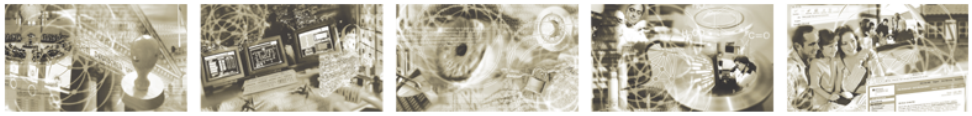
Bundesamt
für Sicherheit in der
Informationstechnik



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
Datum	19.12.14

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 „ArchiSafe-Modul“ (**[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 Erstellung (optional) und Prüfung elektronischer Signaturen, zur Nachprüfung elektronischer Zertifikate und zum Einholen qualifizierter Zeitstempel 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

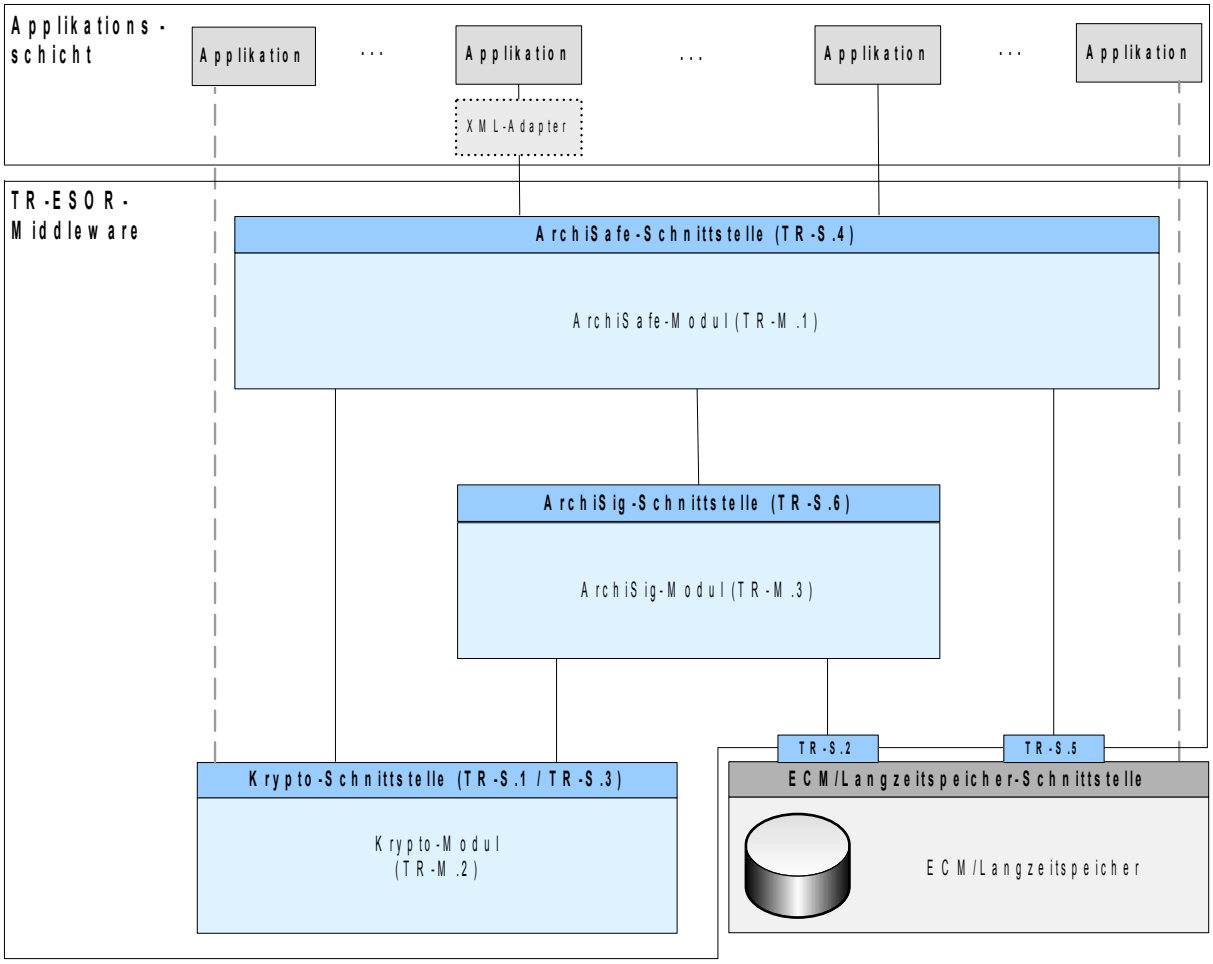


Abbildung 1: Schematische Darstellung der IT-Referenzarchitektur

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 Erzeugen und Validieren von elektronischen Signaturen und den damit zusammenhängenden Zertifikaten, das Berechnen von Hashwerten und das Erzeugen bzw. Abfragen von (qualifizierten) Zeitstempeln.

2. Übersicht

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

2.1 Ziele

Das Krypto-Modul stellt vornehmlich kryptographische Funktionen bereit, die für den langfristigen Beweiswerterhalt elektronisch signierter Daten 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:**
   - Erzeugen elektronischer Signaturen (optional)
   - Verifikation elektronischer Signaturen
   - Validierung elektronischer Zertifikate bis hin zu einem vertrauenswürdigen Wurzelzertifikat
   - Erzeugen von Hash-Werten über vorgelegte elektronische Daten
   - Anforderung qualifizierter Zeitstempel
   - Verifikation (qualifizierter) Zeitstempel
   - Erzeugen (nicht qualifizierter) Zeitstempel (optional)
2. **Unterstützende Funktionen**
   - Integration sicherer Signaturerstellungseinheiten (konform zu den Spezifikationen des eCard-API-Framework **[BSI TR-03112]**).
   - 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 kryptographischen funktionalen Einheiten, die zur Erzeugung und Prüfung elektronischer Signaturen und Zeitstempel im Zusammenhang mit dem Beweiswerterhalt elektronischer Dokumente benötigt werden. Das Krypto-Modul realisiert auf diese Weise wesentliche Teile einer Signaturanwendungskomponente gemäß § 2 Nr. 11 SigG.

Das Krypto-Modul kann darüber hinaus auch weitere Funktionen für die Erstellung oder Prüfung zusätzlicher kryptographischer Sicherungsmittel 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.

Diese grundsätzlichen Realisierungsoptionen entbinden einen Hersteller (Lieferanten) nicht von der Erfüllung von Anforderungen, die aufgrund geltender rechtlicher Vorschriften und Normen an die technische Implementierung von Signaturanwendungskomponenten und (sicheren) Signaturerstellungseinheiten gestellt werden, um gesetzeskonforme fortgeschrittene, bzw. qualifizierte elektronische Signaturen erzeugen und prüfen zu können.[2]

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 Bestätigung durch die Bundesnetzagentur

Die Bundesnetzagentur für Elektrizität, Gas, Telekommunikation, Post und Eisenbahnen (BNetzA) ist die zuständige Behörde gemäß §3 des Signaturgesetzes (SigG). Im Rahmen ihres gesetzlichen Auftrages veröffentlicht sie im Bundesanzeiger und auf den Internetseiten der Bundesnetzagentur Sicherheitsbestätigungen für Produkte für qualifizierte elektronische Signaturen, die von einer nach § 18 SigG anerkannten Stelle erteilt wurden.

Bestätigungen von Produkten, die nicht auf dieser Seite aufgeführt sind, sind durch die Bundesnetzagentur bisher nicht anerkannt und erfüllen somit auch nicht nachweislich die Anforderungen des SigG und der SigV[3].

---

[2] Diese Anforderungen (vgl. auch SigV §15) decken insbesondere die sichere Behandlung von Daten und Schlüsseln vor, während und nach der Verarbeitung ab.

[3] „*Um die bisher bei der Bearbeitung von Produktbestätigungen aufgetretenen zeitlichen Verzögerungen zu minimieren und gleichzeitig die wirtschaftlichen Interessen der betroffenen Unternehmen zu unterstützen, hat sich die Bundesnetzagentur entschlossen, Sicherheitsbestätigungen für Produkte für qualifizierte elektroni-*

Es kann in der Zukunft also der Fall eintreten, dass Signaturen mit den dann verfügbaren zugelassenen Produkten nicht mehr geprüft werden können.

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 elektronischer Signaturen, Zeitstempel und Zertifikate sicher zu stellen.

(A3.3-1) Produkte, die die in Kapitel 2.2 Ziffer 1 und 2 aufgeführten Funktionen des Krypto-Moduls anbieten, sollen eine Bestätigung nach dem Signaturgesetz und der Signaturverordnung aufweisen, um den durch diese Technische Richtlinie bezweckten Beweiswerterhalt zu unterstützen.[4]

sche Signaturen, die von einer nach §18 SigG anerkannten Stelle erteilt wurden, unverzüglich im Bundesanzeiger und auf ihren Internetseiten zu veröffentlichen. Sollten sich im nach hinein Mängel herausstellen, insbesondere dass die Produkte nicht ausreichend geprüft wurden oder diese nicht die an sie gestellten Anforderungen erfüllen, so behält sich die Bundesnetzagentur im Rahmen ihrer Aufsichtsfunktion gemäß Anlage 1 zur Signaturverordnung Abschnitt I Nr. 3 ausdrücklich vor, dazugehörige Bestätigungen für ungültig zu erklären und dies unter Angabe des Zeitpunktes, ab dem diese Maßnahme gilt, ebenfalls im Bundesanzeiger und auf ihren Internetseiten zu veröffentlichen, vgl. Anlage 1 zur Signaturverordnung Abschnitt I Nr. 4.“ Quelle: www.bundesnetzagentur.de Bereich „*Qualifizierte elektronische Signatur*“, Abschnitt „*Bestätigte Produkte*“

[4] Einer nach SigG ausreichenden Herstellererklärung ist weder eine materielle Prüfung der Herstellererklärung noch eine Prüfung der darin aufgeführten Produkte durch die Bundesnetzagentur vorausgegangen. Für den Inhalt der Herstellerklärung und für die Produkte sind deshalb allein die Hersteller verantwortlich. Erst bei einer Bestätigung durch die Bundesnetzagentur ist sicher gestellt, dass es sich tatsächlich um ein Produkt im Sinne des SigG handelt.

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 des Bundesamtes für Sicherheit in der Informationstechnik und werden, was elektronische Signaturen angeht, regelmäßig durch die nach § 3 SigG zuständige Behörde, die BNetzA, im Rahmen der „*Bekanntmachung zur elektronischen Signatur nach dem Signaturgesetz und der Signaturverordnung*“, „*Übersicht über geeignete Algorithmen*“, veröffentlicht. Diese Vorgaben sind für das Krypto-Modul verbindlich und müssen stets den aktuellen Empfehlungen des Bundesamtes für Sicherheit in der Informationstechnik und der Bundesnetzagentur 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.

4.2 Bilden von Hashwerten

Um Veränderungen an elektronischen Daten festzustellen, werden Hash-Funktionen eingesetzt, die unter Verwendung nicht-umkehrbarer mathematischer Funktionen[5] 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.[6]

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

[6] 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.

(A4.2-1) Das Krypto-Modul muss mindestens einen aktuell vom Bundesamt für Sicherheit in der Informationstechnik und von der Bundesnetzagentur als sicherheitsgeeignet eingestuften und veröffentlichten Hash-Algorithmus anbieten (siehe hierzu **[TR 03116]**, **[TR 02102]** und **[ALGCAT]**).

(A4.2-2) Das Krypto-Modul soll darüber hinaus mindestens einen zusätzlichen aktuellen vom Bundesamt für Sicherheit in der Informationstechnik und von der Bundesnetzagentur als sicherheitsgeeignet eingestuften und veröffentlichten Hash-Algorithmus anbieten (siehe hierzu **[TR 03116]**, **[TR 02102]** und **[ALGCAT]**), 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 vom Bundesamt für Sicherheit in der Informationstechnik und der Bundesnetzagentur empfohlenen Hash-Algorithmen und Parameter eingesetzt werden. Das Krypto-Modul muss jedoch alle in der Vergangenheit eingesetzten Hash-Algorithmen gemäß **[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 Erstellen von Signaturen

Für die Erstellung zusätzlicher, über die unmittelbaren Zwecke der Erhaltung des Beweiswertes kryptographisch signierter elektronischer Unterlagen hinausgehender kryptographischer Sicherungsmittel kann das Krypto-Modul imstande sein, selbst elektronische Signaturen zu erzeugen.[7] Die Fähigkeit zur Erzeugung qualifizierter elektronischer Signaturen wird jedoch dann und nur dann benötigt, wenn das Krypto-Modul dazu befähigt und benutzt wird, qualifizierte Zeitstempel zu erzeugen oder die Erzeugung qualifzierter elektronischer Signaturen über die Ziele der TR hinaus anderen Anwendungen oder Systemen zur Verfügung stellen soll.[8]

(A4.3-1) Für Algorithmen im Kontext qualifizierter elektronischer Signaturen muss durch das Krypto-Modul der Algorithmenkatalog „*Geeignete Algorithmen zur Erfüllung der Anforderungen nach §17 Abs. 1 bis 3 SigG vom 22. Mai 2001 in Verbindung mit Anlage 1 Abschnitt I Nr. 2 SigV vom 22. November 2001*“ **[ALGCAT]** in der jeweils aktuellen Fassung eingehalten werden. Für die den Signaturen zugrunde liegende Bildung von Hashwerten müssen die Anforderungen aus Kapitel 4.2 umgesetzt werden.

Gemäß der Signaturverordnung, Anlage 1, Nr. 2 *Algorithmen – Veröffentlichung und Neubestimmung der Eignung* wird die jeweils aktuelle Fassung durch die zuständige Behörde (Bundesnetzagentur) im Bundesanzeiger veröffentlicht und kann grundsätzlich über die Web-Seiten der Bundesnetzagentur (siehe www.bundesnetzagentur.de) abgerufen werden.

(A4.3-2) Für alle anderen Signaturkomponenten im Rahmen des Krypto-Moduls müssen die aktuellen Empfehlungen des Bundesamtes für Sicherheit in der Informationstechnik (siehe **[TR 03116]** und **[TR 02102]**) berücksichtigt werden.

4.4 Kanonisierungsverfahren

Bei der Berechnung von Hashwerten bzw. bei der 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

---

[7] Das ArchiSafe-Modul kann optional eine Eingangssignatur über das zu archivierende Datenobjekt erzeugen. Diese Signatur dient jedoch ausschließlich der Integritätssicherung.

[8] Das ArchiSig-Modul benötigt qualifiziert signierte qualifizierte Zeitstempel zum Aufbau der Hashbäume. Im Regelfall werden derartige Zeitstempel samt Signatur wohl von Zertifizierungsdiensteanbietern angefordert. Es ist aber nicht auszuschließen, dass ein Krypto-Modul selbst in der Lage ist, diese Zeitstempel zu erzeugen.

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.
b. (fortgeschrittene) elektronische Signaturen über Archivdatenobjekte erzeugen kann (Archiveingangssignatur). Die hierfür notwendige Kanonisierung vor der Hashwertbildung muss vom Krypto-Modul durchgeführt werden.
c. in der Lage sein muss, (qualifizierte und fortgeschrittene) Signaturen von zu archivierenden Datenobjekten zu prüfen. 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 Signatur von XML-Inhalten durch das Krypto-Modul ist optional.

(A4.4-2) Die Unterstützung von Kanonisierungsverfahren für die Signaturprüfung 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. 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]**

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 Elektronische Signaturen

Elektronische 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.

Auf Grundlage dieser Verfahren können elektronische Signaturen gesetzeskonform nach §2 SigG erzeugt werden. Dabei wird gemäß §2 Nr. 2 SigG u.a. unterschieden zwischen

- „fortgeschrittenen elektronischen Signaturen“, und
- „qualifizierten elektronischen Signaturen“.

Für beide gelten die grundlegenden Anforderungen, dass

- die Signatur einem Signaturschlüssel-Inhaber zugeordnet sein muss,
- die Signatur die Identifizierung des Inhabers ermöglichen muss,
- die Signatur mit Mitteln erzeugt wird, die der Signaturschlüssel-Inhaber unter seiner alleinigen Kontrolle halten kann, und
- das die Signatur mit den Daten, auf die sie sich bezieht, so verknüpft ist, dass eine nachträgliche Veränderungen der Daten erkannt werden kann.

Für qualifizierte elektronische Signaturen wird gem. § 2 Nr. 3 SigG zusätzlich gefordert, dass sie auf einem zum Zeitpunkt ihrer Erzeugung gültigen qualifizierten Zertifikat beruhen und mit einer sicheren Signaturerstellungseinheit erzeugt werden.

5.1.1 Erzeugung einer elektronischen Signatur

Zur Erzeugung einer elektronischen Signatur wird aus den zu signierenden Daten zunächst ein Hash-Wert gebildet. Aus diesem Hash-Wert wird mit einem Signaturverfahren unter Verwendung des Signaturschlüssels des Schlüssel-Inhabers die Signatur erzeugt.

(A5.1-1) Das Krypto-Modul kann in der Lage sein, elektronische Daten mit fortgeschrittenen elektronischen Signaturen zu versehen.

(A5.1-2) Die Erzeugung qualifizierter elektronischer Signaturen durch ein zu dieser TR konformes Krypto-Modul ist optional. Das Krypto-Modul kann solche Funktionen bereitstellen, um auf Anforderung oder regelbasiert qualifizierte elektronische Signaturen für XML-Daten oder binäre Daten zu erstellen.[9]

(A5.1-3) Elektronische Signaturen für XML-Daten müssen in folgendem Format erzeugt und die grundsätzlichen Empfehlungen in **[Common PKI]** (Part 8) berücksichtigt werden:

[9] Für den Beweiswerterhalt an sich sind keine qualifizierten elektronischen Signaturen notwendig, da für den Beweiswerterhalt keine erneuten Willenserklärungen im juristischen Sinne abzugeben sind. Die für die Signaturerneuerung ggf. notwendigen qualifizierten elektronischen Signaturen (Signatur von qualifizierten Zeitstempeln) werden bei dem Zertifizierungsdiensteanbieter angefordert, der auch den qualifizierten Zeitstempel ausstellt. Nur wenn das Krypto-Modul selbst diese Zeitstempel erzeugt, muss es auch in der Lage sein, qualifizierte elektronische Signaturen zu erzeugen.

- XML Signatur Standard **[XMLDSIG]**, **[RFC3275]**
  Bei Verwendung dieses Formates ist der Einsatz eines Kanonisierungsverfahrens erforderlich.

(A5.1-4) Elektronische Signaturen für binäre Daten sollen in folgendem Format erzeugt und die grundsätzlichen Empfehlungen in **[Common PKI]** (Part 3) berücksichtigt werden:

- Cryptographic Message Syntax (CMS) (**[RFC5652]**, vormals **[RFC3852]**)

(A5.1-5) Die erzeugten Signaturdaten müssen durch das Krypto-Modul an das aufrufende Modul unverändert geliefert werden.

5.1.2 Verifikation elektronischer Signaturen

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

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

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

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

(A5.1-6) Die Verifikation elektronischer Signaturen ist für den Beweiswerterhalt elektronisch signierter Daten unverzichtbar. Ein zu dieser Richtlinie konformes Krypto-Modul muss daher Funktionen zur zuverlässigen Verifikation elektronischer Signaturen zur Verfügung stellen.

(A5.1-7) Die Signatur-Verifikations-Funktion des Krypto-Moduls muss mindestens die im Abschnitt 5.1.1 genannten Signaturdatenformate unterstützen.

(A5.1-8) Die Funktion muss prüfen können, ob das für die Erstellung der Signatur verwendete Nutzer-Zertifikat zum Zeitpunkt der Signaturerstellung gültig war (vgl. Kapitel 5.1.3). Die Gültigkeitsprüfung muss vollständig sein, d. h. die gesamte Zertifikatskette bis hin zu einem vertrauenswürdigen Wurzel-Zertifikat umfassen. Das Krypto-Modul muss bei der Prüfung ermittelte 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.

(A5.1-9) Das Krypto-Modul muss fortgeschrittene und qualifizierte elektronische Signaturen prüfen können.

(A5.1-10) Die Signatur-Prüfergebnisse müssen vom Krypto-Modul in standardisierten Formaten erzeugt werden können. Es wird empfohlen, hierfür den in der eCard-API des BSI spezifizierten Prüfbericht (siehe **[eCard-2]** „VerificationReport“ bzw. **[TR-ESOR-VR]**)) zu nutzen. Die Übergabe eines Prüfberichtes gemäß **[OASIS-VR]** bzw. **[TR-ESOR-VR] muss** vom Krypto-Modul zurückgegeben werden, falls vom Client angefordert.

[10] Die Anfrage beim Aussteller (Zertifizierungsdiensteanbieter), 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 Signaturerstellungszeitpunkt nachweisen zu können (vgl. **[SFD 06]**, S. 96 ff.).

(A5.1-11) Die Signatur-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 Signaturprüfung und eine wesentliche Voraussetzung für die Ermittlung des Beweiswertes elektronisch signierter Dokumente ist die Validierung des der Signatur zugrunde liegenden Nutzer-Zertifikats (vgl. **[SFD 06]**, S. 90). Das Nutzer-Zertifikat bestätigt die Zuordnung des Signaturschlüssel-Inhabers zum Signaturprüfschlüssel (öffentlichen Schlüssel), mit dessen korrespondierenden privaten Signaturschlüssel die Signatur erstellt wurde. Handelt es sich zudem um ein zum Zeitpunkt der Signaturerstellung gültiges qualifiziertes Zertifikat, kann auch der Nachweis der Authentizität eines elektronischen Dokumentes grundsätzlich erbracht werden. Für den Beweiswerterhalt elektronisch signierter Daten ist es daher von entscheidender Bedeutung, dass die Existenz des Nutzerzertifikats und seine Gültigkeit zum Signaturerstellungszeitpunkt nachweisbar bleiben.

Voraussetzung hierfür ist neben der Vorlage des Nutzer-Zertifikats die Prüfung der Signatur des Zertifizierungsdiensteanbieters sowie das Hinzuziehen des Zertifikats des Zertifizierungsdiensteanbieters sowie des Wurzelzertifikats (vgl. **[SFD 06]**, S. 91). Um darüber hinaus ausschließen zu können, dass die Signatur auf einem Zertifikat beruht, das in missbräuchlicher Weise unter dem Namen eines Zertifizierungsdiensteanbieters erstellt worden ist, ist zusätzlich eine Gültigkeitsabfrage beim Zertifizierungsdiensteanbieter erforderlich. Durch diese Abfrage wird nachweislich bestätigt, dass das Zertifikat von ihm ausgestellt wurde und dass es zum Zeitpunkt der Signaturerstellung[11] gültig war.

Der Nutzer/Betreiber des Krypto-Moduls muss sicher stellen, dass das Krypto-Modul alle Zertifizierungsdiensteanbieter[12] unterstützt, deren Zertifikate für die Erstellung von elektronischen Signaturen für zu archivierende Daten von Geschäftsanwendungen verwendet werden. mit der Anforderung des Beweiswerterhaltes verwendet werden - also potenziell alle Zertifizierungsdiensteanbieter, die von Geschäftsanwendungen verwendet werden.

(A5.1-12) Das Krypto-Modul muss eine Funktion anbieten, um das Vorhandensein und den Gültigkeitsstatus von Nutzer-Zertifikaten elektronischer Signaturen zum Zeitpunkt der Erstellung der Signaturen nachweislich verifizieren zu können. Die Verifikation muss vollständig bis hin zu einem vertrauenswürdigen Wurzel-Zertifikat der obersten Zertifizierungsinstanz der Zertifizierungskette erfolgen.[13]

(A5.1-13) 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 Zertifizierungsdiensteanbieters bzw. dessen Verzeichnisdienst zu verwendet.

(A5.1-14) Die Verifikation 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 (Zertifizierungsdiensteanbieter) betrieben und liefert als Antwort „good“ (d. h. das Zertifikat ist nicht

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

[12] Hier wird der Begriff Zertifizierungsdiensteanbieter nicht nur – wie im SigG – mit qualifizierten sondern auch mit nicht-qualifizierten Zertifikaten in Zusammenhang gebracht.

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

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.[14]

- 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.

(A5.1-15) Zur Verifikation 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.[15]

(A5.1-16) 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.

(A5.1-17) Das Krypto-Modul muss über eine Funktion 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.

---

[14] Sofern ein OCSP-Responder auf einer aktuellen Datenbasis (z. B. einer Replikation der Datenbank der Zertifizierungsstelle) arbeitet, gibt er stets den gegenwärtigen Sperrstatus des Zertifikates an. Für die Gültigkeitsprüfung einer elektronischen Signatur ist aber vor allem der Status des Zertifikates zum Zeitpunkt der Signaturerstellung 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 die Zertifizierungsstelle vorübergehende Sperrungen (Suspendierungen) zulässt (was bei qualifizierten Zertifikaten nicht unterstützt wird), 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 Signaturzertifikaten als problematisch für spätere Verifikationen angesehen.

[15] 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.

5.2 Prüfung der technischen Beweisdaten

(A5.1-18) Das Kryptomodul muss in der Lage sein, auf Anforderung beweisrelevante Daten, z.B. Signaturen, Zeitstempel, Zertifikate, Sperrlisten, OCSP-Responses etc, sowie auch technische Beweisdaten (Evidence Records) auf Basis von **[RFC4998]** und **[RFC6283]** zu prüfen.

(A5.1-19) Das Kryptomodul muss technische Beweisdaten und beweisrelevante Daten prüfen, wenn im Zuge eines Aufrufs Evidence Records und weitere beweisrelevante Daten übergeben werden

(A5.1-20) Das Krypto-Modul muss das in Anhang **[TR-ESOR-ERS]** spezifizierte Profil „Basis-ERS-Profil“ gemäß **[RFC4998]** für Evidence Records und darüberhinaus auch das in Anhang **[TR-ESOR-ERS]** spezifizierte Profil „Basis-XERS-Profil“ gemäß **[RFC6283]** für Evidence Records unterstützen.

(A5.1-21) Die Prüfergebnisse müssen entweder in Form eines Prüfberichtes gemäß **[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 Verifikation der Unverfälschtheit archivierter Daten erforderlich. Das bedeutet:

(A5.2-1) 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 elektronischen Signaturen (vgl. Kapitel 5.1) gelten die Anforderungen für qualifizierte Zeitstempel gemäß §2 Nr.14 SigG und §15 Abs. 3 SigV. Hierfür stehen durch die Bundesnetzagentur akkreditierte Zertifizierungsdiensteanbieter 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 Signaturerstellung oder Signaturprüfung und
- des Zeitpunktes der Erstellung technischer Beweisdaten gemäß des ERS-Standards der IETF **[RFC4998]** sowie darüber hinaus **[RFC6283]**[16] 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 angefordert, z. B. bei einem Zertifizierungsdiensteanbieter oder einem entsprechend geprüften und bestätigten Hardware-Modul.

(A5.3-1) Das Krypto-Modul muss über eine Funktion zur Abfrage eines qualifizierten Zeitstempels verfügen. Falls die Abfrage bei einem Zertifizierungsdiensteanbieter erfolgt, muss dieser mindestens die Anforderungen nach den §§ 4 bis 14 sowie § 17 oder § 23 SigG und der sich darauf beziehenden Vorschriften nach § 24 SigV erfüllen. Alternativ kann ein entsprechend von der Bundesnetzagentur geprüftes und bestätigtes Gerät eingesetzt werden, das dann durch das Krypto-Modul angesteuert wird.[17]

---

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

[17] Der Betreiber des Krypto-Moduls muss in diesem Fall selbst ein Zertifizierungsdiensteanbieter sein.

(A5.3-2) Das Krypto-Modul muss prüfen, ob angeforderte qualifizierte Zeitstempel zur Erneuerung von Signaturen gemäß § 17 SigV (siehe auch Anlage **[TR-ESOR-M.3]**) mit einer qualifizierten elektronischen Signatur des Ausstellers des Zeitstempels versehen sind, um auch langfristig die Integrität und Authentizität des Zeitstempels nachweisbar zu machen.

(A5.3-3) Das Krypto-Modul muss prüfen, ob angeforderte Zeitstempel die Anforderungen und Spezifikationen des Zeitstempelprotokolls gemäß **[RFC3161]**, (**[RFC5652]**, vormals **[RFC3852]**) und **[ETSI-TSP]** erfüllen; hierbei müssen durch das Krypto-Modul die Einschränkungen auf Algorithmen und Parameter geprüft werden, die durch das Bundesamt für Sicherheit in der Informationstechnik und die Bundesnetzagentur als sicherheitsgeeignet eingestuft werden (vgl. Abschnitt 4.2).

(A5.3-4) 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 absichern[18] (vgl. 5.4.2).

5.4.2 Verifikation eines qualifizierten Zeitstempels

(A5.3-5) Qualifizierte Zeitstempel mit (qualifizierter) elektronischer Signatur müssen verifiziert werden können, d. h. es muss überprüft werden, ob die Signatur des Zeitstempels zum Zeitpunkt der Zeitstempelerstellung gültig war. Diese Funktion entspricht der Verifikation einer Signatur. Anforderungen an diese Funktion wurden bereits in Abschnitt 5.1.2 dargestellt.

5.4.3 Erzeugung eines nicht-qualifizierten Zeitstempels (optional)

(A5.3-6) Das Krypto-Modul kann zusätzlich über eine Funktion zur Erstellung von nicht-qualifizierten Zeitstempeln verfügen, die nicht die Anforderungen des SigG und der SigV an qualifizierte Zeitstempel erfüllen.

HINWEIS: Die ausschließliche Nutzung nicht-qualifizierter Zeitstempel oder nicht qualifiziert signierter Zeitstempel ist nicht geeignet, den Beweiswert von qualifiziert signierten archivierten Daten zu erhalten.

5.4.4 Kanonisierung von XML-Objekten (optional)

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

(A5.3-7) Das Krypto-Modul kann über eine Funktion zur Kanonisierung von XML-Objekten verfügen.

(A5.3-8) Falls eine Funktion zur Kanonisierung von XML-Objekten implementiert wird, müssen die Anforderungen an Kanonisierungs-Verfahren (vgl. Kapitel 4.4) erfüllt werden.

[18] 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 Signaturen benötigt. Sollte das Krypto-Modul keine Funktion zur Erstellung von Signaturen implementiert haben, sind die Anforderungen dieses Abschnitts nicht relevant.

(A6.1-1) Private Schlüssel für die Erstellung von Signaturen (Signaturschlüssel) können in dem Krypto-Modul hinterlegt sein. Falls mehrere Schlüssel hinterlegt sind, muss das Krypto-Modul über eine Funktion zur Auswahl des zu verwendenden Schlüssels verfügen.

(A6.1-2) Im Krypto-Modul hinterlegte private Schlüssel müssen vor unberechtigtem Zugriff geschützt werden. Der Zugriff auf private Schlüssel darf nur nach erfolgreicher Authentifizierung des jeweiligen Schlüsselinhabers erfolgen.

(A6.1-3) Der private Schlüssel soll in einem als Hardware-Lösung implementierten Schutzsystem gespeichert werden, z.B. Hardware Security Module (HSM), USB-Tokens oder einer Smart-Card.

(A6.1-4) Bei Ablage auf einem Dateisystem müssen private Schlüssel in einem Datenformat hinterlegt werden, das einen ausreichenden Schutz für die privaten Schlüssel bietet. Empfohlen wird das Format Public Key Cryptography Standard #12 **[PKCS#12]** für die kryptographisch geschützte Ablage von Schlüssen und X.509v3-Zertifikaten **[RFC5280]**.

(A6.1-5) Das Krypto-Modul kann Funktionen zur Schlüsselverwaltung, d. h. zum Erzeugen, Speichern, Löschen und Archivieren von Schlüsselpaaren anbieten.

6.1.2 Öffentliche Schlüssel / Zertifikate

(A6.1-6) 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. Kapitel 3.2 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 aufrecht erhalten 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 soll imstande sein, die Ausführung einer Funktion mit einer aussagekräftigen und verständlichen Fehlermeldung abzubrechen, wenn ein unautorisierter Eingriff in die Sicherheitsfunktionen des Moduls erfolgt.

(A6.2-5) Das Krypto-Modul muss über eine Funktion zum Schutz des Schlüsselspeichers verfügen, wenn es Funktionen zur Schlüsselverwaltung, d. h. zum Erzeugen, Speichern, Löschen und Archivieren von Schlüsselpaaren, anbietet. Diese Anforderung kann durch das oben genannte ((A6.1-3) und (A6.1-4)), möglichst als Hardware-Lösung implementierte Schutzsystem erfüllt werden.

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 durch das Bundesamt für Sicherheit in der Informationstechnik und die Bundesnetzagentur 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 Algorithmen und Schlüssellängen vorgibt. Alternativ kann eine Konfigurationsänderung durch den Austausch des Krypto-Moduls oder Teilen des Krypto-Moduls erfolgen.

Die Konfigurationsänderungen sind in jedem Falle in aussagekräftiger und nachvollziehbarer Form zu protokollieren und dauerhaft aufzubewahren.

(A6.3-2) 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 der Standardisierungsprozess der IETF abgeschlossen ist und dieses Format durch die Bundesnetzagentur als geeignet empfohlen wird.

(A6.3-3) Die Konfiguration der kryptographischen Funktionen muss über eine geschützte Schnittstelle des Krypto-Moduls erfolgen, die eine unautorisierte Administration des Moduls verhindert.[19]

[19] 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.