy conditions and other documents forming an integral part with it, as well as the relevant *Qualified Long-Term Preservation Policy*s.

Subscriber Rights

- *Subscriber*s have the right to use the services in accordance with this *Qualified 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 *Qualified 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 *Qualified 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 this regulation (see section: 8.8.), the service agreement and the contracts concluded with the *Client*s.

8.9.2 Indemnification by Subscribers

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

8.9.3 Indemnification by Relying Parties

See section: 8.8.

8.10 Term and Termination

8.10.1 Term

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

8.10.2 Termination

The *Qualified Long-Term Preservation Practice Statement* is valid without a time limit until withdrawal or the issuance of the newer version of the *Qualified Long-Term Preservation Practice Statement*.

8.10.3 Effect of Termination and Survival

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

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

8.11 Individual Notices and Communications with Participants

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

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

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

8.12 Amendments

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

8.12.1 Procedure for Amendment

The *Long-Term Preservation Provider* only discloses those of its procedures in its public domain regulations whose knowledge does not jeopardize the security of the services. The *Long-Term*

Preservation Provider has a number of internal security and other regulations, as well as operative level stipulations which it treats in confidence (this certificate practice statement mentions several such). The procedures described in section 7.4. audit these documents as well.

A team responsible for maintaining regulations and documentation operates within the *Long-Term Preservation Provider*'s certification organization. This team collects change requests, carries out modifications, and meets any internal and external information provision related obligations. The statement is approved by the director of the e-Szignó Certification Authority.

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

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

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

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 Practice Statement*, which is part of the document identifier (OID), so any change to the document will result in an OID change, namely two documents – entered into force – with different content cannot have the same OID.

8.13 Dispute Resolution Provisions

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

The *Long-Term Preservation Provider* and the *Client* mutually agree that in the case of any disputed issue or complaint arising whatsoever, they will attempt amicable consultation through negotiation before taking the dispute to legal channels. The initiating party will be obliged to

notify every other affected party promptly and to inform them fully concerning all of the case's implications.

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

Questions, objections, and complaints related to the activity of the *Long-Term Preservation Provider* shall be addressed to the customer care centre office in written form. The *Long-Term Preservation Provider* notifies submitting parties at the address they specify about having received a submission and the time required for investigation, within 3 business days calculated as of receiving a submission. The *Long-Term Preservation Provider* is obliged to issue a written response to the submitter within the specified time limit. The *Long-Term Preservation Provider* may request the provision of information required for giving a response from the submitter. The *Long-Term Preservation Provider* investigates complaints within 30 days, and notifies submitters about the results thereof.

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

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

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 applicable regulations:

- REGULATION (EU) No 910/2014 of the EUROPEAN PARLIAMENT AND OF THE COUNCIL of 23 July 2014 on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC [1];
- (Hungarian) Act CXII of 2011 on the Right to Freedom Of Information [4];
- (Hungarian) Act V of 2013. on the Civil Code. [5].
- (Hungarian) Act CCXXII of 2015 on electronic administration and the general rules of trust services [6];
- (Hungarian) Ministry of Interior Decree 24/2016. (VI. 30.) on the requirements for trust service providers and their services [7];

- (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 [8];
- (Hungarian) Government Decree 470/2017. (XII. 28.) on the announcement according to trust services and on the content of registers maintained by the trust service supervisory body [9];

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 Practice Statement* may only assign their rights and obligations to a third party with the prior written consent of *Long-Term Preservation Provider*.

8.16.3 Severability

Should some of the provisions of the present *Qualified Long-Term Preservation Practice Statement* 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 Practice Statement*, 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 *Qualified 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] REGULATION (EU) 2016/679 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) .

[3] (Hungarian) Act XXXV of 2001 on Electronic Signatures (repealed from 1st July 2016.) .

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

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

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

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

[8] (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 .

[9] (Hungarian) Government Decree 470/2017. (XII. 28.) on the announcement according to trust services and on the content of registers maintained by the trust service supervisory body .

[10] ETSI EN 319 122-1 V1.1.1 (2016-04) Electronic Signatures and Infrastructures (ESI); CAdES digital signatures; Part 1: Building blocks and CAdES baseline signatures.

[11] ETSI EN 319 122-2 V1.1.1 (2016-04) Electronic Signatures and Infrastructures (ESI); CAdES digital signatures; Part 2: Extended CAdES signatures.

[12] ETSI EN 319 132-1 V1.1.1 (2016-04) Electronic Signatures and Infrastructures (ESI); XAdES digital signatures; Part 1: Building blocks and XAdES baseline signatures.

[13] ETSI EN 319 132-2 V1.1.1 (2016-04) Electronic Signatures and Infrastructures (ESI); XAdES digital signatures; Part 2: Extended XAdES signatures.

[14] ETSI EN 319 142-1 V1.1.1 (2016-04) Electronic Signatures and Infrastructures (ESI); PAdES digital signatures; Part 1: Building blocks and PAdES baseline signatures.

[15] ETSI EN 319 142-2 V1.1.1 (2016-04) Electronic Signatures and Infrastructures (ESI); PAdES digital signatures; Part 2: Additional PAdES signatures profiles.

[16] ETSI EN 319 162-1 V1.1.1 (2016-04) Electronic Signatures and Infrastructures (ESI); Associated Signature Containers (ASiC); Part 1: Building blocks and ASiC baseline containers.

[17] ETSI EN 319 162-2 V1.1.1 (2016-04) Electronic Signatures and Infrastructures (ESI); Associated Signature Containers (ASiC); Part 2: Additional ASiC containers.

[18] ETSI EN 319 401 V2.2.1 (2018-04); Electronic Signatures and Infrastructures (ESI); General Policy Requirements for Trust Service Providers.

[19] 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;.

[20] ETSI TS 101 733 V1.8.1 (2009-11) Technical Specification Electronic Signatures and Infrastructures (ESI); CMS Advanced Electronic Signatures (CAdES).

[21] ETSI TS 101 733 V2.1.1 (2012-03) Electronic Signatures and Infrastructures (ESI); CMS Advanced Electronic Signatures (CAdES).

[22] ETSI TS 101 903 V1.2.2 (2004-04) Technical Specification XML Advanced Electronic Signatures (XAdES).

[23] ETSI TS 101 903 V1.3.2 (2006-03) Technical Specification XML Advanced Electronic Signatures (XAdES).

[24] ETSI TS 101 903 V1.4.1 (2009-06) Technical Specification XML Advanced Electronic Signatures (XAdES).

[25] ETSI TS 101 903 V1.4.2 (2010-12) Technical Specification Electronic Signatures and Infrastructures (ESI); XML Advanced Electronic Signatures (XAdES).

[26] ETSI TS 102 778-1 V1.1.1 (2009-07) Technical Specification Electronic Signatures and Infrastructures (ESI); PDF Advanced Electronic Signature Profiles; Part 1: PAdES Overview - a framework document for PAdES.

[27] ETSI TS 102 778-2 V1.2.1 (2009-07) Technical Specification Electronic Signatures and Infrastructures (ESI); PDF Advanced Electronic Signature Profiles; Part 2: PAdES Basic - Profile based on ISO 32000-1.

[28] ETSI TS 102 778-3 V1.1.2 (2009-12) Technical Specification Electronic Signatures and Infrastructures (ESI); PDF Advanced Electronic Signature Profiles; Part 3: PAdES Enhanced - PAdES-BES and PAdES-EPES Profiles.

[29] ETSI TS 102 778-4 V1.1.2 (2009-12) Technical Specification Electronic Signatures and Infrastructures (ESI); PDF Advanced Electronic Signature Profiles; Part 4: PAdES Long Term - PAdES-LTV Profile.

[30] ETSI TS 102 918 V1.3.1 (2013-06) Electronic Signatures and Infrastructures (ESI); Associated Signature Containers (ASiC).

[31] ETSI TS 103 171 V2.1.1 (2012-03) Electronic Signatures and Infrastructures (ESI); XAdES Baseline Profile.

[32] ISO/IEC 646:1991, Information technology – ISO 7-bit coded character set for information interchange.

[33] ISO/IEC 8859-1:1998, Information technology – 8-bit single-byte coded graphic character sets – Part 1: Latin alphabet No. 1.

[34] ISO/IEC 8859-2:1999, Information technology – 8-bit single-byte coded graphic character sets – Part 2: Latin alphabet No. 2.

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

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

[37] MSZ 7795-3:1992, Computing character codes. A hungarian reference set of graphic characters. .

[38] IETF RFC 2045: Multipurpose Internet Mail Extensions (MIME) Part One: Format of Internet Message Bodies, November 1996.

[39] IETF RFC 2822: Internet Message Format, April 2001.

[40] ISO 19005-1:2005 – Document management – Electronic document file format for long-term preservation – Part 1: Use of PDF 1.4 (PDF/A-1).

[41] Dublin Core Metadata Element Set, Version 1.1, `http://dublincore.org/documents/2006/12/18/dces/`.

[42] E-dossier format specification, Microsec zrt. `http://www.e-szigno.hu/?lap=eakta3` .

[43] Rich Text Format (RTF) Specification, RTF Version 1.7, Microsoft Technical Support, 2001.

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

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

[46] CEN CWA 14171: Procedures for Electronic Signature Verification.

[47] PDF Reference, second edition – Adobe Portable Document Format, Version 1.3, Addison-Wesley, ISBN 0-201-61588-6, 2000.

[48] e-Szignó Hitelesítés Szolgáltató - eIDAS rendelet szerinti minősített archiválási rend.

[49] e-Szignó Hitelesítés Szolgáltató - eIDAS rendelet szerinti minősített elektronikus archiválási szolgáltatás - archiválási szabályzat.

[50] e-Szignó Certification Authority - Qualified Long-Term Preservation Service - Long-Term Preservation Policy. .

[51] e-Szignó Certification Authority - Qualified Long-Term Preservation Service - general terms and conditions. .