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>1.1</td>
</tr>
<tr>
<td>Date</td>
<td>18.02.2011</td>
</tr>
</tbody>
</table>
# Table of Contents

1. Introduction .................................................................................................................. 4  
2. Overview ....................................................................................................................... 6  
   2.1 Goals ......................................................................................................................... 6  
3. Definition of the ArchiSafe-Module ............................................................................. 8  
   3.1 Basic Design and Function Delineation .................................................................. 8  
   3.2 Integration of the ArchiSafe-Module ....................................................................... 8  
   3.3 Fulfilment of basic security requirements ............................................................... 8  
4. Functional Requirements ............................................................................................... 9  
   4.1 Archiving electronic data - Archive Submission Request ......................................... 10  
   4.2 Updating archived data - Archive Update Request .................................................. 11  
   4.3 Retrieving archived data - Archive Retrieval Request ............................................ 13  
   4.4 Deletion of archived data - Archive Deletion Request ............................................ 13  
   4.5 Return of technical Evidence Records - Archive Evidence Request ..................... 14  
   4.6 Return of data elements - Archive Data Request .................................................... 14  
5. Security Functions ........................................................................................................ 15
1. Introduction

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

A Middleware defined for this purpose (TR-ESOR-Middleware) in the sense of this Guideline includes all of the modules (M) and interfaces (S) [for the German "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 in the following:

- The input interface S.4 of the TR-ESOR-Middleware serves to embed the TR-ESOR-Middleware in the existing IT and infrastructure landscape;
- The central Middleware module M.1, which regulates the flow of information in the Middleware, that implements the security requirements for the interfaces with the IT applications and which ensures that the application systems are decoupled from the ECM/long-term storage;
- The “Cryptographic” module M.2 and the associated interfaces S.1 and S.3 that provide the functions needed for the creation (optional) and verification of electronic signatures, the post-verification of electronic certificates, and for the obtainment of qualified time stamps for the Middleware. Furthermore, it can provide the functions for the encryption and decryption of data and documents;
- The “ArchiSig” module (TR-ESOR-M.3) with the interface S.6 that provides the functions needed for the preservation of evidence of the digitally signed documents;
- An ECM/long-term storage with the interfaces S.2 and S.5 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 of 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 this Technical Guideline, either, even though this XML-adapter can be implemented as part of a Middleware.

The IT Reference Architecture depicted in Figure 1 is based on the ArchiSafe 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.

\footnote{For more information, see \url{http://www.archisafe.de}.}
This Technical Guideline is modularly structured, and the individual annexes to the Main Document specify the functional and technological security requirements for the needed IT components and interfaces of the TR-ESOR-Middleware. The specifications are strictly platform, product, and manufacturer independent.

The document at hand bears the designation “Annex TR-ESOR-M.1” and specifies the functional and technical security requirements for the module TR-ESOR-M.1 (referred to in the following as the ArchiSafe-Module2 for short).

---

2 The name “ArchiSafe” refers to the E-Government Project “ArchiSafe - Legally Viable and Auditable Long-Term Storage of Electronic Documents” from the Physikalisch-Technischen Bundesanstalt in 2005 that was promoted in the scope of the E-Government programs “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 specialised applications and the actual ECM/long-term storage, it is recommended that all needed archive functions be 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 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 preservation of the authenticity and the integrity of the saved electronic documents.

Each archive operation of the upstream external IT application that serves to secure, preserve, or prove the conclusiveness of electronic documents must be done through 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 archival information package being transmitted by the application making the request against the configuration data stored in the ArchiSafe-Module (XML schemata, communication and processing rules).

When archival information packages are stored, the ArchiSafe-Module initiates the securing of the conclusive 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 retained. The signature verification is realised with a cryptographic component (module) that must fulfil the requirements described in the Annex TR-ESOR-M.2 of this Technical Guideline.

2. The ArchiSig-Module (see Annex TR-ESOR-M.3 of this Technical Guideline) is commanded to furnish each archival information package with a unique document identifier (archival information package ID, AOID), and calculate one or more hash values for the entire archival package or the parts of the archival information package with AOID that are to be protected cryptographically.

Finally, the data and AOID to be archived are transmitted via a secure communication channel to an authenticated ECM/long-term storage. The successful storing of archival information packages is concluded with the return of the archival information package ID (AOID) to the requesting application.

---

3. This channel can be, for example, physically secured cables or an encrypted connection with suitably strong authentication of both parties (also see TR-ESOR-F, Chapter 6.2).

4. The creation of the archival information package ID (AOID) can also occur in other components, such as the ECM/long-term storage.

5. Details about the elements/areas of an archival information package for which a hash value is created are found in Annex F.
This AOID is needed by the upstream IT application for every retrieval, update, and deletion of archived data. Likewise, retrieval of evidence records on archived data is also only possible when a valid AOID is presented.
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 of the 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 controlling 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 Function Delineation

(A3.1-1) The ArchiSafe-Module should be a Middleware component or a part of a Middleware component that provides and controls the 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 delineated) part of an application (also 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 accesses to the data and functions of the module.

(A3.1-4) The ArchiSafe-Module shall use components for preservation of the conclusive value of electronically signed data, for example by means of legally compliant re-signing, trustworthy cryptographic components, that are described in the annexes TR-ESOR-M.2 and TR-ESOR-M.3 to this Technical Guideline and which are addressed by the S.1 and S.6 interfaces defined in Annex TR-ESOR-S.

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 any time.

(A3.2-2) For the integration of the ArchiSafe-Module in existing or planned IT environments in the sense of this Guideline, the ArchiSafe-Module shall be able to implement or use at least the interfaces S.1, S.4, S.5, and S.6 specified in Annex TR-ESOR-S of this Technical Guideline.

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

3.3 Fulfilment of basic security requirements

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

---

6 The requirement explicitly does not exclude that the functions of the ArchiSafe-Module and the cryptographic components be subsumed in a standard 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 in Annex TR-ESOR-S of this guideline as S.4.

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 Guideline corresponds syntactically to the XML formatted Archival Information Package (XAIP) described in Annex F of this Guideline. An archival information package can thus contain one or more information packages as well as meta data. The archival information package 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 data objects that relate to one of the same, and in particular that the retrieval functions return an archival information package (or parts thereof) in a valid XML format (see Annex F).

- **A data element** is a part of the XML structure of an archival information package. In doing so, this can concern the entire archival information package, a partial tree of the XML structure, an individual XML element, or the value of an XML element.

(A4.0-1) An ArchiSafe-Module that conforms to this Guideline shall provide the following operations, at a minimum.

1. Archiving an (archival) information package in the ECM/long-term storage (Archive Submission Request),
2. Retrieving an archival information package from the ECM/long-term storage (Archive Retrieval Request),
3. Deleting an archival information package in the ECM/long-term storage (Archive Deletion Request),
4. Requesting technical Evidence Records for proving the authenticity and integrity of archived archival information packages (Archive Evidence Request).
5. Requesting individual data elements from archived archival information packages (Archive Data Request)

---

7 An operation is an inquiry from an external client software to the ArchiSafe-Module for execution of defined operations in the TR-ESOR-Middleware or in the ECM/long-term storage.

8 It is stipulated that the interface accept both complete archival information packages and individual data packages. The response is always an AOID that refers to an archival information package.
An ArchiSafe-Module that conforms to this Guideline should provide the following operations additionally:

- Updating an archival information package in the ECM/long-term storage that has already been archived (Archive Update Request),

(A4.0-2) The ArchiSafe-Module shall not let its functions be influenced by false or incorrectly parametrised requests.

(A4.0-3) The ArchiSafe-Module shall have comprehensive and configurable options for logging the various accesses and attempted accesses to the archive.

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

(A4.0-5) Applicable 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 for requesting the function.

(A4.0-6) Applicable to all functions listed in (A4.0-1): A requesting client software shall only receive access to the archival information packages for which it has access rights. This must also be enforced stringently when several archival information packages are requested simultaneously and, as applicable, there are only access rights to a few of them.

4.1 Archiving electronic data - Archive Submission Request

The Archive Submission Request function makes it possible for an authorised IT application (client software\(^\text{10}\)) to store a (new) (archival) information package in the ECM/long-term storage through a secure communication channel.

(A4.1-1) The (archival) information package to be archived shall be a part of the request. Should the (archival) information package to be archived be 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.

(A4.1-2) The ArchiSafe-Module shall be able to initiate the verification of electronic signatures of the (archival) information packages to be stored on the basis of the configuration data saved in the module.

In this case, ArchiSafe-Module transfers the signed data contained in the (archival) information package to the Cryptographic-Module through the S.1 interface (see Annexes TR-ESOR-S and TR-ESOR-M.2) before the actual storage in the ECM/long-term storage. The Cryptographic-Module shall verify the signature(s) and the validity of the associated certificates. The verification results are then entered into the data structures of the (archival) information package stipulated for this purpose by the ArchiSafe-Module.

---

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

10 A client application in the sense of this Guideline is an external (upstream) IT application that is capable of and authorised to search for, update, retrieve, or delete data in the ECM/long-term storage through the ArchiSafe-Module.
Should the signature or certificate verification fail, a clear and understandable error message shall be transmitted to the business application. It is allowed for the archival information package to be stored in the ECM/long-term storage anyway and for a corresponding AOID to be returned to the transaction application.

**NOTICE:** It is urgently recommended that signatures are verified upon archive submission. Otherwise, data that have already been manipulated or invalid signatures could enter into the archive system, in which case the loss of integrity may only be noticed years later.

(A4.1-3) It **shall** be possible for the ArchiSafe-Module to enter signature verification results including the associated certificate information into the XML data elements of the XML based archival information packages stipulated for that purpose (see Annex TR-ESOR-F). If no XML based archival information package is used, the signature verification results **can** be inserted into the transmitted (binary) payload data object if allowed by the format used.

(A4.1-4) The ArchiSafe-Module shall transmit the (archival) information package through the S.6 interface to the ArchiSig-Module (see Annex TR-ESOR-S and TR-ESOR-M.3) before final storage in the ECM/long-term storage. Finally, the (archival) information package is stored in the ECM/long-term storage by the ArchiSig-Module.

Alternatively, the ArchiSafe-Module transmits the (archival) information package directly to the ECM/long-term storage and the functions of the ArchiSig-Module are requested for this (archival) information package at a later point in time or by another authority. In doing so, it **shall** be ensured that the named point in time does not deviate significantly (e.g. weeks) from that of the time of archiving and that all (archival) information packages that have actually (provably) been newly archived are included by this function.

(A4.1-5) The ArchiSafe-Module **shall not in any case** change the data or information packages (in the archival information package).

(A4.1-6) An (archival) information package 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.

(A4.1-7) In the event of successful storage, the unique document identifier, the archive object ID (AOID) **shall** be returned to the requesting client application.

### 4.2 Updating archived data - Archive Update Request

The **Archive Update Request** function makes it possible for an authorised IT application (client software) to add new metadata or information packages to an existing archival information package in the ECM/long-term storage through a secure communication channel or change certain metadata or information packages in a traceable manner that have already been archived.

The conclusiveness of the data that have already been archived may not be compromised by the update request.

(A4.2-1) A valid (syntactically correct and actually issued) archival information package ID (AOID) **shall** be a part of the request.

---

11 The Guideline urgently recommends that the ArchiSafe-Module transmit the information package directly to the ArchiSig-Module for calculation of the hash value and that the information package is not laid in the ECM/long-term storage first. In the latter case the period of time between the saving and calculation of the hash value results in a certain uncertainty.
Furthermore, a part of the request shall be the meta data that is to be newly archived or changed and/or the information package that is to be newly archived or changed. Several meta data and information packages to be changed/archived can be transmitted in a joint structure for this archival information package. The transmission of empty structure elements is not allowed.\textsuperscript{12}.

If the named structure is an XML structure (XAIP), the structure shall be verified in a manner analogous to that for a new archiving (see (A4.1-1)).\textsuperscript{13}

Should signatures, certificates, or signed data be handed over, these data are to be handled in a manner analogous to that for new archiving (see (A4.1-2) and (A4.1-3)).\textsuperscript{13}

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

The “changing” of meta data/information packages in the archival information package shall occur based on the following principle if not necessarily in the sequence indicated:\textsuperscript{14}

1. Creation of a new version manifest\textsuperscript{15} (copy of the old version manifests) together with the issuance of a new version number.
2. Adding the “new” meta data/information package to the archival information package. (In doing so, existing data are neither changed nor deleted).
3. Removal of the entries in the manifest for meta data/information packages that are no longer included in the new version (as needed). However, the actual meta data/information packages are not removed.
4. Addition of or change to manifest entries for the “new” meta data/information packages.

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

The new (changed) archival information package 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 (A4.1-4)).

The response shall receive a status value that displays the success of the operation. In the event of success, the new version number shall also be returned.

\textsuperscript{12} This is intended to prevent the "deletion" of individual meta data or payload data packages. The deletion of individual elements is not supported by the Technical Guideline; only the deletion of the entire archival information package is allowed.

\textsuperscript{13} If a signature is archived retroactively for an existing payload data package, then the payload data package is to be retrieved beforehand from the ECM/long-term storage for the verification of the signature.

\textsuperscript{14} The manufacturer is free to calculate the ERS of the "old" version of the archival information package before this procedure and embed it into the archival information package. This makes it easier to calculate the ERS with the Archive Evidence Request function, but this is not absolutely necessary.

\textsuperscript{15} see XAIP specification in Annex F
4.3 Retrieving archived data - Archive Retrieval Request

The **Archive Retrieval Request** 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 presentation of a valid archival information package ID (AOID) and, if applicable, a VersionID. If no VersionID is indicated, the respective current version is returned.

(A4.3-1) A valid (syntactically correct and actually issued) archival information package ID (AOID) or a list of valid AOID’s shall be a part of the request. Optionally, a valid (syntactically correct and actually issued) VersionID can also be indicated for each AOID.

(A4.3-2) The entire archival information package(s) linked with the AOID(s) and, if applicable, VersionID’s in the ECM/long-term storage shall be returned. In the event of an error (for example: AOID or VersionID is not valid for the request), the request shall be denied with a clear and understandable error message.\(^{16}\)

(A4.3-3) The archival information packages shall be returned in XML format (XAIP). The XML format shall follow a verifiable XML schema that can be configured by users of the total system.\(^{17}\) The requirements from the Annex TR-ESOR-F apply to the XML format or the XML schema.

4.4 Deletion of archived data - Archive Deletion Request

The **Archive Deletion Request** function makes it possible to delete one or more archival information packages in the ECM/long-term storage that belong to an AOID or a list of AOID’s.

(A4.4-1) It shall be possible to confirm the deletion in a traceable manner through the ECM/long-term storage.

(A4.4-2) If the ECM/long-term storage has no deletion function or the media used do not allow deletion, the ArchiSafe-Module should answer the request for this function with a corresponding error.

(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 retention periods and the existence of a reason that can be logged in the event of premature deletion.

(A4.4-4) The 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 reason at hand in the event of premature deletion.\(^{18}\)

---

\(^{16}\) It is left to the manufacturer whether it executes the request completely or only in part or confirms with an error message if one or more AOID’s in a transmitted list of AOID’s is incorrect.

\(^{17}\) It is left up to the manufacturer to require whether the XML schema already has to be defined upon archiving of the archival information package or first at the time of the request.

\(^{18}\) It cannot be defined here where, in which form, and for what period of time this reason must be saved and which people shall have access to it in what form. Conceivable are, among other things, storing in the normal log data of the ArchiSafe-Module or storing of the reason in the data media 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.
4.5 Return of technical Evidence Records - Archive Evidence Request

The Archive Evidence Request function makes it possible to request a set of technical Evidence Records regarding the integrity of one or more archival information packages stored in the ECM/long-term storage. The ArchiSafe-Module passes this request to the ArchiSig-Module through the TR-ESOR-S.6 interface for execution. The ArchiSig-Module uses the same interface to return a so-called reduced archive time stamp (see Annex TR-ESOR-M.3) as an evidence record set.

(A4.5-1) A valid archival information package ID (AOID) or a list of valid AOID’s shall be a part of the request. The return date shall be a reduced archive time stamp in ERS notation for each AOID.

(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 transaction application.

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

(A4.5-4) In the event of changed (versioned) archival information packages, it must be ensured that an ERS 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 13 on page 12).

4.6 Return of data elements - Archive Data Request

The Archive Data Request function makes discrete (read-only) retrieval of individual data elements from archival information packages 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 packages identified by the AOID.

The retrieved data elements are returned to the transaction application making the request through the TR-ESOR-S.4 interface.

(A4.6-1) A valid archival information package ID (AOID) or a list of valid AOID’s as well as the respective unique identifiers for the data elements to be retrieved shall be a part of the request.

(A4.6-2) The retrieved data elements are returned together with the associated AOID. The retrieved data elements may 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.
5. Security Functions

Based on the logical and functional decoupling of the data flow between the business applications and the ECM/long-term storage, the ArchiSafe-Module must provide the following functions with relevance to security at a minimum:

(A5.0-1) the prevention of unauthorised access to the ECM/long-term storage by reliably identifying and authenticating upstream IT applications (also see (A3.1-1) and (A4.0-6),

(A5.0-2) the reliable and traceable storage of the archival information package only in the ECM/long-term storage stipulated for that purpose,

(A5.0-3) the assurance that archived data can only be changed, retrieved, and deleted by applications that are authorised to do so. The unfounded deletion of data before the expiry of the statutory retention periods is to be prevented reliably (also see (A3.1-1), (A4.0-6) and (A4.4-3)).

Measures to protect the confidentiality of the archived information, for example by encryption of the data, are to be realised outside of the ArchiSafe-Module just as the measures for signature creation and re-signing of archived electronically signed data are.


20 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 hands over the archival information packages 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 storing in the ECM/long-term storage. For that reason, the requirement states that ArchiSafe in fact (indirectly) transmits all archival information packages handed over by IT specialist applications (and successfully verified) 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 archival information package ID (AOID) to the IT specialist application through the ArchiSafe-Module.

21 The access permissions model within ArchiSafe should indeed make it possible to issue permissions separately for the listed archiving functions. Thus it should not just be possible to give an application full access rights or none, but rather one should be able to define which functions the application may use.