BSI Technical Guideline 03125
Preservation of Evidence of Cryptographically Signed Documents

Annex TR-ESOR-M.2: Cryptographic-Module

<table>
<thead>
<tr>
<th>Designation</th>
<th>Cryptographic-Module</th>
</tr>
</thead>
<tbody>
<tr>
<td>Abbreviation</td>
<td>BSI TR-ESOR-M.2</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
   2.2 Manner of functioning ......................................................................................................... 6

3. Definition of the Cryptographic-Module ............................................................................... 7
   3.1 Basic design ....................................................................................................................... 7
   3.2 Modular inclusion of the cryptographic functions ............................................................. 7
   3.3 Certification by the Federal Network Agency .................................................................. 7

4. Basic requirements for algorithms and parameters ............................................................. 9
   4.1 Generation of random numbers ....................................................................................... 9
   4.2 Computing hash values ..................................................................................................... 9
   4.3 Creation of signatures ........................................................................................................ 10
   4.4 Canonicalization procedure ............................................................................................. 10

5. Functions of the Cryptographic-Module .............................................................................. 12
   5.1 Electronic signatures .......................................................................................................... 12
      5.1.1 Creation of an electronic signature ........................................................................... 12
      5.1.2 Verification of electronic signatures ......................................................................... 13
      5.1.3 Validation of certificates ............................................................................................ 14
   5.2 Verification of evidence records ....................................................................................... 16
   5.3 Computation of a hash value ............................................................................................. 16
   5.4 Time stamp ....................................................................................................................... 16
      5.4.1 Requesting a qualified time stamp ............................................................................ 16
      5.4.2 Verification of a qualified time stamp (optional) ....................................................... 17
      5.4.3 Creation of a non-qualified time stamp (optional) ................................................... 17
      5.4.4 Canonicalization of XML objects (optional) ............................................................ 17

6. Security functions of the Cryptographic-Module ................................................................ 18
   6.1 Administration of cryptographic keys ................................................................................ 18
      6.1.1 Private keys ............................................................................................................... 18
      6.1.2 Public keys / certificates ........................................................................................... 18
   6.2 Protection of the Cryptographic-Module against manipulation ........................................ 18
   6.3 Configuration of the cryptographic functions ..................................................................... 19
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" ([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 set 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 ArchiSafe Reference Architecture and is supposed to enable 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](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.2: Cryptographic-Module" and specifies the functional and security-related requirements for a module that makes the necessary cryptographic functions available for the preservation of evidence. In doing so, it primarily concerns the creation and validation of electronic signatures and the related certificates, the computation of hash values and the creation or retrieval of (qualified) time stamps.

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.2: Cryptographic-Module" and specifies the functional and security-related requirements for a module that makes the necessary cryptographic functions available for the preservation of evidence. In doing so, it primarily concerns the creation and validation of electronic signatures and the related certificates, the computation of hash values and the creation or retrieval of (qualified) time stamps.
2. Overview

The following section provides an overview of the basic goals and requirements for cryptographic functions for the preservation of evidence of electronic data.

2.1 Goals

The Cryptographic-Module provides mainly cryptographic functions that are needed for the preservation of evidence of electronically signed data. Furthermore, the Cryptographic-Module also may provide functions for the creation or verification of additional cryptographic security measures. In this document, additional basic requirements for the (cryptographic) algorithms used, the required security functionalities and the configuration of the Cryptographic-Module will be defined and described.

2.2 Manner of functioning

The Cryptographic-Module provides the following cryptographic and supporting functions:

1. Cryptographic functions:
   - Creation of electronic signatures (optional)
   - Verification of electronic signatures
   - Validation of electronic certificates up to a trustworthy root certificate
   - Computation of hash values for electronic data presented
   - Requesting of qualified time stamps
   - Verification of (qualified) time stamps
   - Creation of (non-qualified) time stamps (optional)

2. Supporting functions
   - Integration of secure signature creation devices (conforming to the specifications of the eCard-API-Framework [BSI TR-03112]).
   - Canonicalization of XML objects (optional)

The Cryptographic-Module provides these functions through the TR-ESOR-S.1 and TR-ESOR-S.3 interfaces to the ArchiSafe (see also Annex [TR-ESOR-M.3]) and ArchiSig (see also Annex [TR-ESOR-M.1]) modules.

It may provide these and other functions through other interfaces that are not the subject of this Technical Guideline, even to other modules and systems.
3. Definition of the Cryptographic-Module

The term "Cryptographic-Module" includes all cryptographic functional units that are needed for the creation and verification of electronic signatures and time stamps in conjunction with the preservation of evidence of electronic documents. In this manner, the Cryptographic-Module realises a significant part of the signature application component pursuant to § 2 No. 11 SigG.

Furthermore, the Cryptographic-Module may also provide additional functions for the creation or verification of additional cryptographic security measures.

3.1 Basic design

The technical realisation of the Cryptographic-Module is largely up to the product provider as long as it fulfils the requirements described in the following sections. The following implementation variants, for example, are available:

- Direct inclusion of a Cryptographic-Module implemented in a software (as a library or service),
- Direct inclusion of a software library or a service that allows access to a Cryptographic-Module implemented in hardware,
- Direct access to a hardware Cryptographic-Module.

These basic options for realisation do not release the manufacturer (vendor) from the duty to fulfil the requirements set on the basis of applicable legal regulations and standards for the technical implementation of signature application components and (secure) signature creation devices in order to be able to create and verify legally compliant advanced or qualified electronic signatures.²

3.2 Modular inclusion of the cryptographic functions

On account of potentially very long retention periods for electronic documents, it is necessary to take future cryptographic requirements into account from the beginning. This means that:

(A3.2-1) The Cryptographic-Module shall have modular character. A quick and uncomplicated exchange of algorithms and parameters of the Cryptographic-Module that are no longer suitable security measures or that endanger security with suitable algorithms and parameters or of the entire Cryptographic-Module shall be possible at any time.

3.3 Certification by the Federal Network Agency

The Federal Network Agency for Electricity, Gas, Telecommunications, Post and Railway (BNetzA) is the competent authority pursuant to § 3 of the German Signature Act (SigG). In the scope of its legal mandate, the Federal Network Agency publishes security certifications in the Federal Gazette [German Bundesanzeiger] and on its website for products for qualified electronic signatures that were issued by a body recognised pursuant to § 18 SigG.

Certifications of products not listed on this page have so far not been recognised by the Federal Network Agency and thus do not verifiably fulfil the requirements of the SigG and SigV³.

² These requirements (see also German Signature Ordinance (SigV) § 15) particularly cover the secure treatment of data and keys before, during and after processing.

³ "In order to minimize the delays that have arisen up to now during the process of product certifications and support the economic interests of the companies concerned, the Federal Network Agency has decided that security certifications for products for qualified electronic signatures that were issued by a body recognised pursuant to § 18 SigG will also be published without delay in the Federal Gazette [German Bundesanzeiger] and on its website. Should defects be found after the fact, in particular inadequate testing of the products or if they are unable to fulfil the requirements, then the Federal Network Agency expressly reserves the right in
Thus, it is possible in the future that signatures can no longer be verified with the products that are available and authorised at that time.

Therefore, it is necessary for the preservation of evidence of archived data and documents that the opportunity for long-term verification of electronic signatures, time stamps and certificates is ensured by means of suitable technical and organisational safeguards.

**(A3.3-1)** Products that provide the function of the Cryptographic-Module listed in chapter 2.2 No. 1 and 2 should have certification pursuant to the Signature Act and the Signature Ordinance in order to support the preservation of evidence intended by this Technical Guideline.\(^4\)

---

\(^4\) A manufacturer's declaration pursuant to the SigG has been subject neither to a material verification of the manufacturer's declaration nor to a verification of the products listed therein by the Federal Network Agency. For that reason, the manufacturer is solely responsible for the contents of the manufacturer's declaration and for the products. Only after certification by the Federal Network Agency, it is ensured that it is indeed a product in the sense of the SigG.
4. Basic requirements for algorithms and parameters

The requirements for the Cryptographic-Module with regard to the algorithms and parameters used are based on the specifications and recommendations of the Federal Office for Information Security and, insofar as they relate to electronic signatures, are regularly published by the Federal Network Agency (BNetzA), the competent body pursuant to § 3 SigG, in the scope of the "Announcement Regarding the Electronic Signature pursuant to the Signature Act and the Signature Ordinance", "Overview of Suitable Algorithms". These specifications are binding for the Cryptographic-Module and always have to be updated pursuant to the current recommendations of the Federal Office for Information Security and the Federal Network Agency. Additionally, the BSI's general recommendations regarding the cryptographic functions' suitability as security measures are to be observed ([TR-02102]: Cryptographic Procedures: Recommendations and Key Lengths). The Cryptographic-Module is to be adapted to the updated recommendations on an ongoing basis in this case, too.

NOTICE: This chapter describes the respective specifications to be applied to the cryptographic procedures. Both the choice of procedures and the specifications listed are based solely on the functionalities of the Cryptographic-Module that are needed as a bare minimum for the preservation of evidence. This document is not a complete description of all the specifications and procedures that a general Cryptographic-Module can or should fulfil in general.

4.1 Generation of random numbers

Cryptographic procedures employ random numbers in diverse functions, among other to generate

- Cryptographic keys and system parameters (e.g. in the form of prime numbers),
- Data used temporarily for authentication (challenges),
- Random characters to complete character strings (e.g. cryptographic keys and messages) up to a determined length (padding)

(A4.1-1) Random numbers may be generated by using physical effects (physical generators) or mathematical algorithms (pseudo random number generators).

(A4.1-2) As set forth in the BSI Technical Guidelines [TR 03116] and [TR 02102], the random number generators used by the Cryptographic-Module should fulfil the requirements pursuant to [AIS 20] for pseudo random number generators or pursuant to [AIS 31] for physical random number generators.

4.2 Computing hash values

In order to find alterations to electronic data, hash functions are used that map data of any length to a unique resulting value (a so-called "digital fingerprint") with a specified length by using non-reversible mathematical functions. The following considerations only deal with deterministic hash functions without random components that deliver identical hash values for (and only for) identical data.

5 The non-reversibility is usually based on the extremely high computing power needed today for the reversal that makes practical application impossible.

6 Because the generation range of hash functions is usually significantly smaller than the data range to be mapped, collisions can occur, i.e. two different information packages can be mapped to the same hash value. In order to be able to verify the integrity of data without any doubt, the characteristic of collision resistance shall also be required for the algorithms and parameters used. Thus, hash functions are described as collision-resistant if it is practically impossible to find a pair of different input data with the same hash values.
(A4.2-1) The Cryptographic-Module shall offer at least one hash algorithm that has been assessed as suitable as security measures and published by the Federal Office of Information Security and the Federal Network Agency (in this respect, see [TR 03116], [TR 02102] and [ALGCAT]).

(A4.2-2) The Cryptographic-Module should offer at least one additional current hash algorithm that has been assessed as suitable as security measures and published by the Federal Office of Information Security and the Federal Network Agency (in this respect, see [TR 03116], [TR 02102] and [ALGCAT]) in order to be able to react quickly to the loss of security suitability of one of the hash algorithms used.

(A4.2-3) Only those hash algorithms and parameters recommended by the Federal Office of Information Security and the Federal Network Agency shall be used to compute hash values. However, the Cryptographic-Module shall continue to support all hash algorithms previously used pursuant to [ALGCAT] or ([TR-ESOR-ERS], Chap. 5.2.1) in order to enable the verification of hash values computed in the past.

4.3 Creation of signatures

For the creation of additional cryptographic security measures that go beyond the direct purpose of preserving the evidence of cryptographically signed electronic documents, the Cryptographic-Module may be capable of creating electronic signatures itself.7 The ability to create qualified electronic signatures is only needed, though, when the Cryptographic-Module is able to and is used for generating qualified time stamps or for generating qualified electronic signatures to be made available to applications or signatures that go beyond the goals of this Technical Guideline.8

(A4.3-1) As it pertains to algorithms for qualified electronic signatures, the Cryptographic-Module shall comply with the current version of the algorithm catalogue “Geeignete Algorithmen zur Erfüllung der Anforderungen nach § 17 Abs. 1 bis 3 SigG vom 22. Mai 2001 in Verbindung mit Anlage I Abschnitt I Nr. 2 SigV vom 22. November 2001” [Suitable algorithms to fulfil requirements pursuant to § 17 Par. 1 through 3 SigG from 22 May 2001 together with Annex I Clause I No. 2 SigV from 22 November 2001] [ALGCAT]. The requirements from chapter 4.2 shall be implemented for computing the hash values required for signatures.

Pursuant to the Signature Ordinance, Annex 1, No. 2 Algorithms – Publication and New Determination of Suitability, the respective current version will be published by the competent body (Federal Network Agency) in the Bundesanzeiger and can generally be obtained from the Federal Network Agency website (see www.bundesnetzagentur.de).

(A4.3-2) The current recommendations of the Federal Office for Information Security (see [TR 03116] and [TR 02102]) shall be taken into account for all other signature components with regard to the Cryptographic-Module.

4.4 Canonicalization procedure

It shall be ensured during the computation of hash values and signature of XML data that no ambiguity arises. To be able to achieve this, a so-called canonicalization of the contents is necessary. During canonicalization, syntactic differences in the XML data which do not have any semantic meaning are equalised, e.g. empty tags, sequence of the XML elements, line breaks, white spaces and special characters. Canonicalization is the basis for the unique computation of hash values from XML data.

Thus, the recommended Reference Architecture (see Figure 1) assumes that the Cryptographic-Module

---

7 The ArchiSafe-Module can optionally create an entry signature for the data object to be archived. This signature only serves the securing of integrity, though.

8 The ArchiSig-Module needs qualified signed qualified time stamps to generate the hash trees. As a rule, such time stamps with a signature are likely requested from certification service providers. It cannot be ruled out, though, that a Cryptographic-Module could itself be able to create these time stamps.
a. Computes the hash values for the archive data objects (group) that are needed for the ArchiSig hash trees. In this case, the ArchiSig-Module (see TR-ESOR-M.3) shall carry out the canonicalization.

b. May create (advanced) electronic signatures for archive data objects (group) (archive entry signature). Before the hash value is computed the canonicalisation required for this shall be carried out by the Cryptographic-Module.

c. Shall be able to verify (qualified and advanced) signatures from the archive data objects (group) to be archived. Before the hash value is computed the canonicalisation required for this shall be carried out by the Cryptographic-Module.

Thus, the canonicalization functionality in the Cryptographic-Module is an obligatory part; offering this functionality through external interfaces is optional, though.

(A4.4-1) Support of canonicalization procedures for the mere computation of hash values and the signing of XML contents by the Cryptographic-Module is optional.

(A4.4-2) Support of canonicalization procedures for the verification of signatures of XML contents by the Cryptographic-Module is obligatory.

(A4.4-3) The implemented canonicalization procedures shall not change the content data.

(A4.4-4) At the time this Technical Guideline was published, there were no specifications for the implementation of a canonicalization procedure from the Federal Office for Information Security or the Federal Network Agency. As a minimum requirement, the following procedure:

• C14N - Canonical XML Version 1.0 [C14N]

shall be supported. Additionally, support of the following procedures is recommended:

• C14N11 - Canonical XML Version 1.1 [C14N11]
• C14N20 - Canonical XML Version 2.0 [C14N20]
• EC14N - Exclusive XML Canonicalization [EC14N]
5. Functions of the Cryptographic-Module

The following section describes both obligatory and optional functions that are provided to other modules of the TR-ESOR-Middleware by the Cryptographic-Module through external interfaces. The Cryptographic-Module may also make these functions available to other systems and include other functions. However, these other functions shall not impair the functions listed in this section technically or with regard to security, and shall not circumvent the security functions described in chapter 6.

5.1 Electronic signatures

Electronic signatures are a technical solution for the electronic documentation of authorship and for proof of the integrity of electronic data. They are based on asymmetric cryptographic procedures and the computation of hash values.

On the basis of these procedures, electronic signatures can be created in a legally compliant manner pursuant to § 2 SigG. In doing so, the following distinctions are made pursuant to § 2 No. 2 SigG among others:

- "Advanced electronic signatures" and
- "Qualified electronic signatures".

The following basic requirements apply to both:

- The signature shall be assigned to a signature key owner,
- The signature shall enable identification of the owner,
- The signature shall be created by means that the signature key owner has under his sole control, and
- The signature shall be linked with the data to which it refers in such a manner that subsequent changes made to the data can be recognised.

For qualified electronic signatures, § 2 No. 3 SigG additionally stipulates that they are based on a valid qualified certificate at the time of creation and that they are created by a secure signature creation device.

5.1.1 Creation of an electronic signature

To create an electronic signature, first a hash value is computed from the data to be signed. The signature is created from this hash value by a signature procedure that uses the signature key of the key owner.

\[(A5.1-1)\] The Cryptographic-Module may be able to furnish electronic data with advanced electronic signatures.

\[(A5.1-2)\] The creation of qualified electronic signatures by a Cryptographic-Module that complies with this Technical Guideline is optional. The Cryptographic-Module

\[(A5.1-3)\] may provide such functions to create qualified electronic signatures for XML data or binary data upon request or in a rule-based manner.\(^9\)

\(^9\) For the preservation of evidence in and of itself, no qualified electronic signatures are necessary, because no renewed declarations of intent in the legal sense are to be delivered for the preservation of evidence. The qualified electronic signatures that may become necessary for signature renewal (signature of qualified time stamps) are requested from the certification service provider that also issues the qualified time stamp. Only if the Cryptographic-Module itself creates these time stamps must it also be capable of creating qualified electronic signatures.
(A5.1-4) Electronic signatures for XML data shall be created in the following format and follow the basic recommendations in [Common PKI] (Part 8):

- XML Signature Standard [XMLDSIG], [RFC3275]
  The canonicalization procedure shall be used when using this format.

(A5.1-5) Electronic signatures for binary data should be created in the following format and follow the basic recommendations in [Common PKI] (Part 3):

- Cryptographic Message Syntax (CMS) (c.f. [RFC5652], previous [RFC3852])

(A5.1-6) The signature data created shall be delivered by the Cryptographic-Module to the module making the request in an unchanged manner.

5.1.2 Verification of electronic signatures

The signature of electronic data is verified by computing a new hash value from the data (without the signature) and comparing it to the hash value computed upon creation of the signature. To do so, the first step of this process is to extract the signature key owner's user certificate from the signature, which contains his public key (see chapter 6.1.2) or request this certificate from the directory services of the certificate's issuer. At the time the signature was created, the validity of the certificate is verified by a request to the issuer (see chapter 5.1.3). The signature is verified with the signature key owner's public key extracted from the user certificate. If this verification is successful and the public signature verification key originates from a certificate which was valid at the time the signature was created, then the electronic signature is valid.

Verification of the validity and applicability of the assigned certificate shall follow a certification path to a certification authority that is trustworthy from the verifier's perspective. During this process, at least the following points shall be verified (see also [HK 06], section 4.2):

- The mathematical validity of the signatures,
- The validity of the certificates pursuant to the validity model,
- The correctness of the intended use of the certificates.

Depending on the application, the verification of the signature can also include additional aspects, for example whether the certificate of the creator of the signature is qualified, or whether the certificates were issued based on a certain certificate policy.

(A5.1-7) The verification of electronic signatures is indispensable for the preservation of evidence of electronically signed data. Therefore, a Cryptographic-Module that conforms to this Technical Guideline shall provide functions for the reliable verification of electronic signatures.

(A5.1-8) The signature verification function of the Cryptographic-Module shall at least support the signature data formats listed in section 5.1.1.

(A5.1-9) The function shall be able to verify whether the user certificate used to create the signature was valid at the time the signature was created (see chapter 5.1.3). The validity check shall be complete, i.e. include the entire certificate chain up to a trustworthy root certificate. During the verification process, the Cryptographic-Module shall return additionally determined verification information to the module making the request. This verification information determined (certificates, certificate revocation lists, OCSP responses) shall be supplemented in the archive data object or returned as a verification report pursuant to [OASIS-VR] or [TR-ESOR-VR].

(A5.1-10) The Cryptographic-Module shall be able to verify advanced and qualified electronic signatures.

(A5.1-11) The Cryptographic-Module shall be able to create signature verification results in standardised formats. It is recommended to use the verification report specified by the BSI in the eCard-API-Framework (see [eCard-2] "VerificationReport" or [TR-ESOR-VR]) for this purpose.

10 The request to the issuer (certification service provider) of whether they issued this certificate is not only required in order to be able to prove its existence pursuant to the rules; the result of the request is also needed to prove the validity of the certificate at the time the signature was created (see [SFD 06], p. 96 et seq.).
The handover of verification report pursuant to [OASIS-VR] or [TR-ESOR-VR] shall be returned by the Cryptographic-Module if requested by the client.

(A5.1-12) The signature verification results including the related certificate information shall be delivered by the Cryptographic-Module to the module making the request without any changes.

5.1.3 Validation of certificates

Part of every signature verification and an significant aspect for determining the conclusiveness of electronically signed documents is the validation of the user certificate on which the signature is based (see [SFD 06], p. 90). The user certificate confirms the assignment of the signature key owner to the signature verification key (public key), the corresponding private key of which was used to create the signature. If it is a qualified certificate valid at the time the signature was created, proof of the authenticity of an electronic document can be provided in general. Thus, it is of decisive importance for the preservation of evidence of signed data that the existence of the user certificate and its validity at the time the signature was created remain verifiable.

In addition to the presentation of the user certificate, the prerequisite for this is the verification of the signature of the certification service provider including the certificate of the certification service provider and the root certificate (see [SFD 06], p. 91). Furthermore, a validity inquiry at the certification service provider is also required in order to exclude the possibility that the signature is based on a certificate that was created in an abusive manner using the name of a certificate service provider. This inquiry confirms in a verifiable manner that it issued the certificate and that it was valid at the time the signature was created.

The user/operator of the Cryptographic-Module shall ensure that the Cryptographic-Module supports all certification service providers from which certificates are used for the creation of electronic signatures for business application data to be archived with the requirement of the preservation of evidence, and thus potentially all certification service providers used by business applications.

(A5.1-13) The Cryptographic-Module shall offer a function that is able to demonstrably verify the presence and the validity status of user certificates for electronic signatures at the time the signatures were created. The verification shall be complete up to a trustworthy root certificate from the highest certification authority in the certification chain.

(A5.1-14) To request the certificate chain, the following standardised protocols can be used:

- HTTP (see [RFC1945] or [RFC 2616]) or
- LDAP (see [RFC4510])

It is recommended to use a trustworthy communication channel, for example TLS/SSL encryption of the protocols, with an authentication of the certification service provider or its directory service.

(A5.1-15) The validity of the certificate shall be verified on the basis of a standardised protocol. The following protocol is recommended:

- OCSP – Online Certificate Status Protocol ([RFC6960], previously [RFC2560])

OCSP is an IETF-adopted standard ([RFC6960], previously [RFC2560]) for a protocol used to verify the current status of a digital certificate. In contrast to verification with so-called certificate revocation lists (CRLs), the client application, e.g. a browser, can directly inquire about the validity of the certificate. To do so, the verifier sends a request (OCSP request) to an authorised information point (OCSP responder).

This OCSP responder is typically operated by the certificate issuer (certification service provider) and responds with "good" (i.e. the certificate is not revoked), "revoked" (i.e. the certificate was not revoked), or "unknown" (i.e. the certificate status is unknown).

---

11 In order to receive this statement at the OCSP Protocol, it may be necessary to inspect the CRL inquiry (in the case of non-qualified certificates in particular).

12 In this case, the term "certification service provider" is not only associated with qualified certificates as in the SigG, but also with non-qualified certificates.

13 See also [HK 06], chapter 4.5.
certificate is revoked) or "unknown" (i.e. the status could not be determined, for example because the certificate publisher is unknown to the OCSP responder). Furthermore, it is possible that the OCSP responder responds with so-called positive information. In doing so, the response is accompanied by a hash value of the certificate if the certificate actually exists.

The response (OCSP response) is always digitally signed by the OCSP responder, thus allowing the client to verify its authenticity and unaltered status.

OCSP also allows validity inquiries for several certificates in one request; the OCSP responder then delivers its response in a list with the respective certificate status.

- Furthermore, the SCVP - Server-Based Certificate Validation Protocol [RFC5055] may be used:

  The Server-Based Certificate Validation Protocol (SCVP) is an Internet protocol that makes it possible for clients to outsource the creation of an X.509 certificate chain and its validity verification. This is needed primarily for clients that would be overloaded by the chain creation and validity verification due to the lack of resources or protocols. SCVP can relieve the client of all tasks (creation of the chain, checking for revocation, validation) that are part of a complete certificate verification.

  In contrast to OCSP, SCVP consists of two messages:

  - First, the client asks the server for supported validation policies that determine for which applications the server was configured.
  - Then, the client sends the certificate IDs to the server and indicates which actions are to be carried out, which the server answers in a signed manner.

  Up to now, however, SCVP has hardly been used and is only supported by a few applications.

(A5.1-16) To verify the current certificate validity, certificate revocation lists (CRL – Certificate Revocation Lists) can be used in addition. This presupposes that certificates are not temporarily revoked and later re-approved, but rather that all certificate revocations are final.

(A5.1-17) If certificate revocation lists are used to verify the certificate validation and the results of the certificate revocation list inquiry are unclear (or the certificate revocation list cannot be obtained), the respective error messages along with all other available verification information in the verification report or in the archive data object supplemented by this verification information shall be returned to the module making the request.

(A5.1-18) The Cryptographic-Module shall have a function to validate certificate chains in order to be able to verify the integrity of archived certificate chains and archived packages (see [RFC5280] section 6 and [TR-ESOR-M.3]). It should be possible to configure the list of trustworthy certificates.

---

14 If an OCSP responder works on a current database (e.g. a replication of the database of the certification authority), it always indicates the current revocation status of the certificate. For the validity verification of an electronic signature, though, it is the status of the certificate at the time the signature was created that is particularly relevant. Thus, the OCSP responses can also indicate the revocation time in the case of a revoked certificate so that it can be determined if this certificate was still valid at a certain time. If, though, the certification authority initiates temporary revocations (suspensions) (which is not supported for qualified certificates), it cannot be determined on the basis of a positive OCSP response whether this certificate has been suspended in the meantime. However, this is not seen as a disadvantage of OCSP; rather, the suspension of signature certificates is considered a problem for later verifications.

15 When certificate revocation lists are used, it must be noted though that they are in contrast to OCSP responses, which are precise to the second, only created at certain intervals and therefore might not be completely up to date. Furthermore, one cannot tell from a certificate revocation list whether a certificate was ever issued, and therefore non-revoked certificates cannot be differentiated from counterfeit certificates on the basis of a certificate revocation list alone. To do so, it is necessary to request a positive list.
5.2 Verification of evidence records

(A5.1-19) The Cryptographic-Module shall be able to verify supplemental evidence data, e.g. signatures, time stamps, certificates, certificate revocation lists, OCSP responses etc., as well as evidence records on the basis of [RFC4998] and [RFC6283] upon request.

(A5.1-20) The Cryptographic-Module shall verify evidence records and supplemental evidence data when EvidenceRecords and other supplemental evidence data are handed over in the course of a request.


(A5.1-22) The verification results shall be returned either in the form of a verification report pursuant to [TR-ESOR-VR] or as a supplement of the XAIP container handed over pursuant to [TR-ESOR-F].

5.3 Computation of a hash value

The ability to compute and verify hash values is necessary for the preservation of evidence and for the verification of the integrity of archived data. This means that:

(A5.2-1) The Cryptographic-Module shall have functions to compute hash values for information packages. In doing so, the requirements for the hash procedures (see chapter 4.2) shall be fulfilled.

5.4 Time stamp

The time and date of an event are documented in electronic form with the help of an electronic time stamp. In the context of electronic signatures (see chapter 5.1), the requirements for qualified time stamps pursuant to § 2 No. 14 SigG and § 15 clause 3 SigV apply. Certification service providers accredited by the Federal Network Agency are available for this purpose.

Related to the preservation of evidence, qualified time stamps can be relevant to several events to document, among other things,

- The time at which an archive data object (group) was archived,
- The time at which the archive data object(s) provably was(were) of integrity,
- The time at which a signature is created or verified and
- The time at which evidence records pursuant to the IETF ERS standard [RFC4998] and, in addition to this, [RFC6283] were created to prove the authenticity and integrity of archived data.

5.4.1 Requesting a qualified time stamp

When the Cryptographic-Module makes a time stamp request, a qualified time stamp is requested, for example from a certification service provider or a correspondingly verified and approved hardware module.

(A5.3-1) The Cryptographic-Module shall have a function to request a qualified time stamp. If the request is made to a certification service provider, then it shall at least fulfil the requirements pursuant to §§ 4 through 14 and § 17 or § 23 SigG and the related specifications pursuant to § 24 SigV. Alternatively, a device which was accordingly verified and approved by the Federal Network Agency can be used, which is then controlled by the Cryptographic-Module.

16 [RFC4998] shall, [RFC6283] can be supported.

17 In this case, the operator of the Cryptographic-Module themselves shall be a certification service provider.
(A5.3-2) The Cryptographic-Module shall verify whether requested qualified time stamps include a qualified electronic signature from the time stamp issuer for the signatures renewal pursuant to § 17 SigV (see also Annex [TR-ESOR-M.3]) in order to ensure that the integrity and authenticity of the time stamp can also be verified over the long-term.

(A5.3-3) The Cryptographic-Module shall verify whether the time stamp requested fulfills the requirements and specifications of the time stamp protocol pursuant to [RFC3161], ([RFC5652], previously [RFC3852]) and [ETSI-TSP]; here, the limitations for algorithms and parameters assessed as suitable for security by the Federal Office for Information Security and the Federal Network Agency (see section 4.2) shall be verified by the Cryptographic-Module.

(A5.3-4) The Cryptographic-Module shall mathematically verify the integrity of received qualified time stamps immediately upon receipt and prior to further processing and secure the authenticity or trustworthiness\(^\text{18}\) (see section 5.4.2).

5.4.2 Verification of a qualified time stamp

(A5.3-5) Qualified time stamps with (qualified) electronic signatures shall be verifiable, i.e. the validity of the time stamp signature at the time at which the time stamp was created shall be verified. This function corresponds to a signature verification. The requirements for this function have already been described in section 5.1.2.

5.4.3 Creation of a non-qualified time stamp (optional)

(A5.3-6) The Cryptographic-Module may additionally have a function to create non-qualified time stamps which do not fulfill the requirements stipulated in SigG and SigV for qualified time stamps.

\[\text{NOTICE: Only using non-qualified time stamps or non-qualified signed time stamps is not suitable for preserving the evidence of qualified signed archived data.}\]

5.4.4 Canonicalization of XML objects (optional)

In the context of this Technical Guideline, it is assumed that XML data that is or will be electronically signed is already available in a canonicalized form prior to the transfer to the TR-ESOR-Middleware.

(A5.3-7) The Cryptographic-Module can have a function for canonicising XML objects.

(A5.3-8) If a function is implemented to canonise XML objects, it shall then fulfill the requirements for the canonicalization procedure (see chapter 4.4).

\(^{18}\text{A complete verification of the authenticity immediately upon receipt of the time stamp is usually not possible, because certificate revocation lists of the time stamp service provider have not been updated yet.}\)
6. Security functions of the Cryptographic-Module

The following section describes the basic security functions that shall be implemented by a Cryptographic-Module that complies with this Technical Guideline.

6.1 Administration of cryptographic keys

6.1.1 Private keys

Private keys are used primarily to create signatures. The requirements in this section are not relevant if the Cryptographic-Module does not include a function to create signatures.

(A6.1-1) Private keys to create signatures (signature keys) may be stored in the Cryptographic-Module. In the event that multiple keys are stored, then the Cryptographic-Module shall have a function to select which key is to be used.

(A6.1-2) Private keys stored in the Cryptographic-Module shall be protected from unauthorised access. Private keys shall only be accessed after successful authentication of the respective key owner.

(A6.1-3) The private key should be stored in a protection system implemented as a hardware solution, e.g. Hardware Security Module (HSM), USB tokens or a smart card.

(A6.1-4) When deposited in a file system, private keys shall be stored in a data format that offers sufficient protection for the private keys. The Public Key Cryptography Standard #12 [PKCS#12] format is recommended for the cryptographically-protected deposit of keys and X.509v3 certificates [RFC5280].

(A6.1-5) The Cryptographic-Module may offer key administration functions, i.e. for generating, storing, deleting and archiving key pairs.

6.1.2 Public keys / certificates

(A6.1-6) No additional (security) functions are needed for public keys and certificates.

6.2 Protection of the Cryptographic-Module against manipulation

Due to the modular character of the Cryptographic-Module (see chapter 3.2), there is a potential threat of unauthorised exchange or manipulation of the Cryptographic-Module.

(A6.2-1) The Cryptographic-Module shall only be accessed after successful mutual authentication between the Cryptographic-Module and the interface partner. Authentication shall be repeated for each request; alternatively, a secure tunnel may be maintained after successful authentication. (See [ACMPP].)

(A6.2-2) The Cryptographic-Module should include a function to verify its own integrity as internal defence against manipulation.

(A6.2-3) The Cryptographic-Module shall record the execution of all security-related functions in a meaningful and traceable manner. Security-related functions include all functions which can affect the module's security, the security of the cryptographic material, the correct execution of the cryptographic functions (such as software updates, the exchange of keys or the configuration of the random number generator).

(A6.2-4) The Cryptographic-Module shall be capable of cancelling the execution of a function with a meaningful and comprehensible error message in the event of unauthorised intervention in the module's security functions.

(A6.2-5) The Cryptographic-Module shall offer a function to protect key storage if it offers key administration functions, i.e. for generating, storing, deleting and archiving key pairs. These
requirements may be fulfilled by the ((A6.1-3) and (A6.1-4)) above, preferably as a protection system implemented as a hardware solution.

6.3 Configuration of the cryptographic functions

To react to changing cryptographic requirements, it is necessary for authorised persons to be able to modify the Cryptographic-Module configuration.

(A6.3-1) The Cryptographic-Module shall have a central function to configure cryptographic functions in order to control the use of exclusively those algorithms and parameters assessed as suitable for security by the Federal Office for Information Security and the Federal Network Agency. It is recommended to control the configuration through a central configuration file which prescribes the validity of algorithms and key lengths used. Alternatively, configuration changes may also be implemented by exchanging the entire Cryptographic-Module or parts of it.

Configuration changes shall always be logged in a meaningful and traceable form and permanently stored.

(A6.3-2) It is recommended to support the DSSC (Data Structure for Security Suitabilities of Cryptographic Algorithms, see [DSSC]) format for the configuration of the Cryptographic-Module as soon as the standardisation process of the IETF has been completed and this format is assessed as suitable by the Federal Network Agency.

(A6.3-3) The configuration of the cryptographic functions shall take place via a protected Cryptographic-Module interface that prevents unauthorised administration of the module.¹⁹

¹⁹ Because this interface is quite product-specific, it will not be described in more detail in this Technical Guideline. A possible design of such an interface is described in [eCard-3].