Bundesamt
für Sicherheit in der
Informationstechnik

BSI Technical Guideline 03125
Preservation of Evidence of Cryptographically Signed Documents

Annex TR-ESOR-C.3:
Conformity Test Specification (Level 3 - Conformity with the German Federal Agency Profiling)

Designation	Conformity with the German Federal Agency Profiling (Level 3)
Abbreviation	BSI TR-ESOR-C.3
Version	1.2.1 (on base of the eIDAS-Regulation)
Datum	15.03.2018

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

Index of Contents

Index of Figures

Index of Tables

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 (meta data).

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 (**[TR-ESOR-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 (**[TR-ESOR-M.2]**) and the associated interfaces S.1 and S.3 that provide the functions needed for the calculation of hash values, verification of electronic signatures, seals or time stamps, the post-verification of electronic certificates, and for the obtainment of qualified time stamps and (optional) of electronic signatures and seals 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 may be induced 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[1] 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 more information, see http://www.archisafe.de.

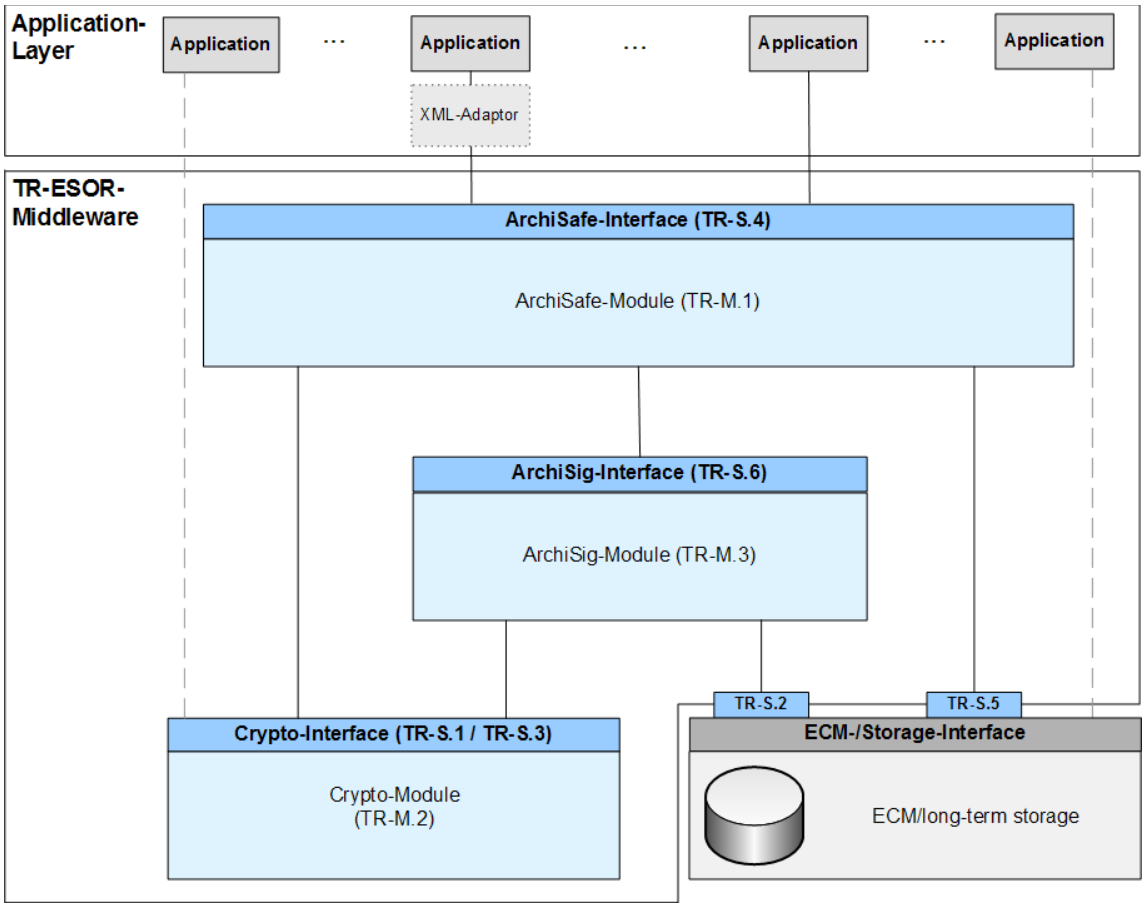

Figure 1: Schematic Depiction of the IT Reference Architecture

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-C.3” and describes and specifies the conformity tests for the conformity level 3 “Conformity with the German Federal Agency Profiling (see [TR-ESOR-B] and [TR-ESOR-XBDP])”.

2 Overview

Products or systems which want to get certified according to this Technical Guideline have to demonstrate their conformance to the specifications. There are three conformance levels defined which mainly differ in the technical detail specifications of interfaces and data formats used.

- Conformity Level 1 – Functional Conformity
- Conformity Level 2 – Technical Conformity
- Conformity Level 3 – Conformity with the German Federal Agency Profiling

The three levels are built on top of each other. This means e.g. in order to demonstrate conformity to level 3 all conformance criteria for level 1 and 2 have to be passed in addition to the conformance criteria for level 3.

This document specifies the test criteria derived from the requirements of the annex TR-ESOR-B for achieving the conformity with German Federal Agency Profiling.

Each test case is identified by a unique ID. All tests, which are required to be performed are marked with the color red. Tests, which are marked grey, may be applied in certain situations.

In order to become certified according to a conformity level 3, a product or system must pass successfully all red marked conformity criteria (tests) for this conformity level and for all lower conformity levels. All other test specifications must be passed or the non-fulfilment must be justified. If one or more mandatory tests are not successful, the conformity cannot be certified.

NOTICE 1: *In the following text „**digital signature**“ subsumes „advanced electronic signature“ according to **[eIDAS-VO, Article 3(11)]**, „qualified electronic signature“ according to **[eIDAS-VO, Article 3(12)]**, „advanced electronic seal“ according to **[eIDAS-VO, Article 3(26)]** and „qualified electronic seal“ according to **[eIDAS-VO, Article 3(27)].***

*The term “**cryptographically signed documents**” means qualified digital signed documents according to **[eIDAS-VO Article 3(12)]** as well as qualified digital sealed documents **[eIDAS-VO Article 3(27)]** and qualified electronically time-stamped documents **[eIDAS-VO 3(34)]** but also documents with advanced digital signatures **[eIDAS-VO, Article 3(11)]**, advanced digital seals **[eIDAS-VO, Article 3(26)]** or electronic time-stamps **[eIDAS-VO, Article 3(33)]** which are often used in the internal communication of public administrations. Not mentioned in this text are documents with simple electronic signatures or seals based on other (e.g. non-cryptographical) procedures*

2.1 Test Approach

NOTICE 2: *The following test specifications are based on Annex TR-ESOR-B and the recommended reference architecture in chapter 7.1 of the main document of this technical guideline. Thus, in the following differences between expected and observed test results should be carefully interpreted by the testers respecting the fact that actual implementations of components and / or modules of the middleware may deviate from the recommended reference architecture.*

Beside this testing the conformity to this guideline may refer to a single module only. This may result also in different characteristics and expected results of implemented and provided features and interfaces.

2.2 Structure of the Test Case Specifications

Some test cases are ordered according to the modules M.1 – M.3 and „all products“. These test cases cannot be assigned to a certain interface of the module but check general properties of the module.

The other test cases are ordered according to the interface specifications S.1 – S.6. The reason for that

is that these tests will only be performed on the level of external interfaces of a certain product. If a product claims compliance with the module specified in the Technical Guideline, the respective interfaces of the module (product) will be tested.

Below this structural level, the test cases are ordered according to the requirements of Annex TR-ESOR-B.

Each test case is identified by a unique ID. The test case description also refers to the respective requirements which will be (partly) tested with this test case. The test case also states the purpose of the test as a summary of the test case. The baseline configuration of the test system will be stated as well as all pre-conditions which must exist prior performance of the test. The test case defines the single test steps which must be performed in the given order. Per test step the expected result is defined and there is space that the tester could document the actual findings. Finally, the tester can state the final verdict of the test case (PASS/FAIL).

FAIL shall be assigned if any of the test steps does not match the expected result and a justification for this difference is not possible.

2.3 Strictness of Test Result Assessment

The Technical Guideline differs between three major classes of requirements (cf. [RFC 2119])

- CAN (or synonymously MAY, COULD): These requirements are just hints or optional features. These requirements will not be tested.
- SHOULD: These requirements are strong recommendations. Respective test cases should demonstrate the specified behaviour. Alternatively, the vendor explains why its product uses another approach and why the resulting security level is equal to the security level described in the Technical Guideline.
- MUST (or synonymously SHALL): These are strict requirements. It is not allowed to use another approach or alternative techniques.

Test cases which tests MUST requirements are identified with a red coloured title line. The expected results of these test cases must exactly be the actual results.

Test cases identified by a grey coloured title line are pure SHOULD requirements. The expected test results may differ from the actual test results, if the vendor can demonstrate the same or higher security level.

2.4 Baseline for all Test Cases

This section describes the basics valid and usable for all test cases.

2.4.1 Standard Test Configurations

Here, a set of standard configurations of the test setup will be described. These setups are referenced in the test cases and should be used to actually perform the tests.

2.4.1.1 CONFIG_Common

This is the standard configuration for all tests.

- The test setup shall contain the product to be tested (Target of Testing, TOT).
- The test setup shall contain all other modules of the reference architecture (including the storage) functionally not covered by the TOT.
  The purpose is that a functionally complete system can be tested.
- The TOT and all other modules required shall be installed and configured according to the respective guidance including all security recommendations.
- The TOT and all other modules shall be physically and logically interconnected. The

connections shall be secured as described in the respective guidance documents (e.g. enabling encryption, explicit physical connection).

- The test system shall be connected to an external Trust Service Provider as required by the TOT or the tests.
- At least it is recommended to install three different client applications for using and testing the multi-client-capability of the middleware (if the TOT supports/provides a multi-client-capability).
  In this case the middleware in turn shall be configured to handle these three applications as different clients (multi-client-capability). Per client application at least two user accounts and an administrator account shall be configured.

The complete test setup shall be up and running and in an operational and working mode.

2.4.1.2 CONFIG_ArchiSafe

This configuration is based on CONFIG_Common.

Additionally, the ArchiSafe-Module (if TOT) shall be configured as follows:

- If configurable, a XSD defining the XAIPs shall be configured. The XAIP described in Annex TR-ESOR-F should be used.
- If configurable, the XSD verification of XAIP containers during Archive Submission and Archive Update shall be enabled.
- The signature verification during Archive Submission and Archive Update shall be enabled.
- The S.4 interface shall only be accessible using a secure tunnel, for example a TLS tunnel, with certificate-based mutual authentication.

2.4.2 Standard Test Objects

For most of the tests test data is required. In order to make the tests repeatable, a set of standard test objects is necessary.

In the annex [TR-ESOR-C.1] a list of test objects is defined in chapter 4.3.2, which is also the basis of the test objects for this annex.

2.5 Occurring Abbreviations

Abbreviation	Meaning
AES-128	Advanced Encryption Standard (128 bits)
AOID	Archive Object Identifier
ATS	Archive Time Stamp
BIN	Binary
BSI	Federal Office for Information Security
C14N	Canonical XML
CMS	Cryptographic Message Syntax
CRL	Certificate Revocation List
DES	Data Encryption Standard
DoS	Denial of Service
e.g.	for example (exempli gratia)

Abbreviation	Meaning
EC14N	Exclusive XML Canonicalization
ECM	Enterprise Content Management
ERS	Evidence Record Syntax
ETSI-TSP	European Telecommunication Standard Institut - Time Stamping Profile
HTTP	Hypertext Transfer Protocol
i.e.	in other words (id est)
ID	Identifier
IT	Information Technology
M	Modules
MER	Merkle hash trees
n/a	not applicable
No.	Number
OCSP	Online Certificate Status Protocol
Par.	Paragraph
PKCS	Public Key Cryptographic Standard
PKI	Public Key Infrastructure
PP-0049	Identifier of the [ACMPP]
RC2	Rivest Cipher 2
resp.	respectively
RFC	Request for Comments
RMI	Remote Method Invocation
RPC	Remote Procedure Call
S	Interfaces
SASL	Simple Authentication and Security Layer
SCVP	Server-based Certification Validation Protocol
Sig	Signature
SigG	Signaturgesetz
SigV	Signaturverordnung
SOAP	Simple Object Access Protocol
SQL	Structured Query Language
SSCD	Secure Signature Creation Device

Abbreviation	Meaning
ST	Security Target
TCP	Transmission Control Protocol
TLS	Transport Layer Security
TOT	Target of Testing
TR	Technische Richtlinie (engl.: Technical Guideline)
TSP	Trust Service Provider
USB	Universal Serial Bus
WSDL	Web Services Description Language
XAIP	XML-based Archive Information Package
XML	Extensible Markup Language
XSD	XML Schema Description

3 The Test Cases for Conformity Level 3 – Conformity with the German Federal Agency Profiling

3.1 Tests for all products or systems

3.1.1 A-01 – Fulfilling Conformity Level 2

Identifier	A-01		
Requirement	B: A2.0-1B (origins from Annex E) B: A2.0-2B (origins from Annex E) B: A5.6.8B (origins from Annex F)		
Test Purpose	The test shall verify that the TOT has fulfilled the requirements of conformity level 2		
Configuration	CONFIG_Common		
Pre-test conditions	• Certificate of conformity level 2 or performance of all tests relevant for conformity level 2		
Step	**Test sequence**	**Expected Results**	**Observations**
1.	Check whether the TOT has fulfilled the requirements of conformity level 2.	The TOT is certified to fulfil the conformity level 2 or all test of conformity level 2 have been passed successfully.	
Verdict			

3.2 Module 1 – ArchiSafe

Pre-supposition:
A product which claims to comply with the M.1 ArchiSafe specification at conformity level 3 of this TR has to pass successfully

- all test cases which the M.1 ArchiSafe Module has to fulfil according to Annex **[TR-ESOR-C.1]** and **[TR-ESOR-C.2]**
- all test cases for the interface S.4 specified in Annex **[TR-ESOR-C.1]** and **[TR-ESOR-C.2]** and in Section 4.4.4 of this document.
- and the following test cases.

3.2.1 M.1-01 – ArchiSafe shall be configured to proof usage of long-term preservation data formats

Identifier	M.1-01
Requirement	B: A5.1-4B (origins from Main Document) B: A6.2-1B (origins from Main Document)
Test Purpose	The test shall verify that the TOT is configured to proof the usage of long-term preservation data formats
Configuration	CONFIG_Common
Pre-test conditions	• User manual and user guide.

Step	Test sequence	Expected Results	Observations
1.	Transfer a “BIN” to the TOT using the interface function “Archive Submission Request”.	The call of the function with this “BIN” as a parameter is possible	
2.	Observe the output of the interface function “Archive Submission Response”.	A clear and understandable error message or error code will be received.	
3.	Check the log files of the TOT for an error record about the XML schema check.	There is an error record showing that the XML schema verification of this BIN failed.	
4.	Check whether the BIN is stored.	The BIN is not stored.	

Verdict

3.2.2 M.1-02 – ArchiSafe shall fullfill the requirements of [TR-ESOR-B], Chapter 3.5

Identifier	M.1-02
Requirement	B: A4.4-1B (origins from Annex M.1) B: A4.4-2B (origins from Annex M.1)
Test Purpose	The test shall verify that it will yield an error, if ArchiveDeletionRequest is called with providing a ReasonOfDeletion and without providing a status element not equal "V" ("Bewertungsvermerk (not equal) "V"), if the element "retentionPeriod" in the XAIP contains a predetermined future date.
Configuration	CONFIG_Common
Pre-test conditions	• User manual and user guide.

Step	Test sequence	Expected Results	Observations
1.	The content of a <*preservationInfo*> of an XAIP_OK_BUND with the AOID="AOID_X", stored in a long-term storage, is changed in such a way, that the <*status*> - *element* is set to „X" .	The long-term storage contains a XAIP_OK_BUND with a changed *VersionManifest*.	
2.	ArchiveDeletionRequest (dss:OptionalInputs(ReasonOfDeletion(RequestorName(SomeName), RequestInfo(SomeInfo)), AOID-X)	The call of the function with this "AOID_X" is possible	
3.	Observe the output of the interface function "Archive Deletion Response".	A clear and understandable error message or error code will be received.	
4.	Check the log files of the TOT for an error record about the status element of <*preservationInfo* >.	There is an error record showing that there is no "V" in the status element and the request failed.	
5.	Check whether the Archive Data Object with AOID = "AOID_X" is deleted.	The Archiv Data Object with AOID = "AOID_X" is not deleted.	
Verdict			

3.2.3 M.1-03 – ArchiSafe shall verify the XML-Scheme according to XAIP (see [TR-ESOR-F], Chapter 3)

Identifier	M.1-03
Requirement	B: A2.0-3B (origins from Annex E) B: A2.0-xB (extension to Annex E) B: A3-1B (origins from Annex F) B: A5.6-1B (origins from Annex F)
Test Purpose	The test shall that ArchiSafe is able to verify an XAIP according to the XAIP XML scheme (see [TR-ESOR-F], Chapter 3) and according to the XBDP scheme (see [TR-ESOR-XBDP])
Configuration	CONFIG_Common
Pre-test conditions	• User manual and user guide.

Step	Test sequence	Expected Results	Observations
1.	Repeat Test-Case SU-1 from ([TR-ESOR-C.2] with a new syntactically correct test object. ArchiveSubmissionRequest (XAIP_OK_new)	ArchiveSubmissionResponse (dss:Result(resultmajor#ok), AOID_new)	
2.	Repeat Test-Case from ([TR-ESOR-C.2] with a new syntactically incorrect test object. ArchiveSubmissionRequest (dss:OptionalInputs(ReturnVerificatonReport)), XAIP_NOK)	ArchiveSubmissionResponse (dss:Result(resultmajor#error, resultminor/arl/XAIP_NOK), dss:OptionalOutput(VerificationReport))	
3.	Replace the XAIP scheme in the ArchiSafe module with the XDBP schema.	Scheme can be replaced.	
4.	peat Test-Case SU-1 from ([TR-ESOR-C.2] with a new syntactically correct test object. ArchiveSubmissionRequest	ArchiveSubmissionResponse (dss:Result(resultmajor#ok),	

	(XAIP_XBDP_OK_new)	AOID_new)	
5.	epeat Test-Case from ([TR-ESOR-C.2] with a new syntactically incorrect test object. ArchiveSubmissionRequest (dss:OptionalInputs(ReturnVerificatonReport)), XAIP_XBDP_NOK)	ArchiveSubmissionResponse (dss:Result(resultmajor#error, resultminor/arl/XAIP_NOK), dss:OptionalOutput(VerificationReport))	
Verdict			

3.3 Interface functions

3.3.1 Interface S.1

The primary purpose of the TR-ESOR-S.1 interface between the ArchiSafe module and the Cryptographic module is the verification of digital signatures accordingng to **[eIDAS-VO, Article 3(12/12/26/27)]** and (optional) the generation of digital signatures by (qualified) trust service providers on request of the Crypto-Module M.2., that were or should be attached to electronic data to be archived (XAIP documents).

A product which claims to comply with conformity level 3 must comply with the conformity level 2 concerning Interface S.1, if Interface S.1 is the most upper interface of this product or system.

3.3.2 Interface S.2

The main purpose of the TR-ESOR-S.2 interface between the ArchiSig-Module and the ECM/long-term storage is to make the necessary read and write access to ArchiSig's own database and the archive database in the ECM/long-term storage possible for the ArchiSig-Module.

This is an interface of a component which is not part of the TR-ESOR middle-ware. Therefore, no conformity tests will be specified here.

3.3.3 Interface S.3

The primary purpose of the TR-ESOR-S.3 interface between the ArchiSig-Module and the Cryptographic-Module is the generation of hash values and the requesting[2] and verification of qualified time stamps. Both kinds of data are needed for the development of the Merkle hash trees [MER 1980].

A product which claims to comply with conformity level 3 must comply with the conformity level 2 concerning Interface S.3, if Interface S.3 is the most upper interface of this product or system.

3.3.4 Interface S.4

The TR-ESOR-S.4 interface should make it possible for the business applications to access the ECM/long-term storage in a standardised manner.

Pre-supposition:

If Interface S.4 is the most upper interface of a product or system, which claims to comply with conformity level 3, it must comply with the conformity level 2 concerning Interface S.4 and has to pass

- all test cases in this section

3.3.4.1 S4-02 – Archive Update Request denies storage of invalid XML-based Delta Archival Information Packages (DXAIP)

Identifier	S4-02
Requirement	B: A5.1-4B (Main Document) B: A3.6-1B (Annex F) B: A6.2-1B (Annex F)

2

The generation of a qualified time stamp shall be done by a (qualified) trust service provider on request of the Crypto-Module M.2

Test Purpose	The test shall verify that the Middleware denies storage of a DXAIP with an invalid XML syntax or with a BINARY. The test fails if the XML format doesn't comply with the structure defined in TR-ESOR Annex TR-ESOR-F and deviations are not explained or doesn't provide equal functionality. The test fails if it is possible to store a DXAIP with an invalid XML syntax. The test fails if all data are not kept in a single data element or are not logically connected to each other (“self contained archive object”).
Configuration	CONFIG_ArchiSafe (includes XSD schema verification enabled).
Pre-test conditions	• The middleware's user manual is available. • If required, establish a session with the TOT in order to perform the following tests • If required, perform identification and authentication.

Step	Test sequence	Expected Results	Observations
1.	Compare the description of the XML data format in the middleware's user manual with the DXAIP structure described in TR-ESOR Annex TR-ESOR-F.	The implemented XML format of DXAIP complies with the structure defined in TR-ESOR Annex TR-ESOR-F. Deviations are explained and equal functionality is provided. If required, it is explained how a transformation of XAIP to the present XML-format is possible.	
2.	Check the interface functions and their possible parameters.	Data and metadata to be archived shall always be contained in an XML-container and only be passed in this container to the ArchiSafe.	
3.	Transfer a DXAIP_OK (transformed in the respective XML format) to TOT using the interface function “Archive Update Request”.	The function call is possible.	
4.	Check the output of the “Archive Update Response” function.	Update is successful, a version ID will be issued and returned. The log records show the XML schema check for storing an DXAIP. The updated XAIP will be retrieved. The retrieved XAIP contains the requested changes/updates. The ERS can be retrieved. The hash value identifies the updated XAIP. Same results in the repetition.	
5.	Transfer a DXAIP_NOK to the TOT using the interface function “Archive Update Request”.	The call of the function with this DXAIP as a parameter is possible	

6.	Observe the output of the interface function “Archive Update Response”.	A clear and understandable error message or error code will be received.	
7.	Check the log files of the TOT for an error record about the XML schema check.	There is an error record showing that the XML schema verification of this DXAIP failed.	
8.	Check whether the updated XAIP is stored.	There is no updated XAIP stored.	
9.	Retrieve the originally stored last version by issuing an “Archive Retrieval Request” with the AOID according ton No. 3. without a version ID.	The call of the function is possible.	
10.	Observe the output of the interface function “Archive Retrieval Response”.	The most current, changed version of the XAIP is successfully retrieved.	
11.	Check whether all data are kept in a single data element or are logically connected to each other.	The test fails if all data are not kept in a single data element or are not logically connected to each other.	
1.	Transfer an additional “BIN” to the TOT using the interface function “Archive Update Request” within a valid DXAIP container as update for the DXAIP transferred in step 3.	The call of the function with this “BIN” as a parameter is possible	
2.	Observe the output of the interface function “Archive Update Response”.	A clear and understandable error message or error code will be received.	
3.	Check the log files of the TOT for an error record about the binary.	There is an error record showing that the binary is not allowed here.	
4.	Check whether the BIN is stored.	The BIN is not stored.	
Verdict			

3.3.5 Interface S.5

The TR-ESOR-S.5 interface enables accesses from the ArchiSafe module to the ECM/long-term storage without technical dependence of the cryptographically secured Evidence Records.

This is an interface of a component not part of the TR-ESOR middleware. Therefore, no conformity tests can be specified here.

3.3.6 Interface S.6

The archiving of (new) archival information packages is possible with the TR-ESOR-S.6 interface described here, which can be used to include the ArchiSig-Module directly in the archiving procedure. This is a direct way to generate the securing hash values. Thus, it is impossible to circumvent this security function.

A product which claims to comply with conformity level 3 must comply with the conformity level 2 concerning Interface S.6, if Interface S.6 is the most upper interface of this product or system.

3.4 Annex TR-ESOR-M.2

All requirements of Annex **[TR-ESOR-M.2]** are tested at the respective modules or interfaces according to Annex C.1 and C.2.

3.5 Annex TR-ESOR-M.3

All requirements of Annex **[TR-ESOR-M.3]** are tested at the respective modules or interfaces according to Annex C.1 and C.2.

3.6 Annex TR-ESOR-E

Besides test case A-01 and M1-03 all requirements of Annex **[TR-ESOR-E]** are tested at the respective modules or interfaces according to Annex C.1 and C.2.

3.7 Annex TR-ESOR-F

Besides test case A-01, M1-03, S4-01 and S4.02all requirements of Annex **[TR-ESOR-F]** are tested at the respective modules or interfaces according to Annex C.1 and C.2.

3.8 Annex TR-ESOR-ERS

All requirements of Annex **[TR-ESOR-ERS]** are tested at the respective modules or interfaces according to Annex C.1 and C.2.

3.9 Annex TR-ESOR-S

All requirements of Annex **[TR-ESOR-S]** are tested at the respective modules or interfaces according to Annex C.1 and C.2.

3.10 Annex TR-ESOR-VR

All requirements of Annex **[TR-ESOR-VR]** are tested at the respective modules or interfaces according to Annex C.1 and C.2.