MICROSEC

e-Szignó Certificate Authority

eIDAS conform
Qualified Long-Term Preservation Service
Preservation Disclosure Statement

ver. 2.13

Date of effect: 05/03/2020

OID	1.3.6.1.4.1.21528.2.1.1.198.2.13
Version	2.13
First version date of effect	01/07/2016
Security classification	PUBLIC
Approved by	Gergely Vanczák
Date of approval	03/03/2020
Date of effect	05/03/2020

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)
2.0	New, eIDAS conform preservation policy.	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.
2.3	Changes according to the NMHH comments.	30/04/2017	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.
2.13	Effect. HSM requirements. Smaller improvements of wording.	05/03/2020	Sándor Szőke, Dr.

Table of Contents

1 Introduction

This document is the *Disclosure statement* concerning the qualified preservation service of e-Szignó Certificate Authority operated by Microsec Micro Software Engineering & Consulting Private Company Limited by Shares (hereinafter: Microsec or *Long-Term Preservation 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 imposed by eIDAS regulation [1], the service provided in accordance with these regulations is a trust service according to the regulation.

The *Long-Term Preservation Provider* announced the trust service provision on the 1st of July 2016. to the National Media and Infocommunications Authority.

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 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	2.13
Date of effect	05/03/2020

1.1.1 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
1.3.6.1.4.1.21528.2.1.1.187.2.13	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.2.13." [34]

1.2 Geographical Scope

The present *Disclosure statement* includes specific requirements for services primarily provided for Hungarian *Client*s, operating by the Hungarian law in Hungary in Hungarian language. The *Long-Term Preservation Provider* can extend the geographical scope of the service, in this case, it shall use not less stringent requirements than those applicable to Hungarian conditions.

The service provided according to the present *Disclosure statement* is available worldwide. The validity of the documents, the long-term validation material and the related issued statements archived according to the present *Disclosure 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 *Disclosure statement* can be only used as described in the present document and in the *Long-Term Preservation Policy*.

1.3 The Trust Service Provider

1.3.1 Data of the 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`

The access of the *Qualified Long-Term Preservation Policy*, the *Qualified Long-Term Preservation Practice Statement* and the Privacy Policy:

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

The access of the price list:

- `https://e-szigno.hu/hitelesites-szolgaltatas/arlista/`

Refund:

The termination of the service agreement does not affect the fees paid by the *Subscriber*.

The *Long-Term Preservation Provider* does not issue refunds on fees that have already been paid, unless the service agreement expires due to the *Long-Term Preservation Provider*'s fault, or if the *Long-Term Preservation Provider* explicitly allows for this – for example in case of several packages.

The certificates of the conformity assessment audit can be found on the official site of TÜViT on the following link:

`https://www.tuvit.de/en/certification-overview-1265-4512.htm`

and they are published also on the site of the *Long-Term Preservation Provider* on the following link:

https://e-szigno.hu/eidas/eidas.html
The identification of the issued certificate:
e-Szignó Qualified Preservation Certificate ID: 9720.16

The access of the Hungarian national trust list:

- 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/

The access of the service agreement:
The *Long-Term Preservation Provider* sends the service agreement to be concluded with the *Client*ss to the notification e-mail address of the *Subject* given during initial registration.

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.

2 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 2.1).
- 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 3).
- 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: 2.2).
- 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.
- At the request of the *Subscriber* the *Long-Term Preservation Provider* deletes the e-documents from its archive.

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 [12] [13] [14] [15]
  - PAdES PDF/A format (ISO 19005) [28]
  - ASiC (Associated Signature Containers) ETSI TS 102 918 [20]
  - 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 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 3.2 in the manner specified therein, subject to the conditions described there.

2.1 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 [29] 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* [30]. 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), 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 [32] and creates a format according to ETSI TS 101 903 [12] [13] [14] [15] .

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 [12] [13] [14] [15] 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.

2.2 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 [29] 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 SSI connection to the *Subscriber*.
   - in case of an ASiC formatted e-document it sends the decoded e-document unencrypted trough a protected SSI 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* , 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 Technical Security Measures

3.1 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*.

3.2 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. 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) [22],
- ISO 8859-1:1998 (Latin-1, 8 bit graphic character set) [23],
- ISO 8859-2:1999 (Latin-2) [24], for the Hungarian reference set, the MSZ 7795-3:1992 [25] derogation under ASCII and ASCII/PC codes,
- Microsoft Rich Text Format 1.7. [31],
- Portable Document Format (PDF) 1.3. [33],
- PDF/A format (ISO 19005) [28],
- every version of the Microsec e-dossier format [30],
- XAdES ETSI TS 101 903 v1.2.2 [12], v1.3.2 [13], v1.4.1 [14] and v1.4.2 [15], 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 [21],
- CAdES ETSI TS 101 733 v1.8.1 [10],
- CAdES Baseline Profile ETSI TS 101 733 v2.1.1 [11],
- ASiC ETSI TS 102 918 v1.3.1 [20],
- PAdES ETSI TS 102 778 -1 v1.1.1 [16], -2 v1.2.1 [17], -3 v1.1.2 [18], -4 v1.1.2 [19],
- 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) [27],
- IETF RFC 2045 (Multipurpose Internet Mail Extensions, MIME) [26],

- 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 [27]) 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 [26]) 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. 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 2.1. 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 Other Business and Legal Matters

4.1 Representations and Warranties

4.1.1 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 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*.

4.1.2 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 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 the *Qualified Long-Term Preservation Practice Statement* and in the corresponding *Qualified Long-Term Preservation Policy*.

4.2 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.

4.3 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.

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

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

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

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

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

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

[16] 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.

[17] 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.

[18] 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.

[19] 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.

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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