BSI Technical Guideline 03125
Preservation of Evidence of Cryptographically Signed Documents

Annex TR-ESOR-B: German Federal Agency Profiling

<table>
<thead>
<tr>
<th>Designation</th>
<th>German Federal Agency Profiling</th>
</tr>
</thead>
<tbody>
<tr>
<td>Abbreviation</td>
<td>BSI TR-ESOR-B</td>
</tr>
<tr>
<td>Version</td>
<td>1.2</td>
</tr>
<tr>
<td>Date</td>
<td>19.12.2014</td>
</tr>
</tbody>
</table>
# Table of contents

1. Introduction............................................................................................................................4
2. Overview..................................................................................................................................6
3. Requirements profiling for the Federal Administration Agencies.................................8
   3.1 TR-ESOR Main Document...............................................................................................8
   3.2 TR-ESOR Annex E........................................................................................................9
   3.3 TR-ESOR Annex F.........................................................................................................11
   3.4 TR-ESOR Annex S.......................................................................................................12
   3.5 TR-ESOR Annex M.1.................................................................................................13
   3.6 TR-ESOR Annex M.2.................................................................................................13
   3.7 TR-ESOR Annex M.3.................................................................................................13
   3.8 TR-ESOR Annex ERS.................................................................................................13
   3.9 TR-ESOR Annex VR.................................................................................................13
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 "ArchiSafe-Module" (see [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" (see [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 may provide functions for the encryption and decryption of data and documents;
- The "ArchiSig-Module" (see [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 set for it through the two interfaces that are still part of the TR-ESOR-Middleware.
  The application layer that may include an XML adapter is not a direct part of the Technical Guideline either, even though this XML adapter may be implemented as part of a Middleware.

The IT Reference Architecture depicted in Figure 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-B" and specifies requirements, data formats and protocols for the storage of cryptographically signed data and documents with preservation of evidence for federal administration issues in particular.

This profile should at least be applied by German federal agencies when the new procurement or update of an archive system or an Archive-Middleware for the storage of cryptographically signed documents is scheduled. For already existing installations which are to be used to store cryptographically signed documents for a long period of time, applying this profile is highly recommended.
2. Overview

The complete and correct storage of electronic documents and data in public administration is defined by the fundamental obligation to ensure total and truthful record management.

The obligation to provide total and truthful record management ensures the continuity and verifiability of administrative acts as well as the traceability of administrative decisions. The inherent informational and evidential value of a record is particularly important for the public administration (protocol and evidence function of the record). Therefore, the record-keeping obligation of the public administration offices already implies the evidential purpose and as its prerequisite also the availability and negotiability of the electronic documents which are to be stored, including the data required for proving the documents' integrity and authenticity.

The "Common Ministerial Rules of Procedure" (GGO - Gemeinsame Geschäftsordnung der Bundesministerien) and the "Directive on the Processing and Management of Records in Federal Ministries" (RegR – Registraturrichtlinie) are particularly significant for the preservation of evidence of electronically signed data and documents in the federal administration. Both regulations explicitly take account of electronic communication and the use of electronic media. This includes the regulation of the electronic receipt in § 13 Clause 2 GGO and the associated annex as well as the use of electronic signatures pursuant to the German Signature Act in documents having direct legal effect or particular political importance (§ 18 Clause 2 GGO). § 18 RegR determines that suitable measures, which have not been specified, must be taken to guarantee the completeness, integrity, authenticity and readability of preserved electronic records (§ 18 Clause 1 Subclause 2 RegR). Furthermore, § 18 Clause 3 RegR clarifies that electronically secured records require ongoing maintenance and continually have to be converted into formats and transferred to data storage media which comply with the current state of technology in a timely manner without changing their contents.

The assumption and proof of the authenticity of electronic documents are based on the following four aspects:

a) The reliability, i.e. there are substantiated and comprehensible facts or indications that a document's content may be regarded as a complete and authentic reproduction of those facts and events of which it claims to be either evidence or report,

b) The negotiability (availability and readability) of electronic documents, i.e. the fact that the data and documents which have been apostrophised as authentic may be localised and retrieved at all times, which means that they may be presented and interpreted (read) using the common IT systems available at that time,

c) The integrity or the unchanged state of electronic documents as well as

d) The unique and verifiable, i.e. non-repudiable, assignment of the authorship of an electronic document to a person or any other source.

The proof of integrity of electronic documents and data may be provided using cryptographic measures based on the creation of a digital "fingerprint" of the document or the data which is suitable to permit the reliable detection of subsequent manipulation.

For a doubtless determination of the authorship of electronic documents and data, the following prerequisites shall also be fulfilled:

---

2. See [KNAACK 2003], p. 46.
3. In the current language, the term "authenticity" is usually associated with the characteristics of being reliable or credible due to facts or events which occurred (or even which only may occur). Hence, an object is considered to be authentic if the perception of the object may be judged in accordance with its nature and purpose due to verifiable facts or events. The claim or the assumption of the authenticity of electronic documents is thus primarily a conclusion, which may be drawn from known and comprehensible or verifiable, facts and events, or which may be justified by them. These facts and events may refer to the way in which the document has been created or how it has been processed and, above all, how it has been stored (preserved) (in this respect, see also [NATARCHUK2002], p. 8).
4. In this respect, see also [HIGGINS 2010], [NATARCHUK 2002].
5. Such "fingerprints" are generated using cryptographically secured hash functions and are sent or stored along with the document so that the recipient or the user of the object may verify the integrity of the object by means of this fingerprint (see [SCHNEIER], p. 491 et seq.)

---
1. A trustworthy and, above all, verifiable digital identity\textsuperscript{6} of the author or the source of the document as well as
2. An indissoluble, fraud-resistant and at all times verifiable connection between this digital identity and the document – for instance an electronic signature.

In order to support and maintain the evidential suitability of electronically signed data and documents for the duration of the retention period, the following steps shall thus be taken:

- The data and documents shall
- be stored in a standardised format that will be negotiable in the long term so that their retrieval may always be taken for granted using the current IT systems available at the time of retrieval
- Electronic signatures and time stamps are securely and reliably created, verified, renewed and stored in the quality stipulated in the legal regulations, and
- Moreover, the verification data needed for signature verification at a later point in time should be obtained in a timely manner, i.e. directly after the creation or the verification of the signature, if possible, and be deposited in a standardised format that will be negotiable in the long term together with the documents and data to be archived.

Within this context and aiming at increasing the interoperability of the electronic archive solutions in the government agencies of the federal administration, this document specifies the functional and technical requirements of the Technical Guideline TR-03125 for the setup and the operations of electronic archives in the federal administration. In doing so, the following sections will only mention the requirements which have been designed particularly for the federal agencies. All the requirements of the Technical Guideline TR-03125 that are not listed here remain unchanged. No additional requirements will be defined in this document, only existing requirements will be further concretised.

(A2.0-1) If the technical conformity of \textit{Conformity Level 3} is to be proven for a product or system consisting of at least one of the modules specified in this Technical Guideline, conformity with the requirements of the Technical Guideline TR-03125 set out in this document shall be proven pursuant to [TR-ESOR-C.3] in addition to \textit{Conformity Level 2}.

\textsuperscript{6} The most common form of electronic identities nowadays are electronic certificates. By means of these certificates, digitally coded real identifiers (name, postal address etc.) of an individual or an object are linked to a digital attribute, which certifies the issuer of the certificate in an electronic, i.e. machine-readable, file with the help of a trustworthy third party and is used for electronic unique identification.

Federal Office for Information Security 7
3. Requirements profiling for the Federal Administration Agencies

The requirements which have been further concretised for the federal agencies are listed below. For better understanding, the original versions of the requirements are listed here and their respective revision. Furthermore, a justification for each modified requirement is given.

3.1 TR-ESOR Main Document

<table>
<thead>
<tr>
<th>5.1 Functions of the Middleware for preservation of evidence</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Original</strong></td>
</tr>
<tr>
<td>[A5.1-4] Prior to the storage in the ECM/Long-Term Storage, the Middleware <strong>should</strong> check the syntax of the archive data objects to be transferred for storage for conformity with the data formats defined and specified by the user and operator of the archive system. In the case of non-conformity, storage in the ECM/Long-Term Storage <strong>shall then</strong> be denied.</td>
</tr>
<tr>
<td><strong>Revision</strong></td>
</tr>
<tr>
<td>[A5.1-4B] Prior to the storage in the ECM/Long-Term Storage, the Middleware <strong>shall</strong> check the syntax of the archive data objects to be transferred for storage for conformity with the data formats defined and specified (on the basis of a valid XML schema) by the user and operator of the archive system. In the case of non-conformity, storage in the ECM/Long-Term Storage <strong>shall then</strong> be denied.</td>
</tr>
</tbody>
</table>

Explanation:

By checking the syntax of the archive data objects to be transferred for storage into the ECM/Long-Term Storage, the correctness of the data retrieved from the upstream applications and stored shall be ensured and, at the same time, it shall be guaranteed that a re-import of the data stored into the upstream applications using the data formats specified for the storage remains easily possible.

<table>
<thead>
<tr>
<th>6.2 Recommended data formats</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Original</strong></td>
</tr>
<tr>
<td>[A6.2-1] In the interest of long-term availability and negotiability of the documents and data to be archived, only those data formats <strong>should</strong> be used that make it possible to archive in a manner that is negotiable in the long term in a platform- and manufacturer-independent way.</td>
</tr>
<tr>
<td><strong>Revision</strong></td>
</tr>
<tr>
<td>[A6.2-1B] In the interest of long-term availability and negotiability of the documents and data to be archived, only those data formats <strong>shall</strong> be used that make it possible to archive in a manner that is negotiable in the long term in a platform- and manufacturer-independent way. Furthermore, the original may be stored additionally if necessary.</td>
</tr>
</tbody>
</table>

Explanation:

§ 18 RegR determines for the preservation of electronic records that the readability, and hence the availability, shall be guaranteed throughout the duration of the retention period by implementing suitable measures. This may be achieved in the easiest way by using standardised, platform- and manufacturer-independent data formats.
2.0 Overview

[A2.0-1] Pursuant to this, only the functional and logical conformity of a product or system consisting of at least one of the modules specified in this Technical Guideline with the requirements of the Technical Guideline shall be proven in Conformity Level 1. Thus, the support of the individual interfaces described here and in [TR-ESOR-S] is optional.

[A2.0-1B] Pursuant to this, only the functional and logical conformity and technical interoperability of a product or system consisting of at least one of the modules specified in this Technical Guideline with the requirements of the Technical Guideline shall be proven for conformity with the Federal Agency Profile. Thus, the support of the individual interfaces described here and in [TR-ESOR-S] is optional.

Explanation:

§ 18 RegR determines for preservation of electronic records that the integrity and authenticity shall be guaranteed by implementing suitable measures. This applies in particular to electronically signed documents. In conformity with the objectives and intentions of this Technical Guideline, it directly follows from this that the functional and logical conformity of a product or system consisting of at least one of the modules specified in this Guideline with the requirements of the Technical Guideline shall be proven for the technical implementation of measures for the preservation of evidence of electronically signed documents.

This requirement does not imply that all purely internal interfaces shall comply with the XML-based interface specifications of this Technical Guideline in the case of a product combining several modules of the Technical Guideline.

---

7 See [TR-ESOR-C.1]
8 See [TR-ESOR-C.2]
## 2.0 Overview

### Original

If the technical conformity and interoperability with Conformity Level 2 is to be proven for an existing product or system consisting of at least one of the modules specified in this Technical Guideline, this shall be carried out on the basis of the eCard-API-Framework profile described in this document. In doing so, those functions and parameter constellations described in more detail in this document shall be supported at a minimum.

If the technical conformity with the Federal Agency Profile is to be proven for an existing product or system consisting of at least one of the modules specified in this Technical Guideline, this shall be carried out on the basis of the eCard-API-Framework profile described in this document. In doing so, those functions and parameter constellations described in more detail in this document shall be supported at a minimum.

### Revision

If the technical conformity and interoperability with Conformity Level 2 is to be proven for an existing product or system consisting of at least one of the modules specified in this Technical Guideline, XAIP as defined in [TR-ESOR-F] should be used as XML data format. Deviations in the XML data format used are permissible, but it shall be explained how an equivalent functionality is realised. It shall be explained in particular how a transformation into the XAIP format specified in [TR-ESOR-F] may be performed.

If the technical conformity and interoperability with the Federal Agency Profile is to be proven for an existing product or system consisting of at least one of the modules specified in this Technical Guideline, this product or system shall use an XML container based on the XML schema XAIP specified in Chapter 3 of Annex F as XML data format on all of its interfaces defined by the Technical Guideline. XAIP as defined in [TR-ESOR-F] should be used as XML data format. Deviations in the XML data format used are permissible, but it shall be explained how an equivalent functionality is realised. It shall be explained in particular how a transformation into the XAIP format specified in [TR-ESOR-F] may be performed.

### Explanation:

The eCard-API-Framework is part of the eCard strategy of the Federal Government and provides a number of standardised, homogeneous interfaces for the execution of cryptographic operations. To ensure interoperability with products (components) certified and already used within the federal administration, it is required to implement interfaces for the preservation of evidence of electronically signed documents on the basis of the eCard-API-Framework profile described in the Technical Guideline.

In order to prove the technical conformity and interoperability of products and components for the storage of electronic documents with preservation of evidence with the objectives and intentions of this Technical Guideline, it is required to use a homogeneous and standardised data format for the archive data objects.
### 2.0 Overview

<table>
<thead>
<tr>
<th>Original</th>
<th>&lt;no equivalent&gt;</th>
</tr>
</thead>
<tbody>
<tr>
<td>Revision</td>
<td>If XBARCH [XBARCH], XDOMEA [XDOMEA] or [PREMIS] is used within the scope of meta data, the integration of XBARCH, XDOMEA or PREMIS should be carried out pursuant to the TR-ESOR-Profile &quot;TR-ESOR-Profile-XBDP: XAIP Profiling with XBARCH, XDOMEA and PREMIS&quot;.</td>
</tr>
</tbody>
</table>

**Explanation:**
In order to achieve the interoperability of products and components for the storage of electronic documents with preservation of evidence with the objectives and intentions of this Technical Guideline in the long term even across agencies, further standardisation of the data format for the archive data objects is required.

### 3.3 TR-ESOR Annex F

#### 3. Definition of the archival information packages (XAIP)

<table>
<thead>
<tr>
<th>Original</th>
<th>For the preservation of evidence of cryptographically signed documents, the XAIP format described in this Section and specified by the corresponding XML schema should be used. Deviations in the XML format used are permissible, but it shall be explained that equivalent functionality is supported. It shall be explained in particular how a transformation into the XAIP format as specified here may be performed.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Revision</td>
<td>For the preservation of evidence of cryptographically signed documents in federal agencies, an XML container based on the XML schema XAIP specified in Chapter 3 of Annex F shall be used as XML data format.</td>
</tr>
</tbody>
</table>

**Explanation:**
In the "Standards and Architectures for E-Government Applications (SAGA)", XML is defined as a mandatory standard for the exchange of data in the federal administration. The XAIP format specified in the Appendix of Annex F addresses this issue in an adequate way.
### 5.6 Recommendations for the implementation

**Original**

[A5.6-1] In order to be able to process any data format and to be able to link the cryptographic data and meta data with the payload data, the XAIP container defined in Chapter 3 or a derivative thereof should be used as the central data element in the protocol. For the protocol, this means in particular that all data are kept in a single data element and are logically connected to each other in this manner. The protocol is not responsible for the logical correctness of this data element after receipt.

**Revision**

[A5.6-1B] In order to be able to process any data format and to be able to link the cryptographic data and meta data with the payload data, an XML container based on the XML schema XAIP specified in Chapter 3 of Annex F shall be used as XML data format.

**Explanation:**

The objective and intention of TR-ESOR are to store and manage evidence records to prove the authenticity and integrity of cryptographically signed documents along with these documents. The specification of the XAIP container addresses this issue in an adequate way by storing (encapsulating) the documents and evidence records together in a self-contained and self-explanatory XML data structure. The requirements are tightened here with respect to the use of XML as the data format. Other container data formats than XML are not desired.

### 5.6 Recommendations for the implementation

**Original**

[A5.6-8] Recommendation for the protocol on the application layer is SOAP document/literal encoding. The external interfaces of all archive system components will be published with WSDL; they may be based on an external XML schema.

**Revision**

[A5.6-8B] In order to achieve conformity with the Federal Agency Profile, Conformity Level 2 of this Technical Guideline shall also be fulfilled beforehand.

**Explanation:**

One of the objectives of this profile is to ensure the technical interoperability of the modules of the entire archive system. For this purpose, reaching Conformity Level 2 of the Technical Guideline is required here. This includes the exact implementation of the external interfaces to the individual modules according to the XML specifications described as well as the use of SOAP as the protocol and XML as the container format.

This requirement does not imply that all purely internal interfaces shall comply with the XML-based interface specifications of this Technical Guideline in the case of a product combining several modules of the Technical Guideline.

### 3.4 TR-ESOR Annex S

The requirements in this document remain unchanged for federal agencies.
3.5 TR-ESOR Annex M.1

4.4 Deleting archived data – ArchiveDeletionRequest

<table>
<thead>
<tr>
<th>Original</th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>[A4.4-1]</td>
<td>In the event of deletion before the retention periods have expired, the request shall have a reason that may be logged. The ArchiSafe-Module shall enforce compliance with the retention periods and the existence of a reason that may be logged in the event of premature deletion.</td>
<td></td>
</tr>
<tr>
<td>[A4.4-2]</td>
<td>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.</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Revision</th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>[A4.4-1B]</td>
<td>In the event of deletion, the appraisal or disposal note of the competent national archive (e.g. Federal Archive) shall be verified. If it is a premature deletion, the order for deletion shall contain a loggable reason and the official appraisal note shall have the value &quot;V&quot;. If the retention period has expired, the appraisal note shall be set to &quot;V&quot;. If the data of archival value has already been submitted to the competent archive and a release of the archivist is available, the appraisal or disposal note of the remaining archival information packages shall thus be changed to &quot;V&quot; prior to deletion.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>The appraisal / disposal note may be available in the archival information package pursuant to Chapter 3.2 in [TR-ESOR-F]. Other implementations with respect to the appraisal / disposal note are also permissible, but it shall then be explained that an equivalent functionality is supported.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>The ArchiSafe-Module shall enforce compliance with the retention periods and the existence of a reason that may be logged in the event of premature deletion.</td>
<td></td>
</tr>
<tr>
<td>[A4.4-2B]</td>
<td>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 or the appraisal / disposal note does not contain a value according to the description above.</td>
<td></td>
</tr>
</tbody>
</table>

Explanation:

Pursuant to § 2 German Federal Archiving Law (BArchG) or pursuant to the corresponding State Archiving Laws, the duty to offer to the competent public archive applies to agencies. According to this, deletion is only possible depending on the value of the so-called appraisal / disposal note. The right of immediate deletion of personal data pursuant to the Data Protection Act remains unaffected by this.

3.6 TR-ESOR Annex M.2

The requirements in this document remain unchanged for federal agencies.

3.7 TR-ESOR Annex M.3

The requirements in this document remain unchanged for federal agencies.

3.8 TR-ESOR Annex ERS

The requirements in this document remain unchanged for federal agencies.

3.9 TR-ESOR Annex VR

The requirements in this document remain unchanged for federal agencies.

9 Setting the appraisal note shall be preceded by a technical-organisational decision of the applying agency according to the appraisal decision of the competent public archive. Legal aspects shall be clarified by the agency together with the archive.