Preservation Evidence Policy for timeproof “TR-ESOR SUITE”

Designation	Preservation Evidence Policy for TR-ESOR
Abbreviation	TP_TR-ESOR_PEP_[BSI TR-ESOR-PEPT]
Version	v1.3 for v1.2.2 TR-ESOR and Appendix C1 and APP
Date	14.01.2022

based on

BSI Technical Guideline 03125

Preservation of Evidence of Cryptographically Signed Documents

Annex TR-ESOR-PEPT:
Preservation Evidence Policy Template for TR-ESOR (PEPT)

Designation	Preservation Evidence Policy Template for TR-ESOR (PEPT)
Abbreviation	BSI TR-ESOR-PEPT
Version	1.2.1 and higher (on base of the eIDAS-Regulation and the ETSI Preservation Standards with a new certification scheme) - Preliminary
Datum	18.11.2021

Manufacturer
timeproof gmbh
Münchnerstr. 33, 82319 Starnberg
E_TR_ESOR@timeproof.de (hier war ein Leerzeichen in der Adresse)
T +49.89.21 53 95-078
W timeproof.de

Federal Office for Information Security
Post Box 20 03 63
53133 Bonn
Phone: +49 228 99 9582-0
E-Mail: tresor@bsi.bund.de
Internet: https://www.bsi.bund.de

Content

Table of Figures

Table List

1. Introduction

1.1 Overview

1.1.1 Purpose

Trust services, as specified in Regulation (EU) No 910/2014 **[**Fehler! Verweisquelle konnte nicht gefunden werden.**]** (short: eIDAS), shall give participants of electronic commerce confidence in the security of these trust services. This confidence is expected to result from a set of procedures, processes and security measures, the Trust Service Provider (TSP) has established in order to minimize the operational and financial threats and risks associated.

eIDAS distinguishes two trust levels with respect to trust services and providers of trust services:

- normal trust services and trust service providers (TSP) and
- **qualified** trust services and trust service providers (**QTSPs**) that need to fulfil additional legal requirements and are subject to periodical independent third party conformity assessments by accredited conformity assessment bodies (CAB).

(Q)TSP means TSP or QTSP.

Especially **qualified** trust services and QTSPs will fulfil such high expectations of participants. The following (qualified) trust services are defined in **[**Fehler! Verweisquelle konnte nicht gefunden werden.**]**:

- creation of (qualified) certificates for signatures, seals and website authentication,
- creation of (qualified) electronic timestamps,
- validation of (qualified) electronic signatures and seals,
- preservation of (qualified) electronic signatures and seals, and
- (qualified) electronic registered delivery service.

To support the eIDAS-conformant implementation of (qualified) trust services, ETSI has issued a series of standards with policy requirements that a (qualified) trust service provider may implement to achieve conformance to **[**Fehler! Verweisquelle konnte nicht gefunden werden.**]**.

[Fehler! Verweisquelle konnte nicht gefunden werden.**]** defines policy and security requirements for operation and management practices of a (Q)TSP, which provides long-term preservation of digital signatures or general data using digital signature techniques, called **Preservation Service Provider (PSP)**.

To-Do-1.1.1-1) According to section 6.5 of **[**Fehler! Verweisquelle konnte nicht gefunden werden.**],** PSP shall have a **Preservation Evidence Policy (PEP)** in place, which consists of a set of rules that specify the requirements and the internal processes to generate or to validate a preservation evidence. #Answer: This will be done by the PSP.

To-Do-1.1.1-2) In case the PSP uses a **TR-ESOR [**Fehler! Verweisquelle konnte nicht gefunden werden.**]** certified product for generation and validation of preservation evidences, the following three-tiered process of generation of a PEP and a PSPS (1. BSI-PEPT → 2. PEP of the TR-ESOR-Product Manufacturer → 3. PSPS of the PSP) shall be fulfilled:

#Answer: This will be done by the manufacturer and the PSP.

a) BSI published this **BSI Preservation Evidence Policy Template (PEPT)**;

b) The TR-ESOR-Product Manufacturer shall

   a. copy this PEPT in his PEP,

   b. precise his new PEP in all cases, where there were still alternatives mentioned in the PEPT,

   c. fulfil all the tables, where there is written "<Must be filled in by the TR-ESOR-Product Manufacturer>",

   d. publish his currently created PEP.

c) The Preservation Service Provider (PSP) shall

   a. fulfil in the PEP of his TR-ESOR-Product Manufacturer all the tables, where there is written "<Must be filled in by the PSP>" or there is written "<Must be filled in by the TR-ESOR-Product Manufacturer or PSP>" and the TR-ESOR-Product Manufacturer did not fill this table, #Answer: This will be done by the manufacturer.

   b. include the supplemented PEP of his TR-ESOR-Product Manufacturer in his Preservation Service Practice Statement, #Answer: This will be done by the PSP.

   c. publish his currently created PSPS and the supplemented PEP, originally provided by this TR-ESOR-Product Manufacturer, as his PEP. #Answer: This will be done by the PSP.

The chapters 1, 2, 4.3, 4.4, 4.6, 4.7, 5.4 and 7 in their PEP(s) must then be taken into account and supplemented or adapted by the TR-ESOR-Product Manufacturer and PSP, if necessary.

This PEPT and the PEPs of the TR-ESOR-Product Manufacturer are structured according to **[**Fehler! Verweisquelle konnte nicht gefunden werden.**]**, although chapters 3 to 6 (except chapter 4.3, 4.4, 4.6, 4.7, 5.4) and 8 to 9 of RFC 3647 are not applicable and do not need to be filled by the TR-ESOR-Product Manufacturer.

When the PSP supplements the PEP of the TR-ESOR-Product Manufacturer and includes it in his (published) PSPS), then the chapters 3 to 6 and 8 to 9 have to be considered by the PSP too.

Whenever an adjustment has to be made, this is highlighted in the following text under "To-Do".

A TR-ESOR-Product Manufacturer using PEP(s) on base of PEPT, as described before,

and a PSP using

a) TR-ESOR certified product(s) and

b) PEP(s) and PSPS(s), created on the base of the PEPT, as described before,

fulfil the requirements of section 6.5 of **[**Fehler! Verweisquelle konnte nicht gefunden werden.**]**.

1.1.2 Scope of the document

The document describes a Preservation Evidence Policy Template (PEPT) that is supplemented and included in the PEP of the TR-ESOR-Product Manufacturer and this PEP of the TR-ESOR-Product Manufacturer is then supplemented and included in the PSPS of the PSP using a TR-ESOR-Product pursuant to clause 1.1.1. To better assign the scope, TR-ESOR and its components are briefly described here (extracted from **[**Fehler! Verweisquelle konnte nicht gefunden werden.**]**):

An overall system for the storage and preservation of cryptographically signed documents therefore includes elements (components) and processes which are used for

1) "*The preservation **over long periods of time, using digital signature techniques**, of the **ability to validate a digital signature**, of the ability to **maintain its validity status** and of the ability to **get a proof of existence** of the associated signed data as they were at the time of the submission to the Preservation Service even if later the signing key becomes compromised, the certificate expires, or cryptographic attacks become feasible on the signature algorithm or the hash algorithm used in the submitted signature.*
   ***NOTE 1:** A qualified Preservation Service for qualified electronic signatures or seals as per Regulation (EU) No 910/2014 [i.2] for which the status of technical validity needs to be preserved, is covered in this case.*
   ***NOTE 2:** The validity status of a signature means the status of the signature that will not change over time. Such a status may be valid (TOTAL_PASSED according to [**Fehler! Verweisquelle konnte nicht gefunden werden.**], [i.6]) or invalid (TOTAL_FAILED and certain cases for INDETERMINATE according to [**Fehler! Verweisquelle konnte nicht gefunden werden.**], [i.6]).*
   NOTE 3: "Digital signature techniques" designates techniques based on digital signatures, time-stamps or evidence records.
2) *The provision of a proof of existence of digital objects, whether they are signed or not, using digital signature techniques (digital signatures, timestamp tokens, evidence records, etc.)"* (**[ETSI TS 119 511]**, clause 1)

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" pursuant to **[**Fehler! Verweisquelle konnte nicht gefunden werden.**]**, even if these elements (components) and processes are not described in this PEP.

Within the following figure is an overview of the typical elements (components) with the positioning of the TR-ESOR-Product and Preservation Service:

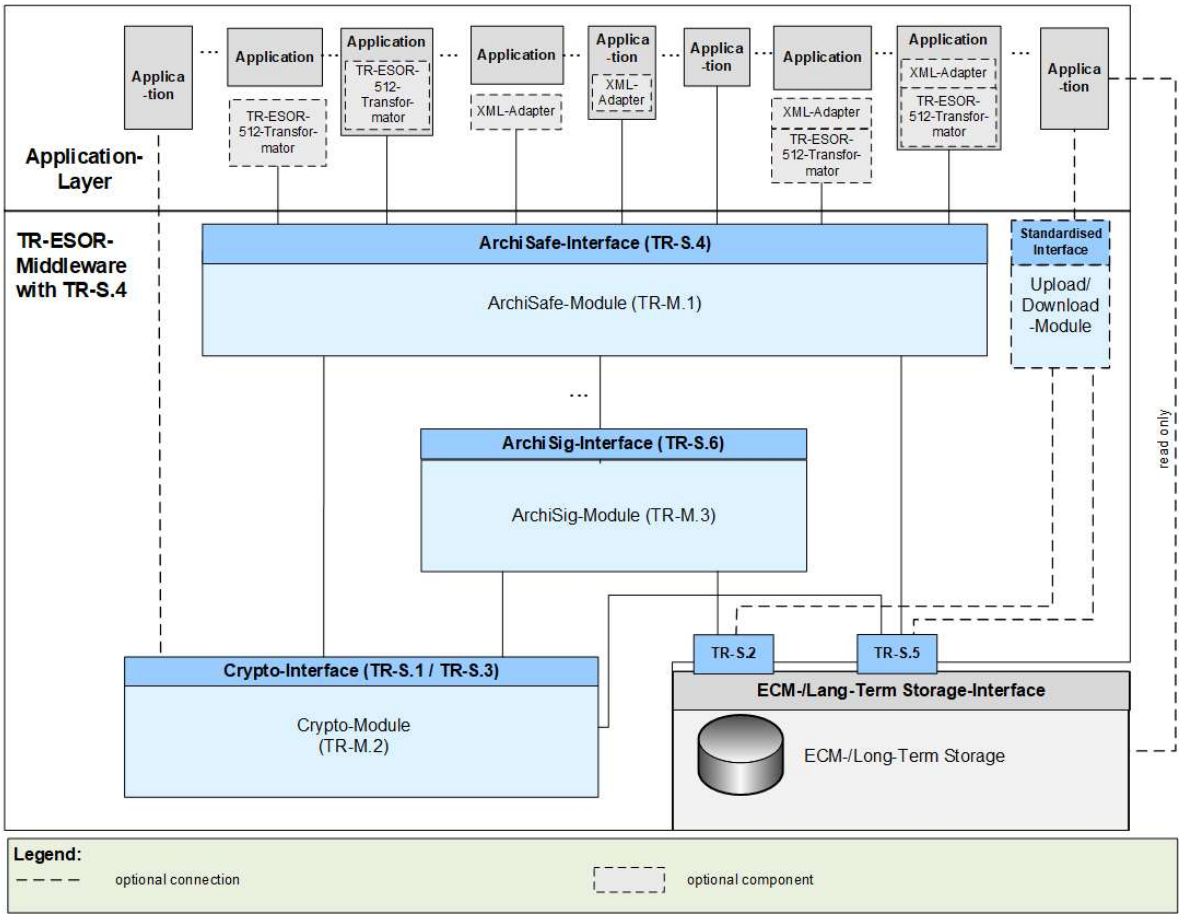

Figure 1: Overview – Positioning of the TR-ESOR-Middleware with S.4-interface

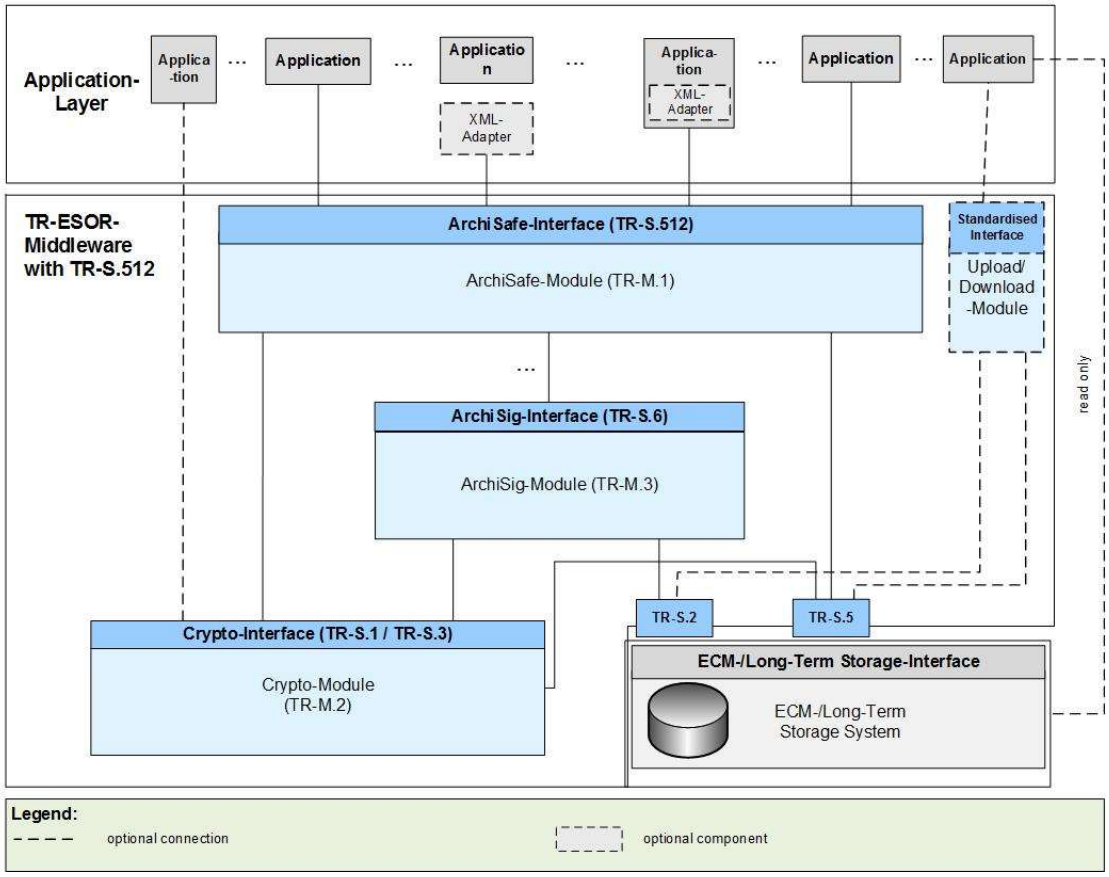

Figure 2: Positioning of the TR-ESOR-Middleware with 512-interface

At this point, important to know is the positioning of the TR-ESOR-Middleware. The TR-ESOR-Middleware is limited to the functions, interfaces and components necessary for the preservation of evidence. Functions, interfaces and components going beyond this are permissible, provided they do not restrict the functions for preserving the value of evidence or endanger their security.

The TR-ESOR-Middleware includes neither the custom applications nor the actual storage or archiving systems, but rather bundles the necessary functions for the cryptographic preservation of evidence. A TR-ESOR-Middleware that complies with this Technical Guideline is capable of maintaining the probative value of signed and unsigned electronic data or documents for the entire duration of the retention period and provides the functions to preserve the evidence of cryptographically signed documents.

Therefore, securing the availability and readability of electronic documents cannot be guaranteed by the TR-ESOR-Middleware at the centre of this PEPT, but must be supported by suitable technical and organisational measures in the upstream IT applications or in the ECM-/ong-term storage systems used. The participants of a Preservation Service are two parties:

- Party of the Preservation Middleware, e.g. TR-ESOR-Product Manufacturer,
- Party of the Trust Service Provider (TSP),
    - the Preservation Trust Service Provider itself,
    - external Trust Service Providers
        - Validation Service

- Time Stamping Authority
- Certificate Status Authority.

Party of the Application Layer is the user of the Preservation Service. The Preservation Service uses the long-term storage.

In Figure 3 the main components of the TR-ESOR-Middleware and its connections to the other participants are outlined:

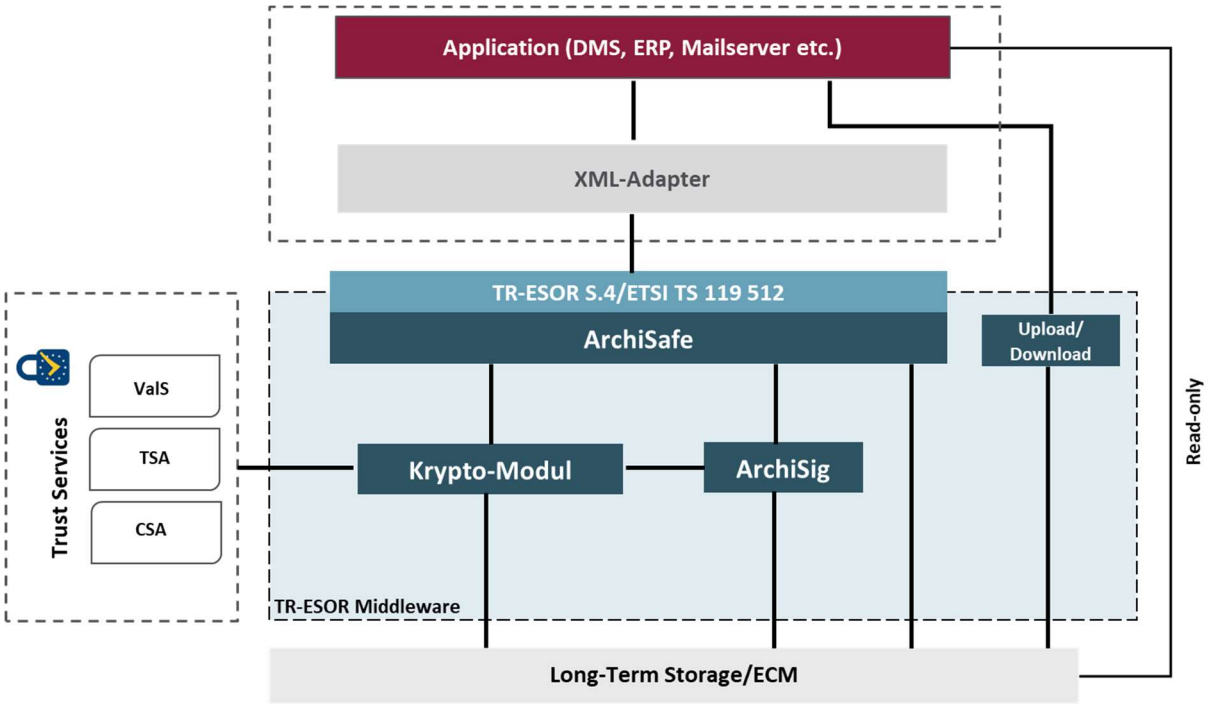

Figure 3: Components of TR-ESOR

Figure 3 shows technical components (e.g. ArchiSafe) of the TR-ESOR-Middleware. But following the scope of this PEPT the details (description of components and related functions) of the technical components will be found in the separated documentations published on the website of the BSI[1].

The "TR-S.4" (short: S.4) and "TR-S.512" (short: S.512) circled within TR-ESOR are interfaces according to a corresponding standard. Here, "S.4" is defined according to **[**Fehler! Verweisquelle konnte nicht gefunden werden.**]**. "S.512" is defined according to **[**Fehler! Verweisquelle konnte nicht gefunden werden.**]** and profiled in **[TR-ESOR-TRANS].** The interface profiles are considered in chapter 7.2.

The TR-ESOR-Middleware supports the preservation of cryptographically signed or unsigned documents. To do so, the following minimal functional requirements are fulfilled:

- the storage of cryptographically unsigned and cryptographically signed data, possibly including already existing Evidence Records pursuant to **[**Fehler! Verweisquelle konnte nicht gefunden werden.**]** or **[**Fehler! Verweisquelle konnte nicht gefunden werden.**]**,
- the retrieval of Archival Information Package (AIP), also called preservation object

[1] DE: bsi.bund.de/tr-esor, EN: bsi.bund.de/EN/tr-esor

container,

- the retrieval of suitable Evidence Records of the authenticity and integrity of the stored data,
- the deletion of data as Archival Information Package,
- Only TR-ESOR-V1.2.2 or higher: the traceable update of already archived metadata and payload data and credentials[2], which also includes the addition of further metadata and payload data to already archived data structures,
- Only TR-ESOR V1.3 and higher: Verifying the Archival Information Package including the supplemental evidence data and technical evidence records (Evidence Records) that are contained therein or were additionally transferred
- ~~Only TR-ESOR V1.3 and higher: The retrieval of Preservation Profiles according to ([**ETSI TS 119 512**], RetrieveInfo).~~

Furthermore, the following functions are possible options:

- ~~Targeted retrieval of individual data elements from an individual archive data object (group) without having to return the respective entire archive data object (group) to the IT application.~~[3]
  - Only TR-ESOR V1.2.1: the traceable update of already archived metadata and payload data, which also includes the addition of further metadata and payload data to already archived data structures.
- Only TR-ESOR V1.2.1 and V1.2.2 Verifying the Archival Information Package including the supplemental evidence data and technical evidence records (Evidence Records) that are contained therein or were additionally transferred.
- ~~Only TR-ESOR V1.3 and higher: The retrieval of data and event logs according to ([**ETSI TS 119 512**], RetrieveTrace).~~

1.2 Document Name and Identification

This PEP is named with “Preservation Evidence Policy for TR-ESOR” based on “Preservation Evidence Policy Template for TR-ESOR” (PEPT).

This PEPT is identified with the following URL:

http://www.bsi.bund.de/DE/tr-esor/prespolicy/default/1.0

To-Do-1.2-1) : The TR-ESOR-Product Manufacturer shall determine a unique OID of his supplemented PEP, based on the PEPT and publish this supplemented PEP with this OID.

To-Do-1.2-2) : The PSP shall also determine a unique OID of his completed PEP and publish this completed PEP with this OID. Answer: OID is published in the PEP

This PEPT and the PEPs, derived from the PEPT are structured according to **[**Fehler! Verweisquelle konnte nicht gefunden werden.**]**.

[2] Supplemental evidence data and technical evidence records

[3] This function can be used, for example, to create search indices, determine the object owner, determine the minimum retention period, or retrieve electronic signatures.

1.3 Preservation Service Participants

Beside the Preservation Client and the Preservation Service, the following external (Q)TSPs are used for the TR-ESOR-Middleware:

- Time Stamping Authority issuing qualified timestamps,
- Validation Service to validate (qualified) electronic signatures, seals or timestamps,
- Certificate Status Authority to validate certificates.

More information are to be found in clause 7.7.3.

1.4 Preservation Usage

This PEPT is reduced to the case "Preservation service with storage [WST]" pursuant to **[**Fehler! Verweisquelle konnte nicht gefunden werden.**]**, clause 4.1.2.

The Preservation Service is used to fulfil the following goals:

- "*http://uri.etsi.org/19512/goal/pgd*
  The preservation goal "Preservation of General Data" (PGD) provides a proof of existence over long periods of time of the submission data object (SubDO) submitted to the Preservation Service.
  ***NOTE 1:** The PGD goal does not distinguish between signed and unsigned data.*
- *http://uri.etsi.org/19512/goal/pds*
  The preservation goal "Preservation of Digital Signatures" (PDS) extends over long periods of time the ability to validate a digital signature, to maintain its validity status and to get a proof of existence of the associated signed data.
- *http://uri.etsi.org/19512/goal/aug*
  The preservation goal "Augmentation" (AUG) indicates that the Preservation Service supports the augmentation of submitted preservation evidences."[4]

1.5 Policy administration

This PEPT is subject to continuous further improvement and adaptation to new requirements. The continuation must be orderly, i.e. agreed versions of the PEPT must be released in a formal act. Formally released versions or patches are published on the BSI website. The publication is regulated.

The Federal Office for Information Security (BSI) is technically responsible for the formulation and supervision of these PEPTs.

Address: Bundesamt für Sicherheit in der Informationstechnik (BSI)
Post Office Box 20 03 63
53133 Bonn
Tel.: +49 228 99 9582-0
E-Mail: tresor@bsi.bund.de
Internet: https://www.bsi.bund.de

[4] See **[**Fehler! Verweisquelle konnte nicht gefunden werden.**, clause 4.2]**

1.6 Definitions and acronyms

Abbreviation	Keyword
[ABC]	for: document ABC
AOID	Archive Data Object Identifier
ASiC-AIP	Associated Signature Container (ASiC)- Archival Information Package
ATS	ArchiveTimeStamp
AUG	Augmentation
CA	Certification Authority
CAB	Conformity Assessment Body
CRL	Certificate Revocation List
DMS	Data Management System
eIDAS	REGULATION (EU) No 910/2014 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 23 July 2014 on electronic identification and trust service for electronic transactions in the internal market and repealing Directive 1999/93/EC
et. seq.	et sequence
ECM	Enterprise Content Management
EU	European Union
EUMS	European Union Member State
GDPR	General Data Protection Regulation
IS-Policy	Information Security Policy (see e.g. **[EN 319 401]**, chapter 6.3.)
IT	Information Technology
LXAIP	Logically XML formatted Archival Information Package
NC	Non-Conformity
OCSP	Online Certificate Status Protocol
OID	Object Identifier
OVR	Overall
PDS	Preservation of Digital Signature
PEP	Preservation Evidence Policy
PEPT	Preservation Evidence Policy Template
PGD	Preservation of General Data
PI	Potential for Improvement
PO	Preservation Object
POC	Preservation Object Container
PP	Preservation Profiles
PRP	Preservation Service Protocol
PS	Preservation Service
PSP	Preservation Service Provider
PSPS	Preservation Service Practice Statement
QES	Qualified Electronic Signature or qualified electronic seal
QTSP	Qualified Trust Service Provider
(Q)TPS	TSP or QTSP
QPSP	Qualified Preservation Service Provider

Abbreviation	Keyword
(Q)PSP	PSP or QPSP
R	Recommendation
SA	Subscriber Agreement
SSL	Secure Sockets Layer
SubDO	Submission Data Object
SVP	Signature Validation Policy
T&C	Terms and Conditions
TL	Trusted List
TR-ESOR	DE: Technische Richtlinie zur Beweiserhaltung kryptographisch signierter Dokumente EN: Technical Guideline for Preservation of Evidence of Cryptographically Signed Documents
TSA	Time-Stamping Authority
TSP	Trust Service Provider
TS-Policy	Trust Service Policy
TSPS	Trust Service Practice Statement (see e.g. **[EN 319 401]**, chapter 6.1.)
UTC	Coordinated Universal Time
WOS	Without Storage
WST	With Storage
WTS	With Temporary Storage
XAIP	XML formatted Archival Information Package
XML	Extensible Markup Language

Table 1: Keywords and Abbreviations

2. Publication and Repository Responsibilities

2.1 Repositories

The valid versions of this PEP Template, module descriptions of ArchiSafe, ArchiSig and Krypto and other relevant documents are available for download on the TR-ESOR websites of BSI:

English at https://www.bsi.bund.de/EN/tr-esor , in German at https://www.bsi.bund.de/tr-esor .

The versions are listed with a description of the extension or change and the date in a list of changes available on the TR-ESOR web pages of BSI.

2.2 Storage of preservation evidences or publication of the preservation evidence policy template

TR-ESOR as middleware of the Preservation Service is responsible for preservation of evidences of cryptographically signed and unsigned documents based on Evidence Records based on Merkle-Hash-trees defined in **[**Fehler! Verweisquelle konnte nicht gefunden werden.**]** ~~or **[RFC6283]**~~ (see **[**Fehler! Verweisquelle konnte nicht gefunden werden.**]**, clause 3 4).

To-Do-2.2-1) The ArchiSig-Module shall have a secure data storage, that is part of or allocated to the ArchiSig-Module, to store the *ArchiveTimeStamp* and the archive data object ID (see **[**Fehler! Verweisquelle konnte nicht gefunden werden.**],** Chapter 3.1, (A3.1-6)) in such a way that concerning the hash trees a hash value corresponding to an AOID and, if applicable, VersionID can be identified with absolute certainty at any time".
#Answer: See the "2.3.6 Ablage der Evidence Records im sicheren Speicher des ArchiSig-Moduls", p.22 [#HB_TP_TR-ESOR_SUITE].

To-Do-2.2-2) The BSI PEP template PEPT shall be published on the German BSI web site https://bsi.bund.de/tr-esor and on the English web site www.bsi.bund.de/EN/tr-esor. #Answer: The PEP will be published on www.timeproof.de/BSI_TR-ESOR .

2.3 Time or frequency of publication

As described in chapter 1.5 this PEP template administration follows a standardised and regular process. The PEP template and other documents, mentioned in chapter 2.1, can only be edited and published from authorized personnel of the BSI.

A change/update of the actual PEP template version will take place, if at least a new version of **[TR-ESOR]** is published.

To-Do-2.3-1) If the used cryptographic algorithm(s) and its parameter(s) have to be changed, e.g. on base of **[**Fehler! Verweisquelle konnte nicht gefunden werden.**]** and **[SOG_IS]**, the PEP of the TR-ESOR-Product Manufacturer shall be changed. #Answer: This will be done by the manufacturer.

To-Do-2.3-2) Then the PSP shall supplement this new PEP of his TR-ESOR-Product Manufacturer and include it in his PSPS as soon as the cryptographic algorithm(s) in his Preservation Service in production is(are) changed (see **(OVR-6.4-13, OVR-6.4-14))** and publish his newly completed PSPS and PEP. #Answer: This will be done by the PSP.

See also:

"*If one of the algorithms or parameters which were used in a preservation evidence, is thought to become less secure or the validity of a relevant certificate is going to expire, the preservation evidence shall be augmented by the preservation service according to a new version of the preservation evidence policy during the preservation period" (**[ETSI TS 119 511]**,* **OVR-7.14-02** *).*

To-Do-2.3-3) In addition, if one or more external trust service providers are to be changed, the PSPS and PEP of the PSP shall be changed. #Answer: This will be done by the PSP and the manufacture.

3. Identification and Authentication

Not applicable for Preservation Evidence Policy.

3.1 Naming

Not applicable for Preservation Evidence Policy.

3.2 Initial identity validation

Not applicable for Preservation Evidence Policy.

3.3 Identification and Authentication for modification requests

Not applicable for Preservation Evidence Policy.

3.4 Identification and Authentication for deleting requests

Not applicable for Preservation Evidence Policy.

4. Preservation Service Life-Cycle Operational Requirements

4.1 Preservation Service Application

Not applicable for Preservation Evidence Policy.

4.2 Preservation Service application processing

Not applicable for Preservation Evidence Policy.

4.3 Preservation Evidence Record issuance

The TR-ESOR-Middleware of the PSP may create Preservation Evidence Records pursuant to (**[**Fehler! Verweisquelle konnte nicht gefunden werden.**]** clause 4.2 or **[**Fehler! Verweisquelle konnte nicht gefunden werden.**]** clause 3.2), **([TR-ESOR-M.3])** and (**[**Fehler! Verweisquelle konnte nicht gefunden werden.**])**.

To-Do-4.3-1) The TR-ESOR-Product Manufacturer shall precise in his PEP in chapter 7.7.1, whether his Preservation Product supports **[**Fehler! Verweisquelle konnte nicht gefunden werden.**]** ~~or **[**Fehler! Verweisquelle konnte nicht gefunden werden.**]** or both~~ Evidence Record formats. #Answer: This will be done by the manufacturer.

The algorithm is chosen on base of **[**Fehler! Verweisquelle konnte nicht gefunden werden.**]** pursuant to (**[**Fehler! Verweisquelle konnte nicht gefunden werden.**]**, clause 4, (A4.0-1)). #Answer: This will be done by the manufacturer.

To-Do-4.3-2) The TR-ESOR-Product Manufacturer shall precise in his PEP in clause 7.7.1, which algorithms currently are used by his Preservation Product. #Answer: This will be done by the manufacturer. #Answer: This will be done by the manufacturer.

To-Do-4.3-3) The PSP shall complete the supplemented PEP of the TR-ESOR-Product Manufacturer, include the completed PEP in his PSPS and then publish his completed PEP and his completed PSPS. #Answer: This will be done by the PSP.

More details are to be found in clause 7.7.1.

NOTE 1: Therefore, (**[**Fehler! Verweisquelle konnte nicht gefunden werden.**]**, OVR-6.5-03 and OVR-6.5-04) are fulfilled by this PEPT, supplemented by the TR-ESOR-Product Manufacturer and PSP later on.

4.4 Preservation Evidence Record acceptance

The TR-ESOR-Middleware of the PSP validates Preservation Evidence Records pursuant to (**[**Fehler! Verweisquelle konnte nicht gefunden werden.**]** clause 4.3/5.3 or **[**Fehler! Verweisquelle konnte nicht gefunden werden.**]** clause 3.3) and **[Fehler! Verweisquelle konnte nicht gefunden werden.]**, clause 3.6, clause 5.2).

NOTE 1: Whether **[**Fehler! Verweisquelle konnte nicht gefunden werden.**]** or **[**Fehler! Verweisquelle konnte nicht gefunden werden.**]** or both Evidence Record formats are supported by the Preservation Product, is to be stated by the TR-ESOR-Product Manufacturer or PSP in chapter 7.7.1, Table 3 in their PEP.

More details are to be found in clause 7.7.2

NOTE 2: Therefore, **[**Fehler! Verweisquelle konnte nicht gefunden werden.**]**, OVR-6.5-06 is fulfilled by this PEPT and the supplemented PEP of the TR-ESOR-Product Manufacturer and the completed PEP of the PSP.

4.5 Preservation Evidence Record usage

Not applicable for Preservation Evidence Policy.

4.6 Preservation Evidence Record renewal

The TR-ESOR-Middleware of the PSP augments Preservation Evidence Records pursuant to (**[**Fehler! Verweisquelle konnte nicht gefunden werden.**]** ~~or [Fehler! Verweisquelle konnte nicht gefunden werden.]~~ and **[**Fehler! Verweisquelle konnte nicht gefunden werden.**]** and **[**Fehler! Verweisquelle konnte nicht gefunden werden.**])** by time-stamp renewal and hash-tree renewal.

How the time-stamp renewal and hash-tree renewal are performed is specified in clause 4.2.1 and 4.2.2 of **[**Fehler! Verweisquelle konnte nicht gefunden werden.**]** and clause 5 of **[**Fehler! Verweisquelle konnte nicht gefunden werden.**]**.

The algorithm is chosen on base of **[**Fehler! Verweisquelle konnte nicht gefunden werden.**]** pursuant to (**[**Fehler! Verweisquelle konnte nicht gefunden werden.**]**, clause 4, (A4.0-1)). More details are to be found in clause 7.7.4.

NOTE 1: The decision, whether **[**Fehler! Verweisquelle konnte nicht gefunden werden.**]** or **[**Fehler! Verweisquelle konnte nicht gefunden werden.**]** or both Evidence Record formats are supported by the TR-ESOR-Product Manufacturer and PSP, is to be found in chapter 7.7.1, **Fehler! Verweisquelle konnte nicht gefunden werden.** in the supplemented PEP of the TR-ESOR-Product Manufacturer.

To-Do-4.6-1) The TR-ESOR-Product Manufacturer shall precise in clause 7.7.4, Table 10, which algorithms currently are used by this Preservation Product. #Answer: This will be done by the manufacturer.

To-Do-4.6-2) The PSP shall complete the supplemented PEP of the TR-ESOR-Product Manufacturer, include the completed PEP in his PSPS and then publish his completed PEP and his completed PSPS. #Answer: This will be done by the PSP.

Therefore, it is clearly specified, which algorithms currently are used by this Preservation Product of the TR-ESOR-Product Manufacturer and this Preservation Service of the PSP.

NOTE 2: Therefore, this PEPT and the supplemented PEP of the TR-ESOR-Product Manufacturer and the completed PEP of the PSP fulfil (**[**Fehler! Verweisquelle konnte nicht gefunden werden.**]**, OVR-6.5-03, OVR-6.5-04 and OVR-6.5-07).

4.7 Preservation Export-Import

[**TR-ESOR-M.3]**, clause 2.7 describes different methods with different Export-Import data formats with different interfaces for exporting and importing export-import package(s) pursuant to **[TR-ESOR-M.3]**, clause 2.7.

NOTE 1: The decision, which of the alternatives pursuant to **[TR-ESOR-M.3]**, clause 2.7, are supported by the TR-ESOR-Product Manufacturer or PSP, is to be found in chapter 7.7.6, Table 12, added by the TR-ESOR-Product Manufacturer.

To-Do-4.7-1) The PSP shall complete the supplemented PEP of the TR-ESOR-Product Manufacturer, include the completed PEP in his PSPS and then publish his completed PEP and his completed PSPS. #Answer: This will be done by the PSP.

NOTE 2: Therefore, this PEPT and the supplemented PEP of the TR-ESOR-Product Manufacturer and the completed PEP of the PSP, fulfils ([Fehler! Verweisquelle konnte nicht gefunden werden.], OVR-6.1-07, OVR-6.1-08, OVR-6.2-05, OVR-6.5-03, OVR-6.5-08.

4.8 Certificate re-key

Not applicable for Preservation Evidence Policy.

4.9 Preservation Object modification

Not applicable for Preservation Evidence Policy.

4.10 Preservation Data Deletion

Not applicable for Preservation Evidence Policy.

4.11 Preservation Status Services

Not applicable for Preservation Evidence Policy.

4.12 End of subscription

Not applicable for Preservation Evidence Policy.

4.13 Key escrow and recovery

Not applicable for Preservation Evidence Policy.

5. Facility, Management and Operational Controls

Not applicable for Preservation Evidence Policy.

5.1 Physical controls

Not applicable for Preservation Evidence Policy.

5.2 Procedural controls

Not applicable for Preservation Evidence Policy.

5.3 Personnel controls

Not applicable for Preservation Evidence Policy.

5.4 Audit logging procedures

The TR-ESOR-Middleware offers comprehensive and configurable options for logging any access to the preservation system.

(See

- **[**Fehler! Verweisquelle konnte nicht gefunden werden.**]**, clause 5, (A5.1-1), (A5.1-17),
- **[**Fehler! Verweisquelle konnte nicht gefunden werden.**]**, clause 5 (A5.1-33), (A5.2-1)
- **[**Fehler! Verweisquelle konnte nicht gefunden werden.**]**, clause (A4.0-3)
- **[**Fehler! Verweisquelle konnte nicht gefunden werden.**]**, clause (A4.4-6)
- **[**Fehler! Verweisquelle konnte nicht gefunden werden.**]**, clause (A6.2-3)).

5.5 Records archival

Not applicable for Preservation Evidence Policy.

5.6 Algorithm changeover

Not applicable for Preservation Evidence Policy.

5.7 Compromise and disaster recovery

Not applicable for Preservation Evidence Policy.

5.8 Preservation Service termination

Not applicable for Preservation Evidence Policy.

5.9 End of the Preservation Period

To-Do-5.9-1) : The TR-ESOR-Product Manufacturer shall precise in this clause in his PEP, what happens to the archived Data Objects at the end of the preservation period. #Answer: The archived Evidence Records will be delivered to their owners on demand. The owners will be informed by letter, that the archived evidence records will be deleted permanently 6 (six) months after notification.

To-Do-5.9-2) : The **PSP** shall complete the supplemented PEP of his **"TR-ESOR-Product Manufacturer",** especially finalise this clause, then include the completed PEP in his PSPS and publish his completed PEP and his completed PSPS. #Answer: This will be done by the PSP.

6. Technical Security Controls

The TR-ESOR Middleware uses cryptographic algorithm as described in **[**Fehler! Verweisquelle konnte nicht gefunden werden.**]**.

To-Do-6-1) The TR-ESOR-Product Manufacturer and the PSP should also consider the national recommendations of its country. #Answer: This will be done by the manufacturer.

To-Do-6-2) TR-ESOR-Product Manufacturer and the PSPs should consider the recommendations of "Bundesnetzagentur" (BNetzA), if they operate in Germany: https://www.bundesnetzagentur.de/EVD/DE/Fachkreis/Empfehlungen/_function/Empfehlungen-table.html#FAQ961416 #Answer: This will be done by the manufacturer and the PSP.

6.1 TR-ESOR Modules

Not applicable for Preservation Evidence Policy.

6.2 Private Key Protection and Cryptographic Module Engineering Controls

Not applicable for Preservation Evidence Policy.

6.2.1 Private Key Protection

Not applicable for Preservation Evidence Policy.

6.2.2 Protection of the Cryptographic Module

Not applicable for Preservation Evidence Policy.

6.2.3 Configuration of the Cryptographic Module

Not applicable for Preservation Evidence Policy.

6.3 Other aspects of key pair management

Not applicable for Preservation Evidence Policy.

6.4 Activation data

Not applicable for Preservation Evidence Policy.

6.5 Computer security controls

Not applicable for Preservation Evidence Policy.

6.6 Life cycle technical controls

Not applicable for Preservation Evidence Policy.

6.7 Network security controls

Not applicable for Preservation Evidence Policy.

6.8 Time stamping

Not applicable for Preservation Evidence Policy.

7. Formats and Profiles

7.1 Algorithm change

To-Do-7.1-1) The TR-ESOR-Middleware shall react before the expiration of the security suitability of the used algorithms and related parameters. Based on monitoring the suitability of the cryptographic algorithms based on **[**Fehler! Verweisquelle konnte nicht gefunden werden.**]** and **[**Fehler! Verweisquelle konnte nicht gefunden werden.**]**, the TR-ESOR-Middleware performs time-stamp- or hash-tree-renewals as specified in **[**Fehler! Verweisquelle konnte nicht gefunden werden.**]** ~~and/or **[**Fehler! Verweisquelle konnte nicht gefunden werden.**]**.~~ #Answer: This will be done by the manufacturer. See the "2.5.2 Policy-Verwaltung", p.25 [#HB_TP_TR-ESOR_SUITE]

See also TR-ESOR V1.2.1/V1.2.2/V1.3:

- **[**Fehler! Verweisquelle konnte nicht gefunden werden.**],** clause 4, (A4.2-1), (A4.2-2)), (A4.2-3), clause 6.3 (A6.3-1)

and
TR-ESOR V1.2.1/V1.2.2

- **[TR-ESOR-APP],** M.2, clause 4, (A4.0-1),

or
TR-ESOR V13:

- **[**Fehler! Verweisquelle konnte nicht gefunden werden.**], clause 4, (A4.0-1).**

The Crypto Module of TR-ESOR supports a fast and easy algorithm and parameter exchange according to **[**Fehler! Verweisquelle konnte nicht gefunden werden.**]**, clause (A3.2-1) and clause 6.3 and **[**Fehler! Verweisquelle konnte nicht gefunden werden.**]**.

To-Do-7.1-2) The ArchiSig Module of TR-ESOR should have a secondary data basis (see **[**Fehler! Verweisquelle konnte nicht gefunden werden.**]**, clause 4.8 (A4.8-7). The secondary data basis of the ArchiSig Module uses other algorithm and parameters as the primary data basis.

#Answer: This will be done by the manufacturer in a further version.

Nevertheless, a fast and easy algorithm change is ensured.

#Answer: This will be done by the manufacturer.

7.2 Preservation Profile

The definition of the Preservation Profile Scheme is to be found in **(**[Fehler! Verweisquelle konnte nicht gefunden werden.**], clause 5.4.7).**

In context of BSI TR 03125 TR-ESOR, there exist currently the following four Preservation Profiles: #Answer: Implemented is only Version 1 b).

1) TR-ESOR ~~V1.2.1/~~V1.2.2 with the S.4-Interface:
   a) ~~BSI-TR-ESOR-v1.2.1-S4-Profile.xml with the identifier: http://www.bsi.bund.de/tr-esor/V1.2.1/profile/S.4/v1.0~~
   b) BSI-TR-ESOR-v1.2.2-S4-Profile.xml with the identifier:

      http://www.bsi.bund.de/tr-esor/ V1.2.2/profile/S.4/v1.0
   c) ~~BSI-TR-ESOR-v1.3-S4-Profile.xml with the identifier:~~

      ~~http://www.bsi.bund.de/tr-esor/ V1.3/profile/S.4/v1.0~~

or

2) TR-ESOR V1.2.1/V1.2.2 with the TS 119 512-Interface together with or without the "ETSI TS119512 TR-ESOR Transformator"[5]:
   a) BSI-TR-ESOR-v1.2.1-ETSI-TS-119512-v1.1.2-Profile.xml with the identifier http://www.bsi.bund.de/tr-esor/V1.2.1/profile/preservation-api/v1.1.2

      NOTE1: Only with the "ETSI TS119512 TR-ESOR Transformator"

   b) BSI-TR-ESOR-v1.2.2-ETSI-TS-119512-v1.1.2-Profile.xml with the identifier http://www.bsi.bund.de/tr-esor/V1.2.2/profile/preservation-api/v1.1.2.

   c) BBSI-TR-ESOR-v1.3-ETSI-TS-119512-v1.1.2-Profile.xml with the identifier http://www.bsi.bund.de/tr-esor/V1.3/profile/preservation-api/v1.1.2

7.2.1 Profile identifier http://www.bsi.bund.de/tr-esor/V1.2.1/profile/S.4/v1.0

This is the Preservation Profile for TR-ESOR V1.2.1 with the S.4-Interface.

```
<?xml version="1.0" encoding="UTF-8"?>
<pres:Profile xmlns:pres="http://uri.etsi.org/19512/v1.1.1#"
        xmlns:md="http://docs.oasis-open.org/dss-x/ns/metadata"
        xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
        xsi:schemaLocation="https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/
TechnischeRichtlinien/TR03125/tr-esor-schema-standalone-v1_2_1_zip.zip">

        <!-- ========================================== -->
        <!-- Profile of BSI-TR-ESOR-S.4-V1_2_1-Interface                    -->
        <!-- ========================================== -->
        <!Version from 12.11.2020                                                                    -->
        <!-- ========================================== -->

   <md:ProfileIdentifier>http://www.bsi.bund.de/tr-
esor/V1.2.1/profile/S.4/v1.0</md:ProfileIdentifier>
<md:Specification>https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/Technische
Richtlinien/TR03125/BSI_TR_03125_Anlage_E_V1_2_1.pdf</md:Specification>
   <md:Description xml:lang="EN">The present Profile describes the interface of the BSI-TR-
ESOR-S.4. V1.2.1</md:Description>
   <md:Operation>
        <md:Name>ArchiveSubmissionRequest</md:Name>
        <md:Specification>https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/Te
chnischeRichtlinien/TR03125/BSI_TR_03125_Anlage_E_V1_2_1.pdf</md:Specification>
        <md:Description xml:lang="DE">See Clause 3.1.</md:Description>
   </md:Operation>
   <md:Operation> <md:Name>ArchiveUpdateRequest</md:Name>
        <md:Specification>https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/Te
chnischeRichtlinien/TR03125/BSI_TR_03125_Anlage_E_V1_2_1.pdf</md:Specification>
        <md:Description xml:lang="DE">See Clause 3.2.</md:Description>
   </md:Operation>
   <md:Operation>
        <md:Name>ArchiveRetrievalRequest</md:Name>
        <md:Specification>https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/Te
chnischeRichtlinien/TR03125/BSI_TR_03125_Anlage_E_V1_2_1.pdf</md:Specification>>
        <md:Description xml:lang="DE">See Clause 3.3.</md:Description>
   </md:Operation>
   <md:Operation>
        <md:Name>ArchiveEvidenceRequest</md:Name>
        <md:Specification>https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/Te
chnischeRichtlinien/TR03125/BSI_TR_03125_Anlage_E_V1_2_1.pdf</md:Specification>
        <md:Description xml:lang="DE">See Clause 3.4.</md:Description>
```

[5] See https://github.com/de-bund-bsi-tr-esor/tresor-ETSITS119512-transformator and https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/TechnischeRichtlinien/TR03125/BSI_TR_03125_Anlage_TRANS_V1_2_2-Appendix.pdf

```
    </md:Operation>
    <md:Operation>
        <md:Name>ArchiveDeletionRequest</md:Name>
        <md:Specification>https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/TechnischeRichtlinien/TR03125/BSI_TR_03125_Anlage_E_V1_2_1.pdf</md:Specification>
        <md:Description xml:lang="DE">See Clause 3.5.</md:Description>
    </md:Operation>
    <md:Operation>
        <md:Name>ArchiveDataRequest</md:Name>
        <md:Specification>https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/TechnischeRichtlinien/TR03125/BSI_TR_03125_Anlage_E_V1_2_1.pdf</md:Specification>
        <md:Description xml:lang="DE">See Clause 3.6.</md:Description>
    </md:Operation>
    <md:Operation>
        <md:Name>VerifyRequest</md:Name>
        <md:Specification>https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/TechnischeRichtlinien/TR03125/BSI_TR_03125_Anlage_E_V1_2_1.pdf</md:Specification>
        <md:Description xml:lang="DE">See Clause 3.7.</md:Description>
    </md:Operation>
    <md:Policy>
        <md:PolicyByRef>
            <md:PolicyID>
                http://www.bsi.bund.de/DE/tr-esor/prespolicy/default/1.0
            </md:PolicyID>
        </md:PolicyByRef>
    </md:Policy>
    <md:Policy>
        <md:PolicyByRef>
            <md:PolicyID>
                http://www.bsi.bund.de/DE/tr-esor/sigpolicy/verify-xaip
            </md:PolicyID>
        </md:PolicyByRef>
    </md:Policy>
    <md:Policy>
        <md:PolicyByRef>
            <md:PolicyID>
                http://www.bsi.bund.de/DE/tr-esor/sigpolicy/verify-timestamp
            </md:PolicyID>
        </md:PolicyByRef>
    </md:Policy>
<pres:SchemeIdentifier>http://uri.etsi.org/19512/scheme/pds+pgd+aug+wst+ers</pres:SchemeIdentifier>
    <pres:ProfileValidityPeriod>
        <pres:ValidFrom>2020-01-01T00:00:00Z</pres:ValidFrom>
    </pres:ProfileValidityPeriod>
    <pres:PreservationStorageModel>WithStorage</pres:PreservationStorageModel>
    <pres:PreservationGoal>http://uri.etsi.org/19512/goal/pds</pres:PreservationGoal>
    <pres:PreservationGoal>http://uri.etsi.org/19512/goal/pgd</pres:PreservationGoal>
    <pres:PreservationGoal>http://uri.etsi.org/19512/goal/aug</pres:PreservationGoal>
    <pres:EvidenceFormat>
        <md:FormatID>urn:ietf:rfc:4998</md:FormatID>
        <md:Specification>https://ietf.org/rfc/rfc4998.txt</md:Specification>
    </pres:EvidenceFormat>
    <pres:EvidenceFormat>
        <md:FormatID>urn:ietf:rfc:6283</md:FormatID>
        <md:Specification>https://ietf.org/rfc/rfc6283.txt</md:Specification>
    </pres:EvidenceFormat>
</pres:Profile>
```

To-Do-7.2.1-1) : If the TR-ESOR-Product Manufacturer supports this Preservation Profile, he shall

a) decide, which Evidence Format is used in this Preservation Product,

b) precise the Evidence Format in his PEP, based on this PEPT, here and in chapter 7.7.1,

c) delete the second <pres:EvidenceFormat> , not used, in his Preservation Profile and

d) publish his completed Preservation Profile.

To-Do-7.2.1-2) If the TR-ESOR-Product Manufacturer supports this Preservation Profile, the PSP also shall publish this Preservation Profile, if his TR-ESOR-Product in production supports this Preservation Profile.

7.2.2 Profile identifier http://www.bsi.bund.de/tr-esor/V1.2.2/profile/S.4/v1.0

This is the Preservation Profile for TR-ESOR V1.2.2 with S.4 Interface.
#Answer: See "#20211213_PEP_TP_v1.3_BSI-TR-ESOR-S.4-V1.2.2.xml" for details. The BSI template follows.

```
<?xml version="1.0" encoding="UTF-8"?>
<pres:Profile xmlns:pres="http://uri.etsi.org/19512/v1.1.1#"
       xmlns:md="http://docs.oasis-open.org/dss-x/ns/metadata"
       xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
       xsi:schemaLocation="https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/
TechnischeRichtlinien/TR03125/tr-esor-schema-standalone-v1_2_2_zip.zip">


       <!-- ======================================== -->
       <!-- Profile of BSI-TR-ESOR-S.4-V1.2.2 Interface   -->
       <!-- ======================================== -->
       <!-- Draft (12.11.2021)                       -->
       <!-- ======================================== -->

       <md:ProfileIdentifier>http://www.bsi.bund.de/tr-
esor/V1.2.2/profile/S.4/v1.0</md:ProfileIdentifier>
       <md:Specification>https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/Te
chnischeRichtlinien/TR03125/BSI_TR_03125_Anlage_E_V1_2_2.pdf</md:Specification>
       <md:Description xml:lang="EN">The present Profile describes the interface of the BSI-
TR-ESOR-S.4. V1.2.2</md:Description>

       <md:Operation>
              <md:Name>ArchiveSubmissionRequest</md:Name>

       <md:Specification>https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/Te
chnischeRichtlinien/TR03125/BSI_TR_03125_Anlage_E_V1_2_2.pdf</md:Specification>
              <md:Description xml:lang="DE">See Clause 3.1.</md:Description>

       <md:Specification>https://www.bsi.bund.de/SharedDocs/Downloads/EN/BSI/Publications/Tec
hGuidelines/TR03125/TR-03125_E_v1_2_2.pdf</md:Specification>
              <md:Description xml:lang="EN">See Clause 3.1.</md:Description>
       </md:Operation>
       <md:Operation>
              <md:Name>ArchiveUpdateRequest</md:Name>

       <md:Specification>https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/Te
chnischeRichtlinien/TR03125/BSI_TR_03125_Anlage_E_V1_2_2.pdf</md:Specification>
              <md:Description xml:lang="DE">See Clause 3.2.</md:Description>

       <md:Specification>https://www.bsi.bund.de/SharedDocs/Downloads/EN/BSI/Publications/Tec
hGuidelines/TR03125/TR-03125_E_v1_2_2.pdf</md:Specification>
              <md:Description xml:lang="EN">See Clause 3.2.</md:Description>
       </md:Operation>
       <md:Operation>
              <md:Name>ArchiveRetrievalRequest</md:Name>

       <md:Specification>https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/Te
chnischeRichtlinien/TR03125/BSI_TR_03125_Anlage_E_V1_2_2.pdf</md:Specification>
              <md:Description xml:lang="DE">See Clause 3.3.</md:Description>

       <md:Specification>https://www.bsi.bund.de/SharedDocs/Downloads/EN/BSI/Publications/Tec
hGuidelines/TR03125/TR-03125_E_v1_2_2.pdf</md:Specification>
              <md:Description xml:lang="EN">See Clause 3.3.</md:Description>

       </md:Operation>
       <md:Operation>
              <md:Name>ArchiveEvidenceRequest</md:Name>

       <md:Specification>https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/Te
chnischeRichtlinien/TR03125/BSI_TR_03125_Anlage_E_V1_2_2.pdf</md:Specification>
              <md:Description xml:lang="DE">See Clause 3.4.</md:Description>

       <md:Specification>https://www.bsi.bund.de/SharedDocs/Downloads/EN/BSI/Publications/Tec
hGuidelines/TR03125/TR-03125_E_v1_2_2.pdf</md:Specification>
              <md:Description xml:lang="EN">See Clause 3.4.</md:Description>
       </md:Operation>
       <md:Operation>
              <md:Name>ArchiveDeletionRequest</md:Name>

       <md:Specification>https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/Te
```

```
chnischeRichtlinien/TR03125/BSI_TR_03125_Anlage_E_V1_2_2.pdf</md:Specification>
                <md:Description xml:lang="DE">See Clause 3.5.</md:Description>

        <md:Specification>https://www.bsi.bund.de/SharedDocs/Downloads/EN/BSI/Publications/Tec
hGuidelines/TR03125/TR-03125_E_v1_2_2.pdf</md:Specification>
                <md:Description xml:lang="EN">See Clause 3.5.</md:Description>
        </md:Operation>
        <md:Operation>
                <md:Name>ArchiveDataRequest</md:Name>

        <md:Specification>https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/Te
chnischeRichtlinien/TR03125/BSI_TR_03125_Anlage_E_V1_2_2.pdf</md:Specification>
                <md:Description xml:lang="DE">See Clause 3.6.</md:Description>

        <md:Specification>https://www.bsi.bund.de/SharedDocs/Downloads/EN/BSI/Publications/Tec
hGuidelines/TR03125/TR-03125_E_v1_2_2.pdf</md:Specification>
                <md:Description xml:lang="EN">See Clause 3.6.</md:Description>

        </md:Operation>
        <md:Operation>
                <md:Name>VerifyRequest</md:Name>

        <md:Specification>https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/Te
chnischeRichtlinien/TR03125/BSI_TR_03125_Anlage_E_V1_2_2.pdf</md:Specification>
                <md:Description xml:lang="DE">See Clause 3.7.</md:Description>

        <md:Specification>https://www.bsi.bund.de/SharedDocs/Downloads/EN/BSI/Publications/Tec
hGuidelines/TR03125/TR-03125_E_v1_2_2.pdf</md:Specification>
                <md:Description xml:lang="EN">See Clause 3.7.</md:Description>
        </md:Operation>
        <md:Policy>
                <md:PolicyByRef>
                        <md:PolicyID>
                                http://www.bsi.bund.de/DE/tr-esor/prespolicy/default/1.0
                        </md:PolicyID>
                </md:PolicyByRef>
        </md:Policy>
        <md:Policy>
                <md:PolicyByRef>
                        <md:PolicyID>
                                http://www.bsi.bund.de/DE/tr-esor/sigpolicy/verify-xaip
                        </md:PolicyID>
                </md:PolicyByRef>
        </md:Policy>
        <md:Policy>
                <md:PolicyByRef>
                        <md:PolicyID>
                                http://www.bsi.bund.de/DE/tr-esor/sigpolicy/verify-timestamp
                        </md:PolicyID>
                </md:PolicyByRef>
        </md:Policy>
        <pres:SchemeIdentifier>http://uri.etsi.org/19512/scheme/pds+pgd+aug+wst+ers</pres:Sche
meIdentifier>
        <pres:ProfileValidityPeriod>
                <pres:ValidFrom>2020-01-01T00:00:00Z</pres:ValidFrom>
        </pres:ProfileValidityPeriod>
        <pres:PreservationStorageModel>WithStorage</pres:PreservationStorageModel>
        <pres:PreservationGoal>http://uri.etsi.org/19512/goal/pds</pres:PreservationGoal>
        <pres:PreservationGoal>http://uri.etsi.org/19512/goal/pgd</pres:PreservationGoal>
        <pres:PreservationGoal>http://uri.etsi.org/19512/goal/aug</pres:PreservationGoal>
        <pres:EvidenceFormat>
                <md:FormatID>urn:ietf:rfc:4998</md:FormatID>
                <md:Specification>https://ietf.org/rfc/rfc4998.txt</md:Specification>
        </pres:EvidenceFormat>
        <pres:EvidenceFormat>
                <md:FormatID>urn:ietf:rfc:6283</md:FormatID>
                <md:Specification>https://ietf.org/rfc/rfc6283.txt</md:Specification>
        </pres:EvidenceFormat>
</pres:Profile>
```

To-Do-7.2.2-1) If the TR-ESOR-Product Manufacturer supports this Preservation Profile, he shall

a) decide which Evidence Format is used in his Preservation Product,
b) precise the Evidence Format in his PEP, based on this PEPT, here and in chapter 7.7.1,

c) delete the second <pres:EvidenceFormat>, not used, in his Preservation Profile, and
d) publish his Preservation Profile.
Answer: This is done by the manufactorer.

To-Do-7.2.2-2) The PSP also shall publish this Preservation Profile, if his TR-ESOR-Product in production supports this Preservation Profile.
Answer: This is done by the PSP.

~~7.2.3 Profile identifier http://www.bsi.bund.de/tr-esor/V1.3/profile/S.4/v1.0~~

~~Notice: This Profile is under development.~~

~~7.2.4 Profile ID http://www.bsi.bund.de/tr-esor/V1.2.1/profile/preservation-api/v1.1.2~~

~~This is the Preservation Profile of~~

- ~~TR-ESOR V1.2.1 with the S.4-interface[6] in combination with the~~
- ~~ETSI TS119512 TR-ESOR Transformator[7].~~

```
<?xml version="1.0" encoding="UTF-8"?>
<pres:Profile xmlns:pres="http://uri.etsi.org/19512/v1.1.2#"
        xmlns:md="http://docs.oasis-open.org/dss-x/ns/metadata"
        xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
        xsi:schemaLocation="http://uri.etsi.org/19512/v1.1.2#
https://forge.etsi.org/rep/esi/x19_512_preservation_protocol/raw/v1.1.2/19512-Preservation-
API.xsd">
<!-- ------------------------------------------------------- -->
<!-- Profile of BSI-TS119512 V1.1.2-S.4-V1.2.1_Transformator ------------------------------------
-->
<!-- ------------------------------------------------------- -->
<!-- Version of 04.12.2020 ----------------------------------------------------------------------
-->
<!-- ------------------------------------------------------- -->

        <md:ProfileIdentifier>http://www.bsi.bund.de/tr-esor/V1.2.1/profile/preservation-
api/V1.1.2</md:ProfileIdentifier>

        <md:Specification>https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/Te
chnischeRichtlinien/TR03125/BSI_TR_03125_Anlage_E_V1_2_1.pdf</md:Specification>
        <md:Specification>https://www.etsi.org/deliver/etsi_ts/119500_119599/119512/01.01.01_6
0/ts_119512v010102p.pdf</md:Specification>
        <md:Specification>https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/Te
chnischeRichtlinien/TR03125/BSI_TR_03125_Anlage_E_V1_2_2-Appendix.pdf</md:Specification>
        <md:Description xml:lang="EN">The present Profile describes the interface of the ETSI
TS119512 TR-ESOR Transformator.</md:Description>

        <md:Operation>
                <md:Name>RetrieveInfo</md:Name>
        <md:Specification>https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/Te
chnischeRichtlinien/TR03125/BSI_TR_03125_Anlage_E_V1_2_2-Appendix.pdf</md:Specification>
                <md:Description xml:lang="DE">See Clause 2.1.</md:Description>
<md:Specification>https://www.bsi.bund.de/SharedDocs/Downloads/EN/BSI/Publikationen/Technische
Richtlinien/TR03125/BSI_TR_03125_Anlage_E_V1_2_2-Appendix.pdf</md:Specification>
                <md:Description xml:lang="EN">See Clause 2.1.</md:Description>
        </md:Operation>
```

[6] See https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/TechnischeRichtlinien/TR03125/BSI_TR_03125_Anlage_E_V1_2_2.pdf

[7] See https://github.com/de-bund-bsi-tr-esor/tresor-ETSITS119512-transformator

```
        <md:Operation>
                <md:Name>PreservePO</md:Name>
        <md:Specification>https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/TechnischeRichtlinien/TR03125/BSI_TR_03125_Anlage_E_V1_2_2-Appendix.pdf</md:Specification>
                <md:Description xml:lang="DE">See Clause 2.2.</md:Description>
        <md:Specification>https://www.bsi.bund.de/SharedDocs/Downloads/EN/BSI/Publikationen/TechnischeRichtlinien/TR03125/BSI_TR_03125_Anlage_E_V1_2_2-Appendix.pdf</md:Specification>
                <md:Description xml:lang="EN">See Clause 2.2.</md:Description>
        </md:Operation>

        <md:Operation>
                <md:Name>UpdatePOC</md:Name>
        <md:Specification>https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/TechnischeRichtlinien/TR03125/BSI_TR_03125_Anlage_E_V1_2_2-Appendix.pdf</md:Specification>
                <md:Description xml:lang="DE">See Clause 2.3.</md:Description>
        <md:Specification>https://www.bsi.bund.de/SharedDocs/Downloads/EN/BSI/Publikationen/TechnischeRichtlinien/TR03125/BSI_TR_03125_Anlage_E_V1_2_2-Appendix.pdf</md:Specification>
                <md:Description xml:lang="EN">See Clause 2.3.</md:Description>
        </md:Operation>

        <md:Operation>
                <md:Name>RetrievePO</md:Name>
        <md:Specification>https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/TechnischeRichtlinien/TR03125/BSI_TR_03125_Anlage_E_V1_2_2-Appendix.pdf</md:Specification>
                <md:Description xml:lang="DE">See Clause 2.4.</md:Description>
        <md:Specification>https://www.bsi.bund.de/SharedDocs/Downloads/EN/BSI/Publikationen/TechnischeRichtlinien/TR03125/BSI_TR_03125_Anlage_E_V1_2_2-Appendix.pdf</md:Specification>
                <md:Description xml:lang="EN">See Clause 2.4.</md:Description>
        </md:Operation>

        <md:Operation>
                <md:Name>DeletePO</md:Name>
        <md:Specification>https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/TechnischeRichtlinien/TR03125/BSI_TR_03125_Anlage_E_V1_2_2-Appendix.pdf</md:Specification>
                <md:Description xml:lang="DE">See Clause 2.5.</md:Description>
        <md:Specification>https://www.bsi.bund.de/SharedDocs/Downloads/EN/BSI/Publikationen/TechnischeRichtlinien/TR03125/BSI_TR_03125_Anlage_E_V1_2_2-Appendix.pdf</md:Specification>
                <md:Description xml:lang="EN">See Clause 2.5.</md:Description>
        </md:Operation>

        <md:Operation>
                <md:Name>ValidateEvidence</md:Name>
        <md:Specification>https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/TechnischeRichtlinien/TR03125/BSI_TR_03125_Anlage_E_V1_2_2-Appendix.pdf</md:Specification>
                <md:Description xml:lang="DE">See Clause 2.6.</md:Description>
        <md:Specification>https://www.bsi.bund.de/SharedDocs/Downloads/EN/BSI/Publikationen/TechnischeRichtlinien/TR03125/BSI_TR_03125_Anlage_E_V1_2_2-Appendix.pdf</md:Specification>
                <md:Description xml:lang="EN">See Clause 2.6.</md:Description>
        </md:Operation>

        <md:Operation>
                <md:Name>Search</md:Name>
        <md:Specification>https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/TechnischeRichtlinien/TR03125/BSI_TR_03125_Anlage_E_V1_2_2-Appendix.pdf</md:Specification>
                <md:Description xml:lang="DE">See Clause 2.7.</md:Description>
        <md:Specification>https://www.bsi.bund.de/SharedDocs/Downloads/EN/BSI/Publikationen/TechnischeRichtlinien/TR03125/BSI_TR_03125_Anlage_E_V1_2_2-Appendix.pdf</md:Specification>
                <md:Description xml:lang="EN">See Clause 2.7.</md:Description>
        </md:Operation>
        <md:Policy>
                <md:PolicyByRef>
         <md:PolicyID>http://www.bsi.bund.de/DE/tr-esor/prespolicy/default/1.0</md:PolicyID>
```

```
                    </md:PolicyByRef>
            </md:Policy>
            <md:Policy>
                    <md:PolicyByRef>
                    <md:PolicyID>http://www.bsi.bund.de/DE/tr-esor/sigpolicy/verify-
xaip</md:PolicyID>
                    </md:PolicyByRef>
            </md:Policy>
            <md:Policy>
                    <md:PolicyByRef>
                    <md:PolicyID>http://www.bsi.bund.de/DE/tr-esor/sigpolicy/verify-
timestamp</md:PolicyID>
                    </md:PolicyByRef>
            </md:Policy>

            <pres:SchemeIdentifier>http://uri.etsi.org/19512/scheme/pds+pgd+aug+wst+ers</pres:Sche
meIdentifier>

            <pres:ProfileValidityPeriod>
                    <pres:ValidFrom>2020-01-01T00:00:00Z</pres:ValidFrom>
            </pres:ProfileValidityPeriod>

            <pres:PreservationStorageModel>WithStorage</pres:PreservationStorageModel>

            <pres:PreservationGoal>http://uri.etsi.org/19512/goal/pds</pres:PreservationGoal>
            <pres:PreservationGoal>http://uri.etsi.org/19512/goal/pgd</pres:PreservationGoal>
            <pres:PreservationGoal>http://uri.etsi.org/19512/goal/aug</pres:PreservationGoal>

            <pres:EvidenceFormat>
                    <md:FormatID>urn:ietf:rfc:4998</md:FormatID>
                    <md:Specification>https://ietf.org/rfc/rfc4998.txt</md:Specification>
            </pres:EvidenceFormat>

            <pres:EvidenceFormat>
                    <md:FormatID>urn:ietf:rfc:6283</md:FormatID>
                    <md:Specification>https://ietf.org/rfc/rfc6283.txt</md:Specification>
            </pres:EvidenceFormat>

</pres:Profile>
```

To-Do-7.2.3-1) : If the TR-ESOR-Product Manufacturer supports this Preservation Profile, he shall

1) decide, which Evidence Format is used in this Preservation Product,
2) precise the Evidence Format it in his PEP, based on this PEPT, here and in chapter 7.7.1,
3) delete the second <pres:EvidenceFormat> , not used in his Preservation Profile and
4) publish his completed Preservation Profile.

To-Do-7.2.3-2) If the TR-ESOR-Product Manufacturer supports this Preservation Profile, the PSP also shall publish this Preservation Profile, if his TR-ESOR-Product in production supports this Preservation Profile.

7.2.5 Profile ID http://www.bsi.bund.de/tr-esor/V1.2.2/profile/preservation-api/v1.1.2

This is the Preservation Profile of

- TR-ESOR V1.2.2 with the TS119512 interface[8] and

[8] See

- ETSI TS119512 TR-ESOR Transformator[9].

```
<?xml version="1.0" encoding="UTF-8"?>
<pres:Profile xmlns:pres="http://uri.etsi.org/19512/v1.1.2#"
        xmlns:md="http://docs.oasis-open.org/dss-x/ns/metadata"
        xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
        xsi:schemaLocation="http://uri.etsi.org/19512/v1.1.2#
https://forge.etsi.org/rep/esi/x19_512_preservation_protocol/raw/v1.1.2/19512-Preservation-
API.xsd">

        <!-- ========================================================== -->
        <!-- Profile of BSI-TR_03125 TR-ESOR V1.2.2 TS119512 interface -->
        <!-- and                                                        -->
        <!-- Profile of BSI-TS119512 V1.1.2-S.4-V1.2.2_Transformator    -->
        <!-- ========================================================== -->
        <!-- Version of 09.09.2020                                      -->
        <!-- ========================================================== -->

        <md:ProfileIdentifier>http://www.bsi.bund.de/tr-esor/V1.2.2/profile/preservation-
api/V1.1.2</md:ProfileIdentifier>

        <md:Specification>https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/Te
chnischeRichtlinien/TR03125/BSI_TR_03125_Anlage_E_V1_2_2.pdf</md:Specification>
        <md:Specification>
https://www.bsi.bund.de/SharedDocs/Downloads/EN/BSI/Publications/TechGuidelines/TR03125/TR-
03125_E_v1_2_2.pdf</md:Specification>

        <md:Specification>https://www.etsi.org/deliver/etsi_ts/119500_119599/119512/01.01.01_6
0/ts_119512v010102p.pdf</md:Specification>
        <md:Specification>https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/Te
chnischeRichtlinien/TR03125/BSI_TR_03125_Anlage_E_V1_2_2-Appendix.pdf</md:Specification>

        <md:Description xml:lang="EN">The present Profile describes the TR-ESOR V1.2.2
TS119512-interface and the interface of the ETSI TS119512 TR-ESOR
Transformator.</md:Description>

        <md:Operation>
                <md:Name>RetrieveInfo</md:Name>

        <md:Specification>https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/Te
chnischeRichtlinien/TR03125/BSI_TR_03125_Anlage_E_V1_2_2-Appendix.pdf</md:Specification>
                <md:Description xml:lang="EN">See Clause 2.1.</md:Description>
        </md:Operation>

        <md:Operation>
                <md:Name>PreservePO</md:Name>

        <md:Specification>https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/Te
chnischeRichtlinien/TR03125/BSI_TR_03125_Anlage_E_V1_2_2-Appendix.pdf</md:Specification>
                <md:Description xml:lang="EN">See Clause 2.2.</md:Description>
        </md:Operation>

        <md:Operation>
                <md:Name>UpdatePOC</md:Name>

        <md:Specification>https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/Te
chnischeRichtlinien/TR03125/BSI_TR_03125_Anlage_E_V1_2_2-Appendix.pdf</md:Specification>
                <md:Description xml:lang="EN">See Clause 2.3.</md:Description>
        </md:Operation>

        <md:Operation>
                <md:Name>RetrievePO</md:Name>

        <md:Specification>https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/Te
chnischeRichtlinien/TR03125/BSI_TR_03125_Anlage_E_V1_2_2-Appendix.pdf</md:Specification>
                <md:Description xml:lang="EN">See Clause 2.4.</md:Description>
        </md:Operation>
```

https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/TechnischeRichtlinien/TR03125/BSI_TR_03125_Anlage_E_V1_2_2.pdf

[9] See https://github.com/de-bund-bsi-tr-esor/tresor-ETSITS119512-transformator

```
        <md:Operation>
                <md:Name>DeletePO</md:Name>
        
        <md:Specification>https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/TechnischeRichtlinien/TR03125/BSI_TR_03125_Anlage_E_V1_2_2-Appendix.pdf</md:Specification>
                <md:Description xml:lang="EN">See Clause 2.5.</md:Description>
        </md:Operation>

        <md:Operation>
                <md:Name>ValidateEvidence</md:Name>
        
        <md:Specification>https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/TechnischeRichtlinien/TR03125/BSI_TR_03125_Anlage_E_V1_2_2-Appendix.pdf</md:Specification>
                <md:Description xml:lang="EN">See Clause 2.6.</md:Description>
        </md:Operation>

        <md:Operation>
                <md:Name>Search</md:Name>
        
        <md:Specification>https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/TechnischeRichtlinien/TR03125/BSI_TR_03125_Anlage_E_V1_2_2-Appendix.pdf</md:Specification>
                <md:Description xml:lang="EN">See Clause 2.7.</md:Description>
        </md:Operation>

        <md:Policy>
                <md:PolicyByRef>
                        <md:PolicyID>http://www.bsi.bund.de/DE/tr-esor/prespolicy/default/1.0</md:PolicyID>
            </md:PolicyByRef>
        </md:Policy>
        <md:Policy>
                <md:PolicyByRef>
                        <md:PolicyID>http://www.bsi.bund.de/DE/tr-esor/sigpolicy/verify-xaip</md:PolicyID>
                </md:PolicyByRef>
        </md:Policy>
        <md:Policy>
                <md:PolicyByRef>
                        <md:PolicyID>http://www.bsi.bund.de/DE/tr-esor/sigpolicy/verify-timestamp</md:PolicyID>
                </md:PolicyByRef>
        </md:Policy>

        <pres:SchemeIdentifier>http://uri.etsi.org/19512/scheme/pds+pgd+aug+wst+ers</pres:SchemeIdentifier>

        <pres:ProfileValidityPeriod>
                <pres:ValidFrom>2020-01-01T00:00:00Z</pres:ValidFrom>
        </pres:ProfileValidityPeriod>

        <pres:PreservationStorageModel>WithStorage</pres:PreservationStorageModel>

        <pres:PreservationGoal>http://uri.etsi.org/19512/goal/pds</pres:PreservationGoal>
        <pres:PreservationGoal>http://uri.etsi.org/19512/goal/pgd</pres:PreservationGoal>
        <pres:PreservationGoal>http://uri.etsi.org/19512/goal/aug</pres:PreservationGoal>

        <pres:EvidenceFormat>
                <md:FormatID>urn:ietf:rfc:4998</md:FormatID>
                <md:Specification>https://ietf.org/rfc/rfc4998.txt</md:Specification>
        </pres:EvidenceFormat>

        <pres:EvidenceFormat>
                <md:FormatID>urn:ietf:rfc:6283</md:FormatID>
                <md:Specification>https://ietf.org/rfc/rfc6283.txt</md:Specification>
        </pres:EvidenceFormat>

</pres:Profile>
```

To-Do-7.2.4-1) If the TR-ESOR-Product-Manufacturer supports this Preservation Profile, he shall

a) decide which Evidence Format is used in his Preservation Product,

b) publish it in his PEP, based on this PEPT, here and in chapter 7.7.1

c) delete the second <pres:EvidenceFormat>, not used, in his Preservation Profile and

~~d) publish his Preservation Profile.~~

~~**To-Do-7.2.4-2)** The PSP also shall publish this Preservation Profile, if his TR-ESOR-Product in production supports this Preservation Profile.~~

~~**7.2.6 Profile ID http://www.bsi.bund.de/tr-esor/V1.3/profile/preservation-api/v1.1.2**~~

~~This profile is under development.~~

7.3 XML Scheme

See attachment of **[**Fehler! Verweisquelle konnte nicht gefunden werden.**]**.

7.4 Archival Information Package (Container)

7.4.1 Archival Information Package (Container) Formats

The Archival Information Package Container Type "XAIP" pursuant to **[TR-ESOR-F]**, clause 3.1 is supported and optionally in addition, the Archival Information Package Container Type "LXAIP" pursuant to **[TR-ESOR-F]**, clause 3.2 and/or "ASiC-AIP" pursuant to **[TR-ESOR-F]**, clause 3.3 may be supported.

The default Archival Information Package Container type is "XAIP".

To-Do-7.4.1-1) The TR-ESOR-Product Manufacturer shall precise in their PEP in Table 2, whether the Archival Information Package Container type "XAIP" is supported as the default format and whether the Archival Information Package Container formats "LXAIP" ~~and/or "ASiC-AIP"~~ or the following `ArchiveData`-Element Types are also supported by this Preservation Product.

Furthermore, the Preservation Product may also support the `ArchiveData`-Element Types:

- CAdES pursuant to **[ETSI TS 119 512]** Annex A.1.1 (http://uri.etsi.org/ades/CAdES). If there is no MIME type filled, then the default application/cms is used;
- XAdES pursuant to **[ETSI TS 119 512]** Annex A.1.2 (http://uri.etsi.org/ades/XAdES). If there is no MIME type filled, then the default application/xml is used;
- PAdES pursuant to **[ETSI TS 119 512]** Annex A.1.3 (http://uri.etsi.org/ades/PAdES). If there is no MIME Type filled, then the default application/pdf is used;
- ~~DigestList pursuant to **[ETSI TS 119 512]** Annex A.1.6 (http://uri.etsi.org/19512/format/DigestList). If there is no MIME Type filled, then the default application/xml is used.~~

Actual Archival Information Package and `ArchiveData`-Element **Type(s) in Use for the generation**	
Default Archival Information Package and `ArchiveData`-	#Answer: XAIP.

Element types	
LXAIP	#Answer: YES
ASiC-AIP	#Answer: NO
CAdES	#Answer: YES
XAdES	#Answer: YES
PAdES	#Answer: YES
DigestList	#Answer: No

Table 2: Actual used Archival Information Package and and `ArchiveData`-Element formats

To-Do-7.4.1-2) The PSP shall complete the supplemented PEP of the TR-ESOR-Product Manufacturer, include the completed PEP in his PSPS and then publish his completed PEP and his completed PSPS.

NOTE 1: See also **[**Fehler! Verweisquelle konnte nicht gefunden werden.], OVR-6.2-06 and **[ETSI TS 119 512],** Annex A.

#Answer: This is done by the PSP.

7.4.2 XAIP

See chapter 3.1 of **[**Fehler! Verweisquelle konnte nicht gefunden werden.**]**.

7.4.3 LXAIP

See chapter 3.2 of **[**Fehler! Verweisquelle konnte nicht gefunden werden.**]**.

7.4.4 ASiC-AIP

See chapter 3.3 of **[**Fehler! Verweisquelle konnte nicht gefunden werden.**]**.

7.4.5 Validation of Archival Information Package (Container)

See Annex F, **[TR-ESOR-F]**, chapter 3.3/4.3 of **[**Fehler! Verweisquelle konnte nicht gefunden werden.**]** and/or chapter 2.3 of **[**Fehler! Verweisquelle konnte nicht gefunden werden.**]** and **[**Fehler! Verweisquelle konnte nicht gefunden werden.**]**, clause 3.6. Which cryptographic algorithms may be used, is described in [**Fehler! Verweisquelle konnte nicht gefunden werden.**] clause 5.2 and **[**Fehler! Verweisquelle konnte nicht gefunden werden.**]**, clause 4 on base of **[**Fehler! Verweisquelle konnte nicht gefunden werden.**]** and **[**Fehler! Verweisquelle konnte nicht gefunden werden.**]**.

To-Do-7.4.5-1) The TR-ESOR-Product Manufacturer shall precise in his PEP in this clause in Table 5, which algorithms currently are used by this Preservation Product for the verification of the timestamp token in the Evidence Record.

To-Do-7.4.5-2) The PSP shall complete the supplemented PEP of the TR-ESOR-Product Manufacturer, include the completed PEP in his PSPS and then publish his completed PEP and his completed PSPS.

7.5 Payload Data Formats

See chapter 4 of **[**Fehler! Verweisquelle konnte nicht gefunden werden.**]**

7.6 Cryptographic Data Formats

See chapter 5 of **[**Fehler! Verweisquelle konnte nicht gefunden werden.**]**.

7.7 Evidence Record Format

7.7.1 Generation

The Evidence Record is generated according to **[**Fehler! Verweisquelle konnte nicht gefunden werden.**]** ~~or [Fehler! Verweisquelle konnte nicht gefunden werden.]~~ pursuant to **[**Fehler! Verweisquelle konnte nicht gefunden werden.**]**, clause 3.3, 3.4, 3.5.

To-Do-7.7.1-1) The TR-ESOR-Product Manufacturer shall precise in his PEP in Table 3, whether [**Fehler! Verweisquelle konnte nicht gefunden werden.**] or [**Fehler! Verweisquelle konnte nicht gefunden werden.**] or both Evidence Record formats are supported by this Preservation Product.

Actual used Preservation Evidence Record Type	
[RFC4998]	#Answer: YES
[RFC6283]	#Answer: NO only for verification.

Table 3: Actual used Preservation Evidence Record Type

Which cryptographic algorithms may be used is described in **[**Fehler! Verweisquelle konnte nicht gefunden werden.**]** clause 5.1 and **[**Fehler! Verweisquelle konnte nicht gefunden werden.**]**, clause 4 on base of **[**Fehler! Verweisquelle konnte nicht gefunden werden.**]** and **[**Fehler! Verweisquelle konnte nicht gefunden werden.**]**.

To-Do-7.7.1-2) The TR-ESOR-Product Manufacturer shall precise in his PEP in Table 4, which algorithms currently are used by this Preservation Product.

Actual Algorithms in Use for the generation of timestamp token	
Hash function	#Answer: rsassaPss
TST signature algorithm	#Answer: SHA256 Fingerprint
Details	Subject: C = DE, O = Utimaco IS GmbH, 2.5.4.97 = VATDE-815496496, CN = Utimaco qualified TSA CA1 Issuer: C = DE, O = Utimaco IS GmbH, 2.5.4.97 = VATDE-815496496, CN =

	Utimaco qualified TSA CA1 Serial Number: 1 (0x1) Validity Not Before: Aug 17 15:43:27 2021 GMT Not After : Aug 17 15:43:27 2051 GMT Signature Algorithm: rsassaPss SHA256 Fingerprint: 04:D0:E4:DC:F0:82:43:BC:4E:54:57:75:95:93:69:2B:3B:D0:56:0D:0C:B7:FD :DF:69:E2:8F:CC:B6:1E:95:9F Link to the entry in the TL: https://esignature.ec.europa.eu/efda/tl-browser/#/screen/tl/DE/25/1 status "granted": Yes

Table 4: Actual Algorithms in Use for timestamp token

To-Do-7.7.1-3) If the TR-ESOR-Product Manufacturer or the PSP creates parallel hash trees with different algorithms, their PEP shall include here in clause 7.7.1 a second table for the second hash tree. #Answer: No parallel hash trees implemented.

To-Do-7.7.1-4) The PSP shall complete the supplemented PEP of the TR-ESOR-Product Manufacturer, include the completed PEP in his PSPS and then publish his completed PEP and his completed PSPS.

#Answer: This is done by the PSP.

NOTE 1: See also (**[**Fehler! Verweisquelle konnte nicht gefunden werden.**],** clause OVR-6.5-03, OVR-6.5-04 and OVR-6.5-08)**.**

NOTE 2: Therefore, **[**Fehler! Verweisquelle konnte nicht gefunden werden.**]**, OVR-6.5-03, OVR-6.5-04 and OVR-6.5-08 are fulfilled.

The Evidence Record contains no explicit information of the Preservation Service, this Preservation Evidence Policy or the Preservation Profile.

NOTE 3: Therefore, **[**Fehler! Verweisquelle konnte nicht gefunden werden.**]**, OVR-6.5-09 is fulfilled.

7.7.2 Validation

7.7.2.1 Evidence Record

See chapter 3.3/4.3 of **[**Fehler! Verweisquelle konnte nicht gefunden werden.**]** and/or chapter 2.3 of **[**Fehler! Verweisquelle konnte nicht gefunden werden.**]** and **[**Fehler! Verweisquelle konnte nicht gefunden werden.**]**, clause 3.6. Which cryptographic algorithms may be used, is described in **[**Fehler! Verweisquelle konnte nicht gefunden werden.**]** clause 5.2 and **[**Fehler! Verweisquelle konnte nicht gefunden werden.**]**, clause 4 on base of **[**Fehler! Verweisquelle konnte nicht gefunden werden.**]** and **[**Fehler! Verweisquelle konnte nicht gefunden werden.**]**.

To-Do-7.7.2-1) The TR-ESOR-Product Manufacturer shall precise in his PEP in this clause in Table 5, which algorithms currently are used by this Preservation Product for the verification of the timestamp token in the Evidence Record.

Actual Algorithms in Use for the verification of timestamp token	
Hash function	#Answer: sha224, sha256, sha384, sha512, sha3-224, sha3-256, sha3-384, sha3-512
TST signature algorithm	<Must be filled in by the TR-ESOR-Product Manufacturer> #Answer: depends on external qTSP

Table 5: Actual Algorithms in Use for the verification of timestamp token

To-Do-7.7.2-2) If the TR-ESOR-Product Manufacturer or the PSP creates parallel hash trees with different algorithms, their PEP shall include here in clause 7.7.2.1 a second table for the second hash tree. #Answer: No parallel hash trees implemented.

To-Do-7.7.2-3) The PSP shall complete the supplemented PEP of the TR-ESOR-Product Manufacturer, include the completed PEP in his PSPS and then publish his completed PEP and his completed PSPS. #Answer: This is done by the PSP.

7.7.2.2 ArchiveTimeStamp

See chapter 4.3 of **[**Fehler! Verweisquelle konnte nicht gefunden werden.**]** and **[**Fehler! Verweisquelle konnte nicht gefunden werden.**]**, clause 3.4 or chapter 3.3 of **[**Fehler! Verweisquelle konnte nicht gefunden werden.**]** and **[TR-ESOR-ERS]**, clause 6.1.

7.7.2.3 ArchiveTimeStampSequence and ArchiveTimeStampChain

See chapter 5.3 of [**Fehler! Verweisquelle konnte nicht gefunden werden.**] and [**Fehler! Verweisquelle konnte nicht gefunden werden.**], clause 3.3.1 or chapter 4.3 of [**Fehler! Verweisquelle konnte nicht gefunden werden.**] and [**Fehler! Verweisquelle konnte nicht gefunden werden.**], clause 6.1.

7.7.3 Applicable Trust Service Provider ((Q)TSP)

The following external TSP are used by the PSP for the TR-ESOR-Middleware:

- Time Stamping Authority issuing qualified timestamps,
- Validation Service to validate (qualified) electronic signatures, seals or timestamps,
- Certificate Status Authority to validate certificates.

A signature is not created by the TR-ESOR-Middleware, when creating a preservation evidence.

NOTE 1: See also (**[**Fehler! Verweisquelle konnte nicht gefunden werden.**]**, clause OVR-6.5-05 and OVR-6.5-06)**.**

7.7.3.1 Time Stamping Authority issuing qualified timestamps

To-Do-7.7.3-1) The TR-ESOR-Middleware shall request qualified time-stamps from a qualified Trust Service Provider, that follows state-of-the-art practices for policy and security requirements for trust service providers conform to ETSI EN 319 421 to create or augment an Evidence Record with `ArchiveTimeStamps` or `ArchiveTimeStamp Chains` or `ArchiveTimeStamp Sequences` pursuant to **[**Fehler! Verweisquelle konnte nicht gefunden werden.**]** ~~or **[**Fehler! Verweisquelle konnte nicht gefunden werden.**]**~~.

For this case, the following certification path (trust anchors) of the timestamps within the preservation evidence are used:

Root CA - Utimaco	
subject	C = DE, O = Utimaco IS GmbH, 2.5.4.97 = VATDE-815496496, CN = Utimaco qualified TSA CA1
issuer	C = DE, O = Utimaco IS GmbH, 2.5.4.97 = VATDE-815496496, CN = Utimaco qualified TSA CA1
serial number (hex)	1 (0x1)
validity	• Not Before: Aug 17 15:43:27 2021 GMT • Not After : Aug 17 15:43:27 2051 GMT
public key length	<Must be filled in by PSP>
signature algorithm	SHA256
SHA-256 fingerprint	04:D0:E4:DC:F0:82:43:BC:4E:54:57:75:95:93:69 :2B:3B:D0:56:0D:0C:B7:FD:DF:69:E2:8F:CC:B6 :1E:95:9F
Link to entry in the TL	https://esignature.ec.europa.eu/efda/tl-browser/#/screen/tl/DE/25/1
status “granted”	Yes
Subordinate CA- #Answer: NO ONE	
subject	<Must be filled in by PSP>
issuer	<Must be filled in by PSP>
serial number (hex)	<Must be filled in by PSP>
validity	<Must be filled in by PSP>
public key length	<Must be filled in by PSP>
signature algorithm	<Must be filled in by PSP>
SHA-256 fingerprint	<Must be filled in by PSP>
Link to entry in the TL	<Must be filled in by PSP>
status “granted”	Yes or No

Table 6: Trust Anchor of the Timestamp Trust Service Provider

To-Do-7.7.3-2) The PSP shall complete the supplemented PEP of the TR-ESOR-Product Manufacturer, with these details of Table 6 and include his completed PEP in his PSPS and then publish his completed PEP and his completed PSPS.

Answer: This is done by the PSP.

7.7.3.2 Validation Service for (qualified) electronic signatures, seals or timestamps by an external Validation Service

The TR-ESOR-Middleware may request the validation of digital signatures or timestamps upon request from an external Trust Service Provider.

#Answer: There is no external validation service. For this purpose the product uses the DSS - Library from the EU commission..

Root CA – Answer: No external validation service	
~~subject~~	~~<Must be filled in by PSP>~~
~~issuer~~	~~<Must be filled in by PSP>~~
~~serial number (hex)~~	~~<Must be filled in by PSP>~~
~~validity~~	~~<Must be filled in by PSP>~~
~~public key length~~	~~<Must be filled in by PSP>~~
~~signature algorithm~~	~~<Must be filled in by PSP>~~
~~SHA-256 fingerprint~~	~~<Must be filled in by PSP>~~
~~**Subordinate CA xyz**~~	
~~subject~~	~~<Must be filled in by PSP>~~
~~issuer~~	~~<Must be filled in by PSP>~~
~~serial number (hex)~~	~~<Must be filled in by PSP>~~
~~validity~~	~~<Must be filled in by PSP>~~
~~public key length~~	~~<Must be filled in by PSP>~~
~~signature algorithm~~	~~<Must be filled in by PSP>~~
~~SHA-256 fingerprint~~	~~<Must be filled in by PSP>~~
~~Link to entry in the TL~~	~~<Must be filled in by PSP>~~
~~status "granted"~~	~~Yes or No~~

Table 7: Trust Anchor of the external Validation Trust Service Provider

To-Do-7.7.3-3) If an external Validation Trust Service Provider is used by the PSP, the PSP shall complete the supplemented PEP of the TR-ESOR-Product Manufacturer, with these details of Table 7, include his completed PEP in his PSPS, and then publish his completed PEP and his completed PSPS.

#Answer: This is done by the PSP.

To-Do-7.7.3-4) The PSP shall include in its PEP, Table 8, an information about the supported validation model (shell or chain), and then publish his completed PEP and his completed PSPS.

#Answer: This is done by the PSP.

Supported Validation Model (Shell or Chain)	
Shell Modell	#Answer: YES
Chain Modell	#Answer: YES

Table 8: Supported Validation Model (Shell or Chain)

7.7.3.3 Certificate Status Authority to validate certificates

The TR-ESOR-Middleware may request the validation of electronic certificates up to a trustworthy root certificate from an external Trust Service Provider.

#Answer: There is no external validation service for certificates. For this purpose the product uses the DSS -Library from the EU commission..

Root CA – Answer: No external validation service	
~~subject~~	~~<Must be filled in by PSP>~~
~~issuer~~	~~<Must be filled in by PSP>~~
~~serial number (hex)~~	~~<Must be filled in by PSP>~~
~~validity~~	~~<Must be filled in by PSP>~~
~~public key length~~	~~<Must be filled in by PSP>~~
~~signature algorithm~~	~~<Must be filled in by PSP>~~
~~SHA-256 fingerprint~~	~~<Must be filled in by PSP>~~
~~**Subordinate CA xyz**~~	
~~subject~~	~~<Must be filled in by PSP>~~
~~issuer~~	~~<Must be filled in by PSP>~~
~~serial number (hex)~~	~~<Must be filled in by PSP>~~
~~validity~~	~~<Must be filled in by PSP>~~
~~public key length~~	~~<Must be filled in by PSP>~~
~~signature algorithm~~	~~<Must be filled in by PSP>~~
~~SHA-256 fingerprint~~	~~<Must be filled in by PSP>~~
~~Link to entry in the TL~~	~~<Must be filled in by PSP>~~
~~status "granted"~~	~~Yes or No~~

Table 9 : Trust Anchor of the external Certificate Status Authority

To-Do-7.7.3-5) If an external Certificate Status Authority is used by the PSP, the PSP shall complete the supplemented PEP of the TR-ESOR-Product Manufacturer with these details of Table 9, include his completed PEP in his PSPS, and then publish his completed PEP and his completed PSPS.

#Answer: This is done by the PSP.

NOTE 1: Therefore, (**[**Fehler! Verweisquelle konnte nicht gefunden werden.**]**, OVR-6.5-05 and OVR-6.5-06) are fulfilled.

7.7.4 Augmentation of Evidence Record

The augmentation of Evidence Records is achieved at the latest by time-stamp renewal and hash-tree renewal[10].
For the data formats and processing Procedures see chapter 5.2 of **[**Fehler! Verweisquelle konnte nicht gefunden werden.**]** and chapter 4.2.1 and/or 4.2.2 of **[**Fehler! Verweisquelle konnte nicht gefunden werden.**]** and **[**Fehler! Verweisquelle konnte nicht gefunden werden.**]**, clause 4.7 and clause 4.8 and **[**Fehler! Verweisquelle konnte nicht gefunden werden.**]**, clause 5.5.

To-Do-7.7.4-1) The TR-ESOR-Product Manufacturer shall precise here in his PEP in this clause in Table 10, which algorithms are currently used for the time-stamp renewal and hash-tree renewal in case of the augmentation of Evidence Records.

Actual Algorithms in Use for the time-stamp renewal and hash-tree renewal	
Hash function	#Answer: ~~sha224, sha256, sha384~~, sha512, sha3-224, sha3-256, sha3-384, sha3-512
TST signature algorithm	#Answer: TST signature algorithm depends on the timestamp server. Please see "7.7.3.1 Time Stamping Authority issuing qualified timestamps" for details

Table 10: Actual Algorithms in Use for the time-stamp renewal and hash-tree renewal

To-Do-7.7.4-2) If the TR-ESOR-Product Manufacturer or PSP creates parallel hash trees with different algorithms, the TR-ESOR-Product Manufacturer or PSP shall create in their PEP here in clause 7.7.4 a second table for the second hash tree.

#Answer: No parallel hash trees implemented.

To-Do-7.7.4-3) The PSP shall complete the following Table *11*.

#Answer: The following is done by the PSP.

[10] It is recommended to do that directly after the corresponding time-stamp has been received.

Self-Declaration of the PSP	
For every supported active preservation profile, the PSP declares whether he monitors the strength of every cryptographic algorithm that is used in connection with this profile.	<Must be filled in by the TR-ESOR-Preservation Service Provider (PSP)>: ☐ Yes ☐ No — In case of „yes“, please explain this process in more details.
In case, one of the used algorithms or parameters is thought to become less secure or the validity of a relevant certificate is going to expire, the PSP declares whether he augments the Evidence Records and updates the related preservation evidence policy to handle newly submitted POs pursuant to • [TR-ESOR-APP], HD, clause 3.6, (A6.1-8), (A6.1-9) or • [TR-ESOR], clause 6.1, (A6.1-8), (A6.1-9) .	<Must be filled in by the TR-ESOR-Preservation Service Provider (PSP)>: ☐ Yes ☐ No — In case of „yes“, please explain this process in more details.

Table 11: Self-Declaration of the PSP concerning the Augmentation of Evidence Records

NOTE 1: This fulfils requirement OVR-7.14-01 Fehler! Verweisquelle konnte nicht gefunden werden.**]**.

To-Do-7.7.4-4) The PSP shall complete the supplemented PEP of the TR-ESOR-Product Manufacturer with these details of Table 10 and Table 11and include his completed PEP in his PSPS and then publish his completed PEP and his completed PSPS.

NOTE 2: Therefore, (**[**Fehler! Verweisquelle konnte nicht gefunden werden.**]**, OVR-6.5-07 is fulfilled.

7.7.5 Validation of Digital Signatures

7.7.5.1 Verify or ValidateEvidence:

Concerning validation of digital signatures, see **[TR-ESOR, V1.2.2]**, clause 5.1, requirement (A5.1-5) and **[**Fehler! Verweisquelle konnte nicht gefunden werden.**]**, clause 5.1.2 and **[**Fehler! Verweisquelle konnte nicht gefunden werden.**]**, clause 5.6.

To-Do-7.7.5-1)

"For further processing it is necessary that at least one of both validation models (shell model or chain model) is successful. If both validation models (shell model and chain model) fail, it should be proceeded as follows eventually on base of configurable options:

a) In case of XAIP ~~or ASiC or ASiC-AIP~~:

ArchiSafe [Fehler! Verweisquelle konnte nicht gefunden werden.] returns an understandable error message to the application and rejects the archiving of the object.

b) In case of LXAIP:

The appropriate error message is stored in the CredentialSection and, if applicable, together with all further existing validation information. After that, the object is stored in the ECM-/long-Term Storage. In addition, an error message is returned to the IT application or to the XML-Adapter."[11] (**[TR-ESOR, V1.2.2]**, (A5.1-5))

#Answer: This is full filled.

"*In case of a logical XAIP (LXAIP) the case (2), specified above, shall be applied. On base of configurable data the IT application or the XML-Adapter may delete the LXAIP and the associated data objects in the ECM-/long-Term Storage after the reception of the error message.*" (**[TR-ESOR, V1.2.2]**, (A5.1-5) NOTICE)

#Answer: This is full filled.

7.7.5.2 Trust Anchor

To-Do-7.7.5-2) If the URL

- `http://www.bsi.bund.de/DE/tr-esor/sigpolicy/verify-xaip` (both shell or chain) or
- `http://www.bsi.bund.de/DE/tr-esor/sigpolicy/verify-xaip/shell` (only in case of TR-ESOR V1.3 and higher) (default) or `http://www.bsi.bund.de/tr-esor/sigpolicy/verify-xaip/chain` (only in case of TR-ESOR V1.3 and higher)

is included in the `DefaultPolicy/SignaturePolicyIdentifier` element within the `dss:OptionalInputs`-Element of a Verify-request (see also **[TR-ESOR-E, clause 3]**) or `ValidateEvidence`-request (see also **[TR-ESOR-E, clause 4]** and **[ETSI TS 119 512] in the profiling of [TR-ESOR-TRANS]**), this means that

a) all digital signature related objects (electronic signatures, electronic seals, electronic time-stamps, certificates, revocation lists, OCSP responses, etc.) contained in the XAIP or LXAIP container ~~or ASiC-AIP~~ (see clause 7.4) shall be verified up to a **trustworthy root certificate** or t**rust anchor** according to the preservation evidence policy (PEP) derived from [TR-ESOR-PEPT] of the TR-ESOR-

[11] "*If at least chain validation or shell validation does not fail, the return code ".../resultmajor#ok" and ".../resultminor/arl/XAIP_OK_SIG" should be returned. In all other cases, the return code shall be ".../resultmajor#error"."*

Product Manufacturer or respectively of the preservation trust service provider;

#Answer: This is full filled.

b) all verified electronic signatures, seals and time-stamps contained in the XAIP or LXAIP container ~~or ASiC-AIP~~ (see clause 7.4), transmitted, shall be supplemented with all the validation data, obtained in doing the verification, in the manner specified in **[**Fehler! Verweisquelle konnte nicht gefunden werden.**]**. If possible, the validation data (certificates, certificate revocation lists, OCSP responses) is stored as unsigned attributes or properties in the corresponding digital signatures or time-stamps or in the `xaip:certificateValues` or `xaip:revocationValues` subelements of the `credential` element of the (L)XAIP or an ASiC-AIP with a (L)XAIP pursuant to [TR-ESOR-F, clause 3.1.5, clause 5.1] and linked to the corresponding digital signatures or time-stamps;

#Answer: This is full filled.

c) if the signature policy

- `http://www.bsi.bund.de/DE/tr-esor/sigpolicy/verify-xaip` or
- `http://www.bsi.bund.de/DE/tr-esor/sigpolicy/verify-xaip/chain` (ONLY in case of TR-ESOR V1.3 and higher) or
- `http://www.bsi.bund.de/tr-esor/sigpolicy/verify-xaip/shell` (ONLY in case of TR-ESOR V1.3 and higher)

as well as the element **ReturnVerificationReport** is submitted in a `Verify`-request or `ValidateEvidence`-request, then the created verification report(s) shall be stored in the child-element **`vr:VerificationReport`** of the **`credential-`** Element of the XAIP or LXAIP ~~or in the ASiC-AIP~~.

#Answer: This is full filled.

To-Do-7.7.5-3) If the type-attribute

- `http://www.bsi.bund.de/DE/tr-esor/sigpolicy/verify-timestamp/chain` (default) or
- `http://www.bsi.bund.de/DE/tr-esor/sigpolicy/verify-timestamp/shell`

in case of TR-ESOR V1.3 or the type-attribute

- `http://www.bsi.bund.de/tr-esor/api/1.2`

in case of TR-ESOR V1.2.1 and V1.2.2 is included in the `DefaultPolicy/SignaturePolicyIdentifier` element within the `ReturnUpdateSignature` of clause 4.5.8 of **[OASIS-DSS]** within the `dss:OptionalInputs`-Element of a Verify-request (see also **[TR-ESOR-E, clause 5.3.2]**) or ValidateEvidence-request (see also **[TR-ESOR-E, clause 4]** and **[ETSI TS 119 512]** in the profiling of **[TR-ESOR-TRANS]**), this means that

a) all certificates and revocation information of a timestamp validation shall be validated up to a **trustworthy root certificate** or **trust anchor** according to the preservation evidence policy (PEP) derived from **[TR-ESOR-PEPT]** of the TR-ESOR-Product Manufacturer or respectively of the preservation trust service

provider and that verification information obtained in doing so shall be inserted into the timestamp in the manner specified in [TR-ESOR-F];

#Answer: This is full filled.

b) if the type-attribute

- `http://www.bsi.bund.de/DE/tr-esor/sigpolicy/verify-timestamp/chain`
  or
- `http://www.bsi.bund.de/DE/tr-esor/sigpolicy/verify-timestamp/shell`

#AUDIT5: That's why we use the ETSI profiling:

https://www.etsi.org/deliver/etsi_ts/119600_119699/119615/01.01.01_60/ts_119615v010101p.pdf

ETSI as the standardization organization for eIDAS services published the technical specification "Procedures for using and interpreting European Union

Member States national trusted lists where section 4.6 is on determination whether a valid time stamp is qualified in the sense of eIDAS.

Please flow the Link above or read it in the ANNEX "PEP ANNEX ETSI ts_119615v010101p.pdf" chapter 4.6.

~~in case of TR-ESOR V1.3 or the type-attribute~~

- ~~`http://www.bsi.bund.de/tr-esor/api/1.2`~~

in case of TR-ESOR ~~V1.2.1 and~~ V1.2.2 as well as the element **`ReturnVerificationReport`** is submitted in a `Verify`-request or `ValidateEvidence`-request, then all certificates and revocation information of a timestamp validation up to a **trustworthy root certificate** or **trust anchor** according to the preservation evidence policy (PEP) derived from [TR-ESOR-PEPT] of the TR-ESOR-Product Manufacturer or respectively of the preservation trust service provider are verified and that verification information obtained in doing so and the created verification report(s) shall be inserted in the child-element **`vr:VerificationReport`** of the **`credential`**-Element of the XAIP or LXAIP or in the ASiC-AIP in the manner specified in [TR-ESOR-F].

#Answer: This is full filled.

NOTE 1: The trust anchor are to be found in PEP, clause 7.7.3 No. 1, 2 and No. 3.

NOTE 2: In Germany, DA:VE (https://www.bundesnetzagentur.de/EVD/DE/Verbraucher/AuskunftDAVE/DAVE/DAVE.html) provides the possibility for long-term storage of trust anchors in case the Trust Service provider has ceased its operation.

7.7.5.3 Unsigned Data and Documents

To-Do-7.7.5-4) The permanent proof of the integrity of cryptographically **unsigned data and documents** may be ensured additionally by an electronic archive entry hash value, and electronic archive entry signature or seal or an electronic archive timestamp at least from the time of the transfer into the archive system. The quality required for the archive entry hash value, the archive entry signature or seal or the archive entry timestamp is based on the purpose of proof required or intended.

#Answer: This is not implemented.

7.7.6 Process of Export and Import of Export-Import-Packages

For the Export-Import- Process of requesting export-import package(s) from the ECM-/ong-Term-Storage, the following method is supported:

- Export-Import of (L)XAIPs with the integrated reduced Evidence Records pursuant to (**[TR-ESOR-M.3, V1.3]**, clause 2.7) or **[TR-ESOR-APP],** clause 5.2 for (**[TR-ESOR], V1.2.1** or **V1.2.2).**

To-Do-7.7.6-1) The TR-ESOR-Product Manufacturer shall specify in his PEP here in this clause 7.7.6 in Table 12,

- which export-import method is used (Table 12, No. 1)
- with which export-import data structure (Table 12, No. 2), and
- how the request for an export-import package can be done (Table 12, No. 3).

Detailed references to the **[TR-ESOR]**-publication (e.g. which annex, which clause, which requirements) are sufficient.

Details of Export and Import of Export-Import-Packages	
1. Choice of export-import method pursuant to **[TR-ESOR-M.3]**, clause 2.7 (A2.7-1)	#Answer: S4 TR-ESOR Appendex E - interfaces ArchiveRetrivalRequest ArchiveSubmissionRequest
2. Choice of Export-Import data structure: - a set of XAIPs with reduced EvidenceRecords pursuant to [TR-ESOR-F]	#Answer: YES
3. Choice of how the request for an export-import package can be done. - With the conventional operations ArchiveRetrievalRequest for the Export und ArchiveSubmissionRequest for the Import pursuant to **[TR-ESOR-E]**, Clause 3, interface TR-ESOR-S.4 ~~or **[TR-ESOR-E]**, Clause 4, interface TS119512~~	#Answer: S4 TR-ESOR Appendex E - interfaces ArchiveRetrivalRequest ArchiveSubmissionRequest

Table 12: Details of Export and Import of Export-Import-Packages

In the other cases

To-Do-7.7.6-2) The PSP shall complete the supplemented PEP of the TR-ESOR-Product Manufacturer with these details of Table 12 and include his completed PEP in his PSPS and then publish his completed PEP and his completed PSPS. Furthermore, the **PSP** shall copy the content of his PEP, clause 7.7.6 in its terms and conditions.

#Answer: This is done by the PSP:

8. Compliance Audit and other Assessments

Not applicable for Preservation Evidence Policy.

8.1 Frequency or circumstances of assessment

Not applicable for Preservation Evidence Policy.

8.2 Identity/qualifications of assessor

Not applicable for Preservation Evidence Policy.

8.3 Assessor's relationship to assessed entity

Not applicable for Preservation Evidence Policy.

8.4 Topics covered by assessment

Not applicable for Preservation Evidence Policy.

8.5 Actions taken as a result of deficiency

Not applicable for Preservation Evidence Policy.

8.6 Communication of results

Not applicable for Preservation Evidence Policy.

9. Other Business and legal Matters

Not applicable for Preservation Evidence Policy.

9.1 Fees
Not applicable for Preservation Evidence Policy.

9.2 Financial responsibility
Not applicable for Preservation Evidence Policy.

9.3 Confidentiality of business information
Not applicable for Preservation Evidence Policy.

9.4 Privacy of personal information
Not applicable for Preservation Evidence Policy.

9.5 Intellectual property rights
Not applicable for Preservation Evidence Policy.

9.6 Representations and warranties
Not applicable for Preservation Evidence Policy.

9.7 Disclaimers of warranties
Not applicable for Preservation Evidence Policy.

9.8 Limitations of liability
Not applicable for Preservation Evidence Policy.

9.9 Indemnities
Not applicable for Preservation Evidence Policy.

9.10 Term and termination
Not applicable for Preservation Evidence Policy.

9.11 Individual notices and communications with participants
Not applicable for Preservation Evidence Policy.

9.12 Amendments
Not applicable for Preservation Evidence Policy.

9.13 Dispute resolution provisions
Not applicable for Preservation Evidence Policy.

9.14 Governing law
Not applicable for Preservation Evidence Policy.

9.15 Compliance with applicable law
Not applicable for Preservation Evidence Policy.

9.16 Miscellaneous provisions

Not applicable for Preservation Evidence Policy.

9.17 Other provisions

Not applicable for Preservation Evidence Policy.