BSI Technical Guideline 03125
Preservation of Evidence of Cryptographically Signed Documents

Annex TR-ESOR-M.1: ArchiSafe-Module

<table>
<thead>
<tr>
<th>Designation</th>
<th>ArchiSafe-Module</th>
</tr>
</thead>
<tbody>
<tr>
<td>Abbreviation</td>
<td>BSI TR-ESOR-M.1</td>
</tr>
<tr>
<td>Version</td>
<td>1.2</td>
</tr>
<tr>
<td>Date</td>
<td>19.12.14</td>
</tr>
</tbody>
</table>
# Table of contents

1. Introduction........................................................................................................................................4
2. Overview........................................................................................................................................6
   2.1 Goals........................................................................................................................................6
3. Definition of the ArchiSafe-Module.................................................................................................7
   3.1 Basic design and functional differentiation.................................................................7
   3.2 Integration of the ArchiSafe-Module...............................................................................7
   3.3 Fulfilment of basic security-related requirements..................................................7
4. Functional requirements..............................................................................................................8
   4.1 Archiving electronic data – ArchiveSubmissionRequest...........................................9
   4.2 Updating archived data – ArchiveUpdateRequest..................................................10
   4.3 Retrieving archived data – ArchiveRetrievalRequest.............................................12
   4.4 Deleting archived data – ArchiveDeletionRequest................................................12
   4.5 Returning evidence records – ArchiveEvidenceRequest.......................................13
   4.6 Returning data elements – ArchiveDataRequest..................................................13
   4.7 Verifying the archival information package including the supplemental evidence data and evidence records that are contained therein or were additionally transferred – VerifyRequest..............13
5. Security functions......................................................................................................................15
1. Introduction

The goal of the Technical Guideline "Preservation of Evidence of Cryptographically Signed Documents" is to specify security-related requirements for the long-term preservation of evidence of cryptographically signed electronic documents and data along with associated electronic administrative data (meta data).

A Middleware defined for this purpose (TR-ESOR-Middleware) in the sense of this Technical Guideline includes all the modules (M) and interfaces (S) ["S" for the German word "Schnittstellen"] used for securing and preserving the authenticity and proving the integrity of the stored documents and data.

The Reference Architecture introduced in the Main Document of this Technical Guideline consists of the functions and logical units described below:

- The S.4 input interface of the TR-ESOR-Middleware which serves to embed the TR-ESOR-Middleware in the existing IT and infrastructure landscape;
- The central Middleware module ([TR-ESOR-M.1]) which regulates the flow of information in the Middleware, implements the security requirements for the interfaces with the IT applications and ensures that the application systems are decoupled from the ECM/Long-Term Storage;
- The "Cryptographic-Module" ([TR-ESOR-M.2]) and the associated S.1 and S.3 interfaces that provide all the functions needed for creating (optional) and verifying electronic signatures, post-verifying electronic certificates and for obtaining qualified time stamps for the Middleware. Furthermore, it can provide functions for the encryption and decryption of data and documents;
- The "ArchiSig-Module" ([TR-ESOR-M.3]) with the S.6 interface that provides the functions needed for the preservation of evidence of the digitally signed documents;
- An ECM/Long-Term Storage with the S.2 and S.5 interfaces that assumes the physical archiving/storage and also the storage of the meta data that preserve evidence.

This ECM/Long-Term Storage is no longer directly a part of the Technical Guideline, but requirements will be made for it through the two interfaces that are still part of the TR-ESOR-Middleware.

The application layer that can include an XML adapter is not a direct part of the Technical Guideline either, even though this XML adapter can be implemented as part of a Middleware.

The IT Reference Architecture depicted in 1 is based on the ArchiSafe1 Reference Architecture and is supposed to make possible and support the logical (functional) interoperability of future products with the goals and requirements of the Technical Guideline.

---

1 For further information, see http://www.archisafe.de.
This Technical Guideline has a modular design and the individual annexes to the Main Document specify the functional and security-related requirements for the needed IT components and interfaces of the TR-ESOR-Middleware. The specifications are strictly platform-, product-, and manufacturer-independent.

This document bears the designation "Annex TR-ESOR-M.1" and specifies the functional and security-related requirements for the module TR-ESOR-M.1 (in the following abbreviated to ArchiSafe-Module).

Figure 1: Schematic depiction of the IT Reference Architecture

This Technical Guideline has a modular design and the individual annexes to the Main Document specify the functional and security-related requirements for the needed IT components and interfaces of the TR-ESOR-Middleware. The specifications are strictly platform-, product-, and manufacturer-independent.

This document bears the designation "Annex TR-ESOR-M.1" and specifies the functional and security-related requirements for the module TR-ESOR-M.1 (in the following abbreviated to ArchiSafe-Module).

---

2 The name "ArchiSafe" refers to the E-Government Project "ArchiSafe – Legally Viable and Auditable Long-Term Storage of Electronic Documents" from the Physikalisch-Technische Bundesanstalt in 2005 that was promoted in the scope of the E-Government Program "BundOnline 2005". The goal of the project was to specify and implement a service-oriented information technology solution for the legally viable and auditable Long-Term Storage of electronic documents (for more information, see: http://www.archisafe.de)
2. Overview

2.1 Goals

The goal and purpose of the ArchiSafe-Module is the realisation of a standardised interface with at least those archive functions that play a role in the preservation of evidence. In order to achieve strict logical separation between the upstream IT specialist applications and the actual ECM/Long-Term Storage systems, it is recommended that all needed archive functions are abstracted from the ArchiSafe-Module in a manufacturer-independent manner.

The ArchiSafe-Module logically and functionally decouples the flow of data between the IT specialist applications and the electronic ECM/Long-Term Storage for the storage or retrieval of archived data and documents. Furthermore, this module offers standardised interfaces for communication with the cryptographic components ([TR-ESOR-M.2] and [TR-ESOR-M.3] in Figure 1) that support the authenticity and integrity of the saved electronic documents.

Each archive operation of the upstream external IT applications that serve to ensure, maintain or prove the preservation of evidence of electronic documents shall be carried out by the ArchiSafe-Module.

For this purpose, the external IT application opens a secure communication channel with the ArchiSafe-Module and sends an archive inquiry (archive function name request). The ArchiSafe-Module identifies and authenticates the application making the request and offers the configurable option to verify the syntactic validity of the (submission) information packages being transmitted by the application making the request against the configuration data stored in the ArchiSafe-Module (XML schemata, communication and processing rules).

When (submission) information packages are stored, the ArchiSafe-Module initiates the securing of evidential quality of the information to be archived in that:

1. Existing electronic signatures are verified for validity and the results of the verification are stored in a standardised form so that the association with the signature data is maintained. Signature verification is realised by a cryptographic component (module) that shall fulfil the requirements described in Annex [TR-ESOR-M.2] to this Technical Guideline.

2. The ArchiSig-Module (see Annex [TR-ESOR-M.3] to this Technical Guideline) is commanded to furnish each archive data object to be archived with a unique document identifier (archive data object ID, AOID) if this element is not already available, and calculate with AOID one or several hash values for the entire archival package or the parts of the archive data object that are to be protected cryptographically.

Finally, the data to be archived and the AOID is transmitted to an authenticated ECM/Long-Term Storage via a secure communication channel. The successful storing of archive data objects is completed by returning the archive data object ID (AOID) to the application making the request.

This AOID is needed by the upstream IT specialist applications for each retrieval, each update and deletion of archived data. Likewise, retrieval of evidence records is also only possible when a valid AOID is presented.

---

3 For example, this channel may be physically secured cables or an encrypted connection with suitably strong authentication of both parties (see also TR-ESOR-F, chapter 5.6).

4 Note on the terminology used in this Annex: In this Annex M.1 to the Technical Guideline 03125, the more specific technical term “data objects” is also used in some cases to refer to “information packages”.

5 The archive data object ID (AOID) may also be created in other components, such as the ECM/Long-Term Storage. Furthermore, a syntactically correct document identifier (AOID) may also be generated and transferred by the business application.

6 Details about the elements/areas of an archival information package for which a hash value is computed can be found in Annex F.
3. Definition of the ArchiSafe-Module

The term "ArchiSafe-Module" includes all functions that serve the realisation of the input interface of the TR-ESOR-Middleware and the administration and control access of external upstream IT specialist applications to the ECM/Long-Term Storage (see Figure 1). The primary purpose of the ArchiSafe-Module is the implementation of a reliable security gateway for communication, and thus also the decoupling from external applications, with an ECM/Long-Term Storage, the regulation of the information flow within the TR-ESOR-Middleware and the control of the functions provided by the TR-ESOR-Middleware for the long-term preservation of evidence of the cryptographically signed documents.

3.1 Basic design and functional differentiation

(A3.1-1) The ArchiSafe-Module should be a Middleware component or a part of a Middleware component that provides and controls access to the ECM/Long-Term Storage in a trustworthy and reliable manner.

(A3.1-2) The ArchiSafe-Module shall run as an independent application or as an independent (functionally differentiated) part of an application (also of the ECM/Long-Term Storage) on a trustworthy IT system (IT platform).

(A3.1-3) The system platform on which the ArchiSafe-Module is operated shall be protected adequately against unauthorised access to the data and functions of the module.

(A3.1-4) The ArchiSafe-Module shall use trustworthy cryptographic components that are described in the Annex [TR-ESOR-M.2] and Annex [TR-ESOR-M.3] to this Technical Guideline and which are controlled by the S.1 and S.6 interfaces defined in Annex [TR-ESOR-S] for the preservation of the probative value of electronically signed data, for example for legally compliant signature renewal. 7

3.2 Integration of the ArchiSafe-Module

(A3.2-1) The ArchiSafe-Module should have a modular character and be able to be replaced by new, functionally compatible implementations at all times.

(A3.2-2) For the integration of the ArchiSafe-Module in existing or planned IT environments in the sense of this Technical Guideline, the ArchiSafe-Module shall be able to implement or use at least the S.1, S.4, S.5 and S.6 interfaces specified in Annex [TR-ESOR-S] to this Technical Guideline. In doing so, the ArchiSafe-Module is called by external applications via the S.4 interface and calls the Cryptographic-Module via the S.1 interface, the ArchiSig-Module via the S.6 interface and the ECM/Long-Term Storage system via the S.5 interface.

(A3.2-3) The implementation and use of additional interfaces shall not compromise the guarantee that the basic security-related requirements (see also section 3.3) are fulfilled.

3.3 Fulfilment of basic security-related requirements

(A3.3-1) An ArchiSafe-Module that conforms to this Technical Guideline shall fulfil the security objectives and requirements of the [ACMPP] protection profile.

7 The requirement explicitly does not exclude that the functions of the ArchiSafe-Module and the cryptographic components are subsumed in a standardised security gateway.
4. Functional requirements

This section of the Technical Guideline specifies and explains the functional requirements for an ArchiSafe-Module on the basis of the [ACMPP] protection profile. The requesting interfaces (interface signatures) of the ArchiSafe-Module are specified as S.4 in Annex [TR-ESOR-S] to this Technical Guideline.

Definition of terms:

- An **information package** is a document or date to be archived. An information package can be present in any format, preferably though in those formats recommended in Annex F.
- An **archival information package** in the sense of this Technical Guideline corresponds syntactically to the XML formatted Archival Information Package (XAIP) described in Annex F to this Technical Guideline. An archival information package can thus contain one or several information packages as well as meta data. The archive data object ID (AOID), though, always refers to one archival information package. It is not necessary for information packages to be transferred into an archival information package for archiving, and it is also not necessary that archival information packages are stored physically in the ECM/Long-Term Storage. It is merely required that all functions of the TR-ESOR-Middleware relate to an archival information package and thus to all information packages that relate to one of the same and, in particular, that the retrieval functions return an archival information package (or parts thereof) in valid XML format (see Annex F).
- A **data element** is a part of the XML structure of an archival information package. In this respect, it can be the entire archival information package, a partial tree of the XML structure, an individual XML element or also only the value of an XML element.

(A4.0-1) An ArchiSafe-Module that conforms to this Technical Guideline shall at least provide the following operations:

1. Archiving an (archival) information package in the ECM/Long-Term Storage (ArchiveSubmissionRequest),
2. Requesting an archival information package from the ECM/Long-Term Storage (ArchiveRetrievalRequest),
3. Deleting an archival information package in the ECM/Long-Term Storage (ArchiveDeletionRequest),
4. Requesting evidence records for proving the authenticity and integrity of archived archival information packages (ArchiveEvidenceRequest).

An ArchiSafe-Module that conforms to this Technical Guideline should additionally provide the following operations:

1. Updating an archival information package in the ECM/Long-Term Storage that has already been archived (ArchiveUpdateRequest)
2. Requesting individual data elements from an archived archival information packages (ArchiveDataRequest)
3. Verifying supplemental evidence data (signatures, time stamps, certificates, certificate revocation lists, OCSP responses etc.) and evidence records that are contained in an archive data object or were additionally transferred when retrieving a function (VerifyRequest / -Response)

(A4.0-2) False or incorrectly parametrised requests shall not result in improper functioning of the ArchiSafe-Module.

---

8 An information package or archival information package is also called „archive data object (group)” in this technical guideline.
9 An operation is an inquiry from an external client software to the ArchiSafe-Module for the execution of defined operations in the TR-ESOR-Middleware or in the ECM/Long-Term Storage.
10 It is stipulated that the interface accepts both complete archival information packages and individual information packages. The response is always an AOID that refers to an archival information package.
(A4.0-3) The ArchiSafe-Module shall have comprehensive and configurable options for logging the various accesses or access attempts to the archive.

(A4.0-4) The logs created by the ArchiSafe-Module shall be secured against access so that only authorised persons\(^{11}\) (e.g. the data protection officer, the security officer or the administrator of the archive system) actually have access.

(A4.0-5) The following applies to all functions listed in (A4.0-1): The ArchiSafe-Module shall be capable of establishing a secure communication channel with the requesting client application to request the function.

(A4.0-6) The following applies to all functions listed in (A4.0-1): A requesting client software shall only be granted access to the archival information packages for which it has access rights and authorisations.

4.1 Archiving electronic data – ArchiveSubmissionRequest

The ArchiveSubmissionRequest function makes it possible for an authorised IT application (client software\(^{12}\)) to store a (new) archive data object in the ECM/Long-Term Storage through a secure communication channel.

(A4.1-1) The ArchiSafe-Module shall be able to archive XML-based archive data object (group) with an ArchiveSubmissionRequest. Furthermore, it should also be able to archive binary data with an ArchiveSubmissionRequest.

(A4.1-2) The archive data object to be archived shall be part of the request. If the archive data object to be archived is an XML structure (XAIP), it shall be possible to verify it for syntactic correctness against an authorised XML schema stored in the ArchiSafe-Module. If the syntax verification fails, the archiving shall be denied with a clear and understandable error message.

(A4.1-3) The ArchiSafe-Module shall be able to initiate the verification of the archive data object including the supplemental evidence data (signatures, time stamps, certificates, certificate revocation lists, OCSP responses etc.) and/or evidence records that are contained therein or were additionally transferred. If the archive data object to be archived includes electronic signatures and supplemental evidence data or evidence records, the ArchiSafe-Module shall verify the validity of the signatures and evidence records (or let it be verified) and store the verification results in a standardised form in the archive data object. If the verification of the evidence records fails, the archive data object shall not be processed further.

For this purpose, the ArchiSafe-Module transfers the archive data object including the supplemental evidence data (signatures, time stamps, certificates, certificate revocation lists, OCSP responses etc.) and/or evidence records that are contained therein or were additionally transferred to the Cryptographic-Module through the S.1 interface prior to the actual storage in the ECM/Long-Term Storage (see Annex [TR-ESOR-S] and Annex [TR-ESOR-M.2] as well as Annex [TR-ESOR-E]).

The Cryptographic-Module verifies the supplemental evidence data (signatures, time stamps, certificates, certificate revocation lists, OCSP responses etc.) and/or evidence records. The verification results determined during this verification (certificates, certificate revocation lists, OCSP responses) should be stored by the Cryptographic-Module in the data structures of the archive data object provided for this purpose. The so enriched archive data object or a verification report (see [OASIS-VR] or [TR-ESOR-VR]) is then to be returned to the ArchiSafe-Module. Alternatively, the Cryptographic-Module only returns the verification results as a verification report pursuant to [OASIS-VR] or [TR-ESOR-VR] to the ArchiSafe-Module which then stores the verification results in the provided data structures of the archive data object.

The Middleware should provide the possibility that a comprehensive verification report [TR-ESOR-VR] about the successful storage can be requested for an XML-based archival

---

11 Those persons who should receive actual access to the logs should be specified in a locally applicable IT security concept.

12 A client application in the sense of this Technical Guideline is an external (upstream) IT application that is capable of and authorised to use the ArchiSafe-Module to archive data in the ECM/Long-Term Storage and search for, update, retrieve or delete archived data.
information package (XAIP) including the supplemental evidence data (signatures, time stamps, certificates, certificate revocation lists, OCSP responses etc.) that are contained therein or were additionally transferred.

If the signature or certificate verification fails (e.g. due to obsolete algorithms which are no longer supported by the Cryptographic-Module), a clear and understandable error message shall be transmitted to the business application. Storage is possible in such a case if a reason is stored together with a clear and understandable verification report in the CredentialSection of the archive data object. Otherwise, storage should be denied.

**NOTICE:** It is urgently recommended to make use of the possibility to verify the signatures upon archive submission. Otherwise, data that has already been manipulated or invalid signatures could enter the archive system, in which case this loss of integrity may only be noticed several years later.

(A4.1-4) It shall be possible for the ArchiSafe-Module to store signature verification results including the associated certificate information into the XML data elements of the XML-based archive data object provided for that purpose (see Annex [TR-ESOR-F]) as long as this has not been carried out by the Cryptographic-Module yet. If no XML-based archive data object is used, the signature verification results may be inserted into the transmitted (binary) content information package if allowed by the format being used.

(A4.1-5) Prior to the final storage in the ECM/Long-Term Storage, the ArchiSafe-Module should transfer the archive data object to the ArchiSig-Module (see Annex [TR-ESOR-S] and Annex [TR-ESOR-M.3]) through the S.6 interface. Then, the archive data object is stored by the ArchiSig-Module in the ECM/Long-Term Storage.

Alternatively, the ArchiSafe-Module transmits the archive data object directly to the ECM/Long-Term Storage and the functions of the ArchiSig-Module are requested for this archive data object at a later point in time by another entity. In doing so, it shall be ensured that this mentioned point of time is close to the time of archiving (e.g. not after several weeks) and that all newly archive data objects are actually (verifiably) included by this function and that adequate procedures have been implemented for responding to any possible error.

(A4.1-6) The ArchiSafe-Module shall not in any case change or delete the payload data (in the archive data object).

(A4.1-7) An archive data object that already exists in the ECM/Long-Term Storage shall not be overwritten or changed (modified) in the ECM/Long-Term Storage with this request.

(A4.1-8) In the case of successful storage, the unique document identifier, the archive data object ID (AOID), shall be returned to the client application making the request.

### 4.2 Updating archived data – ArchiveUpdateRequest

The ArchiveUpdateRequest function makes it possible for an authorised IT application (client software) to add a new version for an already existing archive data object in the ECM/Long-Term Storage through a secure communication channel.

The reason for this new version could be an additional element, a changed element or a deleted element. From a technical point of view, however, only the new version is added; existing data is not changed or deleted anywhere because of this request.

The evidence-based value of the data that has already been archived shall not be compromised by the ArchiveUpdateRequest.

(A4.2-1) A valid (syntactically correct and actually issued) archive data object ID (AOID) shall be part of a request.

---

13 The Technical Guideline urgently recommends that the ArchiSafe-Module transmits the archive data object directly to the ArchiSig-Module for the computation of the hash value and does not store the archive data object in the ECM/Long-Term Storage first. In the latter case, the period of time between the saving and computation of the hash value results in a certain uncertainty.
A syntactically correct, supplementing XML-based archival information package (Delta-XAIP-element) pursuant to [TR-ESOR-F] shall be part of the request with the purpose of adding and deleting documents, data, meta data, signatures, signature verification information (credentials) or other evidence records to/from archive data objects as well as changing documents, data or meta data in a new version as well as indicating the previous version.

Several elements to be changed/added/deleted for this archival information package can be transmitted in a common structure. The transmission of empty structure elements with the goal of overwriting (deleting) existing structure elements by circumventing the version control mechanism is not allowed.\footnote{14}

A supplementing XML-based archive data object (Delta-XAIP-element) in compliance with [TR-ESOR-F] shall be transmitted, whose structure shall be verified in the same way like during the archive submission process (see (A4.1-1)).

If supplemental evidence data (signatures, time stamps, certificates, certificate revocation lists, OCSP responses etc.) and/or evidence records are transferred, procedures analogue to the archive submission process shall be applied to this data (see (A4.1-3) and (A4.1-4)).\footnote{15}

Each update shall result in a new version of the archival information package. In doing so, a significant characteristic is a new version number with the same AOID and a new version manifest (for details in this respect, see Annex F).

"Updating" meta data/data objects in the archive data object shall occur within the Middleware based on the following principle, but not necessarily in the same sequence given below:\footnote{16}

1. Creating a new version manifest\footnote{17} on the basis of the respective data of the Delta-XAIP-element, among other things by accepting the new version manifest from the Delta-XAIP-element.
2. Creating/assigning a new version number. Using the <prevVersion> element contained in the Delta-XAIP-element, it can be verified whether new versions have already been generated in the meantime and conflicts may arise for this reason.
3. Adding "new" meta data/information packages/credentials to the archive data object. (In doing so, existing data is neither changed nor deleted).
4. Removing the manifest entries\footnote{18} of the meta data/information packages from the new version manifest, which are no longer included in the new version (as needed). However, the actual meta data/information packages are not removed.
5. Adding manifest entries to or changing them for "new" meta data/information packages in the new version manifest.

Only adding version manifests, meta data, information packages and credentials in new versions of the archival information package is allowed. Actual changes to existing data are not allowed. Requests for changes for version-independent meta data (or meta data otherwise labelled as non-changeable) (e.g. AOID or packageInfo) are not allowed.

The new (updated) archive data object should then be transmitted directly to the ArchiSig-Module. Alternatively, it shall be ensured that the new version is also secured by the ArchiSig-Module (see (A4.1-5)).
The response shall receive a status value that indicates the success of the operation. In case of success, the new version number shall also be returned.

4.3 Retrieving archived data – ArchiveRetrievalRequest

The ArchiveRetrievalRequest function makes it possible for an authenticated client application to retrieve an archival information package from the ECM/Long-Term Storage through a secure communication channel with submission of a valid archive data object ID (AOID) and, if necessary, one or several VersionIDs in addition. If no VersionID is indicated, the respective current version is returned. It shall be possible to retrieve all versions of an archival information package.

(A4.3-1) A valid (syntactically correct and actually issued) archive data object ID (AOID) shall be part of a request. Optionally, one or several valid (syntactically correct and actually issued) VersionIDs can be indicated.

(A4.3-2) The archival information package linked with the AOID and, if applicable, the VersionID in the ECM/Long-Term Storage shall be returned. If the VersionID contains the value all, all existing versions of an archival information package shall be returned. In the event of an error (for example no valid AOID or no valid VersionID for the request), the request shall be denied with a clear and understandable error message.¹⁹

(A4.3-3) The archival information package shall be returned in an XML format (XAIP). The XML format shall follow a verifiable XML schema that can be configured by the user of the overall system. The requirements from Annex [TR-ESOR-F] are mandatory for the XML format or the XML schema.²⁰

(A4.3-4) When requesting (returning) archived data, it may be required that the returned XAIP should contain a corresponding EvidenceRecord in the specified format (pursuant to [RFC4998] and, in addition to this, pursuant to [RFC6283] if necessary) for each version.

4.4 Deleting archived data – ArchiveDeletionRequest

The ArchiveDeletionRequest function makes it possible to delete an archival information package that belongs to an AOID in the ECM/Long-Term Storage.

(A4.4-1) The deletion shall be confirmed by the ECM/Long-Term Storage in a comprehensible manner.

(A4.4-2) If the ECM/Long-Term Storage has no deletion function or if the media used do not allow deletion, the ArchiSafe-Module should respond to the request for this function with an appropriate error message.

(A4.4-3) In the event of deletion before the retention periods have expired, the request shall have a reason that can be logged. The ArchiSafe-Module shall enforce compliance with the retention periods and the existence of a reason that can be logged in the event of premature deletion.

(A4.4-4) Deletion shall be denied with a clear and understandable error message if an AOID is invalid or in the event that no reason was given for the premature deletion.

(A4.4-5) The ArchiSafe-Module should be able to initiate a deletion of archival information packages in the ECM/Long-Term Storage that cannot be restored physically by means of configuration or parameterisation of the ECM/Long-Term Storage.

(A4.4-6) The ArchiSafe-Module shall save/log the respective available reason in the event of premature deletion.²¹

¹⁹ It is left to the manufacturer whether they execute the request completely or only partially or confirm them with an error message if one or several VersionIDs in a transmitted list of VersionIDs is/are not correct.

²⁰ It must be noted that this XML schema may change in the course of time and that already archived XAIPs might then no longer correspond to the new schema. It is up to the manufacturer to find a solution for this problem. It would be conceivable, for example, that it is specified which XAIP had then been archived on the basis of which schemas, the periods of validity of the diverse schemas could be documented generally, the XAIP to be returned is embedded in the respective new XAIPs based on the new schema etc. (see also [TR-ESOR-M.3], A2.6-1)
4.5 Returning evidence records – ArchiveEvidenceRequest

The ArchiveEvidenceRequest function makes it possible to request a set of evidence records regarding the integrity of a version of a archival information package stored in the ECM/Long-Term Storage. The ArchiSafe-Module passes this request to the ArchiSig-Module via the TR-ESOR-S.6 interface for execution. The ArchiSig-Module uses the same interface to return a version-specific EvidenceRecord (see Annex TR-ESOR-M.3) as a set of evidence records.

(A4.5-1) An valid archive data object ID (AOID) as well as one or several VersionID(s) shall be part of the request. The return date shall be an EvidenceRecord for each VersionID in ERS notation pursuant to [RFC4998] as well as additionally pursuant to [RFC6283]22.

(A4.5-2) In the event of an error (for example no valid AOID), the request shall be answered with a clear and understandable error message to the business application.

(A4.5-3) The ArchiSafe-Module shall not change the AOID or VersionIDs transmitted and the evidence records received, but shall only forward them.

(A4.5-4) In the event of changed (versioned) archival information packages, it shall be ensured that an ER is created and returned for each version so that the integrity and authenticity can be proven up to the time of the initial archiving (see (A4.2-6) and footnote 16 on page 11).

4.6 Returning data elements – ArchiveDataRequest

The ArchiveDataRequest function makes discrete (read-only) retrieval of individual data elements from an archival information package possible without having to retrieve the respective entire archival information package from the ECM/Long-Term Storage.

The ArchiSafe-Module accesses the ECM/Long-Term Storage through the [TR-ESOR-S.5] interface and requests the relevant data elements from the archival information package identified by the AOID. The data elements retrieved are returned to business application making the request via the [TR-ESOR-S.4] interface.

(A4.6-1) No more than one valid archive data object ID (AOID) as well as unique identifiers for the data elements to be retrieved shall be part of the request.

(A4.6-2) The data elements retrieved are returned. The data elements shall not be manipulated or changed during retrieval.

(A4.6-3) In the event of an error (for example no valid AOID), the request shall be answered with a clear and understandable error message to the application making the request.

4.7 Verifying the archival information package including the supplemental evidence data and evidence records that are contained therein or were additionally transferred – VerifyRequest

The VerifyRequest function makes it possible to verify an archival information package including the supplemental evidence data (signatures, time stamps, certificates, certificate revocation lists, OCSP responses etc.) and/or evidence records that are contained therein or were additionally transferred.

The ArchiSafe-Module accesses the Cryptographic-Module ([TR-ESOR-M2]) through the TR-ESOR-S.1 interface and transfers the data required for verification. The verification information (certificates, certificate revocation lists, OCSP responses) determined by the Cryptographic-Module are returned as attributes or properties in the corresponding signatures or in the corresponding elements of the archival information package or as an independent verification report. The result of this function call is returned to the business application via the TR-ESOR-S.4 interface. The syntactic

21 Here, it cannot be defined where, in which form and for what period of time this reason is stored and which people shall have access to it in which form. Conceivable are, among other things, storage in the normal log files of the ArchiSafe-Module or storing the reason in the data storage devices of the ArchiSig-Module together with the hash value of the document, which is still present. The manufacturer is free to implement another solution that is adequately secure.

22 [RFC4998] shall, [RFC6283] may be supported.

Federal Office for Information Security
verification of XML-based archival information packages is carried out by the ArchiSafe-Module itself.

(A4.7-1) The data required for verification as well as the supplemental evidence data or evidence records that are contained therein or were additionally transferred (see [TR-ESOR-S.1] or [TR-ESOR-E]) shall be part of the request.

(A4.7-2) Either the archival information package supplemented by the verification information generated or a verification report pursuant to [OASIS-VR] or [TR-ESOR-VR] which also includes the results of the conformity evaluation of an XAIP shall be returned.

(A4.7-3) In the event of an error (e.g. an invalid signature), the request shall be answered with a clear and understandable error message to the application making the request. The transfer of a verification report pursuant to [OASIS-VR] or [TR-ESOR-VR] may be requested explicitly.
5. Security functions

Based on the logical and functional decoupling of the data flow between the IT specialist applications and the ECM/Long-Term Storage, the ArchiSafe-Module shall at least provide the following security-related functions:

(A5.0-1) The prevention of unauthorised access to the ECM/Long-Term Storage by reliably identifying and authenticating of upstream external IT applications (see also (A3.1-1) and (A4.0-6)),

(A5.0-2) The reliable and verifiable storage of the archive data objects only in the ECM/Long-Term Storage systems allowed for this purpose.

(A5.0-3) The assurance that archived data can only be changed, retrieved, and deleted by applications that are authorised to do so.

Unfounded deletion of data prior to the expiry of the statutory retention period is to be prevented in a reliable manner (see also (A3.1-1), (A4.0-6) and (A4.4-3)).

Safeguards to protect the confidentiality of the archived information, for example by encrypting data, as well as the safeguards to create signatures and to perform signature renewal on archived, electronically signed data are to be realised outside of the ArchiSafe-Module.

---


24 Pursuant to the recommended IT Reference Architecture (see Figure 1) and the description of the processes in the Main Document of this Technical Guideline [TR-ESOR], the ArchiSafe-Module transfers the archive data objects that are to be newly archived to the ArchiSig-Module first (see Annex [TR-ESOR-M.3]). For that reason, the ArchiSafe-Module can only indirectly influence the actual storage in the ECM/Long-Term Storage. For that reason, the requirement states that ArchiSafe in fact (indirectly) transmits all archive data objects transferred (and successfully verified) by the IT application to the ECM/Long-Term Storage. Thus, the storage in the ECM/Long-Term Storage is only then considered to have taken place when the ECM/Long-Term Storage has returned an archive data object ID (AOID) to the IT application through the ArchiSafe-Module.

25 The authorisation model within ArchiSafe should indeed make it possible to issue the authorisations separately for the archiving functions listed. Thus, it should not only be possible to give an application full access rights or none, but one should also be able to define which functions this application may use.