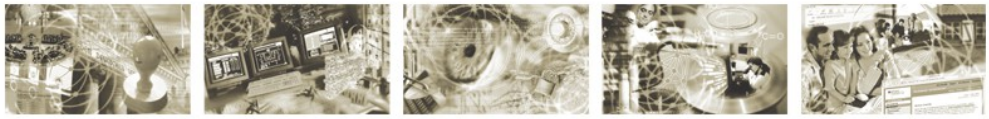
Bundesamt
für Sicherheit in der
Informationstechnik



BSI Technische Richtlinie 03125
Beweiswerterhaltung kryptographisch signierter Dokumente

Anlage TR-ESOR-M.2: Krypto-Modul

Bezeichnung	Krypto-Modul
Kürzel	BSI TR-ESOR-M.2
Version	1.2.1 (auf Basis der eIDAS-Verordnung)
Datum	15.03.2018

Bundesamt für Sicherheit in der Informationstechnik
Postfach 20 03 63
53133 Bonn
Tel.: +49 228 99 9582-0
E-Mail: tresor@bsi.bund.de
Internet: https://www.bsi.bund.de

Inhaltsverzeichnis

1. Einführung

Ziel der Technischen Richtlinie „Beweiswerterhaltung kryptographisch signierter Dokumente“ ist die Spezifikation sicherheitstechnischer Anforderungen für den langfristigen Beweiswerterhalt von kryptographisch signierten elektronischen Dokumenten und Daten nebst zugehörigen elektronischen Verwaltungsdaten (Metadaten).

Eine für diese Zwecke definierte Middleware (TR-ESOR-Middleware) im Sinn dieser Richtlinie umfasst alle diejenigen Module (**M**) und Schnittstellen (**S)**, die zur Sicherung und zum Erhalt der Authentizität und zum Nachweis der Integrität der aufbewahrten Dokumente und Daten eingesetzt werden.

Die im Hauptdokument dieser Technischen Richtlinie vorgestellte Referenzarchitektur besteht aus den nachfolgend beschriebenen funktionalen und logischen Einheiten:

- der Eingangs-Schnittstelle S.4 der TR-ESOR-Middleware, die dazu dient, die TR-ESOR-Middleware in die bestehende IT- und Infrastrukturlandschaft einzubetten;
- dem zentralen Middlewaremodul (**[TR-ESOR-M.1]**), welches den Informationsfluss in der Middleware regelt, die Sicherheitsanforderungen an die Schnittstellen zu den IT-Anwendungen umsetzt und für eine Entkopplung von Anwendungssystemen und ECM/Langzeitspeicher sorgt;
- dem „Krypto“-Modul (**[TR-ESOR-M.2]**) nebst den zugehörigen Schnittstellen S.1 und S.3, das alle erforderlichen Funktionen zur Berechnung von Hashwerten, Prüfung elektronischer Signaturen bzw. Siegeln bzw. Zeitstempeln, zur Nachprüfung elektronischer Zertifikate und zum Einholen qualifizierter Zeitstempel sowie (optional) elektronischer Signaturen bzw. Siegel für die Middleware zur Verfügung stellt. Darüber hinaus kann es Funktionen zur Ver- und Entschlüsselung von Daten und Dokumenten zur Verfügung stellen;
- dem „ArchiSig-Modul“ (**[TR-ESOR-M.3]**) mit der Schnittstelle S.6, das die erforderlichen Funktionen für die Beweiswerterhaltung der digital signierten Unterlagen bereitstellt;
- einem ECM/Langzeitspeicher mit den Schnittstellen S.2 und S.5, der die physische Archivierung/Aufbewahrung und auch das Speichern der beweiswerterhaltenden Zusatzdaten übernimmt.
  Dieser ECM/Langzeitspeicher ist nicht mehr direkt Teil der Technischen Richtlinie, gleichwohl werden über die beiden Schnittstellen, die noch Teil der TR-ESOR-Middleware sind, Anforderungen daran gestellt.
  Ebenso wenig ist die Applikationsschicht, die auch einen XML-Adapter enthalten kann, direkter Teil der Technischen Richtlinie, auch wenn dieser XML-Adapter als Teil einer Middleware implementiert werden kann.

Die in Abbildung Abbildung 1 dargestellte IT-Referenzarchitektur orientiert sich an der ArchiSafe[1] Referenzarchitektur und soll die logische (funktionale) Interoperabilität künftiger Produkte mit den Zielen und Anforderungen der Technischen Richtlinie ermöglichen und unterstützen.

1

Siehe dazu http://www.archisafe.de

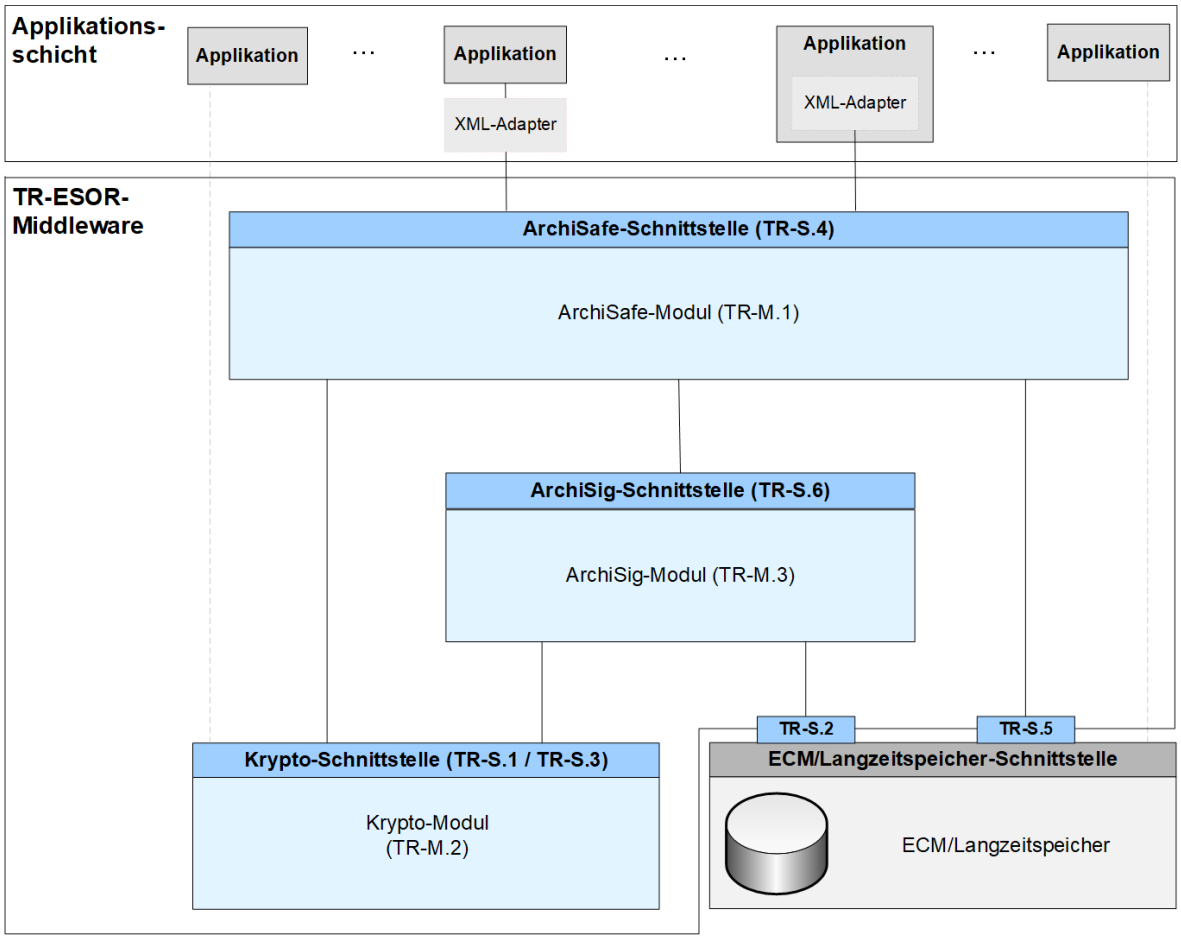


Abbildung 1: Schematische Darstellung der IT-Referenzarchitektur

Diese Technische Richtlinie ist modular aufgebaut und spezifiziert in einzelnen Anlagen zum Hauptdokument die funktionalen und sicherheitstechnischen Anforderungen an die erforderlichen IT-Komponenten und Schnittstellen der TR-ESOR-Middleware. Die Spezifikationen sind strikt plattform-, produkt-, und herstellerunabhängig.

Das vorliegende Dokument trägt die Bezeichnung „Anlage TR-ESOR-M.2: Krypto-Modul“ und spezifiziert die funktionalen und sicherheitstechnischen Anforderungen an ein Modul, dass die für den Beweiswerterhalt notwendigen kryptographischen Funktionen zur Verfügung stellt. Hierbei handelt es sich im Wesentlichen um das Validieren von elektronischen Signaturen bzw. Siegeln bzw. Zeitstempeln und den damit zusammenhängenden Zertifikaten, das Berechnen von Hashwerten und das Abfragen von (qualifizierten) Zeitstempeln sowie (optional) von elektronischen Signaturen bzw. Siegeln.

2. Übersicht

Der folgende Abschnitt gibt einen Überblick über grundsätzliche Ziele und Anforderungen an die für den Beweiswerterhalt elektronischer Daten erforderlichen kryptographischen Funktionen.

HINWEIS:

Im folgenden Text umfasst der Begriff ***„Digitale Signatur“*** *„fortgeschrittene elektronische Signaturen“ gemäß* ***[eIDAS-VO, Artikel 3 Nr. 11],*** *„qualifizierte elektronische Signaturen“ gemäß* ***[eIDAS-VO, Artikel 3 Nr. 12]****, „fortgeschrittenen elektronische Siegel“ gemäß* ***[eIDAS-VO, Artikel 3 Nr. 26]*** *und „qualifizierte elektronische Siegel“ gemäß* ***[eiDAS-VO, Artikel 3 Nr. 27]****. Insofern umfasst der Begriff „digital signierte Dokumente“ sowohl solche, die fortgeschrittene elektronische Signaturen oder Siegel bzw. qualifizierte elektronische Signaturen oder Siegel tragen.*

Mit dem Begriff der ***„kryptographisch signierten Dokumente“*** *sind in dieser TR neben den gemäß* ***[eIDAS-VO, Artikel 3 Nr. 12]*** *qualifiziert signierten, den gemäß* ***[eIDAS-VO, Artikel 3 Nr. 27]*** *qualifiziert gesiegelten oder den gemäß* ***[eIDAS-VO, Artikel 3 Nr. 34]*** *qualifiziert zeitgestempelten Dokumenten (im Sinne der eIDAS-Verordnung)) auch Dokumente mit einer fortgeschrittenen Signatur gemäß* ***[eIDAS-VO, Artikel 3 Nr. 11]*** *oder mit einem fortgeschrittenen Siegel gemäß* ***[eIDAS-VO, Artikel 3 Nr. 26]*** *oder mit einem elektronischen Zeitstempel gemäß* ***[eIDAS-VO, Artikel 3 Nr. 33]*** *erfasst, wie sie oft in der internen Kommunikation von Behörden entstehen. Nicht gemeint sind hier Dokumente mit einfachen Signaturen oder Siegeln basierend auf anderen (z. B. nicht-kryptographischen) Verfahren.*

2.1 Ziele

Das Krypto-Modul stellt vornehmlich kryptographische Funktionen bereit, die für den langfristigen Beweiswerterhalt digital signierter Dokumente benötigt werden. Das Krypto-Modul kann darüber hinaus auch Funktionen für die Erstellung oder Prüfung zusätzlicher kryptographischer Sicherungsmittel bereitstellen.

In diesem Dokument werden darüber hinaus grundlegende Anforderungen an die eingesetzten (kryptographischen) Algorithmen, sowie an erforderliche Sicherheitsfunktionalitäten und die Konfiguration des Krypto-Moduls definiert und beschrieben.

2.2 Funktionsweise

Das Krypto-Modul stellt folgende kryptographischen und unterstützenden Funktionen zur Verfügung:

1. **Kryptographische Funktionen:**
   - Validierung digitaler Signaturen (selbst oder per Anfrage bei einem externen Vertrauensdiensteanbieter)
   - Validierung elektronischer Zertifikate bis hin zu einem vertrauenswürdigen Wurzelzertifikat (selbst oder per Anfrage bei einem externen Vertrauensdiensteanbieter)
   - Erzeugen von Hash-Werten über vorgelegte elektronische Daten
   - Anforderung qualifizierter Zeitstempel bei einem qualifizierten Vertrauensdiensteanbieter
   - Validierung von (qualifizierten) Zeitstempeln (selbst oder per Anfrage bei einem externen Vertrauensdiensteanbieter)
   - Anforderung digitaler Signaturen bei einem externen Vertrauensdiensteanbieter (optional)

2. Unterstützende Funktionen

- Kanonisierung von XML-Objekten (optional)

Das Krypto-Modul stellt diese Funktionen über die Schnittstellen **[TR-ESOR-S.1]** und **[TR-ESOR-S.3]** den Modulen ArchiSafe (siehe auch Anlage **[TR-ESOR-M.1]**) und ArchiSig (siehe auch Anlage **[TR-ESOR-M.3]**) zur Verfügung.

Es kann diese und weitere Funktionen über andere Schnittstellen, die nicht Gegenstand dieser TR sind, auch anderen Modulen und Systemen zur Verfügung stellen.

3. Definition des Krypto-Moduls

Der Begriff „Krypto-Modul“ umfasst sämtliche funktionalen Einheiten, die zur Validierung digitaler Signaturen und Zeitstempel, zum Hashen und zum Abfragen von (qualifizierten) elektronischen Zeitstempeln und (optional) zum Anfordern von digitalen Signaturen im Zusammenhang mit dem Beweiswerterhalt elektronischer Dokumente benötigt werden.

Das Krypto-Modul kann darüber hinaus auch weitere Funktionen für die Erstellung oder Prüfung zusätzlicher kryptographischer Sicherungsmittel nach dem Stand der Technik und unter Beachtung der aktuell geltenden rechtlichen Vorgaben und Normen bereitstellen.

3.1 Grundlegender Aufbau

Die technische Realisierung des Krypto-Moduls steht dem Produkt-Anbieter weitgehend frei, solange er die Anforderungen der folgenden Abschnitte erfüllt. Folgende Implementierungsvarianten stehen beispielsweise zur Verfügung:

- Direkte Einbindung eines in Software implementierten Krypto-Moduls (als Bibliothek oder Service),
- Direkte Einbindung einer Software-Bibliothek oder eines Service, die einen Zugriff auf ein in Hardware implementiertes Krypto-Modul erlaubt,
- Direkter Zugriff auf ein Hardware-Krypto-Modul.

Darüber hinaus besitzt das Krypto-Modul eine

- Verbindung zu einem (qualifizierten) Vertrauensdiensteanbieter gemäß **[eIDAS-VO, Artikel 3 Nr. 19 bzw. Nr. 20**].

Diese grundsätzlichen Realisierungsoptionen entbinden einen Hersteller (Lieferanten) nicht von der Erfüllung von Anforderungen, die aufgrund geltender rechtlicher Vorschriften und Normen gestellt werden, um gesetzeskonforme fortgeschrittene, bzw. qualifizierte elektronische Signaturen, Siegel und (qualifizierte) Zeitstempel anfordern und prüfen zu können.

3.2 Modulare Einbindung der kryptographischen Funktionen

Aufgrund möglicher sehr langer Aufbewahrungsfristen elektronischer Dokumente ist es erforderlich, von Anfang an mögliche zukünftige kryptographische Anforderungen zu berücksichtigen. Das bedeutet:

(A3.2-1) Das Krypto-Modul muss Modul-Charakter besitzen. Ein schneller und unkomplizierter Austausch nicht mehr sicherheitsgeeigneter oder sicherheitsgefährdeter Algorithmen und Parameter des Krypto-Moduls durch sicherheitsgeeignete Algorithmen und Parameter oder des gesamten Krypto-Moduls muss jederzeit möglich sein.

3.3 Vertrauenslisten

Gemäß **[eIDAS-VO, Artikel 22 Absatz 1]** müssen von jedem Mitgliedstaat sogenannte Vertrauenslisten, die Angaben zu den **qualifizierten Vertrauensdiensteanbietern** im jeweiligen Mitgliedsstaat sowie zu den von diesen erbrachten Vertrauensdiensten, aufstellen, führen und veröffentlichen. Die Veröffentlichung muss auf einer gesicherten Weise in einer elektronisch unterzeichneten bzw. besiegelten Form erfolgen, die für eine automatisierte Verarbeitung geeignet ist (vgl. **[eIDAS-VO, Artikel 22 Absatz 2]**). Die Informationen über die erstellenden nationalen Stellen werden gem. **[eIDAS-VO, Artikel 22 Absatz 3]** an die Kommission übermittelt.

Für Deutschland verantwortlicher Herausgeber ist die Bundesnetzagentur für Elektrizität, Gas, Telekommunikation, Post und Eisenbahnen (BNetzA) und die korrespondierende Vertrauensliste wird auf der Internetseite https://www.nrca-ds.de/tsl.htm im Bundesanzeiger und auf den Internetseiten der Bundesnetzagentur veröffentlicht.

Die Kommission dagegen publiziert eine Vertrauensliste mit der Zusammenstellung der Eingaben über die einzelnen nationalen Stellen, zumindest den Ort der Herausgabe sowie die zur Unterzeichnung oder Besiegelung verwendeten Zertifikate (vgl. **[eIDAS-VO, Artikel 22 Absatz 4]**).

HINWEIS:

Die entsprechende Vertrauensliste der Europäischen Kommission, die auf die nationalen Vertrauenslisten verweist, und für die BSI TR-03125 (TR-ESOR) verbindlich ist, ist unter der folgenden Web-Adresse https://ec.europa.eu/information_society/policy/esignature/trusted-list/tl-mp.xml zu beziehen.

Vertrauensdiensten, die nicht mit dem Status „**granted**“ auf dieser Seite aufgeführt sind, sind bisher nicht anerkannt und erfüllen somit auch nicht nachweislich die Anforderungen gemäß **[eIDAS-VO]** und **[VDG]**.

Für den Erhalt des Beweiswertes von archivierten Daten und Dokumenten ist es daher notwendig, durch geeignete technische und organisatorische Maßnahmen die Möglichkeit der dauerhaften Prüfung von digitalen Signaturen bzw. elektronischen Zeitstempeln gemäß **[eIDAS-VO, Artikel 3 Nr. 33, 34]** und Zertifikate gemäß **[eIDAS-VO, Artikel 3 Nr. 14, 15]** sicher zu stellen.

3.4 Verbindung zu (qualifizierten) Vertrauensdiensteanbieter

(A3.4-1) Das Krypto-Modul muss mindestens eine Verbindung zu einem Vertrauensdienst gemäß **[eIDAS-VO, Artikel 2 Absatz 20]** besitzen, über den es qualifizierte Zeitstempel gemäß **[eIDAS-VO, Artikel 3 Nr. 34]** anfordern kann.

(A3.4-2) **Optional** kann ein Krypto-Modul auch Verbindungen zu Vertrauensdiensten gemäß der **[eIDAS-VO]** besitzen, um

- die Validierung von digitalen Signaturen oder elektronischen Zeitstempeln gemäß **[eIDAS-VO, Artikel 3 Nr. 33, 34]**,
- die Validierung von Zertifikaten oder
- die Erzeugung von digitalen Signaturen

anzufordern.

In Deutschland kann ein Krypto-Modul zusätzlich auch eine Verbindung

- zur Bundesnetzagentur als Vertrauensinfrastruktur zur dauerhaften Prüfbarkeit qualifizierter elektronischer Zertifikate und qualifizierter elektronischer Zeitstempel gemäß **[VDG, § 16]**

besitzen, um

- die Validierungen von Zertifikaten und Zeitstempeln, dessen herausgebender qualifizierter Vertrauensdiensteanbieter seinen Dienst nicht mehr wahr nimmt,

zu ermöglichen.

(A3.4-3) Es wird empfohlen, den Kommunikationskanal zu den Vertrauensdiensteanbietern in geeigneter Weise zu schützen (siehe z.B. **[TR 03116] (Teil 4) und [TR 02102]** sowie **[TR-ESOR], Kap. 8.2.2**).

4. Grundlegende Anforderungen an Algorithmen und Parameter

Die Anforderungen an das Krypto-Modul hinsichtlich der verwendeten Algorithmen und Parameter basieren auf den Vorgaben und Empfehlungen gemäß **[ETSI TS 119 312]**[2] und **[SOG-IS]**[3]. Diese Vorgaben sind für das Krypto-Modul verbindlich und müssen stets den aktuellen Empfehlungen gemäß **[ETSI TS 119 312]** und **[SOG-IS]** folgend angepasst werden. Weiterhin sind die allgemeinen Empfehlungen des BSI hinsichtlich der Sicherheitseignung kryptographischer Funktionen zu beachten (**[TR-02102]**: Kryptographische Verfahren: Empfehlungen und Schlüssellängen). Auch hier ist das Krypto-Modul an aktualisierte Empfehlungen laufend anzupassen.

HINWEIS:

Dieses Kapitel beschreibt für einzelne kryptographische Verfahren die jeweils anzuwendenden Vorgaben. Sowohl die Auswahl der Verfahren als auch die aufgeführten Vorgaben richten sich dabei ausschließlich an der für den Beweiswerterhalt minimal notwendigen Funktionalität des Krypto-Moduls aus. Dieses Dokument beschreibt nicht umfassend alle Verfahren und Vorgaben, die ein allgemeines Krypto-Modul erfüllen sollte bzw. kann.

4.1 Erzeugen von Zufallszahlen

Kryptographische Verfahren verwenden Zufallszahlen in verschiedenen Funktionen, u.a. zur Erzeugung von

- kryptographischen Schlüsseln bzw. Systemparametern (z. B. in Form von Primzahlen),
- temporär zur Authentisierung genutzten Daten (Challenges),
- Zufallszeichen zur Ergänzung von Zeichenfolgen (z. B. kryptographischer Schlüssel und Nachrichten) bis zu einer festgelegten Länge (Padding)

(A4.1-1) Zufallszahlen können unter Ausnutzung physikalischer Effekte (physikalische Generatoren) oder mathematischer Algorithmen (Pseudozufallszahlengeneratoren) erzeugt werden.

(A4.1-2) Die vom Krypto-Modul genutzten Zufallszahlgeneratoren sollen gemäß den Technischen Richtlinien **[TR 03116]** und **[TR 02102]** des BSI die Anforderungen nach **[AIS 20]** für Pseudozufallszahlengeneratoren bzw. nach **[AIS 31]** für physikalische Zufallszahlgeneratoren erfüllen.

2

ETSI TS 119 312: "ETSI: Electronic Signatures and Infrastructures (ESI); Cryptographic Suites"

3 SOG-IS Crypto Working Group: "SOG-IS Crypto Evaluation Scheme – Agreed Cryptographic Mechanisms", 2016, https://www.sogis.org/uk/supporting_doc_en.html

4.2 Bilden von Hashwerten

Um Veränderungen an elektronischen Daten festzustellen, werden Hash-Funktionen eingesetzt, die unter Verwendung nicht-umkehrbarer mathematischer Funktionen[4] Daten beliebiger Länge auf einen eindeutigen Ergebniswert (einen so genannten „digitalen Fingerabdruck“) mit festgelegter Länge abbilden. Im Folgenden wird ausschließlich von deterministischen Hash-Funktionen ohne Zufallskomponenten ausgegangen, die für (und nur für) identische Daten auch identische Hash-Werte liefern.[5]

(A4.2-1) Das Krypto-Modul muss mindestens einen aktuell gemäß **[ETSI TS 119 312]** und **[SOG-IS]** als sicherheitsgeeignet eingestuften und veröffentlichten Hash-Algorithmus anbieten (siehe hierzu auch **[TR 03116]**, **[TR 02102]** und **[ETSI TS 119 312]** und **[SOG-IS]**).

(A4.2-2) Das Krypto-Modul soll darüber hinaus mindestens einen zusätzlichen aktuellen gemäß **[ETSI TS 119 312]** und **[SOG-IS]** als sicherheitsgeeignet eingestuften und veröffentlichten Hash-Algorithmus anbieten (siehe hierzu **[TR 03116]**, **[TR 02102]** und **[ETSI TS 119 312]** und **[SOG-IS]**), um auf einen Verlust der Sicherheitseignung eines eingesetzten Hash-Algorithmus unverzüglich reagieren zu können.

(A4.2-3) Für die Bildung neuer Hash-Werte dürfen keine anderen als die von gemäß **[ETSI TS 119 312]** und **[SOG-IS]** empfohlenen Hash-Algorithmen und Parameter eingesetzt werden. Das Krypto-Modul muss jedoch alle in der Vergangenheit eingesetzten Hash-Algorithmen gemäß **[ETSI TS 119 312]** und **[SOG-IS] und [ALGCAT]** bzw. (**[TR-ESOR-ERS]**, Kap. 5.2.1) weiterhin unterstützen, um eine Prüfung der in der Vergangenheit erzeugten Hash-Werte zu ermöglichen.

4.3 Anforderung von digitalen Signaturen (optional)

Für die unmittelbaren Zwecke der Erhaltung des Beweiswertes kryptographisch signierter elektronischer Unterlagen ist es nicht erforderlich, dass das Krypto-Modul imstande ist, selbst digitale Signaturen bzw. elektronische Zeitstempel zu erzeugen.[6] [7].

HINWEIS:

Diese möglichen zusätzlichen Fähigkeiten der Erstellung digitaler Signaturen (Signaturen bzw. Siegel) sind nicht Betrachtungsgegenstand dieser BSI TR-03125 (TR-ESOR).

*In dieser TR muss das Krypto-Modul qualifizierte Zeitstempel von einem qualifizierten Vertrauensdiensteanbieter gemäß **[eIDAS-VO, Artikel 3 Nr. 20]** anfordern können (siehe (A3.4-1)).*

*Darüber hinaus kann das Krypto-Modul auch digitale Signaturen bzw. elektronische Zeitstempel von einem Vertrauensdiensteanbieter gemäß **[eIDAS-VO, Artikel 3 Nr. 19 bzw. Nr. 20]** erzeugen oder validieren lassen (siehe (A3.4-2)).*[8]

---

[4] Die Nicht-Umkehrbarkeit beruht dabei meist auf dem heute notwendigen extrem hohen Rechenaufwand für die Umkehrung, der eine praktikable Anwendung nicht zulässt.

[5] Da der Bildbereich von Hashfunktionen zumeist erheblich kleiner ist als der abzubildende Datenbereich, können Kollisionen auftreten, d. h. zwei unterschiedliche Datenobjekte können auf den gleichen Hashwert abgebildet werden. Um die Integrität von Daten zweifelsfrei nachprüfen zu können, muss für die eingesetzten Algorithmen und Parameter daher zusätzlich die Eigenschaft der Kollisionsresistenz gefordert werden. Hashfunktionen werden als kollisionsresistent bezeichnet, wenn es praktisch unmöglich ist, ein Paar verschiedener Eingabedaten zu finden, deren Hashwerte übereinstimmen.

[6] Auf Verlangen des ArchiSafe-Moduls kann das Krypto-Modul optional einen Eingangszeitstempel oder eine Eingangssignatur bzw. ein Eingangssiegel **von einem (qualifizierten) Vertrauensdiensteanbieter anfordern** oder selbst einen Hashwert über das zu archivierende Datenobjekt erzeugen. Diese Signatur bzw. dieser Siegel oder dieser Zeitstempel oder dieser Hashwert dient jedoch ausschließlich der Integritätssicherung.

[7] Das ArchiSig-Modul benötigt qualifizierte elektronische Zeitstempel zum Aufbau der Hashbäume. Im Regelfall werden derartige Zeitstempel samt Signatur bzw. Siegel durch das Krypto-Modul von **qualifizierten Vertrauensdiensteanbietern** angefordert, da gemäß **[eIDAS-VO, Artikel 42 Absatz 1 Buchstabe c]** gilt, dass i.d.R. ein qualifizierter elektronischer Zeitstempel „mit einer fortgeschrittenen elektronischen Signatur unterzeichnet oder einem fortgeschrittenen elektronischen Siegel des qualifizierten Vertrauensdiensteanbieters versiegelt“ wird.

4.4 Kanonisierungsverfahren

Bei der Berechnung von Hashwerten bzw. bei der digitalen Signatur von XML-Daten muss sichergestellt werden, dass es zu keinen Mehrdeutigkeiten kommt. Um dies erreichen zu können, ist zunächst eine so genannte Kanonisierung des Inhalts erforderlich. Bei der Kanonisierung werden syntaktische Unterschiede der XML-Daten angeglichen, die keine semantische Bedeutung haben, z.B. leere Tags, Reihenfolge der XML-Elemente, Zeilenumbrüche, Whitespaces und Sonderzeichen. Die Kanonisierung ist die Grundlage für eine eindeutige Bildung von Hash-Werten aus XML-Daten.

Die empfohlene Referenzarchitektur (vgl. Abbildung 1) geht davon aus, dass das Krypto-Modul

a) die Hashwerte über die Archivdatenobjekte berechnet, die für die ArchiSig-Hashbäume notwendig sind. In diesem Fall muss das ArchiSig-Modul (siehe **[TR-ESOR-M.3]**) die Kanonisierung vornehmen.

a) (fortgeschrittene oder qualifizierte) elektronische Signaturen bzw. Siegel über Archivdatenobjekte durch Vertrauensdiensteanbieter erzeugen lässt (Archiveingangssignatur bzw. -siegel). Die hierfür notwendige Kanonisierung vor der Hashwertbildung muss vom Krypto-Modul oder Vertrauensdiensteanbieter durchgeführt werden.

a) in der Lage sein muss, (qualifizierte und fortgeschrittene) elektronische Signaturen bzw. Siegel von zu archivierenden Datenobjekten lokal oder mittels eines externen Vertrauensdienstes zu validieren. Die hierfür notwendige Kanonisierung vor der Hashwertbildung muss vom Krypto-Modul durchgeführt werden.

Daher ist die Kanonisierungsfunktionalität im Krypto-Modul ein obligatorischer Bestandteil; ein Anbieten dieser Funktionalität über externe Schnittstellen ist jedoch optional.

(A4.4-1) Die Unterstützung von Kanonisierungsverfahren für die reine Hashwertberechnung und die digitale Signatur von XML-Inhalten durch das Krypto-Modul ist optional.

(A4.4-2) Die Unterstützung von Kanonisierungsverfahren für die lokale Signatur- bzw. Siegelprüfung von XML-Inhalten durch das Krypto-Modul ist verpflichtend.

(A4.4-3) Durch die implementierten Kanonisierungsverfahren dürfen Inhaltsdaten nicht verändert werden.

(A4.4-4) Für die Implementierung eines Kanonisierungsverfahrens gibt es zum Zeitpunkt der Veröffentlichung dieser Richtlinie keinerlei Vorgaben durch das Bundesamt für Sicherheit in der Informationstechnik oder die Bundesnetzagentur oder die **[eIDAS-VO]** und ihre Durchführungsrechtakte oder das **[VDG**]. Es muss mindestens das Verfahren

- C14N - Canonical XML Version 1.0 **[C14N]**

unterstützt werden. Zusätzlich wird die Unterstützung des folgenden Verfahrens empfohlen:

- C14N11 - Canonical XML Version 1.1 **[C14N11]**
- C14N20 - Canonical XML Version 2.0 **[C14N20]**
- EC14N - Exclusive XML Canonicalization **[EC14N].**

[8] Für Algorithmen im Kontext qualifizierter elektronischer Signaturen bzw. Siegel bzw. Zeitstempel muss durch den Vertrauensdiensteanbieter der Algorithmenkatalog gemäß **[ETSI TS 119 312] und [SOG-IS]** in der jeweils aktuellen Fassung eingehalten werden. Für die den kryptographischen Signaturen zugrunde liegende Bildung von Hashwerten müssen die Anforderungen aus Kapitel 4.2 umgesetzt werden.

5. Funktionen des Krypto-Moduls

Der folgende Abschnitt beschreibt sowohl verpflichtende als auch optionale Funktionen, die durch das Krypto-Modul über externe Schnittstellen anderen Modulen der TR-ESOR-Middlware zur Verfügung gestellt werden. Das Krypto-Modul kann diese Funktionen auch anderen Systemen anbieten und auch weitere Funktionen beinhalten. Allerdings dürfen diese anderen Funktionen die in diesem Abschnitt aufgeführten Funktionen weder technisch noch sicherheitstechnisch beeinträchtigen oder die in Kapitel 6 beschriebenen Sicherheitsfunktionen umgehen.

5.1 Digitale Signaturen

Digitale Signaturen sind eine technische Lösung zur elektronischen Dokumentation der Urheberschaft und zum Nachweis der Integrität elektronischer Daten. Sie basieren auf asymmetrischen kryptographischen Verfahren und der Bildung von Hash-Werten. Es gelten die aktuellen Vorgaben gemäß der **[eIDAS-VO]** und des Vertrauensdienstegesetzes gemäß **[VDG]**.

Auf Grundlage dieser Verfahren können digitale Signaturen gesetzeskonform nach **[eIDAS-VO, Artikel 3]** erzeugt werden. Dabei wird gemäß **[eIDAS-VO, Artikel 3]** u.a. unterschieden zwischen

- „fortgeschrittenen elektronischen Signaturen“ **[eIDAS-VO, Artikel 3 Nr. 11 und Artikel 26] und**
- „qualifizierten elektronischen Signaturen“ **[eIDAS-VO, Artikel 3 Nr. 12 und Artikel 32] sowie**
- „fortgeschrittenen elektronischen Siegeln“ **[eIDAS-VO, Artikel 3 Nr. 26 und Artikel 36] und**
- „qualifizierten elektronischen Siegeln“ **[eIDAS-VO, Artikel 3 Nr. 27 und Artikel 40]**

5.1.1 Anfordern einer digitalen Signatur

Für den unmittelbaren Zweck der Erhaltung des Beweiswertes kryptographisch signierter elektronischer Unterlagen ist es nicht erforderlich, dass das Krypto-Modul selbst digitale Signaturen erzeugen kann. Daher ist die Erzeugung einer digitalen Signatur hier nicht Gegenstand dieser TR.

(A5.1-1) Das Krypto-Modul kann in der Lage sein, digitale Signaturen von (qualifizierten) Vertrauensdiensteanbietern gemäß der **[eIDAS-VO]** anzufordern.[9]

(A5.1-2) Der Abruf qualifizierter elektronischer Signaturen bzw. Siegel durch ein zu dieser TR konformes Krypto-Modul mittels Abruf bei einem qualifizierten Vertrauensdiensteanbieter ist optional. Das Krypto-Modul kann solche Funktionen bereitstellen, um auf Anforderung oder regelbasiert qualifizierte elektronische Signaturen oder qualifizierte elektronische Siegel für XML-Daten oder binäre Daten abzurufen.

(A5.1-3) Digitale Signaturen für XML-Daten sollen gemäß den folgenden Formatvorgaben bzgl. XAdES-Signaturen erzeugt werden:

9 Für den Beweiswerterhalt an sich sind keine qualifizierten elektronischen Signaturen bzw. Siegel notwendig, da für den Beweiswerterhalt keine erneuten Willenserklärungen im juristischen Sinne abzugeben sind. Die für die Signatur- bzw. Siegelerneuerung ggf. notwendigen digitalen Signaturen von qualifizierten Zeitstempeln werden bei dem qualifizierten Vertrauensdiensteanbieter gemäß [**eIDAS-VO, Artikel 3 Nr. 20]** angefordert, der auch den qualifizierten Zeitstempel gemäß **[eIDAS-VO, Artikel 42]** ausstellt. Nur wenn das Krypto-Modul selbst diese Zeitstempel erzeugt, muss es auch in der Lage sein, digitale Signaturen zu erzeugen, und es muss durch oder im Auftrag eines qualifizierten Vertrauensdiensteanbieters betrieben werden.

- gemäß der jeweils aktuellen Fassung der Durchführungsrechtakte **[2015/1506/EU]** und
- gemäß den Anforderungen in **[TR-ESOR-F, (A5.1-2)].**

Bei Verwendung dieses Formates ist der Einsatz eines Kanonisierungsverfahrens erforderlich.

(A5.1-4) Digitale Signaturen für binäre Daten sollen gemäß den folgenden Formatvorgaben bzgl. CAdES-Signaturen erzeugt werden:

- gemäß der jeweils aktuellen Fassung der Durchführungsrechtakte **[2015/1506/EU]** und
- gemäß den Anforderungen in **[TR-ESOR-F, (A5.1-1)]**.

(A5.1-5) Digitale PAdES-Signaturen sollen gemäß den folgenden Formatvorgaben erzeugt werden:

- gemäß der jeweils aktuellen Fassung der Durchführungsrechtakte **[2015/1506/EU]** und
- gemäß den Anforderungen in **[TR-ESOR-F, (A5.1-3)]**.

(A5.1-6) ASiC-Container mit AdES-Signaturen, Zeitstempeln bzw. Evidence Records sollen gemäß den folgenden Formatvorgaben erzeugt werden:

- gemäß der jeweils aktuellen Fassung der Durchführungsrechtakte **[2015/1506/EU]** und
- gemäß den Anforderungen in **[TR-ESOR-F, (A5.1-4)]**.

(A5.1-7) Die auf Anforderung von einem (qualifizierten) Vertrauensdiensteanbieter erzeugten digitalen Signaturdaten müssen durch das Krypto-Modul an das aufrufende Modul unverändert geliefert werden.

5.1.2 Validierung digitaler Signaturen

Die digitale Signatur elektronischer Daten wird validiert, indem aus den Daten (ohne die digitale Signatur) erneut ein Hash-Wert gebildet und dieser mit dem bei der Signatur- bzw. Siegelerzeugung errechneten Hash-Wert verglichen wird. Dazu wird zunächst das Nutzer-Zertifikat des Signatur- bzw. Siegelschlüssel-Inhabers, das dessen öffentlichen Schlüssel[10] (vgl. Kapitel 6.1.2) enthält, der digitalen Signatur entnommen oder im Verzeichnisdienst des Ausstellers des Zertifikates abgerufen. Durch eine Anfrage beim Aussteller wird anschließend die Gültigkeit des Zertifikats zum Zeitpunkt der Signatur- bzw. Siegelerstellung validiert (vgl. Kapitel 5.1.3).[11] Mit dem aus dem Nutzer-Zertifikat extrahierten öffentlichen Schlüssel des Signatur- bzw. Siegelschlüssel-Inhabers wird die digitale Signatur geprüft. Ist diese Prüfung positiv und entstammt der öffentliche Signatur- bzw. Siegelprüfschlüssel aus einem zum Zeitpunkt der digitalen Signaturerstellung gültigen Zertifikat, ist die digitale Signatur gültig.

Die Prüfung der Gültigkeit und Anwendbarkeit des zugeordneten Zertifikates muss entlang eines Zertifizierungspfades zu einer – aus Sicht des Prüfenden – vertrauenswürdigen Vertrauensdiensteanbieter erfolgen. Dabei müssen mindestens die folgenden Punkte geprüft werden(siehe auch **[HK 06]**, Abschnitt 4.2):

- Mathematische Gültigkeit der digitalen Signaturen,
- Gültigkeit der Zertifikate gemäß Gültigkeitsmodell,
- Korrektheit des Verwendungszwecks der Zertifikate.

Je nach Anwendungsfall kann die Validierung der digitalen Signatur noch weitere Aspekte umfassen, z.B. ob das Zertifikat des Erstellers der digitalen Signatur ein qualifiziertes ist, oder ob die Zertifikate unter einer bestimmten Zertifizierungspolitik (*Certificate Policy*) ausgestellt wurden.

---

[10] Der öffentliche Schlüssel wird gemäß **[2014/910/EU, Anhang I]** bzw. **[2014/910/EU, Anhang III]** auch Signatur- bzw. Siegel- Validierungsdaten genannt.

[11] Die Anfrage beim Aussteller (Vertrauensdiensteanbieter), ob er dieses Zertifikat ausgestellt hat, ist nicht nur erforderlich, um dessen ordnungsgemäße Existenz nachweisen zu können, sondern das Ergebnis der Abfrage wird auch benötigt, um die Gültigkeit des Zertifikats zum Signatur- bzw. Siegelerstellungszeitpunkt nachweisen zu können (vgl. auch **[eIDAS-VO, Artikel 32 bzw. Artikel 40]**, **[SFD 06],** S. 96 ff.).

(A5.1-8) Die Validierung digitaler Signaturen ist für den Beweiswerterhalt digital signierter Daten unverzichtbar. Ein zu dieser Richtlinie konformes Krypto-Modul muss daher die Validierung digitaler Signaturen **sowohl auf Basis des Schalenmodells als auch des Kettenmodells entweder** bei einem externen Vertrauensdiensteanbieter gemäß **[eIDAS-VO]** anfordern oder Funktionen zur zuverlässigen lokalen Validierung digitaler Signaturen gemäß **[EN 319 102]** zur Verfügung stellen.

(A5.1-9) Die Validierungsfunktion des Krypto-Moduls, ausgeführt mittels Abruf bei einem Vertrauensdiensteanbieters oder als lokaler Service, muss mindestens die in der Durchführungsrechtakte **[2015/1506/EU]** und die in **[TR-ESOR-F, (A5.1-1) - (A5.1-4)]** sowie in Kapitel 5.1.1 genannten Signatur- bzw. Siegeldatenformate unterstützen.

(A5.1-10) Diese Funktion muss selbst prüfen können oder durch den beauftragten Vertrauensdiensteanbieter prüfen lassen, ob das für die Erstellung der digitalen Signatur verwendete Nutzer-Zertifikat zum Zeitpunkt der Signatur- bzw. Siegelerstellung gültig war (vgl. Kapitel 5.1.3 und **[eIDAS-VO, Artikel 32 bzw. 40]**) sowie ob die durch den Aussteller der Zertifikats gesetzte Signatur bzw. das Siegel gültig ist und ob Zertifikatserweiterungen gemäß **[eIDAS-VO, Artikel 28 bzw. 38 Absatz 3]** und der Verwendungszweck des Zertifikates richtig gesetzt wurden. Die Gültigkeitsprüfung muss vollständig sein, d. h. die gesamte Zertifikatskette bis hin zu einem vertrauenswürdigen Wurzel-Zertifikat umfassen. Diese Funktion des Krypto-Moduls muss bei der Prüfung ermittelte oder erhaltene zusätzliche Prüfinformationen an das aufrufende Modul zurückgeben. Diese hierbei ermittelten Prüfinformationen (Zertifikate, Sperrlisten, OCSP-Responses) sind im Archivdatenobjekt zu ergänzen oder als Prüfbericht gemäß **[OASIS-VR]** bzw. **[TR-ESOR-VR]** zurückzugeben.

(A5.1-11) Diese Funktion, ausgeführt mittels Abruf bei einem Vertrauensdiensteanbieters oder als lokaler Service, muss fortgeschrittene elektronische Signaturen bzw. Siegel gemäß **[eIDAS-VO, Artikel 26 bzw. 36]** und qualifizierte elektronische Signaturen bzw. Siegel gemäß **[eIDAS-VO, Artikel 32 bzw. 40]** prüfen können.

(A5.1-12) Die Signatur- bzw. Siegel-Prüfergebnisse müssen von dieser Funktion des Krypto-Moduls in standardisierten Formaten erzeugt werden können. Es wird empfohlen, hierfür die Prüfbericht **[OASIS-VR]** bzw. **[TR-ESOR-VR]))** zu nutzen. Die Übergabe eines Prüfberichtes gemäß **[OASIS-VR]** bzw. **[TR-ESOR-VR]** muss vom Krypto-Modul vollzogen werden, falls vom Client angefordert.

(A5.1-13) Die Signatur- bzw. Siegel-Prüfergebnisse, inklusive der zugehörigen Zertifikatsinformationen, müssen vom Krypto-Modul unverändert an das aufrufende Modul geliefert werden.

5.1.3 Validierung von Zertifikaten

Teil einer jeden Signatur- bzw. Siegelprüfung und eine wesentliche Voraussetzung für die Ermittlung des Beweiswertes digital signierter Dokumente ist die Validierung des der digitalen Signatur zugrunde liegenden Nutzer-Zertifikats (vgl. **[eIDAS-VO, Artikel 32 bzw. 40], [SFD 06]**, S. 90). Das Nutzer-Zertifikat bestätigt die Zuordnung des Signatur- bzw. Siegelschlüssel-Inhabers[12] zum Signatur- bzw. Siegelprüfschlüssel (öffentlichen Schlüssel)[13], mit dessen korrespondierenden privaten Signatur- bzw. Siegelschlüssel[14] die digitale Signatur erstellt wurde. Handelt es sich zudem um ein zum Zeitpunkt der Signatur- bzw. Siegelerstellung gültiges qualifiziertes Zertifikat, kann auch der Nachweis der Authentizität eines elektronischen Dokumentes grundsätzlich erbracht werden. Für den Beweiswerterhalt digital signierter Daten ist es daher von entscheidender Bedeutung, dass die Existenz des Nutzerzertifikats und seine Gültigkeit zum Signatur- bzw. Siegelerstellungszeitpunkt nachweisbar bleiben.

Voraussetzung hierfür ist neben der Vorlage des Nutzer-Zertifikats die Prüfung der digitalen Signatur des Vertrauensdiensteanbieters sowie das Hinzuziehen des Zertifikats des Vertrauensdiensteanbieters sowie des Wurzelzertifikats (vgl. **[SFD 06]**, S. 91). Um darüber hinaus ausschließen zu können, dass die digitale Signatur auf einem Zertifikat beruht, das in missbräuchlicher Weise unter dem Namen eines Vertrauensdiensteanbie-

[12] In der **[eIDAS-VO]** auch „Signatur- bzw. Siegel-ersteller“ genannt, in **[VDG]** „verantwortende Person“ genannt.

[13] In **[2014/910/EU, Anhang I]** bzw. **[2014/910/EU, Anhang III]** auch „Signatur- bzw. Siegel- Validierungsdaten“ genannt.

[14] In **[2014/910/EU, Artikel 3 und 26]** bzw. **[2014/910/EU, Artikel 3 und 36]** auch „Signatur- bzw. Siegel-Erstellungsdaten“ genannt.

ters erstellt worden ist, ist zusätzlich eine Gültigkeitsabfrage beim Vertrauensdiensteanbieter erforderlich. Durch diese Abfrage wird nachweislich bestätigt, dass das Zertifikat von ihm ausgestellt wurde und dass es zum Zeitpunkt der Signatur- bzw. Siegelerstellung[15] gültig war.

Der Nutzer/Betreiber des Krypto-Moduls muss sicher stellen, dass das Krypto-Modul alle Vertrauensdiensteanbieter[16] unterstützt, deren Zertifikate für die Erstellung von digitalen Signaturen für zu archivierende Daten von Geschäftsanwendungen mit der Anforderung des Beweiswerterhaltes verwendet werden - also potenziell alle Vertrauensdiensteanbieter, die von Geschäftsanwendungen verwendet werden.

(A5.1-14) Das Krypto-Modul muss eine Funktion, ausgeführt mittels Abruf bei einem Vertrauensdiensteanbieters oder als lokaler Service, anbieten, um das Vorhandensein und den Gültigkeitsstatus von Nutzer-Zertifikaten digitaler Signaturen zum Zeitpunkt der Erstellung der digitalen Signaturen nachweislich verifizieren zu können. Die Validierung muss vollständig bis hin zu einem vertrauenswürdigen Wurzel-Zertifikat der obersten Vertrauensdiensteanbieterinstanz der Zertifizierungskette erfolgen.[17]

(A5.1-15) zur Abfrage der Zertifikatskette können, die Standardprotokolle

- HTTP (vgl. **[RFC1945]** bzw. **[RFC 2616]**) oder
- LDAP (vgl. **[RFC4510]**)

eingesetzt werden. Es wird empfohlen, einen vertrauenswürdigen Kommunikationskanal, z.B. TLS/SSL-Verschlüsselung der Protokolle, mit einer Authentisierung des Vertrauensdiensteanbieters bzw. dessen Verzeichnisdienst zu verwendet.

(A5.1-16) Die Validierung der Zertifikatsgültigkeit muss auf der Basis eines Standardprotokolls erfolgen. Empfohlen wird das Protokoll:

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

  OCSP ist ein vom IETF verabschiedeter Standard (**[RFC6960]**, vormals **[RFC2560]**) für ein Protokoll zur Prüfung des aktuellen Status eines digitalen Zertifikates. Entgegen der Prüfung mit sogenannten Sperrlisten (Certificate Revocation List, CRL) kann hier die Client-Anwendung, z. B. ein Browser, direkt die Gültigkeit eines Zertifikates abfragen. Dazu schickt der Prüfer eine Anfrage (OCSP-Request) an eine autorisierte Auskunftsstelle (OCSP-Responder).

  Dieser OCSP-Responder wird in der Regel vom Aussteller des Zertifikats (Vertrauensdiensteanbieter) betrieben und liefert als Antwort „good“ (d. h. das Zertifikat ist nicht gesperrt), „revoked“ (d. h. Zertifikat ist gesperrt) oder „unknown“ (d. h. der Status konnte nicht ermittelt werden, z. B. weil der Herausgeber des Zertifikats dem OCSP-Responder nicht bekannt ist). Darüber hinaus besteht die Möglichkeit, dass der OCSP-Responder so genannte Positiv-Auskünfte erteilt. Dabei wird der Antwort ein Hash-Wert des Zertifikats mitgegeben, wenn das Zertifikat tatsächlich existiert.

  Die Antwort (OCSP-Response) ist stets vom OCSP-Responder digital signiert und kann somit vom Client auf ihre Echtheit und Unverfälschtheit geprüft werden.

  OCSP erlaubt es auch, in einer Anfrage die Gültigkeit mehrerer Zertifikate abzufragen; der OCSP-Responder liefert dann in seiner Antwort eine Liste mit dem jeweiligen Zertifikatsstatus.[18]

---

[15] Um diese Aussage beim OCSP Protokoll zu erhalten, bedarf es (insbesondere bei nicht-qualifizierten Zertifikaten) ggf. zusätzlich einer Abfrage der CRL.

[16] Hier wird der Begriff Vertrauensdiensteanbieter nicht nur mit qualifizierten sondern auch mit nicht-qualifizierten Zertifikaten in Zusammenhang gebracht.

[17] Vgl. auch **[HK 06]**, Kapitel 4.5

[18] Sofern ein OCSP-Responder auf einer aktuellen Datenbasis (z. B. einer Replikation der Datenbank des Vertrauensdiensteanbieters) arbeitet, gibt er stets den gegenwärtigen Sperrstatus des Zertifikates an. Für die Gültigkeitsprüfung einer digitalen Signatur ist aber vor allem der Status des Zertifikates zum Zeitpunkt der Signatur- bzw. Siegelerstellung relevant. Daher können die OCSP-Antworten bei einem gesperrten Zertifikat auch den Sperrzeitpunkt angeben, so dass sich daraus ermitteln lässt, ob dieses Zertifikat zu einem bestimmten Zeitpunkt noch gültig war. Falls jedoch der Vertrauensdiensteanbieter vorübergehende Sperrungen (Suspendierungen) zulässt, kann man einer positiven OCSP-Antwort nicht entnehmen, ob dieses Zertifikat zwischenzeitlich suspendiert war. Allerdings wird dies nicht als Nachteil von OCSP gewertet, sondern vielmehr die Suspendierung von Signatur- bzw.

- Darüber hinaus kann das SCVP - Server-Based Certificate Validation Protocol **[RFC5055]** eingesetzt werden:

  Das Server-Based Certificate Validation Protocol (SCVP) ist ein Internet-Protokoll, das es Clients ermöglicht, den Aufbau einer X.509-Zertifikatskette und deren Gültigkeitsprüfung auszulagern. Dies wird vor allem bei Clients, die mit dem Kettenaufbau und der Gültigkeitsprüfung aufgrund fehlender Ressourcen oder Protokolle überlastet sind, benötigt. SCVP kann dem Client alle Aufgaben (Aufbau der Kette, Überprüfung auf Widerruf, Validierung) einer vollständigen Zertifikatsprüfung abnehmen.

  Im Gegensatz zu OCSP besteht SCVP aus zwei Nachrichten:

  - Zunächst fragt der Client den Server nach unterstützen Validation Policies, welche bestimmen, für welche Anwendungen der Server konfiguriert wurde.
  - Danach schickt der Client dem Server die Zertifikat-IDs und gibt an, welche Aktionen durchzuführen sind, die der Server signiert beantwortet.

  Bisher wird SCVP allerdings kaum eingesetzt und nur von wenigen Anwendungen unterstützt.

(A5.1-17) Zur Validierung der aktuellen Zertifikatsgültigkeit können ergänzend Sperrlisten (CRL – Certificate Revocation Lists) verwendet werden. Hierbei wird vorausgesetzt, dass Zertifikate nicht vorübergehend gesperrt und wieder freigegeben werden, sondern dass alle Zertifikatssperren endgültig sind.[19]

(A5.1-18) Wenn Sperrlisten für die Zertifikatsgültigkeitsprüfung eingesetzt werden und die Ergebnisse der Sperrlistenabfrage nicht eindeutig sind (oder die Sperrliste nicht abgefragt werden kann), müssen die entsprechenden Fehlermeldungen zusammen mit allen anderen ggf. vorhandenen Prüfinformationen im Prüfbericht oder in dem um diese Prüfinformationen ergänzten Archivdatenobjekt an das aufrufende Modul zurückgegeben werden.

(A5.1-19) Das Krypto-Modul muss über eine Funktion oder Aufruffunktion beim Vertrauensdiensteanbieter zur Validierung von Zertifikatsketten verfügen, um die Integrität von archivierten Zertifikatsketten und von archivierten Objekten nachweisen zu können (vgl. **[RFC5280]** Abschnitt 6 und **[TR-ESOR-M.3]**). Die Liste der vertrauenswürdigen Zertifikate soll konfigurierbar sein.

5.2 Prüfung der technischen Beweisdaten

(A5.2-1) Das Kryptomodul muss in der Lage sein, auf Anforderung beweisrelevante Daten, z.B. Signaturen, Siegel, Zeitstempel, Zertifikate, Sperrlisten, OCSP-Responses etc, auf Basis von **[EN 319 102-1]** sowie auch technische Beweisdaten (Evidence Records) auf Basis von **[RFC4998]** und **[RFC6283]** lokal oder teils lokal im Zusammenspiel mit einem Vertrauensdiensteanbieter zu prüfen oder durch einen Vertrauensdiensteanbieter prüfen zu lassen.

(A5.2-2) Das Kryptomodul muss technische Beweisdaten und beweisrelevante Daten lokal oder teils lokal im Zusammenspiel mit einem Vertrauensdiensteanbieter prüfen oder durch einen Vertrauensdiensteanbieter prüfen zu lassen, wenn im Zuge eines Aufrufs Evidence Records und weitere beweisrelevante Daten übergeben werden

(A5.2-3) Das Krypto-Modul muss das in Anhang **[TR-ESOR-ERS]** spezifizierte Profil „Basis-ERS-Profil“ gemäß **[RFC4998]** für Evidence Records und darüber hinaus auch das in Anhang **[TR-ESOR-ERS]** spezifizierte Profil „Basis-XERS-Profil“ gemäß **[RFC6283]** für Evidence Records unterstützen.

Siegelzertifikaten als problematisch für spätere Validierungen angesehen.

[19] Bei der Verwendung von Sperrlisten ist jedoch zu beachten, dass diese im Gegensatz zu den sekundengenauen OCSP-Antworten nur in bestimmten Intervallen erstellt werden, und damit nicht notwendig aktuell sind. Hinzu kommt, dass aus einer Sperrliste nicht hervorgeht, ob ein Zertifikat jemals ausgestellt wurde, somit nicht gesperrte Zertifikate von gefälschten Zertifikaten auf Grundlage einer Sperrliste allein nicht sicher unterschieden werden können. Hierfür ist die zusätzliche Abfrage einer Positivliste erforderlich.

(A5.2-4) Die Prüfergebnisse müssen entweder in Form eines Prüfberichtes gemäß **[OASIS-VR]** bzw. **[TR-ESOR-VR]** oder als Ergänzung des übergebenen XAIP Containers gemäß **[TR-ESOR-F]** zurückgegeben werden.

5.3 Erzeugung eines Hash-Wertes

Für den Beweiswerterhalt ist die Bildung und Prüfung von Hash-Werten für die Validierung der Unverfälschtheit archivierter Daten erforderlich. Das bedeutet:

(A5.3-1) Das Krypto-Modul muss über Funktionen verfügen, um Hash-Werte für Datenobjekte zu berechnen. Hierbei müssen die Anforderungen an Hash-Verfahren (vgl. Kapitel 4.2) erfüllt werden.

5.4 Zeitstempel

Mit Hilfe eines elektronischen Zeitstempels werden die Uhrzeit und das Datum eines Ereignisses in elektronischer Form dokumentiert. Im Zusammenhang mit digitalen Signaturen (vgl. Kapitel 5.1) gelten die Anforderungen für qualifizierte Zeitstempel gemäß **[eIDAS-VO, Artikel 42]**. Hierfür stehen gemäß der veröffentlichten Vertrauensliste der Europäischen Kommission (siehe Kapitel 3.3) qualifizierte Vertrauensdiensteanbieter zur Verfügung.

Im Zusammenhang mit dem Beweiswerterhalt können qualifizierte Zeitstempel für mehrere Ereignisse relevant sein, unter anderem zur Dokumentation

- des Zeitpunktes der Archivierung eines Datenobjekts,
- eines Zeitpunktes, zu dem das (oder die) archivierte(n) Objekt(e) noch nachweislich integer war(en),
- des Zeitpunktes einer Signatur- bzw. Siegelerstellung oder Signatur- bzw. Siegelprüfung und
- des Zeitpunktes der Erstellung technischer Beweisdaten gemäß des ERS-Standards der IETF **[RFC4998]** sowie darüber hinaus **[RFC6283]**[20] zum Nachweis der Authentizität und Integrität archivierter Daten.

5.4.1 Anforderung eines qualifizierten Zeitstempel

Mit einer Zeitstempel-Anfrage durch das Krypto-Modul wird ein qualifizierter Zeitstempel bei einem qualifizierten Vertrauensdiensteanbieter angefordert.

(A5.4-1) Das Krypto-Modul muss über eine Funktion zur Abfrage eines qualifizierten Zeitstempels verfügen. Falls die Abfrage bei einem qualifizierten Vertrauensdiensteanbieter erfolgt, muss dieser mindestens die Anforderungen nach den **[eIDAS-VO, Artikel 24],** erfüllen, in der Vertrauensliste der Europäischen Kommission gemäß Kapitel 3.3 mit dem Status „**granted**“ gelistet sein und qualifizierte Zeitstempel gemäß **[eIDAS-VO, Artikel 42]** erzeugen.

(A5.4-2) Das Krypto-Modul muss prüfen, ob angeforderte qualifizierte Zeitstempel von einem qualifizierten Vertrauensdiensteanbieter mit dem Status „granted“ zur Erneuerung von digitalen Signaturen gemäß § 15 des Vertrauensdienstegesetzes (siehe auch **[VDG]** und Anlage **[TR-ESOR-M.3]**) die Anforderungen gemäß **[eIDAS-VO, Artikel 42]** erfüllen und mit einer gültigen digitalen Signatur des Ausstellers des Zeitstempels versehen sind, um auch langfristig die Integrität und Authentizität des Zeitstempels nachweisbar zu machen.

(A5.4-3) Das Krypto-Modul muss prüfen, ob angeforderte Zeitstempel die Anforderungen und Spezifikationen des Zeitstempelprotokolls gemäß **[RFC3161], [RFC5816], [RFC5652] und [EN 319 422]** erfüllen; hierbei müssen durch das Krypto-Modul die Einschränkungen auf Algorithmen und Parameter geprüft werden, die gemäß **[ETSI TS 119 312]** und **[SOG-IS]** als sicherheitsgeeignet eingestuft werden (vgl. Kapitel 4.2).

[20] **[RFC4998]** muss, **[RFC6283]** kann unterstützt werden.

(A5.4-4) Das Krypto-Modul muss die Integrität erhaltener qualifizierter Zeitstempel sofort nach deren Eingang und vor der Weiterverarbeitung mathematisch prüfen und die Authentizität bzw. die Vertrauenswürdigkeit gemäß **[eIDAS-VO, Artikel 42]** selbst oder mittels einer Abfrage bei einem Vertrauensdiensteanbieters gemäß **[eIDAS-VO, Artikel 33]** absichern[21] (vgl. Kapitel 5.4.2).

5.4.2 Validierung eines qualifizierten Zeitstempels

(A5.4-5) Qualifizierte Zeitstempel mit digitaler Signatur müssen validiert werden können, d. h. es muss überprüft werden, ob die digitale Signatur des Zeitstempels zum Zeitpunkt der Zeitstempelerstellung gültig war. Diese Funktion entspricht der Validierung einer digitalen Signatur. Anforderungen an diese Funktion wurden bereits in Abschnitt 5.1.2 dargestellt.

HINWEIS:

Die Nutzung nicht-qualifizierter Zeitstempel ist nicht geeignet, den Beweiswert von qualifiziert signierten archivierten Dokumente zu erhalten.

5.4.3 Kanonisierung von XML-Objekten (optional)

Im Kontext dieser Technischen Richtlinie wird davon ausgegangen, dass digital signierte oder zu signierende XML-Daten beim Übergang in die TR-ESOR-Middleware bereits in kanonisierter Form vorliegen.

(5.4-6) Das Krypto-Modul kann über eine Funktion zur Kanonisierung von XML-Objekten verfügen.

(5.4-7) Falls eine Funktion zur Kanonisierung von XML-Objekten implementiert wird, müssen die Anforderungen an Kanonisierungs-Verfahren (vgl. Kapitel 4.4) erfüllt werden.

[21] Eine vollständige Prüfung der Authentizität zeitnah zum Empfang des Zeitstempels ist in der Regel nicht möglich, da die Sperrlisten des Zeitstempeldiensteanbieters dann noch nicht aktualisiert sind.

6. Sicherheitsfunktionen des Krypto-Moduls

Der folgende Abschnitt beschreibt grundlegende Sicherheitsfunktionen, die durch ein zu dieser TR konformes Krypto-Modul umgesetzt werden müssen.

6.1 Verwaltung von kryptographischen Schlüsseln

6.1.1 Private Schlüssel

Private Schlüssel werden vornehmlich für die Erzeugung von digitalen Signaturen benötigt.

Da die Erzeugung von digitalen Signaturen für den unmittelbaren Zweck der Erhaltung des Beweiswertes kryptographisch signierter elektronischer Dokumente nicht erforderlich ist und das Krypto-Modul daher selbst keine digitalen Signaturen erzeugen kann, ist die Betrachtung der Verwaltung privater kryptographischer Schlüssel nicht Gegenstand dieser TR.

6.1.2 Öffentliche Schlüssel / Zertifikate

(A6.1-1) Für öffentliche Schlüssel und Zertifikate sind keine zusätzlichen (Sicherheits-)Funktionen notwendig.

6.2 Schutz des Krypto-Moduls vor Manipulation

Aufgrund des modularen Charakters des Krypto-Moduls (vgl. Abschnitt 3.2) besteht eine potentielle Gefahr des unberechtigten Austausches bzw. der Manipulation des Krypto-Moduls.

(A6.2-1) Der Zugriff auf das Krypto-Modul darf erst nach einer erfolgreichen gegenseitigen Authentifizierung zwischen dem Krypto-Modul und dem Schnittstellenpartner erfolgen. Die Authentifizierung ist für jeden Aufruf zu wiederholen, alternativ kann nach einer erfolgreichen Authentisierung ein sicherer Tunnel aufrechterhalten werden. (vgl. **[ACMPP]**)

(A6.2-2) Das Krypto-Modul soll über eine Funktion zur Prüfung der eigenen Integrität zum Selbstschutz vor Manipulationen verfügen.

(A6.2-3) Das Krypto-Modul muss die Ausführung aller sicherheitsrelevanten Funktionen in aussagekräftiger und nachvollziehbarer Form protokollieren. Sicherheitsrelevante Funktionen sind alle Funktionen, welche die Sicherheit des Moduls, die Sicherheit des kryptographischen Materials, die Korrektheit der Ausführung kryptographischer Funktionen beeinflussen können (wie bspw. Softwareupdates, Schlüsselaustausch oder die Konfiguration des Zufallszahlengenerators).

(A6.2-4) Das Krypto-Modul muss imstande sein, die Ausführung einer Funktion mit einer aussagekräftigen und verständlichen Fehlermeldung abzubrechen, wenn ein unautorisierter Eingriff in die Sicherheitsfunktionen des Moduls erfolgt.

6.3 Konfiguration der kryptographischen Funktionen

Um veränderten kryptographischen Anforderungen begegnen zu können, ist es erforderlich, dass die Konfiguration des Krypto-Moduls durch dazu berechtigte Personen angepasst werden kann.

(A6.3-1) Das Krypto-Modul muss über eine zentrale Funktion zur Konfiguration der kryptographischen Funktionen verfügen, um den Einsatz von ausschließlich gemäß **[ETSI TS 119 312]** und **[SOG-IS]** als sicherheitsgeeignet eingestufte Algorithmen und Parameter steuern zu können. Es wird empfohlen, die Konfiguration durch eine zentrale Konfigurationsdatei zu steuern, die die Gültigkeit der verwendenden Algorith-

men und Schlüssellängen vorgibt. Alternativ kann eine Konfigurationsänderung durch den Austausch des Krypto-Moduls oder Teilen des Krypto-Moduls erfolgen.

(A6.3-2) Die Konfigurationsänderungen sind in jedem Falle in aussagekräftiger und nachvollziehbarer Form zu protokollieren und dauerhaft aufzubewahren.

(A6.3-3) Es wird empfohlen, für die Konfiguration des Krypto-Moduls das Format DSSC (Data Structure for Security Suitabilities of Cryptographic Algorithms, vgl. **[DSSC]**) zu unterstützen, sobald dieses Format durch **[ETSI TS 119 312]** als geeignet empfohlen wird.

(A6.3-4) Die Konfiguration der kryptographischen Funktionen muss über eine geschützte Schnittstelle des Krypto-Moduls erfolgen, die eine unautorisierte Administration des Moduls verhindert.[22]

[22] Da diese Schnittstelle äußerst produktspezifisch sein kann, wird sie in dieser Technischen Richtlinie nicht weiter erörtert. Eine mögliche Ausprägung eines solchen Interfaces wird in **[eCard-3]** beschrieben.