QUALIFIED LONG TERM PRESERVATION SERVICE

Policy And Practice Statement

Ver. 1.1

Date of effect: 02.03.2020

General information	
OID	*1.3.6.1.4.1.39965.5.1.1.1.1.0*
Version	*1.1*
Security classification	*Public*
Approved by	*Camelia Ivan*
Date of approval	*2.03.2020*
Date of effect	*2.03.2020*

Change history			
Version	**Description**	**Effect date**	**Author(s)**
1.0	First release	3.02.2020	Mihaela Bunea
1.1	Content alignment with ETSI TS 119 511	2.03.2020	Mihaela Bunea

Contents

1. Introduction

It is common practice for a Trust Service Provider to have two documents in place:

- a Certification Practice Statement (CPS) describing the practices which a TSP employs in managing certificates (application, issuance, use, and revocation) or trusted services;
- a Certificate Policy (CP) describing the vetting processes and allowing an estimation of the trustworthiness and reliability of its services;

Because all qualified trusted services underlie the same regulations and requirements defined in the eIDAS Regulation, both above mentioned documents (CPS and CP) have been merged into one single document, this **Policy and Practice Statement**.

This document contains the *Qualified Long-Term Preservation Policy and Practice Statement* defined and operated by Trans Sped (hereinafter: Trans Sped or ***Long-Term Preservation Provider***) concerning the qualified preservation service.

The *Qualified Long-Term Preservation service* complies with the requirements set by the eIDAS Regulation [1], the service provided according to these regulations is an EU qualified trust service.
The prerequisites for the qualified trust service provision and the "EU Trust Mark" indication are:

- the service shall be audited by an independent assessment body accredited under eIDAS Regulation, it shall issue a conformity assessment report and a certificate for the *Long-Term Preservation Provider* about the successful assessment;
- the *Long-Term Preservation Provider* shall submit the conformity assessment certificate to a Supervisory Body;
- the Supervisory Body shall accept the submitted conformity assessment certificate and it shall publish the service in the national trusted list.

1.1. Overview

The *Qualified Long-Term Preservation Policy* is a set of rules that specify the qualified preservation service usability for a community and/or a class of applications with common safety requirements.
The *Qualified Long-Term Preservation Policy* sets out basic requirements for the *Long-Term Preservation Provider* related to the qualified preservation to be established.
The *Qualified Long-Term Preservation Policy* is one of several documents issued by the *Long- Term Preservation Provider* that collectively govern conditions of the services provided by the *Long-Term Preservation Provider*. Other important documents include General Terms and Conditions, *Long- Term Preservation Practice Statements*, and other customer and partner agreements.

1.1.1. Long-term preservation policy

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

(1)	International Organization for Standardization (ISO)
(3)	Organization identification schemes registered according to ISO/IEC 6523-2
(6)	United States Department of Defense (DoD)
(1)	Internet
(4)	Private projects
(1)	Private enterprises
(39965)	Trans Sped srl

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

(1.3.6.1.4.1. 39965)	Trans Sped srl
(5)	Trans Sped Long Term Preservation
(1)	Documents
(1)	Public documents
(x)	unique identifier number of the document
(y)	Document version
(z)	Document subversion

The present document defines the following *Policy*:

OID	DENOMINATION	SHORT NAME
1.3.6.1.4.1.39965.5.1.1.1.1.0	qualified long-term preservation policy according to eIDAS Regulation	QLTP

1.1.2. Effect

This *Qualified Long-Term Preservation Policy and Practice Statement* is in effect from the February 2020 date of entry into force to withdrawal.
The present *Qualified Long-Term Preservation Policy and Practice* should be reviewed at least annually and their amendment to the potentially changed requirements and prerequisites shall be ensured.
The effect of the *Qualified Long-Term Preservation Policy and Practice Statement* extends each of the participants mentioned in section 1.3.

1.2. LTP Participants

1.2.1. LTP Providers

The long term service provider is a Trust Service Provider, within the framework of which Trust Service deals with validity preservation of the electronic signatures, electronic seals, time stamps and their creator Certificates, optionally including the signed and sealed electronic document preservation too.
The requirements of the present document apply to every *Long-Term Preservation Provider* who undertake in their *Long-Term Preservation Practice Statement* the compliance with any of the *Qualified Long-Term Preservation Policy* (s) described in the present document.

1.2.2. Subscribers

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

1.2.3. Relying Parties

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

1.3. Policy Administration

1.3.1. Organization Administering the Document

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

Organization name	Trans Sped srl
Organization address	38 Despot Voda, 2nd District, 020656, Bucharest, Romania
Telephone number	+40212107500
Fax number	+40212110207
Email address	office@transsped.ro

1.3.2. Contact person

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

Contact person	Camelia IVAN
Organization name	Trans Sped srl
Organization address	38 Despot Voda, 2nd District, 020656, Bucharest, Romania
Telephone number	+40212107500
Fax number	+40212110207
Email address	office@transsped.ro

1.3.3. Practice Statement Approval Procedures

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

1.4. Definitions and Acronyms

Data Centre	A facility designed for the placement and operation of computer systems and associated components. These components typically include telecommunications systems and communication connections, redundant power supply, data storage, air conditioning, fire protection and safety systems.
Supervisory Body	As defined by eIDAS Regulation
Trust Service	"Means an electronic service normally provided for remuneration which consists of: the creation, verification, and validation of electronic signatures, electronic seals or electronic time stamps, electronic registered delivery services and certificates related

	to those services, or the creation, verification and validation of Website Authentication Certificate; or the preservation of electronic signatures, seals or certificates related to those services; " (eIDAS [1] 3. article 16. point)
Trust Service Provider	"A natural or a legal person who provides one or more Trust Services either as a qualified or as a non-qualified Trust Service Provider." (eIDAS [1] 3. article 19. point)
Long-Term Preservation Provider	Trans Sped S.R.L.
E-dossier	The electronic file (e-dossier) is a container format electronic signature, a type of e-document. An e-dossier may contain documents, or the related profiles (metadata), signatures, countersignatures and time-stamps.
E-document	An e-document is such an electronic document that contains at least one eIDAS regulation conformant electronic signature or seal. Depending on the type of the e- document it may contain further electronic documents and the corresponding profiles (metadata), signatures, countersignatures and time stamps.
Electronic Document	"Means any content stored in electronic form, in particular text or sound, visual or audiovisual recording" (eIDAS [1] 3. Article 35. point)
Electronic Time Stamp	"Means data in electronic form which binds other data in electronic form to a particular time establishing evidence that the latter data existed at that time." (eIDAS [1] 3.article 33.point)
Export-import package(s)	Information extracted from the preservation service including the submission data object, the preservation evidence and preservation-related metadata, allowing another preservation service to import it in order to continue to achieve the preservation goal based on this information
Subscriber	A person or organization signing the service agreement with the Long-Term Preservation Provider in order to use some of its services.
Suspension	The temporary termination of the Certificate's validity before the end of the validity period indicated on the Certificate. The Certificate suspension is not definitive; the suspended Certificate's validity can be restored.
Root Certificate	Also known as top level certificate. Self- signed Certificate, which is issued by a specific Certification Unit for itself, which is signed with its own private key, so it can be verified with the Signature-Verification Data–indicated on the certificate.

HSM: Hardware Security Module	A hardware-based secure tool that generates, stores and protects cryptographic keys and provides a secure environment for the implementation of cryptographic functions.
Compromise	A cryptographic key is compromised, when unauthorized persons might have gained access to it.
Intermediate Certification Unit	A Certification Unit whose Certificate was issued by another Certification Unit.
Cryptographic Key	An individual digital signal series controlling cryptographic transformation, the knowledge of which is required for encryption, decryption, electronic signature creation and verification.
Key Management	The production of cryptographic keys, their delivery to users or its algorithmic implementation, as well as the registration, storage, archival, revocation and termination of keys which are closely linked to the used security method.
Long-term preservation	Extension of the validity status of a digital signature over long periods of time and/or extension of provision of proofs of existence of data over long periods of time, in spite of obsolescence of cryptographic technology such as crypto algorithms, key sizes or hash functions, key compromises or of the loss of the ability to check the validity status of public key certificates.
Preservation profile	Uniquely identified set of implementation details pertinent to a preservation storage model and one or more preservation goals which specifies how preservation evidences are generated and validated.
Private Key	In the public key infrastructure, the element of an asymmetric cryptographic key pair for an actor that the Subject shall keep strictly secret. During the issuance of Certificates, the Certification Authority uses the private keys of the Certification Unit for placing an electronic signature or seal on the Certificate to protect it.
Qualified Trust Service	"A Trust Service that meets the applicable requirements laid down in the eIDAS Regulation." (eIDAS [1] article 3. point 17.)
Qualified Trust Service Provider	"A Trust Service Provider who provides one or more Qualified Trust Services and is granted the qualified status by the supervisory body." (eIDAS [1] article 3. Point 20.)
Public Key	In the public key infrastructure, the element of an asymmetric cryptographic key pair belonging to an actor, which should be made public. The disclosure is typically in the form of a Certificate, which links the name of the actor with its public key. The authenticity of the Certificates can be

	verified with the public key of the Certification Unit.
Public Key Infrastructure, PKI	An infrastructure based on asymmetric cryptography, including the cryptographic algorithms, keys, certificates, the related standards and legislation, the underlying institutional system, a variety of providers and devices.
Unencrypted e-dossier	An e-dossier, which includes unencrypted files and electronic signatures or electronic seals on them. In the unencrypted e-dossier the signed, stamped files and signatures, seals are included unencrypted.
Extraordinary Operational Situation	An extraordinary situation causing disturbance in the course of the operation of the Long-Term Preservation Provider, when the continuation of the normal operation of the Long-Term Preservation Provider is not possible either temporarily or permanently.
Organization	Legal person.
Certificate Repository	Data repository containing various Certificates. A Certification Authority has a Certificate Repository in which the issued certificates are disclosed, but the system containing Certificates available to the application on the computer of the Relying Party is also called Certificate Repository.
Revocation	The termination of the Certificate's validity before the end of the validity period indicated on the Certificate too. The Certificate revocation is permanent, the revoked Certificate cannot be reinstated any more.
Revocation Status Records	The records of the suspended and revoked Certificates which includes the fact of the suspension or revocation and the time of the suspension or revocation maintained by the Certification Authority.

1.4.2. Acronyms

CRL Certificate Revocation List
eIDAS electronic Identification, Authentication and Signature
LDAP Lightweight Directory Access Protocol
LTP Long Term Preservation
SB Supervisory Body
OCSP Online Certificate Status Protocol
OID Object Identifier
PKI Public Key Infrastructure
TSP Trust Service Provider
VM Virtual Machine

2. Publication and Repository Responsabilities

2.1. Repositories

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

2.2. Publicaton of Certification Information

2.2.1. Publication of the Long-Term Preservatin Provider Information

The *Long-Term Preservation Provider* shall disclose the contractual conditions and policies electronically on its website.
The new documents to be introduced shall be disclosed on the website 30 days before coming into force.
The documents in force shall be available on the site in addition to all previous versions of all documents.
The actual version of policies and contractual conditions shall be readable in printed form at the customer service of the *Long-Term Preservation Provider*.

The *Long-Term Preservation Provider* shall make available the *Qualified Long-Term Preservation Policy*, the *Long-Term Preservation Practice Statement* and the Service Agreement to the *Client* on a durable medium following the conclusion of the contract.
The *Long-Term Preservation Provider* shall notify its *Client* s about the change of the General Terms and Conditions.

2.3. Time of Frequency of Publication

2.3.1. Frequency of the Publication of Terms and Conditions

The disclosure of the *Qualified Long-Term Preservation Policy* related new versions is compliant with the methods described in Section 8.12.
The *Long-Term Preservation Provider* discloses other regulations, contractual conditions and their new versions if necessary.
The *Long-Term Preservation Provider* shall publish extraordinary information without delay in accordance with the legal requirements and in the absence thereof when necessary.

3. Electronic Long-Term Preservation Service

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

- The Subscriber can upload electronically signed e-documents to the archive operated by the Long-Term Preservation Provider.
- 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 cannot 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 usually, except if the validity of the service agreement ceases before the end of this period (for details see section 4).

- The *Subscriber* has access continuously to the e-documents, signatures and seals placed by them in the archive of the *Long-Term Preservation Provider* and to the corresponding long-term validation material, and they can download them (see section: 3.3).
- After the reception of the e-document the *Long-Term Preservation Provider* could check the electronic signature(s) or seal(s) on the e-document, based on individual agreement, or on the files included into the e-documents, completes or compiles the long-term validation material, places electronic archive time stamps on the long-term validation material, and saves the accepted e-document. (see section 3.2).
- 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 (see section: 3.4).
- At the request of the *Subscriber* the *Long-Term Preservation Provider* deletes the e- documents from its archive (see section: 3.6).

The primary task of the long-term preservation service is the preservation of the validity of the digitally signed documents or seal placed on the electronic document.
The *Long-Term Preservation Provider* can provide other services to the *Subscriber* besides the provision of the basic task, for example:

- preservation of the electronic documents with an electronic signature or seal, ensuring the readability and human interpretability of the electronic documents uploaded to the archive,
- performing the file format conversions that become necessary,
- preservation of electronic documents without electronic signature or seal
- certified copies of electronic documents preserved in the Long-Term Preservation System

The present *Qualified Long-Term Preservation Policy and Practice Statement* define the requirements for the long-term validity assurance of electronic signatures and seals.
The *Long-Term Preservation Provider* may specify and restrict the format of the accepted electronic signatures or seals, the accepted Certification Authorities and any other parameter.

3.1. Concluding a Service Agreement

Before using the service the *Subscriber* shall conclude a service agreement with the *Long-Term Preservation Provider*.
The *Long-Term Preservation Practice Statement* and the other regulations cited shall clearly specify the details of the service to be provided, and the tools needed for using the service.

3.2. Uploading the Document

The *Long-Term Preservation Provider* shall only accept the e-documents to be archived after the identification of the *Subscriber* within the framework of a secure procedure. The procedures ensure the integrity, confidentiality of the e-documents.
It shall be clearly specified which signature and file format the *Long-Term Preservation Provider* accepts in the e-document, how it verifies the electronic signatures and seals and under what conditions it accepts the electronic documents.
The validity of the electronic signature(s) or seal(s) on the received e-document shall be verified using the full long-term validation material. The verification may be based on the partial or full long-term

validation material attached to the electronic signature(s) or seal(s). Any still necessary information for the validation is collected by the *Long-Term Preservation Provider* and preserved that linked to the e-document. After compiling the long-term validation materials the *Long-Term Preservation Provider* shall place a qualified archive *Time Stamp* on each long-term validation material.
The *Long-Term Preservation Provider* shall verify the received e-documents as soon as possible, but no later than 3 days from admission and shall send confirmation to the *Subscriber* that the long-term validation material has been compiled successfully, and it accepted the e-document. If the process is interrupted somewhere, the *Long-Term Preservation Provider* shall notify the *Subscriber* in an error message. Based on the error message it must be clearly identifiable that which e-document is involved and what was the reason for rejection.
If the verification on the acceptance of the e-document does not arrive to the *Subscriber* within the stated deadline, it shall be considered that the *Long-Term Preservation Provider* did not accept the e-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 sending positive confirmation.

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

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

3.4. Issuance of the Acknowledgement

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

1. The hash of the e-document, the name and identifier of the *Subscriber*.
2. The statement that the given e-document has the given hash, so it is identical to the e-document with the same hash presented by the *Subscriber*.
3. The time of the e-document acceptance into the archive.
4. The file size and customer IP address
5. The statement that the advanced or qualified electronic signatures, seals, time stamps on the given e-documents and the corresponding certificates were valid at the time of the time stamping and the validation after their upload.

The Long-Term Preservation Provider issues the acknowledgement in an e-receipt with a qualified electronic signature. The acknowledgement is created by an official responsible for issuing the archive acknowledgement, and in case of an electronic acknowledgement places his qualified electronic signature, in case of a paper based acknowledgement he authenticates the printed acknowledgement with his handwritten signature.
Knowledge of the archived e-document is not needed for the issuance of the acknowledgement, it is issued based on the hash of the unencrypted e-document preserved in clear text. No information can be obtained from the hash value in relation to the content of the preserved electronic document.
The applied solution ensures that the officials responsible for issuing the archive acknowledgement do not get to know the contents of the unencrypted electronic document in connection with the issuance of the acknowledgement.

The Subscriber can request the issuance of the acknowledgement from the Long-Term Preservation Provider with a paper based hand signed request submitted by any delivery manner or by filing an electronic request certified with at least an advanced electronic signature or seal.
The issuance of the acknowledgement may be requested by the authorized representative of the Subscriber if he presented the authorization of the Subscriber contained in a fully conclusive private document beforehand.

3.5. Document Display

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

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

The *Long-Term Preservation Provider* makes available the selective deletion of the e- documents and all the corresponding long-term validation materials preserved in the archive at the request of the *Subscriber*. The deletion means the physical deletion of the preserved e- document and its overwriting in such a way that it cannot be restored (or only with unrealistically high financial expenditure) from the data medium later. The deletion is performed on the whole system of the *Long-Term Preservation Provider*, and during the deletion will destroy every preserved copy of the e-document.
The *Long-Term Preservation Provider* shall specify in the *Long-Term Preservation Practice Statement* the manner and conditions of the admission and processing of the deletion request.

3.7. Termination of the Service Agreement

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

3.8. Long-term preservation goals

The long-term preservation services cover the following goals:

- Proof of integrity of an electronic document;
- Proof of existence of an electronic document (at a time/in the past);
- Maintenance of the validity status of e-signatures/seals over long periods;
- Data availability.

Data integrity is verified during the preservation time frame by means of a proof of integrity (hash, signature/seal).
The proof of existence indicates that the digital object(s) existed at a specific time and it is implemented by combining a proof of integrity and a trusted time indication (qualified time-stamp).
To maintain the validity status of the electronic signature/seal, all elements needed to verify the validity and which cannot be guaranteed to be available in the future, need to be preserved as well. This can include certificates, revocation information (CRLs, OCSP responses), trusted lists, etc.
Data availability is ensured by using dedicated storage devices in two different locations in a highly available configuration using a clustered backend that provides mirrored copies of all documents and associated meta-data.

3.9. Preservation profiles

The *Long-Term Preservation Provider* supports the following preservation profile:

```
    "type": "object",
    "properties": {
        "pid": {
            "type": "https://link.catre.profile.identifier"
        },
        "op": {
            "type": "array",
            "items": {
                "https://lta.transsped.ro/api/PreservePO": "PreservePO",
                "https://lta.transsped.ro/api/RetrievePO": "RetrievePO",
                "https://lta.transsped.ro/api/DeletePO": "DeletePO",
                "https://lta.transsped.ro/api/UpdatePOC": "UpdatePOC",
                "https://lta.transsped.ro/api/Search": "Search"
            }
        },
        "pol": {
            "type": "array",
            "items": {
                "http://uri.etsi.org/19512/policy/preservation-
evidence": "http://uri.etsi.org/19512/policy/preservation-evidence",
            }
        },
        "ext": {
            "type": "array",
            "items": {
                "$ref": "#\/definitions\/md-ExtensionType"
            }
        },
        "sid": {
            "type": "http://uri.etsi.org/19512/scheme/pds+pgd+wst"
        },
        "pvp": {
            "type": "object",
            "properties": {
                "vfrom": {
                    "type": "string",
                    "format": "01-04-2020 00:00:00.000"
                },
            }
        },
        "psm": {
            "http://uri.etsi.org/19512/scheme/wst": "WithStorage"
        },
        "pg": {
            "type": "array",
            "items": {
```

```
                "http://uri.etsi.org/19512/goal/pgd": "http://uri.etsi.org/19512/goal/pgd"
            }
        },
        "ef": {
            "type": "array",
            "items": {
                "http://uri.etsi.org/ades/XAdES/ArchiveTimeStamp": "http://uri.etsi.org/ades/XAdES/ArchiveTimeStamp"
            }
        },
        "eed": {
            "type": "One Year"
        }
    }
}
```


The same preservation profile will apply during the whole preservation period and preservation evidence retention period.

3.10. Preservation evidence policy

The preservation evidence is created after the document's signatures and timestamps are validated. The validation process takes into account the signature's integrity and that it matches with the document's digest, the certificate used to sign it must be part of the EU trusted list and not revoked.

After the validation, a XADES-A xml is created, containing all the information required to confirm in the future that the validation has been successful at the time of testing:

- The document digest
- Signing time
- Signing certificate and certificate path
- Signatures and timestamps
- Revocation data from OCSP and/or CRL

After building the XADES-A it is then time stamped and stored alongside the file, ready to be downloaded at the client's request using the provided API. The provider of qualified time stamps is Trans Sped S.R.L.

3.11. Signature validation policy

The validation of signatures is done using the Release 5.5 of the DSS framework, created by ESIG and delivered under the terms of the Lesser General Public License (LPGL), version 2.1.
The framework checks the document for signature integrity, trust list compliance and also checks revocation services. The entire certificate chain is verified. After completion the data is extracted and inserted into a XADES-A XML compliant with the ETSI standard.
The trust list used is the European Trusted List where Trans Sped S.R.L. is also a member.

3.12. Export-import package(s)

The *Long-Term Preservation Provider* allows the *Subscriber* to request the export-import package(s), containing the preserved data, the evidences and all information needed to validate the evidence;
The export-import package(s) requests will be accepted as follows:

- by e-mail: the request needs to be submitted from a previously known and approved e-mail address;
- by physical presence: any person who has a formal empowerment to represent the User can submit a request in Trans Sped's office.

Importing large amounts of documents from different platforms requires a different approach.
The documents must be present in their original form and accompanied by a XADES-A XML. The import service has to revalidate the data and check the XADES-A XML for accuracy, after which it timestamps the evidence again.
The *Long-Term Preservation Provider* can export all the contents of the database and provide the original document and the XADES-A XML that is associated with it.

4. Technical Security Measures

4.1. Security Guarantees

The *Long-Term Preservation Provider* uses reliable systems and products protected against modification. It uses a uniform IT system consisting of reliable, technically evaluated and certified security products for the provision of its services. The Long-Term Preservation Provider uses reliable systems and products that are protected against unauthorized modification. Both the Long-Term Preservation Provider, and the system supplier and installer contractors have significant experience in building certification services and use internationally recognized technology.
If the *Long-Term Preservation Provider* uses a trusted service of a third party, it shall verify whether that third party complies with every necessary requirement. The *Long-Term Preservation Provider* stores the archived e-documents in a physically protected environment, according to the physical and procedural requirements described in section 5, the safety of which is guaranteed by the internal security policies and the regular internal and external security audits.
The Long- Term Preservation Provider ensures that the stored e-documents cannot be read even by its employees. The Long-Term Preservation Provider only submits the e-documents to a third party (e.g. authority) if the Subscriber authorizes it or when it is required by law.
The integrity of the stored e-dossiers is ensured by the physical protection of the e-dossiers, as well as by technologies related to electronic signatures or data encryption.
The availability of the e-documents is ensured by the high quality system of the Long-Term Preservation Provider and the internal regulations and procedures governing the system, the business continuity and emergency management procedures and other procedures for managing emergency situations.
The Long-Term Preservation Provider avoids errors arising during operation and maintenance using these processes, and their continuous internal and external monitoring and testing.
The Long-Term Preservation Provider stores the archived e-documents at two physical locations far from each other.
The Long-Term Preservation Provider destroys the archived e-documents – at the request of the Subscriber or in case of the termination of the contract – under the conditions described in section 3.6.
The Long-Term Preservation Provider monitors the development of technology and if it detects that a key is no longer secure or the algorithm is no longer usable immediately replaces the affected key or keys.

4.2. Computer Security Precautions

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

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

4.3. Life-Cycle Related Technical Precaution

In order to meet the high level of security requirements in all the system development projects of the Long-Term Preservation Provider, the elevated requirements shall be taken into account in the overall development process (even in the planning and requirement definition phase).
Products used for the provision of services are applied by taking into account the life cycle related security considerations.

4.4. Continuous Monitoring of Technology

The Long-Term Preservation Provider is free to decide at any time to change the used cryptographic algorithm sets and their parameters in case of an algorithm and parameter is deprecated or could bring security issues.

4.5. Acceptance of the Certification and Time-Stamping Providers

The Long-Term Preservation Provider may specify under what conditions it accepts the Certificates of a given Certification Authority and what Certification Authorities it accepts, along with the criteria for the Certification Authorities to be included in this list or to be excluded from it within the framework of the long term preservation service. Basically the Qualified Trust Service Providers for electronic signatures and time stamps, published on EU Trusted Lists, are accepted.

4.6. The Maintenance of the Readability and Interpretability of the Electronic Documents

The *Long-Term Preservation Provider* clearly determines in the agreements signed with Subscribers which file format and electronic document readability it ensures within the framework of the long term preservation service.

4.7. The Availability of Certain Elements of the Electronic Long-Term Preservation Service

The annual availability of the following electronic long term preservation service elements is 98% and the occasional service interruptions shall not exceed 3 days:

- the electronic download of the archived e-documents and validity chains;
- search of archived e-documents;
- receiving deletion requests;
- receiving timed deletion requests (with the help of which the *Subscriber* can specify how long a given e-document is archived by the *Long-Term Preservation Provider*), and the modification of former timed deletion requests;
- requesting information on the status of previously sent requests.

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

5. Facility, Management and Operational Controls

The Long-Term Preservation Provider applies physical, procedural, and personnel security precautions that comply with acknowledged standards, along with the administrative and governance related procedures that enforce these.
The Long-Term Preservation Provider keeps a record of the system units and resources related to the service provision, and conducts a risk assessment on these. It uses protective measures proportional to the risks related to the individual elements.
The Long-Term Preservation Provider monitors the capacity demands, and ensures that the adequate processing power and storage are available for the provision of the service.

5.1. Physical Controls

The Long-Term Preservation Provider takes care that physical access to critical services is controlled, and keeps physical risk of the assets related to critical services at a minimum.
The purpose of physical precautions is to prevent illegitimate access, damage, and unauthorized access to the Long-Term Preservation Provider's information, and physical zones.
Services that process critical and sensitive information are implemented at secure locations. The provided protection is proportional to the identified threats of the risk analysis that the Long-Term Preservation Provider performed.

5.1.1. Site Location and Construction

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

5.1.2. Physical Access

The Long-Term Preservation Provider protects devices and equipment that take part in the service provision from unauthorized physical access in order to prevent tampering with the devices.
Long-Term Preservation Provider ensures that:

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

The activation data (passwords, PIN codes) of the devices are not stored openly even in the Data Centre.
In the presence of unauthorized persons:

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

When leaving the computer room the administrator shall verify that:

- every equipment of the Data Centre is in an adequately secure operation state;
- there's no terminal left logged-in;
- physical storage devices are locked properly;

- systems, devices providing physical protection operate properly;
- the alarm system has been activated.

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

5.1.3. Power and Air Conditioning

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

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

The *Data Centre* air purity is controlled with adequate filter system to detect a variety of contaminants from the air (dust, pollutants, and corrosive materials, toxic or flammable substances). The ventilation provides the necessary amount of fresh air with adequate filtration for the safe working conditions of the operators.
The humidity is controlled to the level required by the IT systems.
Cooling systems with proper performance are used to provide the necessary operating temperature, to prevent overheating of IT devices.

5.1.4. Water Exposure

The *Data Centre* of the *Long-Term Preservation Provider* is adequately protected from water intrusion and flooding.

5.1.5. Fire Prevention and Protection

Smoke and fire detectors are installed in the Data Centre of the Long-Term Preservation Provider that automatically alerts in case of event. Manual fire extinguishers of the appropriate type and amount compliant with the relevant regulations are placed in a visible place in each room.
Also, automatic fire extinguishers are applied in the Data Centre.

5.1.6. Media Storage

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

5.1.7. Waste Disposal

The Long-Term Preservation Provider takes care of the destruction of its devices, media storages becoming superfluous in compliance with environmental regulations. Such devices and media storages shall be permanently deleted or made unusable in accordance with the widely accepted methods under the personal supervision of employees of the Long-Term Preservation Provider.

5.1.8. Off-site Backup

The *Long-Term Preservation Provider* creates regular backups from which the whole service can be restored in case of a fatal error. The backups (including the last full backup) is stored at an external

location that's physical and operational protection is identical to the primary site. The secure data transmission from the primary to the backup locations is resolved.

5.2. Procedural Controls

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

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

The *Long-Term Preservation Provider*'s internal governance system ensures that its operation complies with legal, as well as its internal regulations. Responsible persons are assigned for every given system unit and process.

Individuals responsible for a given system element or process are assigned unambiguously to every system element and every process in its system. Development and operations related tasks are sharply segregated in the *Long-Term Preservation Provider* 's system. The auditing activity of the independent system auditor and the *Long-Term Preservation Provider's* internal auditor ensures the system's appropriate operation.

5.2.1. Trusted Roles

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

The Long-Term Preservation Provider implemented the following roles:

- manager with overall responsibility for the IT system;
- security officer: individual with overall responsibility for the security of the service;
- system administrator: individual performing the IT system installation, configuration and maintenance;
- operator: individual performing the IT system's continuous operation, backup and restore;
- independent system auditor: individual who audits the logged, as well as archived dataset of the provider, responsible for verifying the enforcement of control measures the provider implements in the interest of operation that complies with regulations, moreover for the continuous auditing and monitoring of existing procedures.
- long term preservation officer: it is possible to decrypt an electronic document with the co-operation of two long term preservation officer. The long term preservation officers are responsible for the secure management of the decrypted electronic document, and for its destruction after use.
- officer responsible for long term preservation statement issuance: his duty is the issuance and certification of the long term preservation statements.

For the provision of trusted roles the manager responsible for the security of the Long-Term Preservation Provider formally appoints the Long-Term Preservation Provider 's employees. Only those persons may hold a trusted role who are in employment relationship with the Long-Term Preservation Provider. Trusted roles shall not be hold in the context of a commission contract.

5.2.2. Identification and Authentication for Each Role

The users managing the IT system of the Long-Term Preservation Provider have unique identification data, enabling secure identification and authentication of the users.

The users can only access the IT systems critical from the aspect of the provision of the certification service after identification and authentication.
The identification and authentication data are revoked without delay in case of the cessation of user rights.

5.2.3. Roles Requiring Separation of Duties

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

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

5.3. Personnel Controls

The Long-Term Preservation Provider takes care that its personnel policy, and its practices applicable to employing staff members intensify and support the reliability of the Long-Term Preservation Provider's operation. The objective of precautions applicable to personnel is to reduce the risk of human errors, theft, fraud and cases of misuse.
The Long-Term Preservation Provider addresses personnel security already during the hiring stage, including the conclusion of contracts, as well as their validation when they are being employed. In the case of all trusted roles, applicants have valid certificate of no criminal record at the time of the application. Every employee in a trusted role and external parties who get in contact with the Long-Term Preservation Provider 's services shall sign a non-disclosure agreement.
At the same time, the Long-Term Preservation Provider ensures for its employees obtaining as well as further developing of common, general know-how along with the specialized professional knowledge necessary for performing the various jobs.

5.3.1. Qualifications, Experience and Clearance Requirements

Each employee of the *Long-Term Preservation Provider* shall have the necessary education, practice and professional experience for the provision of his scope of activities. Even during recruitment, particular emphasis is given to the personality traits when selecting potential employees and only reliable persons can be hired for trusted roles.
Trusted roles can be held at the *Long-Term Preservation Provider* only by persons, who have no external influence and possess the necessary expertise validated by the *Long-Term Preservation Provider*.
The manager with overall responsibility for the IT system can only be a person who has:

- specialized degree (mathematics, physics college or university degree or a college/university degree acquired at an engineering department belonging to the technical field of science);
- at least three years of expertise in professional working experience related to information security.

5.3.2. Background Check Procedures

The *Long-Term Preservation Provider* only hires employees for trusted or leading roles, who:

- have a clean record and there's no proceeding in progress against them that may affect the impunity.

- are not subject to professional disqualifications prohibiting to exercise electronic signatures related services.

At the time of the appointment, shall the leading role holder Long-Term Preservation Provider employee with a statement, a trusted role holder employee with a certificate of good conduct less than 3 months old justify the clean criminal record.
The Long-Term Preservation Provider verifies the authenticity of the relevant information given in the applicant's CV during the hiring process.

5.3.3. Training Requirements

The *Long-Term Preservation Provider* trains the newly recruited employees, over the course of which they acquire

- basic PKI knowledge;
- the specifics and the way of handling the *Long-Term Preservation Provider* 's IT system;
- the necessary special knowledge for fulfilling their scope of activities;
- processes and procedures defined in the public and inner regulations of the *Long- Term Preservation Provider* ;
- the legal consequences of the individual activities;
- the applicable IT security regulations to the extent necessary to the specific scope of activities;
- the data protection rules.

Only employees having passed the training will gain access to the he production IT system of the *Long-Term Preservation Provider*.

5.3.4. Retraining Frequency and Requirements

The Long-Term Preservation Provider ensures that the employees have the necessary knowledge continuously, so if needed, further or repeater type of training is held.
Further training is held if there's a change within the processes or the IT system of the Long-Term Preservation Provider.
The training is adequately documented, from what the syllabus and the scope of the participator employees can be clearly determined.

5.3.5. Job Rotation Frequency and Sequence

No stipulation

5.3.6. Sanctions for Unauthorized Actions

The Long-Term Preservation Provider regulates the prosecution possibilities of the employees in an employment contract in case of failures, errors, accidental or intentional damage. If the employee – due to negligence or intentionally – violates their obligations, sanctions could be taken against him by the Long-Term Preservation Provider, which it sets out having regard to the offense and the consequences. The sanctions may include disciplinary proceedings, dismissal, revocation of appointment, criminal liability.

5.3.7. Independent Contractor Requirements

The same rules are applied to workers employed with a contractual relationship as to employees, when applicable.
The trusted role holder person shall be in an employment relationship with the *Long-Term Preservation Provider*.

5.4. Audit Logging Procedures

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

5.4.1. Types of Events Recorded

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

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

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

LONG TERM PRESERVATION

- information related to the upload of the e-dossiers and the validation of the electronic signatures within them;
- information related to the availability of data, integrity preservation, authenticity and non-repudiation preservation, maintenance of the information readability and deletion;
- information related to the e-dossier download, statement request fulfilment, and the handover of the archive to another provider;

LOGGING:

- the shutdown, restart of the logging system or some of its components;
- the modification of any parameter of the logging settings, for example the frequency, alert threshold, and the event to be examined;
- the modification or deletion of the stored logging data;
- the activities performed because of the logging system's failure.

SYSTEM LOGINS:

- successful logins, unsuccessful login attempts for trusted roles;
- in case of password based authentication:
- the change of the number of permitted unsuccessful attempts;
- reaching the limit of the permitted number of the unsuccessful login attempts in case of user login;
- readmission of the user blocked because of the unsuccessful login attempts;
- changing the authentication technique (for example from password based to PKI based).

KEY MANAGEMENT:

- all events for the entire life cycle of service keys (key generation, loading, saving, etc.);

DATA FLOWS:

- any kind of safety-critical data manually entered into the system;
- safety-relevant data, messages received by the system;

HSM:

- installing an HSM;
- removing an HSM;
- disposing, destructing an HSM;
- delivering HSM;
- clearing (resetting) an HSM;
- uploading keys, certificates to the HSM.

CONFIGURATION CHANGE:

- hardware;
- software;
- operating system;
- patch;

PHYSICAL ACCESS, LOCATION SECURITY:

- person entry to and exit from the security zone holding the CA components;
- access to a CA system component;
- a known or suspected breach of physical security;
- firewall or router traffic.

OPERATIONAL ANOMALIES:

- system crash, hardware failure;
- software failures;
- software integrity validation error;
- incorrect or wrongly addressed messages;
- network attacks, attack attempts;
- equipment failure;
- electric power malfunctions;
- uninterruptible power supply error;
- an essential network service access error;
- violation of the Qualified Long-Term Preservation Policy or the Long- Term Preservation Practice Statement ;
- deletion of the operating system clock.

OTHER EVENTS:

- appointment of a person to a security role;
- operating system installation;
- PKI application installation;
- initiation of a system;
- entry attempt to the PKI application;
- password modification, setting attempt;
- saving the inner database, and restore from a backup;
- file operations (for example creating, renaming, moving);
- database access.

5.4.2. Frequency of Audit Log Processing

The *Long-Term Preservation Provider* ensures the regular evaluation of the created logs.
The created daily log files shall be evaluated in the next working day if possible, but not later than 1 week.

The evaluation of the log files shall be performed by an independent system auditor with the right expertise, system privileges and appointment.
The *Long-Term Preservation Provider* uses also automatized tools to assist the evaluation of the electronic logs.
During the evaluation, the authenticity and integrity of the examined logs is ensured. During the evaluation, the system generated error messages are analysed.
The significant changes in the traffic should be analyzed with statistical methods.
The fact of the audit, the audit results and the measures taken in order to remove any deficiencies found shall be properly documented.

5.4.3. Retention Period for Audit Log

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

5.4.4. Protection of Audit Log

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

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

5.4.5. Audit Log Backup Procedures

Daily log files are created from the continuously generated log entries during the operation in each system.
The daily log files are archived in two copies after the evaluation and stored physically apart from each other, at separate sites for the required time.
The exact process of backups is defined in the backup regulations of the *Long-Term Preservation Provider*.

5.4.6. Audit Collection System (Internal vs. External)

The Long-Term Preservation Provider specifies the operation of its logging processes in its Long-Term Preservation Practice Statement.
The Long-Term Preservation Provider can use automatic audit and logging systems if it can ensure that they are active at the time of the system launch and they operate continuously until the system's shutdown.
If there's any anomaly in the automatic audit and logging systems, the operation of the Long-Term Preservation Provider will be suspended until the incident is resolved.

5.4.7. Notification of Event-causing Subject

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

5.4.8. Vulnerability Assessments

Vulnerability assessment is carried out each year by the *Long-Term Preservation Provider* to help discover potential internal and external threats, which may lead to unauthorized access. The occurrence probability of the event and the expected damage is be mapped too. It regularly assesses the

implemented processes, safety measures, information systems, so that they are able to correctly withstand the threats detected.
After evaluation of the detected errors, if necessary the defense systems is be amended to prevent similar mistakes in the future.

5.5. Records Archival

5.5.1. Types of Records Archived

The *Long-Term Preservation Provider* is be prepared to the proper secure long-term archiving of electronic and paper documents.
The *Long-Term Preservation Provider* archives the following types of information:

- every document related to the accreditation of the Long-Term Preservation Provider ;
- all issued versions of the Certificate Policies and Long-Term Preservation Practice Statement's;
- all issued versions of the Terms and Conditions;
- contracts related to the operation of the Long-Term Preservation Provider ;
- Every electronic and paper based log entry.

5.5.2. Retention Period for Archive

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

- *Long-Term Preservation Policy and Practice Statement*: 10 years and 6 months after the repeal;

5.5.3. Protection of Archive

The Long-Term Preservation Provider is bound to store every archived data in two copies at locations physically apart from efach other. Authentic paper or electronic copy can be made in accordance with the applicable law from the only authentic paper based copy of the document available.
Each of the two locations fulfil the requirements for archiving security and other requirements. During the preservation of the archived data, it shall be ensured that:

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

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

5.5.4.Archive Backup Procedures

The duplicate of the archived data is be stored at a physically separate location from the *Long-Term Preservation Provider*'s site as per Section 5.1.8.

5.5.5. Requirements for Time-stamping of Records

Every electronic log entry is provided with a time sign, on which the system provided time is indicated at least to one second precision.
The Long-Term Preservation Provider ensures that in its service provider systems, the system clock is at maximum different from the reference time with 1 second. The system time used for generating the time signal is synchronized to the UTC time at least once a day.
The daily log files shall be provided with a Time Stamp.
During the preservation of the archived data, if necessary (for example algorithm change expiration of the original Time Stamp) the authenticity of the data shall be ensured.

5.5.6. Archive Collection System (Internal or External)

The log entries shall be generated in the Long-Term Preservation Provider's protected computer system, and only the log files that are electronically signed can leave it.

5.5.7. Procedures to Obtain and Verify Archive Information

The Long-Term Preservation Provider can create the log files manually or automatically. In case of automatic logging system, the certified log files shall be generated daily.
The archived files shall be protected from unauthorized access.
Controlled access to the archived data shall be available to the eligible persons:

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

5.6. Compromise and Distaster Recovery

In case of a disaster, the Long-Term Preservation Provider takes all necessary measures in order to minimize the damage resulting from the shortfall of the service, and it restores the services as quickly as possible.
Based on the assessment of the incident that occurred, it takes the necessary amendments, corrective measures to prevent future occurrence of the incident.
Once the problem resolved, the event is reported to the supervisory authority.

5.6.1. Incident and Compromise Handling Procedures

The Long-Term Preservation Provider has a business continuity plan.
The Long-Term Preservation Provider establishes and maintains a fully functional backup system, which is at a safe distance from the primary location, geographically located at a different place and is independently capable of supplying the full range of services.
The Long-Term Preservation Provider continually tests the operation of the backup system and reviews its business continuity plans annually.
In case of a disaster, the availability of the services is restored as quickly as possible.

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

The IT systems of the Long-Term Preservation Provider is built from reliable hardware and software components. The critical functions are implemented using redundant system elements so that in the event of an item failure they shall be able to operate further.
The Long-Term Preservation Provider shall make a full daily backup of its databases and the generated log events.

The Long-Term Preservation Provider makes full backups as frequently as necessary to be able to restore the full service in case of a disaster.
The business continuity plan of the Long-Term Preservation Provider includes accurate requirements for the tasks to be performed in case of critical system component failure.
Once the problem resolved and the integrity restored, the Long-Term Preservation Provider will restart its services as soon as possible.

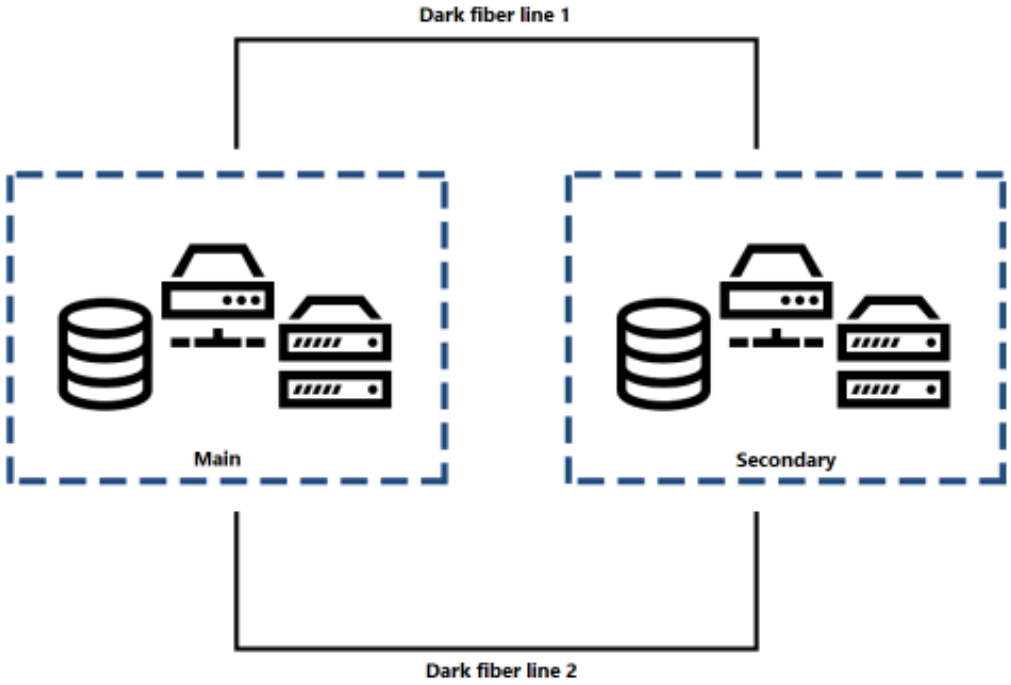
5.6.3. Business Continuity Capabilities After a Disaster

The tasks to be performed in case of service failure due to natural or other disaster are defined in the Long-Term Preservation Provider 's business continuity plan. In the event of disaster, the regulations shall come into force, the damage control and the restoration of the services shall begin.

The secondary services site is placed so far away from the primary site that a probable disaster cannot reach both locations simultaneously.
The Long-Term Preservation Provider notifies the affected users as quickly as possible in the event of the disaster.
After the restoration of the services, the Long-Term Preservation Provider restores its devices damaged during the disaster and the original service security level as quickly as possible.

5.6.4. Data Availability Controls

The *Long-Term Preservation Provider* uses an infrastructure which is placed in two sites which are interconnected via two redundant Dark Fiber lines, providing an extremely secured communication channel between the two data centers.



The preservation system is distributed across two physical data centers in active – standby topology.
All VM's hosting the components of the preservation system are backed up on a daily basis with a retention period of 30 days, as follows:

- On-Site - Using a dedicated storage device located in the main datacenter
- Off-Site – Using a dedicated storage device located in Trans Sped's secondary datacenter

All VM's hosting the components of the preservation system are replicated on a daily basis from the main datacenter to the secondary datacenter.
The preservation system is implemented in a highly available configuration using a clustered backend that provides mirrored copies of all documents and associated meta-data.
Application components are run on virtual servers hosted on a cluster in an active - standby configuration.
The persistence of the documents stored is mirrored on two dedicated and physically distinct storage devices.

Applications and data are backed up and replicated on dedicated infrastructures at the secondary data center site. Replication procedures are executed via redundant Dark Fiber data center interconnects between Main and Secondary.

5.7. Long-Term Preservation Service Termination

The Long-Term Preservation Provider complies with the requirements laid down in the legislation in case of service termination.
During the termination the priority tasks are:

- the Relying parties and the Subscribers shall be notified about the planned termination in time;
- the Long-Term Preservation Provider shall make every effort to ensure that at the latest by the service termination another provider takes over the records and service obligations;
- after the termination of the service, a full system backup and archiving shall be carried out;
- the archived data shall be handled over to the provider that takes over the services.

6.Technical Security Controls

The Long-Term Preservation Provider uses reliable systems and equipment protected against modification for the management of the whole life-cycle of electronic documents.
The capacity demands are continuously monitored and the future capacity demands aree estimated, so that the necessary availability of processing and storage needs is ensured.

6.1. Activation Data

6.1.1.Activation Data Generation and Installation

The Long-Term Preservation Provider's private keys are protected in accordance with the procedures, requirements defined in the used Hardware Security Module user guide and the certification documents.
In case of password based activation data usage, the passwords need to be sufficiently complex in order to ensure the required level of protection.

6.1.2. Activation DataProtection

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

6.1.3. Other Aspects of Activation Data

No stipulation.

6.2. Computer Security Controls

6.2.1. Specific Computer Security Technical Requirements

During the configuration and operation of the IT system of the Long-Term Preservation Provider the compliance with the following requirements is ensured:

- the user identity is verified before granting access to the system or the application;
- roles are assigned to users and it shall be ensured that all users only have permissions appropriate for its roles;
- a log entry is created for every transaction, and the log entries shall be archived;
- for the security-critical processes it is ensured that the internal network domains of the Long-Term Preservation Provider are sufficiently protected from unauthorized access;

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

6.2.2. Computer Security Rating

In order to provide IT security and service quality the Long-Term Preservation Provider implements a control system by internationally accepted methodologies, and the adequacy of those is certified by a certificate issued by an independent certification body.

6.3. Life Cycle Technical Controls

6.3.1. System Development Controls

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

- are commercial boxed software, designed and developed by a documented design methodology, or;
- custom hardware and software solutions developed by a reliable party for the Long- Term Preservation Provider during which design structured development methods and controlled development environment were used, or;
- open source software which comply with the security requirements and their adequacy is ensured by software verification and structured development and life-cycle management.

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

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

The Long-Term Preservation Provider with proper protection measures prevents malicious software to enter the devices used in the certification service.

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

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

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

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

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

The Long-Term Preservation Provider implements procedures for unauthorized change detection.

6.3.2. Security Management Controls

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

6.3.3. Life Cycle Security Controls

The Long-Term Preservation Provider ensures the protection of the used Hardware Security Modules during their whole life cycle:

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

6.4. Network Security Controls

The Long-Term Preservation Provider keeps its IT system configuration under strict control, and it documents every change including the smallest modification, development, software update too. The Long-Term Preservation Provider implements proper procedures for the detection of any hardware or software change, system installation, and maintenance occurred on the IT system. The Long-Term Preservation Provider checks the authenticity and integrity of every software component at their first loading.

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

- disables unused network ports and services;
- runs network applications unconditionally necessary for the proper operation of the IT system.

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

- within one week of receiving a request from the CA/Browser Forum;
- after any system or network changes that the CA determines are significant;
- at least once per quarter.

6.5. Time-stamping

The Long-Term Preservation Provider uses Time Stamps provided by a qualified time- stamp provider listed on the trusted list of one of the European Union member states for the protection of the integrity of the log files and other electronic files to be archived.

7. Compliance Audit and Other Assessments

The operation of the Long-Term Preservation Provider is supervised by a Supervisory Body (SB) in line with European Union regulations (eIDAS Regulation). The Long-Term Preservation Provider shall have a screening of its operations by an accredited CAB (Conformity Assessment Body) and shall send the detailed report of the audit to within 3 days from its receipt. During the screening it is to be determined whether the operation of the Long- Term Preservation Provider meets the requirements of the eIDAS Regulation [1] and the requirements of the applied Qualified Long-Term Preservation Policy (s) and the corresponding Long-Term Preservation Practice Statement(s).

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

- REGULATION (EU) No 910/2014 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 23 July 2014 on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC [1];
- ETSI EN 319 403 V2.2.2 (2015-08) Electronic Signatures and Infrastructures (ESI); Trust Service Provider Conformity Assessment - Requirements for conformity assessment bodies assessing Trust Service Providers; [9]
- ETSI EN 319 401 V2.1.1 (2016-02); Electronic Signatures and Infrastructures (ESI); General Policy Requirements for Trust Service Providers [8]
- 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
- Order no. 449 on the procedure for granting, suspending and withdrawing the status as a trust service provider, according to EU Regulation no. 910/2014 issued by the Minister of Communications and Information Society

The result of the assessment is a confidential document accessible only to authorized persons. The conformity certificate issued in accordance with the conformity assessment report shall be published on the webpage of the Long-Term Preservation Provider.
The Long-Term Preservation Provider reserves the right to inspect at any time involving an independent expert the operation of the providers who operate according to the present Qualified Long-Term Preservation Policy (s) in order to verify compliance with the requirements.

7.1. Frequency or Circumstances of Assessment

The Long-Term Preservation Provider shall have the conformance assessment carried out every two years, according to eIDAS Regulation.

7.2. Identity/Qualifications of Assessor

The Long-Term Preservation Provider can perform the internal audits with the help of its employees who hold the independent system auditor role.
The eIDAS and ETSI conformity assessment can be performed by an organization, which has a qualifying mandate issued by the national accreditation organization of an EU Member State.

7.3. Assessor's Relationship to Assessed Entity

External audit can be performed only by a person who:

- is independent from the owners, management and operations of the examined Long- Term Preservation Provider ;
- is independent from the examined organization, namely neither himself or herself nor his or her immediate relatives have any employment or business relationship with the Long-Term Preservation Provider.

7.4. Topics Covered by Assessment

The review shall cover at least the following areas:

- compliance with the legislation currently in force;
- compliance with technical standards;
- compliance with the Certification Policy and the Long-Term Preservation Practice Statement ;
- adequacy of the employed processes;

- documentation;
- physical security;
- adequacy of the personnel;
- IT security;
- compliance with the data protection rules.

7.5. Actions Taken as a Result of Deficiency

The independent auditor shall summarize the result of the screening in a detailed screening report that covers the tested system components, processes, and contains the evidence used in the screening and the auditor statements. The discrepancies revealed during the examination and the deadlines set for correcting them shall be recorded in a separate chapter of the report.
The independent auditor may record based on their severity the differences and discrepancies revealed during the examination:

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

The independent auditor shall report the revealed serious derogations without delay to the corresponding Supervisory Body that is authorized to take the necessary measures.
The Long-Term Preservation Provider shall answer the problems stated by the independent auditor in writing, and to report the measures taken to avert them at the occasion of the next authority review.

7.6. Communication of Results

The Long-Term Preservation Provider shall publish the summary report on the assessment. It is not needed to disclose the discrepancies revealed during the independent system assessment, they can be treated as confidential information.

8. Other Business and Legal Matters

8.1. Fees

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

8.1.1. Refund Policy

No stipulation.

8.2. Financial Responsibility

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

8.2.1. Insurance Coverage

In order to cover the costs associated with the termination of the service activity and to sustain reliability the Long-Term Preservation Provider shall meet the legal requirements for qualified trust service providers.

8.3. Confidentiality of Business Information

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

8.3.1. Scope of Confidential Information

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

8.3.2. Information Not Within the Scope of Confidential Information

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

8.3.3. Responsibility to Protect Confidential Information

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

The Long-Term Preservation Provider shall oblige its employees, subcontractors, affiliated partners to protect all confidential data by signing declaration of confidentiality or by contract. Circumstances when the Long-Term Preservation Provider may disclose the confidential data shall be determined case-by-case in the Long-Term Preservation Practice Statement.

8.4. Privacy of Personal Information

The Long-Term Preservation Provider shall take care of the protection of the personal data it manages. The operation and regulations of the Long-Term Preservation Provider shall comply with the requirements of Data Protection Regulations and national legislation.

8.4.1. Privacy Plan

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

8.4.2. Information Treated as Private

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

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

8.4.3. Information Not Deemed Private

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

8.4.4. Responsibility to Protect Private Information

The Long-Term Preservation Provider shall store securely and protect the personal data it manages. The data shall be protected by appropriate measures in particular against unauthorized access, alteration, and against disclosure.

The Long-Term Preservation Provider is generally responsible to comply with the requirements described in its Privacy policy and its liability extends to activities carried out by the subcontractors too.

8.4.5. Notice and Consent to Use Private Information

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

8.4.6. Disclosure Pursuant to Judicial or Administrative Process

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

8.4.7. Other Information Disclosure Circumstances

No stipulation.

8.5. Intellectual Property Rights

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

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

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

The rules of the application of the software provided for the use of the service by the Long- Term Preservation Provider shall be determined in the Long-Term Preservation Practice Statement.

8.6. Representations and Warranties

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

The Long-Term Preservation Provider ’s basic obligations is that it shall provide the services in line with the Qualified Long-Term Preservation Policy, this Long-Term Preservation Practice Statement and other regulations in the public domain, the contractual terms and conditions, furthermore corporate and security related internal regulations. These basic obligations are as follows:

- to establish the legal, regulatory, material, contractual, etc. framework appropriate for the service;
- to provide high standard and secure services in accordance with the applicable regulations;
- to continuously operate and audit organisations associated with the services (certification body, customer service, etc.);
- to abide by the procedures prescribed in the regulations, and to avoid or eliminate any potentially occurring incorrect operation;
- to ensure the Services to every applicant who accepts the terms and conditions specified in the regulations;
- to maintain public and proprietary records, as well as to make them continuously available to anybody over the internet.

8.6.1. 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 Policy, the service agreement and its attachments – in particular the general terms and conditions -– and the Long-Term Preservation Practice Statement.

8.6.2. 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 Stamps. During the verification of the validity for keeping the security level guaranteed by the Long-Term Preservation Provider it is necessary for the Relying Party to act with caution, so it is particularly recommended to:

- comply with the requirements, regulations defined in the present Qualified Long- Term Preservation Policy and the corresponding Long-Term Preservation Practice Statement;
- use reliable IT environment and applications;
- verify the based on the current CRL or OCSP response;
- take into consideration every restriction in relation to the usage which is included in the Qualified Long-Term Preservation Policy and the Long-Term Preservation Practice Statement.

8.6.3. Representations and Warranties of Other Participants

No stipulation.

8.7. Disclaimers of Warranties

The Long-Term Preservation Provider excludes its liability if:

- it is unable to provide information or fulfil communication obligations due to the problems of the Internet, or part of it;
- the damage comes from a vulnerability or error of the cryptographic algorithms accepted by the customers.

8.8. Limitations of Liability

No stipulation.

8.9. Indemnities

8.9.1. Indemnification by the Long-Term Preservation Provider

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

8.9.2. Indemnification by Subscribers

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

8.9.3. Indemnification by Relying Parties

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

8.10. Term and Termination

8.10.1. Term

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

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

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

8.11. Individual Notices and Communications with Participants
The Long-Term Preservation Provider shall operate a customer service in order to maintain contact with its Clients.

8.12. Amendments
The Long-Term Preservation Provider reserves the right to change the Qualified Long-Term Preservation Policy in a controlled way in case of the change of normative rules, safety requirements, market conditions or other circumstances.
In exceptional cases (for example the need for taking critical security measures) the changes can be put into force with immediate effect.

8.12.1. Procedure for Amendment
The Long-Term Preservation Provider reviews the Qualified Long-Term Preservation Policy annually or in case of exceptional request for change with priority and performs the necessary changes. The document will receive a new version number even after the smallest change and by taking into account the time required by the endorsement process, the planned date of coming into effect will be determined too.
The accepted document will be published on the webpage of the Long-Term Preservation Provider 30 days prior to the planned entry into force date and it will be sent to the Supervisory Body.

8.12.2. Circumstances Under Which OID Must Be Changed
The Long-Term Preservation Provider issues a new version number in case of even the smallest change to the Qualified Long-Term Preservation Policy, which is part of the document identifier (OID), so any change to the document will result in an OID change, namely two documents – entered into force – with different content cannot have the same OID.

8.13. Dispute Resolution Provisions
The Long-Term Preservation Provider shall aim for the peaceful and negotiated settlement of the disputes arising from its operation. The settlement shall follow the principle of gradual approach.

8.14. Governing Law
The Long-Term Preservation Provider at all times operates in accordance with the eIDAS Regulation and all Romanian national rules on digital trust services

8.15. Compliance with Applicable Law
The present Qualified Long-Term Preservation Policy is compliant with the following regulations.

- REGULATION (EU) No 910/2014 of the EUROPEAN PARLIAMENT AND OF THE COUNCIL of 23 July 2014 on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC [1];

- ETSI EN 319 401 V2.1.1 (2016-02); Electronic Signatures and Infrastructures (ESI); General Policy Requirements for Trust Service Providers [8];

8.16. Miscellaneous Provisions

8.16.1. Entire Agreement

No stipulation.

8.16.2. Assignment

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

8.16.3. Severability

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

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

The Long-Term Preservation Provider is entitled to claim payment for damages and attorney fees for reimbursement of the damages, losses, expenses caused by its partners. If in a particular case the Long-Term Preservation Provider does not exercise its claim for damages that does not mean that in similar cases in the future or in case of violation of other provisions of the present Qualified Long-Term Preservation Policy, it would waive the enforcement of claims for damages.

8.16.5. Force Majeure

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

8.17. Other Provisions

No stipulation.

REFERENCES

[1] Regulation (EU) No 910/2014 of the European Parliament and of the Council of 23 July 2014 on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC.

[2] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation)

[3] ETSI EN 319 401 V2.1.1 (2016-02) Electronic Signatures and Infrastructures (ESI); General Policy Requirements for Trust Service Providers

[4] 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

[5] ETSI TS 101 533-1 V1.3.1 (2012-04) Electronic Signatures and Infrastructures (ESI); Information Preservation Systems Security

[6] 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

[7] ETSI TS 119 512 V1.1.1 (2020-01) Electronic Signatures and Infrastructures (ESI); Protocols for trust service providers providing long-term data preservation services

[8] Order no. 449 on the procedure for granting, suspending and withdrawing the status as a trust service provider, according to EU Regulation no. 910/2014 issued by the Minister of Communications and Information Society