MICROSEC

e-Szignó Certificate Authority

eIDAS conform
Qualified Long-Term Preservation Service
Preservation Disclosure Statement

ver. 2.22

Date of effect: 2021-06-30

OID	1.3.6.1.4.1.21528.2.1.1.198.2.22
Version	2.22
First version date of effect	2016-07-01
Security classification	PUBLIC
Approved by	Gergely Vanczák
Date of approval	2021-06-23
Date of effect	2021-06-30

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

Version	Effect date	Description
2.0	2016-07-01	New, eIDAS conform preservation policy.
2.1	2016-09-05	- Changes according to the NMHH comments.
2.2	2016-10-30	- Changes according to the auditor comments.
2.3	2017-04-30	- Changes according to the NMHH comments.
2.4	2017-09-30	- Yearly revision.
2.6	2018-03-24	- Global revision. - Smaller improvements.
2.7	2018-09-15	- Yearly revision.
2.8	2018-12-14	- Changes based on the suggestions of the auditor.
2.11	2019-09-25	- Yearly revision.
2.13	2020-03-05	- Effect. - HSM requirements. - Smaller improvements of wording.
2.14	2020-05-26	- Smaller improvements.
2.17	2020-10-28	- Rewriting according to the requirements of ETSI TS 119 511. - Improvements according to the auditor's and the supervisory body's findings. - Smaller improvements.
2.19	2020-12-28	- Smaller improvements.
2.22	2021-06-30	- Clarifications and additions in accordance with the CPS in Chapters 1 and 2. - Publication of conformity assessment results. - Service fees. - Protection of personal data. - Smaller improvements.

Table of Contents

1 Introduction

This document is the *Disclosure statement* concerning the qualified preservation service of e-Szignó Certificate Authority operated by Microsec ltd. (hereinafter: Microsec or *Long-Term Preservation Service Provider*).

The *Disclosure statement* contains comprehensive information of the conditions for consumers using the service corresponding to the provisions of the *Qualified Long-Term Preservation Practice Statement*, according to the provisions of the decree 24/2016. (VI. 30.) of Ministry of Interiors concerning detailed requirements for trust services and their providers.

The *Disclosure 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 Service Provider* announced the provision of the trust service to the National Media and Infocommunications Authority on the 1st of July 2016.

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

Based on the successful conformity assessment audit the National Media and Infocommunications Authority registered the qualified trust service and published it in the Hungarian Trusted List [36] on the 20th of December 2016.

The conformity assessment of the qualified trust service will be performed by Hunguard Kft (hereinafter Hunguard) as an independent auditor from October 2020.

1.1 Document Name and Identification

Issuer	e-Szignó Certificate Authority
Document name	eIDAS conform Qualified Long-Term Preservation Service Preservation Disclosure Statement
OID	1.3.6.1.4.1.21528.2.1.1.198
Document version	2.22
Date of effect	2021-06-30

1.1.1 Compliance

The *Long-Term Preservation Service Provider* supports the following ETSI service policy:

- normative requirements defined in ETSI TS 119 511 [24] including those defined in Annex A
  OID: itu-t(0) identified-organization(4) etsi(0) pres-service-policies(19511) policy-identifiers(1) qualified (2)

The *Long-Term Preservation Service Provider* includes its own OID in the service and declares the conformance to the ETSI policy through this *Disclosure statement*.

1.1.2 Long-term preservation policy

The trust 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
1.3.6.1.4.1.21528.2.1.1.187.2.22	qualified long-term preservation policy according to eIDAS Regulation.	MAR

The detailed requirements can be found in " e-Szignó Certificate Authority – eIDAS Qualified Long-Term Preservation Service – Long-Term Preservation Policy ver.2.22." [38]

1.2 Geographical Scope

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

The *Long-Term Preservation Service Provider* may 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 *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 *Qualified Long-Term Preservation Practice Statement* is independent of the geographical location where they were sent into the archive from, and where they where queried from.

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

1.3 The Trust Service Provider

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

1.3.2 Contact information of the customer service

The name of the provider unit:	e-Szignó Certificate 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.

1.4 Policy Administration

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

Person responsible for compliance with the *Qualified Long-Term Preservation Practice Statement* and the *Qualified Long-Term Preservation Policy* referenced therein is:

Responsible person	Head of Process Management Department
Organization name	Microsec ltd.
Organization address	Hungary, H-1033 Budapest, Ángel Sanz Briz str. 13.
Telephone number	+36 1 505-4444
Fax number	+36 1 505-4445
Email address	info@e-szigno.hu

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 Service Provider*s applying these policies.

2 Publication and Repository Responsibilities

2.1 Repositories

The *Long-Term Preservation Service Provider* discloses the contractual conditions and policies electronically on its website on the following link:

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

The draft version of 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 at the customer service of the *Long-Term Preservation Service Provider*.

After concluding the contract, the *Long-Term Preservation Service Provider* makes the General Terms and Conditions, the *Disclosure Statement*, the *Qualified Long-Term Preservation Policy* and the *Qualified Long-Term Preservation Practice Statement* available to the *Client* in the form of an electronically signed PDF file that can be downloaded from its website. The *Long-Term Preservation Service Provider* makes the individual Service Agreement available to the *Client* on paper, authenticated with a handwritten signature and seal, or in the form of an electronic document in PDF format with a qualified electronic signature.

The *Long-Term Preservation Service Provider* notifies its *Client*s about the change of the General Terms and Conditions.

2.2 Time or Frequency of Publication

2.2.1 Frequency of the Publication of Terms and Conditions

The most important terms and conditions for the service are contained in the service contract to be signed by the *Client* during the conclusion of the contract, or in the General Terms and Conditions [39] document referenced therein.

The *Long-Term Preservation Service Provider* reviews the General Terms and Conditions 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 Service 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 Service Provider* will accept comments connected to the General Terms and Conditions 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 Service Provider* will close and publish the version of the General Terms and Conditions as amended with remarks on the 7th day prior to its becoming effective.

3 Electronic Long-Term Preservation Service

The *Long-Term Preservation Service 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 Service Provider*. At the reception of the e-document the *Long-Term Preservation Service 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 preservation evidence, places electronic archive *Time Stamp* on the preservation evidence, and saves the accepted e-document. (see section 3.1).
- The *Long-Term Preservation Service Provider* securely preserves the accepted e-documents – the included files and preservation evidence – 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 Service 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 Service 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 Service Provider* and to the corresponding preservation evidence, and they can download them (see section: 3.2).
- At the request of the *Subscriber* the *Long-Term Preservation Service 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.
- At the request of the *Subscriber* the *Long-Term Preservation Service Provider* deletes the e-documents from its archive.

In each case the *Long-Term Preservation Service 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 Service 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 Service 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 Service 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 Service 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 [14] [15] [16] [17]
  - PAdES PDF/A format (ISO 19005) [31]
  - ASiC (Associated Signature Containers) ETSI TS 102 918 [22]
  - CAdES ETSI EN 319 122 [2], [3]
  - XAdES ETSI EN 319 132 [4], [5]
  - PAdES ETSI EN 319 142 [6], [7]
  - ASiC ETSI EN 319 162 [8], [9]

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 Service Provider*.

The archival period is specified by the service agreement concluded between the *Subscriber* and the *Long-Term Preservation Service Provider*. Unless otherwise agreed, the default retention period is 50 years.

The *Long-Term Preservation Service Provider* ensures the long-term readability of the file formats listed in section 4.2 in the manner specified therein, subject to the conditions described there.

3.1 Uploading the Document

The *Long-Term Preservation Service 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 Service Provider* as follows:

1. The *Subscriber* creates a SSL/TLS connection with the *Long-Term Preservation Service Provider* based on mutual authentication using their client authentication *Certificate*. The *Long-Term Preservation Service Provider* identifies the *Subscriber* based on the client authentication *Certificate* used for establishing the SSL/TLS connection. The *Subscriber* can upload e-documents through the SSL/TLS connection to the archive of the *Long-Term*

Preservation Service Provider. The *Subscriber* can provide metadata according to Dublin Core [32] in connection with the electronic documents. The metadata can be inserted into the e-document or provided upon uploading.

2. The *Long-Term Preservation Service 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 Service 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 Service Provider* [33]. 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 Service 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 Service 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 Service 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 Service 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 Service 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 Service 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 Service 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 Service 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 Service Provider* does not verify the validity of the electronic signatures, seals in those. The *Long-Term Preservation Service 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 Service 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 Service 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* , 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 Service 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 [35] and creates a format according to ETSI TS 101 903 [14] [15] [16] [17] .

The *Long-Term Preservation Service 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 Service 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 Service 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 Service 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 Service 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 Service Provider* performs the necessary verifications after the grace period is over according to the related standards and international recommendations. The *Long-Term Preservation Service Provider* rejects the e-document if it can not perform the verification under 3 days.

   The *Long-Term Preservation Service Provider* compiles the preservation evidence 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 preservation evidence in ETSI TS 101 903 [14] [15] [16] [17] format, namely as an archive signature into the e-document.

5. The *Long-Term Preservation Service 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 Service 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 Service 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 Service*

Provider also notifies the *Subscriber*. In this case the *Subscriber* receives an error message that informs him that the *Long-Term Preservation Service Provider* could not accept the electronic document (for example because it was not able to build the certificate chain). The *Long-Term Preservation Service 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 Service 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 Service Provider* did not accept the e-document. The *Long-Term Preservation Service 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 Service 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 Service 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/TLS 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 *Long-Term Preservation Service 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 Service Provider* also according to the aforementioned principles. The *Long-Term Preservation Service 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.

3.2 Provision of the Long-Term Validation Material/Preservation Evidence Availability – E-Document Download

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

The *Subscriber* only has access to the e-documents and the preservation evidence preserved in the archive of the *Long-Term Preservation Service Provider* through a secure channel.

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

1. The *Subscriber* establishes a mutual identification based SSL/TLS connection with the server of the *Long-Term Preservation Service Provider* using his client authentication *Certificate*. The *Long-Term Preservation Service Provider* identifies the *Subscriber* based on the client authentication *Certificate* used for establishing the SSL/TLS 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 [32] 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 Service Provider* determines whether the *Subscriber* is entitled to access the selected electronic document.

4. In case of appropriate access rights the *Long-Term Preservation Service 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/TLS 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/TLS connection to the *Subscriber*.
   - in case of an ASiC formatted e-document it sends the decoded e-document unencrypted trough a protected SSL/TLS connection to the *Subscriber*.

   The *Long-Term Preservation Service Provider* does not guarantee the downloadability of e-document if the *Subscriber* has previously submitted a deletion request for e-document.

For certain types of subscriptions, the *Long-Term Preservation Service Provider* may refuse to download e-document if the *Subscriber* has already exceeded the download size limit available to him in the given period.

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 preservation evidence and the electronic documents stored in the e-dossier.

In case previously agreed on with the *Long-Term Preservation Service Provider* the *Subscriber* may receive the e-documents and the preservation evidence preserved in the archive of the *Long-Term Preservation Service 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 Service 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* , 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*.

4 Technical Security Measures

4.1 Acceptance of the Certification and Time-Stamping Providers

The *Long-Term Preservation Service 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/en/supported-service-providers.html`

The *Long-Term Preservation Service 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 Service Provider* executes in case of a private key compromise of a previously accepted *Certification Authority* or *Time-Stamping Service Provider*.

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

The *Long-Term Preservation Service Provider* ensures, that during the archival period certain file format displayer necessary software and hardware devices are made available continuously. The *Long-Term Preservation Service Provider* for this purpose developed regulated and audited internal processes. The *Long-Term Preservation Service 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 Service Provider* ensures the readability of the original signed bit sequence, so the *Long-Term Preservation Service Provider* does not transform the signed file to another format.

The *Long-Term Preservation Service 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 Service 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 Service 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 Service Provider* hands over the service to another service provider. Then, in addition to the archived e-documents the *Long-Term Preservation Service 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 Service 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) [25],
- ISO 8859-1:1998 (Latin-1, 8 bit graphic character set) [26],
- ISO 8859-2:1999 (Latin-2) [27], for the Hungarian reference set, the MSZ 7795-3:1992 [28] derogation under ASCII and ASCII/PC codes,
- Microsoft Rich Text Format 1.7. [34],
- Portable Document Format (PDF) 1.3. [37],
- PDF/A format (ISO 19005) [31],
- every version of the Microsec e-dossier format [33],
- XAdES ETSI TS 101 903 v1.2.2 [14], v1.3.2 [15], v1.4.1 [16] and v1.4.2 [17], format XAdES signatures (if an XML file contains XAdES signature, the *Long-Term Preservation Service Provider* ensures the interpretability of the signature),
- XAdES Baseline Profile ETSI TS 103 171 v2.1.1 [23],
- CAdES ETSI TS 101 733 v1.8.1 [12],
- CAdES Baseline Profile ETSI TS 101 733 v2.1.1 [13],
- ASiC ETSI TS 102 918 v1.3.1 [22],
- PAdES ETSI TS 102 778 -1 v1.1.1 [18], -2 v1.2.1 [19], -3 v1.1.2 [20], -4 v1.1.2 [21],
- ETSI EN 319 122-1 [2] format CAdES signatures
- ETSI EN 319 122-2 [3] format CAdES signatures
- ETSI EN 319 132-1 [4] format XAdES signatures

- ETSI EN 319 132-2 [5] format XAdES signatures
- ETSI EN 319 142-1 [6] format PAdES signatures
- ETSI EN 319 142-2 [7] format PAdES signatures
- ETSI EN 319 162-1 [8] format ASiC signatures
- ETSI EN 319 162-2 [9] format ASiC signatures
- IETF RFC 2822 (Internet Message Format) [30],
- IETF RFC 2045 (Multipurpose Internet Mail Extensions, MIME) [29],
- XML formats used in the electronic company procedures [1],
- Such XML formats, for which the *Subscriber* submits to the *Long-Term Preservation Service 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 Service 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 Service Provider*, the *Long-Term Preservation Service Provider* shall examine the format according to the relevant procedural rules if this is feasible and under what conditions. If the *Long-Term Preservation Service Provider* includes the format requested by the *Subscriber* to the formats supported in respect of readability and legibility, that means the modification of the *Qualified Long-Term Preservation Practice Statement*.

The *Long-Term Preservation Service 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 Service 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 Service Provider* is not responsible for any resulting damages.

The *Long-Term Preservation Service 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 Service Provider* does not undertake the provision of the display of these embedded objects. Since the e-mail format (RFC 2822 [30]) does not specify the character coding of the e-mail, the *Long-Term Preservation Service 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 [29]) the *Long-Term Preservation Service Provider* only undertakes the display of only those attachments which has one of the aforementioned formats.

The *Long-Term Preservation Service Provider* undertakes the readability and display of files according to the definition of the files. This means that the *Long-Term Preservation Service 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 Service Provider* does not undertake the

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

readability of files encoded with other (further) transformations, particularly the encrypted files. Besides the files the *Long-Term Preservation Service 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 Service Provider* considers the given electronic document format unrecognized and does not ensures the interpretability of the electronic document. The *Long-Term Preservation Service Provider* supports the usage of the "mimeType" values in the following list:

- text/txt
- application/xml
- 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 Service 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 Service 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 Service 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 Service 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 Service 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 3.1. contains that the format of which file is unknown – the readability of such files is not guaranteed by the *Long-Term Preservation Service Provider*. The check carried out at the reception is not complete, the *Long-Term Preservation Service Provider* assumes no responsibility that the file format not considered unknown have supported format and correct syntax.

5 Compliance Audit and Other Assessments

The operation of the *Long-Term Preservation Service 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 Service Provider* location. Before the site inspection, the *Long-Term Preservation Service 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 Service 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 Electronic Signatures and Infrastructures (ESI); Trust Service Provider Conformity Assessment - Requirements for conformity assessment bodies assessing Trust Service Providers; [11]
- ETSI EN 319 401 Electronic Signatures and Infrastructures (ESI); General Policy Requirements for Trust Service Providers [10]
- ETSI TS 119 511 Electronic Signatures and Infrastructures (ESI); Policy and security requirements for trust service providers providing long-term preservation of digital signatures or general data using digital signature techniques [24]

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 Service Provider*.

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

The *Long-Term Preservation Service 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 Service 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 Service 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 Service 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

For more information on the governing law and compliance audits see sections 8. and 9.15 of the *Qualified Long-Term Preservation Practice Statement*.

5.1 Communication of Results

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

The certificates of the conformity assessment audit can be found on the official site of the auditor [2], and they are published also on the site of the *Long-Term Preservation Service Provider* on the following link:

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

The availabilities of the Hungarian National Trusted List are:

- human readable PDF format: `http://www.nmhh.hu/tl/pub/HU_TL.pdf`
- machine-processable XML format: `http://www.nmhh.hu/tl/pub/HU_TL.xml`

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

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

6 Other Business and Legal Matters

6.1 Fees

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

Price list availability:

- `https://e-szigno.hu/en/price-list`

The *Long-Term Preservation Service Provider* may unilaterally change the price list. The *Long-Term Preservation Service 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.

6.1.1 Refund Policy

See section: 6.1.

[2] `https://www.hunguard.hu/en/ugyfeleinknek/tanusitott-termekek-rendszerek/eidas-rendelet-szerinti-bizalmi-szolgaltatas/microsec-zrt/`

6.2 Privacy of Personal Information

6.2.1 Privacy Plan

The *Long-Term Preservation Service Provider* has a Privacy Policy and a Privacy Notice document, which contain detailed regulations on the handling of personal data.

The Privacy Policy is published on the webpage of the e-Szignó Certificate Authority on the following URL:

`https://e-szigno.hu/en/all-documents.html`

The Privacy Notice is published on the webpage of the e-Szignó Certificate Authority on the following URL:

`https://e-szigno.hu/en/privacynotice.html`

6.3 Representations and Warranties

6.3.1 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 Service Provider* while using the service .

The obligations of the *Subscriber* are determined by the *Qualified Long-Term Preservation Practice Statement*, the service agreement, the General Terms and Conditions, as well as the relevant *Qualified Long-Term Preservation Policy*.

Subscriber Rights

- *Subscriber*s have the right to use the services in accordance with the *Qualified Long-Term Preservation Practice Statement*.

6.3.2 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 Service 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 revocation status of all *Certificate*s based on the current CRL or OCSP response;
- take into consideration every restriction which is included in the *Qualified Long-Term Preservation Practice Statement* and in the corresponding *Qualified Long-Term Preservation Policy*.

6.4 Dispute Resolution Provisions

The *Long-Term Preservation Service 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 Service 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 Service Provider* shall be addressed to the customer care centre office in written form. The *Long-Term Preservation Service 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 Service Provider* is obliged to issue a written response to the submitter within the specified time limit. The *Long-Term Preservation Service Provider* may request the provision of information required for giving a response from the submitter. The *Long-Term Preservation Service 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 Service Provider* involved, the submitter may initiate consultation with the *Long-Term Preservation Service 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 Service 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.

6.5 Governing Law

The *Long-Term Preservation Service 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 Service Provider* contracts, regulations, and their execution, and they are to be construed by the Hungarian law.

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] 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.

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

[4] 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.

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

[6] 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.

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

[8] 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.

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

[10] ETSI EN 319 401 V2.3.1 (2021-05); Electronic Signatures and Infrastructures (ESI); General Policy Requirements for Trust Service Providers.

[11] 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;.

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

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

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

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

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

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

[18] 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.

[19] 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.

[20] 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.

[21] 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.

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

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

[24] ETSI TS 119 511 V1.1.1 (2019-06); Electronic Signatures and Infrastructures (ESI); Policy and security requirements for trust service providers providing long-term preservation of digital signatures or general data using digital signature techniques.

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

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

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

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

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

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

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

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

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

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

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

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

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

[38] e-Szignó Certification Authority - eIDAS conform Qualified Long-Term Preservation Service - Long-Term Preservation Policy.

[39] e-Szignó Certification Authority - General Terms and Conditions. .