Bundesamt
für Sicherheit in der
Informationstechnik

BSI Technische Richtlinie 03125
Beweiswerterhaltung kryptographisch signierter Dokumente

Bezeichnung	TR-ESOR – Beweiswerterhaltung kryptographisch signierter Dokumente
Kürzel	BSI TR-ESOR - 03125
Version	1.2
Datum	19.12.2014

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

Vorwort des Präsidenten

Papier ist geduldig, heißt es. Und darüber hinaus hat es viele weitere, ganz handfeste, positive Eigenschaften. Doch Papier ist nicht mehr en vogue: Unternehmen, die öffentliche Verwaltung und die Justiz sind schon seit längerem bestrebt, ihre Geschäftsprozesse möglichst weitgehend in elektronischer Form durchzuführen und die zugehörigen Unterlagen auch in digitaler Form aufzubewahren. Das Substituieren der bisher üblichen, gar sprichwörtlichen Papierberge durch elektronische Dokumente beeinflusst dabei nicht nur die Kommunikation und die unmittelbare Vorgangsbearbeitung oder Geschäftsabwicklung, sondern hat ohne Zweifel für die Archivierung elektronischer Dokumente weitreichende Folgen.

Papierdokumente verfügen aufgrund ihrer Körperlichkeit über Eigenschaften, die elektronische Dokumente per se nicht aufweisen. Aus sich heraus können elektronische Dokumente weder wahrgenommen oder gelesen werden, noch Anhaltspunkte für Integrität und Authentizität aufweisen. Diese Eigenschaften zum Beweiswert aber sind entscheidend. Sie müssen bei der Migration von papiergetragenen zu elektronischen Datenformaten zwingend bedacht werden. Insbesondere für den längerfristigen Beweiswerterhalt signierter elektronischer Dokumente ist neben der Erhaltung der Lesbarkeit und Vollständigkeit auch der Nachweis der Integrität und Authentizität unabdingbar und muss durch technische und organisatorische Maßnahmen hergestellt und dauerhaft erhalten werden – mindestens für die Dauer gesetzlich vorgeschriebener Aufbewahrungsfristen.

Tatsächlich existiert bereits eine Reihe von nationalen und internationalen Anforderungskatalogen oder Standards für elektronische Vorgangs- oder Aufbewahrungssysteme. So haben etwa die amerikanische Luft- und Raumfahrtbehörde NASA, das europäische DLM-Forum oder die IETF-LTANS-Arbeitsgruppe Anstrengungen in dieser Sache unternommen. In Deutschland sind aus dem durch das BMWi geförderten Verbundprojekt „ArchiSig“ umfangreiche Ausführungen zu den rechtlichen Anforderungen an die Aufbewahrung elektronisch signierter Dokumente hervorgegangen. Diese Regelungen für die Aufbewahrung gelten jedoch in den meisten Fällen nur für bestimmte Branchen oder beziehen sich auf einzelne konkrete Fragestellungen und spezifizieren in der Regel wenig detaillierte Anforderungen für den Beweiswerterhalt elektronisch signierter Dokumente insgesamt.

Die mit diesem Dokument vorgelegte „Technische Richtlinie zur Beweiswerterhaltung kryptographisch signierter Dokumente (TR-ESOR)“ spezifiziert auf der Grundlage bestehender rechtlicher Normen und technischer Standards sowie nationaler und internationaler Erfahrungen in einem modular aufgebauten Gesamtkonzept übergreifende Anforderungen und Kriterien für die langfristige Be-

weiswerterhaltung kryptographisch signierter Dokumente im Kontext ihrer Aufbewahrung und schreibt diese fort.

Ziel der TR-ESOR ist es, die Auswahl und den adäquaten Einsatz geeigneter Sicherungsmittel für die Beweiswerterhaltung signierter elektronischer Dokumente nachhaltig zu unterstützen. Auf der Basis einer hersteller- und produktunabhängigen Referenzarchitektur werden funktionale und sicherheitstechnische Mindestanforderungen definiert, gemäß denen Systeme, Komponenten, Schnittstellen und deren Zusammenspiel für den Beweiswerterhalt aufgebaut, überprüft und in Betrieb genommen werden können.

Denn Papier ist nicht nur geduldig, sondern vor allem auch verlässlich. Wir können heute noch problemlos Jahrhunderte alte Papierschriften entziffern. Eine solche Dauerhaftigkeit ist bekanntermaßen mit elektronisch lesbaren Datenträgern nicht zu erreichen. Sechs Jahrhunderte lang war Papier der wichtigste Datenträger, besser: Wissensträger. Jenseits aller gesetzlichen Vorgaben ist es daher auch unser Auftrag, das digitale Wissen unserer Zeit für künftige Generationen nutzbar zu machen.

Bonn, im Dezember 2014

Michael Hange , Präsident des BSI

Inhaltsverzeichnis

Verzeichnis der Abbildungen

1. Vorbemerkungen

Kapitel 1 enthält Angaben zur Bezeichnung dieser Technischen Richtlinie (TR), zur fachlich zuständigen Stelle, zur Versionsverwaltung, zum Änderungsdienst und der Fortschreibung der TR.

1.1 Titel

Diese TR trägt den Titel
"Technische Richtlinie zur Beweiswerterhaltung kryptographisch signierter Dokumente (ESOR)".

1.2 Kennzeichnung

Diese TR wird gekennzeichnet mit „BSI TR-03125".

1.3 Fachlich zuständige Stelle

Fachlich zuständig für die Formulierung und Betreuung dieser TR ist das Bundesamt für Sicherheit in der Informationstechnik (BSI).

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

1.4 Versionsverwaltung

Diese TR besteht aus diesem Dokument und weiteren separaten normativen Anhängen (siehe hierzu Kapitel 10). Darüber hinaus wird es weitere Anhänge mit den entsprechenden Prüfspezifikationen für die notwendigen Konformitätsprüfungen geben.
Die zur Zeit gültigen Teile dieser TR sind:

Teil der TR	Version	Datum (JJJJ-MM-TT)	Bemerkung
Hauptdokument (dieses Dokument)	1.2	2014-12-19	
Anlage TR-ESOR-M.1 ArchiSafe-Modul	1.2	2014-12-19	
Anlage TR-ESOR-M.2 Krypto-Modul	1.2	2014-12-19	
Anlage TR-ESOR-M.3 ArchiSig-Modul	1.2	2014-12-19	
Anlage TR-ESOR-S Definition der Schnittstellen der Referenzarchitektur	1.2	2014-12-19	
Anlage TR-ESOR-E Konkretisierung der Schnittstellen auf Basis des eCard-API-Frameworks	1.2	2014-12-19	
Anlage TR-ESOR-F Formate	1.2	2014-12-19	

Teil der TR	Version	Datum (JJJJ-MM-TT)	Bemerkung
Anlage TR-ESOR-B Profilierung für Bundesbehörden	1.2	2014-12-19	
Anlage TR-ESOR-C.1 Conformity Test Specification (Level 1 - Functional Conformity)	1.2	2014-12-19	
Anlage TR-ESOR-C.2 Conformity Test Specification (Level 2 - Technical Conformity)	1.2	2014-12-19	
Anlage TR-ESOR-C.3 Conformity Test Specification (Level 3 - Conformity with the German Federal Agency Profiling)	1.2	2014-12-19	
Anlage TR-ESOR-ERS Profilierung der Evidence Records gemäß RFC 4998 und RFC 6283	1.2	2014-12-19	
Anlage TR-ESOR-VR Verification Reports for Selected Data Structures	1.2	2014-12-19	

1.5 Änderungsdienst / Fortschreibung

Die TR und ihre normativen Anhänge unterliegen fortwährender weiterer Verbesserung und Anpassung an neue Anforderungen. Die Fortführung muss geordnet verlaufen, d. h. dass abgestimmte Versionen der TR in einem formalen Akt freigegeben werden.

Formal freigegebene Versionen oder Patches werden auf der Webseite des BSI veröffentlicht. Die Veröffentlichung erfolgt geregelt.

1.6 Veröffentlichung

Die gültigen Versionen werden auf den TR-ESOR Webseiten des BSI zum Download angeboten.

In einem auf den TR-ESOR Webseiten des BSI verfügbaren Änderungsverzeichnis werden die Versionen mit Beschreibung der Erweiterung oder Änderung und des Datums geführt.

1.7 Konventionen

Die in dieser Technischen Richtlinie spezifizierten Anforderungen und Empfehlungen an Systeme zur Beweiswerterhaltung kryptographisch signierter Dokumente werden eindeutig gekennzeichnet. Hierbei gilt:

- Der Anforderung wird ihre eindeutige Kennung der Form **(Ax.y-z)** vorangestellt, wobei
  x das jeweilige Hauptkapitel
  y das jeweilige Unterkapitel und
  z eine fortlaufende Nummer innerhalb des Unterkapitels ist.

Jede Anforderung wird in Anlehnung an **[RFC2119]** explizit als verpflichtend, empfohlen oder als optional spezifiziert.

Verpflichtende Anforderungen (MUSS-Anforderungen), sind Anforderungen, deren Umsetzung zwingend gefordert wird. Sie sind im Text mit den Worten muss (müssen) / ist (sind) / darf (dürfen) nur / darf (dürfen) nicht, ausgezeichnet.

Empfohlene Anforderungen (SOLL-Anforderungen) sollten umgesetzt werden. Sie sind im Text mit den Worten soll (sollen) / empfohlen ausgezeichnet.

Optionale Anforderungen (KANN-Anforderungen) können umgesetzt werden. Sie sind im Text mit den Worten kann (können) / darf (dürfen) ausgezeichnet.

In manchen Fällen ist es unumgänglich, leicht modifizierte Varianten der oben genannten Wörter zu benutzen. Der Sinn von MUSS, SOLL und KANN wird dabei jedoch immer klar und die obigen Definitionen gelten entsprechend. Weitere Erläuterungen zu diesen kennzeichnenden Begriffen sind in Kapitel 9.3 zu finden.

Unter dem in dieser TR in der Regel verwendeten Begriff „Dokumente“ werden, sofern nicht ausdrücklich in anderer Bedeutung gebraucht, Daten und Dokumente subsumiert.

2. Anwendungsbereich

Vornehmlicher Anwendungsbereich der vorliegenden Technischen Richtlinie sind die Bundesbehörden im Rahmen der gesetzlichen Aufbewahrungspflichten. Darüber hinaus besitzt die Technische Richtlinie empfehlenden Charakter.

3. Allgemeines und Übersicht

In diesem Kapitel werden der Aufbau und die Inhalte der Technischen Richtlinie sowie die grundsätzlichen Ziele und Herausforderungen an eine langfristige Beweiswerterhaltung im Kontext der Aufbewahrung elektronischer Dokumente erläutert.

3.1 Aufbau und Inhalte der Technischen Richtlinie

Die Technische Richtlinie besteht aus diesem Hauptdokument sowie einer Reihe ergänzender Anlagen, in denen einzelne Aspekte näher spezifiziert und erläutert werden.

In diesem Hauptdokument werden die rechtlichen Rahmenbedingungen und Normen, die grundsätzlichen Ziele und Anforderungen, sowie die abzubildenden Prozesse und Funktionen beschrieben. Daraus abgeleitet werden Anforderungen an das Einrichten sowie die Systemtechnik an sich und eine empfohlene Systemarchitektur (Referenzarchitektur). Ergänzend folgen die Sicherheitsziele und Sicherheitsmaßnahmen für ein solches System. Der Umfang und die Inhalte einer Konformitätsprüfung technischer Produktlösungen gegen die in dieser Richtlinie definierten Anforderungen bilden den Abschluss.

Darüber hinaus enthält dieses Hauptdokument in Kapitel 10 eine Übersicht über die mit diesem Dokument veröffentlichten und geplanten Anlagen. In diesen ergänzenden Anlagen werden die in diesem Hauptdokument definierten Anforderungen auf der Grundlage einer in Kapitel 6.5 beschriebenen plattform- und produktneutralen, funktionalen Referenzarchitektur spezifiziert und erläutert.

Die Beschreibung der Ziele und Anforderungen ist strikt produkt- und herstellerneutral und orientiert sich allein an den entsprechenden Anforderungen zur gesetzlich geregelten Beweiswerterhaltung bei kryptographisch signierten elektronischen Unterlagen.

3.2 Untersuchungsgegenstand und Begriffsdefinitionen

Die dauerhafte und unveränderbare Aufbewahrung (Speicherung) von elektronischen Dokumenten und anderen Daten wird im informationstechnischen Sprachgebrauch allgemein als „**elektronische Archivierung**“ bezeichnet. Der mit dem Begriff „dauerhaft“ bezeichnete Zeithorizont ist dabei aus informationstechnischer Sicht die Umschreibung eines nicht näher fixierten Zeitraums, in dem wesentliche, im Allgemeinen aber kaum vorhersehbare technische oder technologische Veränderungen eintreten können, die u. U. dazu führen, dass die informationstechnischen Systeme, mit denen Dokumente ursprünglich erfasst, erstellt und gespeichert wurden, nicht mehr zur Verfügung stehen. Hierfür wird im deutschen Sprachgebrauch mitunter auch der Begriff der „**elektronischen (digitalen) Langzeitspeicherung**“ verwendet, um den Unterschied zur kurzzeitigen „**lebenden Schriftgutablage**“ bzw. zum Backup hervorzuheben.[1]

Aus rechtlicher Sicht ist der Begriff der **„Archivierung“** in Deutschland durch die Archivgesetze des Bundes und der Länder konkretisiert und belegt und daher von der zeitlich beschränkten Aufbewahrung zu unterscheiden. Archivierung im juristisch korrekten Sinne betrifft allein Unterlagen der öffentlichen Verwaltung und bezieht sich darauf, dass Unterlagen einer Behörde, sobald sie für die Zwecke der Behörde nicht mehr benötigt werden, ausgesondert und durch eine zuständige staatliche Einrichtung (Bundesarchiv) auf unbegrenzte Zeit verwahrt werden sollen (vgl. §§ 1 und 2 BArchG).

Behördliche elektronische Unterlagen unterliegen damit den rechtlich geregelten Archivregelungen gemäß BArchG. Das heißt für Bundesbehörden, dass nach Ablauf der Aufbewahrungsfristen eine gesetzlich festgelegte Anbietungspflicht an das Bundesarchiv besteht. Die damit zusammenhängenden Fragestellungen und Anforderungen sind jedoch nicht Gegenstand dieser Technischen Richtlinie.

Ebenso wenig formuliert diese Technische Richtlinie generelle Anforderungen an die Aufbewahrung und Speicherung beliebiger elektronischer Dokumente.

[1] Die Begriffsdefinitionen „lebende Schriftgutablage“, „Langzeitspeicher“ und „Archivspeicher“ finden sich im eGovernment-Masterplan 2010 des Landes Niedersachsen auf Seite 26; siehe http://www.niedersachsen.de/download/45825

Gegenstand und Ziel dieser Technischen Richtlinie ist die **Beweiswerterhaltung von kryptographisch signierten Dokumenten** im Kontext ihrer Aufbewahrung. Erwähnenswert ist hier, dass die Notwendigkeit einer solchen Beweiswerterhaltung nicht per se gegeben ist sondern fachlichen Anforderungen entsprechen soll.

Zum Begriff der „Beweiswerterhaltung“ ist anzumerken, dass jedes elektronische Dokument als Beweismittel gemäß § 286 ZPO im Rahmen der freien Beweiswürdigung fungieren kann. Davon zu unterscheiden ist der erleichterte Anscheinsbeweis nach § 371a ZPO. Um diesen zu führen, sind nach der heutigen Rechtslage ggf. besondere Maßnahmen (wie z.B. eine Neusignierung nach § 17 SigV) erforderlich. Werden diese Maßnahmen unterlassen, verliert ein Dokument dadurch nicht jeglichen Beweiswert, sondern es entfällt lediglich die besondere Beweiskraft nach § 371a ZPO. Der Begriff „Beweiswerterhalt“ in dieser Richtlinie ist in diesem Sinne zu verstehen und zu interpretieren.

Elektronische Signaturen im Sinne der deutschen Signaturgesetzgebung und der Richtlinie 1999/93/EG des Europäischen Parlaments und Rates über gemeinschaftliche Rahmenbedingungen für elektronische Signaturen dienen dem Nachweis der Authentizität und Integrität elektronischer Dokumente und Daten. Dabei kann allerdings der Beweiswert dieser Signaturen im Laufe der Zeit abnehmen, z.B. weil die Sicherheitseignung der verwendeten kryptographischen Verfahren nicht mehr gegeben ist. Zur Erhaltung des vollen Beweiswerts und der Möglichkeit der erleichterten Beweisführung (s.o.) sind daher neben der unveränderbaren Aufbewahrung der Dokumente und Signaturen in vielen Fällen noch weitere Maßnahmen erforderlich. Diese Maßnahmen werden in dieser Technischen Richtlinie definiert und spezifiziert.

Die Technische Richtlinie geht dabei von der Nutzung stabiler Datenformate aus, die für die angedachten Aufbewahrungszeiträume angemessen sind; die Transformation kryptographisch signierter Dokumente in andere Datenformate wird hier nicht betrachtet.[2]

Eine geeignete IT-Komponente zur Sicherung des Beweiswerts wird in dieser Technischen Richtlinie als „**TR-ESOR-Middleware**“ bezeichnet. Eine derartige Komponente umfasst weder die Fachanwendungen noch die eigentlichen Speicher- bzw. Archivierungssysteme, sondern bündelt die notwendigen Funktionen zur kryptographischen Beweiswerterhaltung. Eine zu dieser Richtlinie konforme TR-ESOR-Middleware ist imstande, den beweisrechtlichen Wert signierter elektronischer Daten oder Dokumente über die gesamte Dauer des Aufbewahrungszeitraumes zu erhalten.

Mit dem Begriff der „**kryptographisch signierten Dokumente**“ sind in dieser TR neben den qualifiziert signierten Dokumenten (im Sinne der deutschen Signaturgesetzgebung) auch Dokumente mit einer fortgeschrittenen Signatur erfasst, wie sie oft in der internen Kommunikation von Behörden entstehen. Nicht gemeint sind hier Dokumente mit einfachen Signaturen basierend auf anderen (nichtkryptographischen) Verfahren.

Weitere wichtige Begriffsdefinitionen wie z.B. Daten, Dokument, Metadaten etc. sind dem Kapitel 12 zu entnehmen.

3.3 Übersicht

Das Ziel einer auch auf lange Zeiträume angelegten Beweiswerterhaltung kryptographisch signierter Unterlagen ist, die für die Dauer der Aufbewahrung mögliche Nachweisführung, dass bestimmte digitale Dokumente und Daten (Inhaltsdaten) sowie zugehörige Metainformationen zu einem nachweisbaren Zeitpunkt vorgelegen haben und seitdem nicht verändert wurden (Integrität). Soweit erforderlich, sind zusätzlich nachprüfbare Nachweise über den Aussteller (Authentizität) der aufbewahrten Dokumente und Daten entsprechend den rechtlichen Anforderungen vorzuhalten.

Das Ziel und die Herausforderung eines Gesamtsystems zur Speicherung und zum Beweiswerterhalt kryptographisch signierter Unterlagen ist es, für die digitalen Inhalte und die beweisrelevanten Zusatzdaten

- die Verfügbarkeit und Lesbarkeit,
- die Integrität (Unversehrtheit),
- die Authentizität (daraus folgt auch die Nichtabstreitbarkeit) und
- Datenschutz, Datensicherheit und Vertraulichkeit

[2] Mit der Transformation solcher Dokumente befasste sich das TransiDoc Projekt, siehe http://www.transidoc.de

für lange Zeiträume zu gewährleisten.

Ein solches Gesamtsystem umfasst deshalb auch diejenigen Elemente (Komponenten) und Prozesse, die zur Erzeugung, Speicherung, Indexierung, Suche, Verwaltung, Lesbarmachung und langfristigen und unveränderlichen Aufbewahrung von zu speichernden Daten eingesetzt werden, auch wenn diese Elemente (Komponenten) und Prozesse nicht in dieser TR beschrieben werden. Dazu gehören i. d. R.

- die zur Archivierung (Langzeitspeicherung) eingesetzte IT-Infrastruktur (siehe unten)
- die IT-Anwendungen, die Daten und Dokumente archivieren bzw. mit archivierten Daten arbeiten.

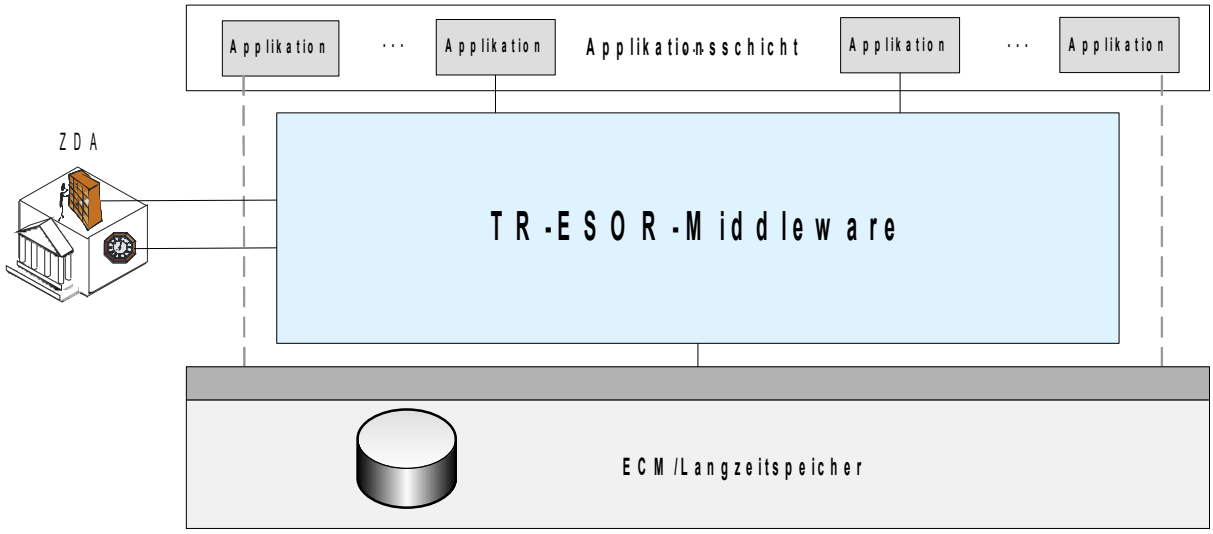


Abbildung 1: Typische Infrastruktur zur beweiswerterhaltenden Langzeitarchivierung

Die zur Archivierung eingesetzte IT-Infrastruktur besteht typischerweise, wie auch in Abbildung 1 dargestellt, aus

- einem Enterprise Content Management (ECM)-/Langzeitspeichersystem, das die unterschiedlichen zur Archivierung eingesetzten Speichermedien umfasst und verwaltet, und den zuverlässigen und sicheren Zugriff auf die Speichermedien für die Ablage, den Abruf oder die Löschung archivierter Dokumente und Daten gewährleistet,
- der Middleware inklusive der darin enthaltenen kryptographischen Komponente, die den Erhalt des beweisrechtlichen Wertes der archivierten Unterlagen (Dokumente und Daten) unterstützt. Diese Middleware wird in dieser TR als TR-ESOR-Middleware oder einfach nur als Middleware bezeichnet.

Die zur Archivierung eingesetzten IT-Anwendungen umfassen typischerweise Programme zur Erzeugung, Indexierung und Verwaltung der zu archivierenden Unterlagen, zur Recherche sowie zur Wiedergabe oder auch dem Löschen von Daten und Dokumenten aus dem Archivierungssystem. Die Technische Richtlinie beschränkt sich auf die für den Beweiswerterhalt erforderlichen Funktionen, Schnittstellen und Komponenten. Darüber hinausgehende Funktionen, Schnittstellen und Komponenten sind zulässig, sofern sie die Funktionen zum Beweiswerterhalt nicht einschränken oder deren Sicherheit gefährden. Dies ist in Abbildung 1 mit den gestrichelten Linien angedeutet. Diese zusätzlichen Funktionen, Schnittstellen und Komponenten werden jedoch hier nicht weiter betrachtet.

Die Sicherung der **Verfügbarkeit und Lesbarkeit** elektronischer Unterlagen kann dabei von der im Zentrum dieser Technischen Richtlinie stehenden Middleware nicht alleine gewährleistet werden, sondern muss durch geeignete technische und organisatorische Maßnahmen sowohl in den vorgelagerten IT-Anwendungen als in den eingesetzten Langzeitspeichersystemen unterstützt werden.

Unabhängig von der eingesetzten Technologie, den eingesetzten Verfahren und Anwendungen sind die gesetzlichen Vertreter verantwortlich für die Einhaltung der gesetzlichen Anforderungen, die für den langfristigen Beweiswerterhalt erforderlich sind. Im Einzelnen sind diese in den nachfolgenden Abschnitten beschrieben.

4. Allgemeine Anforderungen an eine beweiswerterhaltende Aufbewahrung

Die vorliegende Technische Richtlinie befasst sich mit der langfristigen Beweiswerterhaltung kryptographisch signierter Dokumente.

Die Aufbewahrung von Unterlagen ist grundsätzlich so auszugestalten, dass die aus rechtlicher Sicht bestehenden Aufbewahrungspflichten und –ziele für die Dauer der gesetzlich festgelegten Aufbewahrungsfristen erfüllt werden können.[3]

Strebt der die Unterlagen Aufbewahrende an, die Aufbewahrung kryptographisch signierter Dokumente so auszugestalten, dass der Beweiswert der Dokumente erhalten bleibt, sind die diesbezüglichen rechtlichen Rahmenbedingungen[4] zu berücksichtigen und die funktionalen Anforderungen entsprechend zu bestimmen.

4.1 Bundesarchivgesetz und Landesarchivgesetze

Alle öffentlichen Stellen des Bundes und der Länder sind gesetzlich verpflichtet, Unterlagen, die für die Aufgabenwahrnehmung nicht mehr benötigt werden, vor ihrer Vernichtung dem Bundes- bzw. Landesarchiv zur Übernahme als Archivgut des Bundes / des Landes anzubieten (vgl. §2 Abs. 1 BArchG und entsprechende Landesarchivgesetze). Diese Anbietungspflicht gilt selbstverständlich auch für elektronische Unterlagen. Da die Archivierung jedoch nicht Gegenstand dieser TR ist, wird auf die entsprechenden rechtlichen Anforderungen nicht näher eingegangen.[5]

Hinweis: Nach § 2 BArchG sind zunächst grundsätzlich alle Unterlagen von Bundesbehörden aufzubewahren; die bereichsspezifischen Regelungen nach BGB, HGB etc. stellen keine Löschungsermächtigung dar, sondern bezeichnen gesetzliche Mindestfristen für die Aufbewahrung. Die Entscheidung über die Aufbewahrungswürdigkeit (»Archivwürdigkeit«) steht nach § 3 BArchG allein dem Bundesarchiv im Benehmen mit den anbietenden Stellen des Bundes zu. Die Kriterien einer Entscheidung über den „bleibenden Wert“ ergeben sich nicht zwingend aus den fachrechtlichen Gründen für die Entstehung der Unterlagen

4.2 Rechtliche Rahmenbedingungen

4.2.1 Deutsches Signaturrecht

Nach dem deutschen Prozessrecht kommt einem elektronischen Dokument ein besonderer, einer Urkunde vergleichbarer Beweiswert zu, wenn es qualifiziert signiert ist. Nach § 371a Abs. 1 ZPO wird von der Vorlage einer qualifizierten elektronischen Signatur auf den Anschein der Echtheit des Dokuments geschlossen, sofern keine ernstlichen Zweifel bestehen, dass die Erklärung vom Signaturschlüssel-Inhaber abgegeben worden ist.[6] Für qualifiziert signierte öffentliche elektronische Dokumente gilt nach § 371a Abs. 2 Satz 2 ZPO darüber hinaus die Vermutung der Echtheit nach § 437 Abs. 1 ZPO, sofern das Dokument nach Form und Inhalt sich als öffentliches Dokument darstellt. Der Anschein bzw. die Vermutung der Echtheit signierter elektronischer Dokumente bezieht sich dabei sowohl auf die Zurechnung des Dokuments zu dem Signaturschlüssel-Inhaber als auch, dass er die im Dokument enthaltene Erklärung so abgegeben hat (vgl. § 416 ZPO). Soweit es sich bei dem Dokument um eine öffentliche Urkunde im Sinne von § 415 ZPO handelt, erbringt es sogar vollen Beweis über die beurkundeten Tatsachen.

Tatbestandsvoraussetzung des § 371 Abs. 1 S. 2 ZPO ist, dass es sich um eine qualifizierte elektronische Signatur handelt. Dadurch wird klargestellt, dass die Beweiserleichterung bei einfachen oder fortgeschrittenen Signaturen nicht in Betracht kommt. Wesentliche Voraussetzung für die Bestimmung

[3] Siehe hierzu § 18 Abs. 1 Satz2 Registraturrichtlinie der Bundesministerien (RegR)
[4] Siehe beispielsweise §§ 110a-d Sozialgesetzbuch IV
[5] Siehe hierzu Kapitel 3.2.
[6] § 371a Abs. 1 Satz 2 ZPO: Der Anschein der Echtheit einer in elektronischer Form vorliegenden Erklärung, der sich auf Grund der Prüfung nach dem Signaturgesetz ergibt, kann nur durch Tatsachen erschüttert werden, die ernstliche Zweifel daran begründen, dass die Erklärung vom Signaturschlüssel-Inhaber abgegeben worden ist.

des Beweiswerts eines elektronisch signierten Dokuments ist die Durchführung einer Signaturprüfung. Für die langfristige Sicherstellung der Beweiskraft elektronischer Signaturen sind daher Sicherungsmaßnahmen notwendig, die geeignet sind, die Authentizität und Integrität der elektronisch signierten Daten dauerhaft, mindestens aber für die Zeit der gesetzlich vorgeschriebenen Aufbewahrungsfristen, zu gewährleisten. Dies gilt insbesondere dann, wenn die aufzubewahrenden Unterlagen über die Dauer der Aufbewahrung weiterhin in signierter Form benötigt werden und zugleich festgestellt wird, dass die den elektronischen Signaturen zugrunde liegenden Algorithmen und Parameter keine ausreichende Sicherheit mehr für den vorgeschriebenen oder gewünschten Aufbewahrungszeitraum bieten und damit einen neuen Integritätsschutz i. S. von § 17 SigV erforderlich machen.

4.2.1.1 Dauerhafter Nachweis der Authentizität kryptographisch signierter Dokumente

Hinsichtlich der Sicherung der Authentizität der signierten Daten muss vor allem langfristig nachweisbar sein und bleiben, wem die Signatur zugerechnet werden kann, d. h. der Urheber der signierten Daten muss eindeutig erkennbar sein. Die für eine langfristige Aufbewahrung elektronischer Daten erforderlichen Vorkehrungen zur Sicherung der Authentizität sind im Signaturgesetz nur zum Teil enthalten. Fehlende Vorkehrungen müssen daher aus einer sicherheitstechnischen Betrachtung und den beweisrechtlichen Anforderungen an eine Prüfung von Zertifikaten gemäß Signaturgesetz entwickelt werden.

Die Zurechnung der Signatur erfolgt über Nutzerzertifikate mit dem in § 7 SigG bestimmten Inhalt. Ein solches Zertifikat ist die Bestätigung der Zuordnung eines zuverlässig identifizierten Signaturschlüssel-Inhabers zum Signaturprüfschlüssel, mit dessen korrespondierenden Signaturschlüssel die Signatur erstellt wurde. Handelt es sich – wie im § 7 SigG beschrieben – um ein qualifiziertes Zertifikat, und war es darüber hinaus zum Signaturerstellungszeitpunkt gültig, kann der Nachweis der Authentizität grundsätzlich erbracht werden, sofern eine Prüfung des Zertifikats gemäß Signaturgesetz erfolgreich verlaufen ist.

Prüfbarkeit der erforderlichen Zertifikate

Für den langfristigen Nachweis der Authentizität signierter Daten ist daher wesentlich, dass die Existenz des Nutzerzertifikats sowie seine Gültigkeit zum Signaturerstellungszeitpunkt nachweisbar bleiben.

Eine notwendige Voraussetzung für eine Prüfung eines qualifizierten Zertifikats gemäß Signaturgesetz ist es, dass das Zertifikat überhaupt vorliegt. Ein Zertifizierungsdiensteanbieter hat die von ihm ausgestellten Zertifikate gemäß § 5 Abs. 1 Satz 2 SigG über öffentlich erreichbare Kommunikationsverbindungen jederzeit nachprüfbar und mit Zustimmung des Signaturschlüssel-Inhabers auch abrufbar zu halten.

Die Nachprüfbarkeit setzt voraus, dass das Zertifikat in dem vom Zertifizierungsdiensteanbieter gemäß § 4 Abs. 1 SigV zu führenden Zertifikatsverzeichnis vorhanden ist. Eine Signaturprüfung nach Signaturgesetz erfordert daher, zusätzlich zur Überprüfung der technischen Gültigkeit der Signatur, also der Überprüfung, ob die Signatur im kryptographischen Sinne korrekt verifiziert werden kann und die Signatur und die signierten Daten technisch zueinander gehören, stets auch eine Abfrage beim Zertifizierungsdiensteanbieter, ob das der Signatur zugrunde liegende Zertifikat zum angegebenen Zeitpunkt der Signatur vorhanden, gültig und nicht gesperrt war. Der Zertifizierungsdiensteanbieter hat diese Auskunft gemäß § 5 Abs. 1 Satz 2 SigG über öffentlich erreichbare Kommunikationsverbindungen zu erteilen. Da die Authentizität der Auskunft nachweisbar sein muss, werden Auskünfte der Zertifizierungsdiensteanbieter üblicherweise mit einer qualifizierten elektronischen Signatur versehen.

Allerdings sind diese Pflichten des Zertifizierungsdiensteanbieters zweifach beschränkt. Zunächst kann der Signaturschlüssel-Inhaber gemäß § 5 Abs. 1 Satz 3 SigG bestimmen, dass sein Zertifikat nicht abrufbar sein soll. Dem Zertifizierungsdiensteanbieter ist in diesem Fall nicht gestattet, das Zertifikat zum Abruf bereitzustellen. Der Signaturschlüssel-Inhaber selbst muss das Zertifikat dem bestimmungsgemäßen Empfänger der von ihm signierten Daten auf andere Weise zur Verfügung stellen, beispielsweise dadurch, dass das Zertifikat der Signatur beigefügt wird.

Die Verpflichtung des Zertifizierungsdiensteanbieters ist aber auch zeitlich begrenzt. Nach § 4 Abs. 1 SigV besteht die gesetzliche Verpflichtung nur für einen Zeitraum von bis zu fünf Jahren nach dem

Schluss des Jahres, in dem die Gültigkeit des Zertifikats abläuft. Dieser Zeitraum verlängert sich um weitere 25 Jahre, falls der Zertifizierungsdiensteanbieter akkreditiert ist (vgl. § 4 Abs. 2 SigV).

Sofern ein Zertifizierungsdiensteanbieter mit Anbieterakkreditierung seinen Betrieb einstellt, ist die Bundesnetzagentur (BNetzA) verpflichtet, die Dokumentation zu den ausgegebenen Zertifikaten zu übernehmen – nicht jedoch, den technischen Betrieb fortzuführen (vgl. § 15 Abs. 6 SigG). Eine automatisierte Prüfung wird somit bspw. nicht mehr ohne weiteres möglich sein. Bei qualifizierten Signaturverfahren im Zusammenhang mit Zertifizierungsdiensteanbietern mit Anbieterakkreditierung sind Zertifikate und Dokumentation nach §§ 4 Abs. 2 und 8 Abs. 3 SigV 30 Jahre nach Ablauf des Jahres der Gültigkeit des Zertifikats aufzubewahren.[7] Im Falle der vorherigen Einstellung des Betriebs übernimmt dies ein anderer Zertifizierungsdiensteanbieter oder die BNetzA.

Vorhalten der erforderlichen Verifikationsdaten

Aus der gesetzlichen Beschränkung der Aufbewahrungspflicht des Zertifizierungsdiensteanbieters ergibt sich somit die Obliegenheit bzw. Verpflichtung des Empfängers signierter Daten, selbst dafür zu sorgen, dass er das Zertifikat und die zugehörigen Prüfinformationen[8] vorlegen kann, wenn sie für ein Beweisbegehren benötigt werden. In der Regel wird der Empfänger daher die Vorkehrung treffen, nicht nur die signierten Daten und die Signatur, sondern auch die erforderlichen Zertifikate und Prüfinformationen, wenn schon nicht beim Eingang oder der Ausstellung signierter Daten, so doch dann spätestens bei der Ablage im elektronischen Langzeitspeicher, einzuholen und gemeinsam mit den signierten Daten zu speichern.[9]

Für elektronische Signaturen basierend auf einem qualifizierten Zertifikat sind für den schlüssigen und nachvollziehbaren Nachweis der Existenz und der Gültigkeit des Zertifikats zum Signaturerstellungszeitpunkt die Vorlage und technische Verifikation folgender Daten erforderlich (s. **[ARO 07]**, S. 73):

- das Nutzerzertifikat und ggf. Attributzertifikat mit Zertifikatskette bis zum Wurzelzertifikat,
- eine Status-(OCSP-)Auskunft[10] des Zertifizierungsdiensteanbieters über die Existenz und die Gültigkeit des Zertifikats, ebenfalls mit Zertifikatskette bis zum Wurzelzertifikat,
- ein qualifizierter Zeitstempel bezogen auf die Signatur ebenfalls mit Zertifikatskette bis zum Wurzelzertifikat.

Dabei ist es dem Anwender überlassen, wo er die Daten aufbewahrt. Er kann diese unmittelbar der Signatur oder den signierten Daten beifügen oder aber in einer gesonderten Objektdatenbank vorhalten und über eine eindeutige Referenzierung einen Zugriff auf diese zur Sicherstellung der Verfügbarkeit gewährleisten.

4.2.1.2 Neusignierung nach § 17 SigV

Zu den für die langfristige Prüfbarkeit erforderlichen Sicherheitsmaßnahmen gehört auch die Neusignierung nach § 17 SigV, die zur Gewährleistung der Integrität erforderlich ist. Gemäß § 17 SigV sind Daten mit einer qualifizierten elektronischen Signatur neu zu signieren, wenn sie für längere Zeit in signierter Form benötigt werden, als der Signaturalgorithmus als geeignet (technisch sicher) beurteilt werden kann. Da auch Verifikationsdaten elektronische Signaturen enthalten, unterliegen sie ebenso dem Erfordernis der Neusignierung nach § 17 SigV. Erst durch ihre Einbeziehung in die Neusignierung kann die Unversehrtheit und damit Echtheit eines Zertifikats, einer Gültigkeitsabfrage oder eines Zeitstempels langfristig überprüft werden.

---

[7] Für fortgeschrittene Signaturverfahren sind keine Vorhaltefristen vorgesehen.

[8] „Prüfinformationen“ sind die Ergebnisse einer Gültigkeitsprüfung einer Signatur und aller damit in Zusammenhang stehenden Zertifikate, die die Gültigkeit der Signatur und der Zertifikate zu einem gewissen Zeitpunkt (normalerweise dem Zeitpunkt der Signaturerstellung) angeben.

[9] Die Auskunft des Zertifizierungsdiensteanbieters enthält neben den Angaben darüber, ob das Zertifikat im Verzeichnis vorhanden ist, auch eine Information über den Status des Zertifikats. Sperrungen hat der Zertifizierungsdiensteanbieter gemäß § 7 Abs. 2 SigV im Zertifikatsverzeichnis mit Angabe von Datum und Uhrzeit kenntlich zu machen. Da der Sperrstatus für eine Prüfung eines Zertifikats nach Signaturgesetz benötigt wird, sollten die Auskünfte auch aus diesem Grund unverzüglich einholt, geprüft und gespeichert werden.

[10] Online Certificate Status Protocol (OCSP), Client-Server Protokoll für die Online Statusabfrage eines Zertifikats bei einem Zertifizierungsdiensteanbieter, http://www.ietf.org/rfc/rfc2560.txt

§ 17 SigV begründet allerdings keine Rechtspflichten. Der Zweck dieser technischen Vorschrift ist darauf beschränkt, ein geeignetes Verfahren für eine langfristige Datensicherung zu beschreiben. Der Zertifizierungsdiensteanbieter hat jedoch den Signaturschlüssel-Inhaber gemäß § 6 Abs. 1 Satz 2 SigG in Verbindung mit § 6 Nr. 5 SigV darauf hinzuweisen, dass Daten mit einer qualifizierten elektronischen Signatur bei Bedarf gemäß § 17 SigV neu zu signieren sind. Die Anwendung des Verfahrens ist damit grundsätzlich als eine Obliegenheit im Umgang mit signierten Daten anzusehen.

Auch wenn § 17 SigV somit grundsätzlich lediglich eine Obliegenheit begründet, kann eine Rechtspflicht zur Anwendung des § 17 SigV bestehen. Diese muss sich dann jedoch aus anderen Gesetzen, Normen oder aus vertraglichen Regelungen ergeben. Eine Rechtspflicht zur Anwendung des § 17 SigV besteht immer dann, wenn der Empfänger auf Grund von Gesetzen oder Verträgen verpflichtet ist, den besonderen Beweiswert qualifiziert signierter elektronischer Dokumente zu erhalten.

Die Signaturverordnung sieht in § 17 SigV ein Verfahren vor, wie und wann die erforderliche Neusignierung zu erfolgen hat:

„Daten mit einer qualifizierten elektronischen Signatur sind nach § 6 Abs. 1 Satz 2 des Signaturgesetzes neu zu signieren, wenn diese für längere Zeit in signierter Form benötigt werden, als die für ihre Erzeugung und Prüfung eingesetzten Algorithmen und zugehörigen Parameter als geeignet beurteilt sind. In diesem Falle sind die Daten vor dem Zeitpunkt des Ablaufs der Eignung der Algorithmen oder der zugehörigen Parameter mit einer neuen qualifizierten elektronischen Signatur zu versehen. Diese muss mit geeigneten neuen Algorithmen oder zugehörigen Parametern erfolgen, frühere Signaturen einschließen und einen qualifizierten Zeitstempel tragen."

Droht der Verlust der Sicherheitseignung der verwendeten Algorithmen und der zugehörigen Parameter, so sind die Daten und alle bestehenden Signaturen also gemäß § 17 SigV erneut zu signieren. Dies ist die Grundlage der Beweiswerterhaltung elektronischer Dokumente.

Mit § 17 SigV wurde eine Norm geschaffen, die den Rahmen für eine technische Lösung umreißt, die den Anforderungen an die Beweiswerterhaltung genügt. Intention des vom Gesetzgeber normierten Verfahrens ist die fortdauernde Sicherstellung der Integrität und Authentizität des ursprünglich signierten Dokuments. Nach vorherrschender Rechtsmeinung (siehe hierzu **[ARO 07]**, Kap. 4.2.1.1) ist die durch § 17 SigV geforderte erneute qualifizierte elektronische Signatur keine (erneute) Willenserklärung, sondern ein Sicherungsmittel für vorhandene Willenserklärungen.

Das Ziel des Verfahrens ist es, die Integrität einer qualifizierten elektronischen Signatur auch dann noch feststellen zu können, wenn die mathematische Signaturprüfung aufgrund mangelnder Sicherheitseignung der verwendeten Algorithmen nicht mehr geeignet ist, die Integrität der Signatur zu belegen. Um sicherzustellen, dass die Echtheit qualifizierter elektronischer Signaturen – trotz später möglicherweise bekannt werdender Sicherheitsmängel - auf Dauer nachweisbar ist, wird eine Integritätssicherung benötigt, die die Signaturen zu einem Zeitpunkt „konserviert", zu dem diese Mängel im Nachhinein als noch nicht relevant anzusehen sind. Diese Integritätssicherung muss den Nachweis darüber erbringen können, dass die Signatur und die signierten elektronischen Daten bereits zu diesem Zeitpunkt vorlagen. Die Integritätssicherung muss daher die Daten und die Signatur umfassen, und die Dokumentation des Zeitpunktes muss durch einen vertrauenswürdigen Dritten erfolgen, z. B. durch einen Zertifizierungsdiensteanbieter.

Qualifizierte Zeitstempel gemäß Signaturgesetz können genau diesem Zweck dienen. Ein qualifizierter Zeitstempel ist gemäß § 2 Nr. 14 SigG die elektronische Bescheinigung eines Zertifizierungsdiensteanbieters darüber, dass ihm bestimmte elektronische Daten zu einem bestimmten Zeitpunkt vorgelegen haben. Die aktuelle Fassung des Signaturgesetzes schreibt nicht mehr vor, dass ein qualifizierter Zeitstempel eine qualifizierte elektronische Signatur enthalten muss. Damit ist ein qualifizierter Zeitstempel alleine nicht ausreichend, eine Neusignierung durchzuführen. Ein qualifizierter Zeitstempel kann jedoch eine qualifizierte elektronische Signatur enthalten. Wird ein solcher signierter Zeitstempel für die Neusignatur verwendet, ist eine weitere Signatur für die Beweiswerterhaltung weder notwendig noch sinnvoll (siehe dazu **[SFD 06]**, S. 178 ff.).

Die erneute Signatur muss rechtzeitig, d. h. vor Ablauf der Sicherheitseignung der verwendeten Algorithmen und zugehörigen Parameter mit neuen sicherheitsgeeigneten Algorithmen erfolgen. Entsprechende Übersichten geeigneter Algorithmen werden von der BNetzA nach Eignungsfeststellung durch das BSI veröffentlicht.

Die Neusignierung muss alle vorhandenen Signaturen umschließen. Nur so lässt sich die Gesamtstruktur des Dokuments und der dazugehörigen Signaturen und Informationen erhalten. Da die Neusignierung lediglich als Sicherungsmittel dient, kann die (Neu-)Signatur beliebig viele Daten umschließen. Es muss sich jedoch beweisen lassen, dass ein bestimmtes Dokument in der Umschließung enthalten ist, das heißt (gemeinsam mit anderen) erneut signiert wurde.

Zeitstempel sind technisch gesehen in der Regel ebenfalls elektronische Signaturen, deren sicherheitstechnische Eignung im Laufe der Zeit verloren gehen kann. Bevor dies geschieht, müssen diese Zeitstempel daher ebenfalls konserviert werden, indem ein erneuter Zeitstempel eingeholt wird.

§ 17 SigV unterscheidet nicht danach, ob der Hash-Algorithmus, der Signatur-Algorithmus oder beide ihre Eignung verlieren. Der qualifizierte Zeitstempel muss sich aber nur dann sowohl auf die signierten Daten als auch auf die Signatur beziehen, wenn das verwendete Hash-Verfahren unsicher zu werden droht. Falls der Hash-Algorithmus noch geeignet ist, muss sich der zu bildende Zeitstempel nur auf die Signatur beziehen. Dies reicht aus, da die Daten weiterhin zuverlässig mit der alten Signatur verknüpft sind. Sicherheitstechnisch gesehen ist es nicht erforderlich, für die Daten einen neuen Hashwert zu bilden, um diesen dann neu zu signieren.

Um eine wirtschaftliche Neusignierung zu ermöglichen, ist es zudem nach § 17 SigV nicht erforderlich, für jedes elektronische Datum, das erneut signiert werden muss, einen eigenen Zeitstempel einzuholen. Ein Zeitstempel darf sich vielmehr auf beliebig viele signierte Daten beziehen.

Sicherheitstechnisch gesehen ist dies ohne weiteres möglich. Die Wirkung eines Zeitstempels als Mittel zur Integritätssicherung ist nicht davon abhängig, wie viele Signaturen gleichzeitig konserviert werden. Auch wurde bereits in der amtlichen Begründung zu § 18 SigV 1997 ausgeführt, dass „für eine beliebige Anzahl signierter Daten eine (übergreifende) neue digitale Signatur “ angebracht werden kann.

Die Neusignierung von Teilen eines elektronischen Archivs ist damit auch automatisiert möglich. Als automatisierte elektronische Signatur wird eine Signatur verstanden, die von einem automatischen Prozess ohne Mitwirkung eines Menschen erzeugt wird. Dabei wird davon ausgegangen, dass ein Mensch diesen Prozess zwar bewusst einleitet, er aber weder die zu signierenden Daten im Einzelfall vor der Signatur überprüft, noch den Signaturschlüssel im Einzelfall freischaltet. Die Erstellung qualifizierter elektronischer Signaturen oder qualifizierter Zeitstempel im Massenverfahren ist ebenfalls zulässig.[11]

4.2.2 Europäische Signaturrichtlinie

Am 19. Januar 2000 trat die Richtlinie **[1999/93/EG]** nach Verkündung im Amtsblatt der Europäischen Union in Kraft.

Der Anwendungsbereich der Richtlinie **[1999/93/EG]** gilt nicht unmittelbar für Anbieter und Nutzer von Zertifizierungsdiensten und Produkten für elektronische Signaturen, sondern muss jeweils von den Mitgliedstaaten in nationales Recht umgesetzt werden.

Dieser Richtlinie ist in Artikel 1 zu entnehmen:

„*Diese Richtlinie soll die Verwendung elektronischer Signaturen erleichtern und zu ihrer rechtlichen Anerkennung beitragen. Sie legt rechtliche Rahmenbedingungen für elektronische Signaturen und für bestimmte Zertifizierungsdienste fest, damit das reibungslose Funktionieren des Binnenmarktes gewährleistet ist.*“

Ein wesentlicher Punkt der Richtlinie ist die Klärung des Beweiswerts elektronischer Signaturen in Artikel 5:

„*(1) Die Mitgliedstaaten tragen dafür Sorge, dass fortgeschrittene elektronische Signaturen, die auf einem qualifizierten Zertifikat beruhen und die von einer sicheren Signaturerstellungseinheit erstellt werden,*

a) die rechtlichen Anforderungen an eine Unterschrift in Bezug auf in elektronischer Form vorliegende Daten in gleicher Weise erfüllen wie handschriftliche Unterschriften in Bezug auf Daten, die auf Papier vorliegen, und

b) in Gerichtsverfahren als Beweismittel zugelassen sind.“

[11] Siehe hierzu eingehend **[ARO 07]**, Kap. 4.2.1.2

Es existieren keine weiteren mittelbar oder unmittelbar wirkenden EG-Rechtsakte und entsprechende nationale Umsetzungsakte, die man im europäischen Kontext als rechtlichen Rahmen für eine Beweiswerterhaltung kryptographisch signierter Dokumente im Rahmen elektronischer Systeme heranziehen könnte.

4.2.3 Sarbanes-Oxley-Act (SOX)

In den USA existiert seit 2002 der sogenannte „Sarbanes-Oxley-Act“ (SOX). Das Gesetz findet Anwendung für alle Unternehmen, die an der New York Stock Exchange notiert sind. SOX hat die Aufgabe, die Transparenz und Nachvollziehbarkeit in den Unternehmen bei Prüfungen durch die SEC (Securities und Exchange Commission) zu verbessern. Unternehmen werden verpflichtet, u. a. ein internes Kontrollsystem für die Rechnungslegung zu unterhalten, die Wirksamkeit der Systeme zu beurteilen und die Richtigkeit der Jahres- und Quartalsberichte beglaubigen zu lassen. Die Erfüllung dieser Verpflichtungen wird unter dem Stichwort „Compliance“ (Übereinstimmung, Erfüllung) zusammengefasst.

Direkte Auswirkungen auf die Anforderungen zur Langzeitspeicherung elektronischer Dokumente hat vor allem der Abschnitt 802 von SOX, wonach Sanktionen im Falle der Zerstörung, der Veränderung oder Manipulation aufbewahrungspflichtiger elektronischer Unterlagen angedroht werden. Die Unternehmen werden dabei durch SOX nicht nur verpflichtet aufbewahrungspflichtige elektronische Dokumente gegen vorsätzliche Löschung, Veränderung oder Zerstörung zu schützen, sondern müssen darüber hinaus auch den Nachweis erbringen können, dass Veränderungen oder Manipulationen an diesen Dokumenten nicht stattgefunden haben.

4.2.4 Naibutousei - SOX auf Japanisch

Die japanische "Financial Services Agency" hat am 15. Februar 2007 neue Anforderungen für Unternehmen veröffentlicht, die an der japanischen Börse gelistet sind.

Der japanische Standard Naibutousei - auch J-SOX genannt - orientiert sich an den Anforderungen des US-Wertpapiergesetzes Sarbanes-Oxley Act von 2002 (SOX). J-SOX stellt für japanische Unternehmen eine ähnlich hohe Herausforderung dar wie für Unternehmen, die zuvor nach den Richtlinien der US-amerikanischen Börsenaufsicht, der Securities and Exchange Commission (SEC), gelistet waren.

4.3 Funktionale Anforderungen an die Beweiswerterhaltung kryptographisch signierter Dokumente

Die Maßnahmen zur Beweiswerterhaltung gliedern sich (wie oben in Kapitel 3.3 beschrieben) in den Kontext eines Gesamtsystems ein, in dem auch die Aufbewahrung der Dokumente, Signaturen und Verifikationsdaten in einem Archiv- / ECM- / Storage-System erfolgt. Diese Aufbewahrung muss in einer Form erfolgen, welche die Vollständigkeit, Verfügbarkeit, Lesbarkeit und Integrität der gespeicherten Daten über den gesamten Aufbewahrungszeitraum sicherstellt. Neben zahlreichen anderen Aspekten impliziert dies insbesondere die Verwendung von offen standardisierten und eindeutig interpretierbaren Nutzdatenformaten, für die eine nachhaltige Verkehrsfähigkeit mindestens über die Dauer der gesetzlichen Aufbewahrungsfristen nach heutigem Wissensstand angenommen werden kann und deren Spezifikation standardisiert und öffentlich zugänglich ist. Ebenso dürfen während der Aufbewahrungszeit keine Formatkonvertierungen erfolgen, durch die vorhandene Signaturen wertlos werden können.

Auch die vorgelagerten IT-Fachanwendungen müssen im Rahmen des Gesamtsystem ihre Aufgaben in geeigneter Weise erfüllen. Sie müssen z.B. sicherstellen, dass die zu signierenden Dokumente von den dafür autorisierten Personen mit geeigneten Signaturverfahren und Signaturanwendungskonponenten zum richtigen Zeitpunkt signiert werden und dass die Dokumentenablage und die Nutzung von TR-ESOR-Middleware-Funktionen zur richtigen Zeit in der richtigen Weise erfolgt.

Diese oben genannten Punkte sind nicht Gegenstand der vorliegenden Richtlinie. Die folgenden Anforderungen zum Beweiswerterhalt setzen allerdings voraus, dass das Gesamtsystem diese Voraussetzungen erfüllt.

4.3.1 Nachweis von Integrität und Authentizität

Voraussetzung für eine mögliche oder auch beabsichtigte Rechtswirkung elektronisch aufbewahrter Informationen ist, die aufbewahrten Daten und Dokumente so zu erhalten, wie sie ursprünglich abgefasst worden sind, d. h. ohne nachträgliche Änderungen und der Möglichkeit, auch nach langer Zeit den Aussteller des Dokuments zweifelsfrei bestimmen zu können. Das bedeutet:

Die aus rechtlicher Sicht geforderten und zu erbringenden Nachweise über die Integrität und Authentizität der Dokumente und Daten müssen noch nach langer Zeit geführt werden können.

Da zu den Wesensmerkmalen elektronischer Daten und Dokumente die Flüchtigkeit und ihre fehlende Verkörperung gehören, bezeichnet Integritätsnachweis im Sinne dieser Richtlinie die (technische) Fähigkeit, die Unverändertheit elektronischer Informationen nachzuweisen.

Die Feststellung der Authentizität elektronischer Daten und Dokumente im Sinne dieser Richtlinie bezeichnet die (technische) Fähigkeit, auch nach langer Zeit den Aussteller eines elektronischen Dokumentes erkennen und zuordnen zu können.

Zum Beweiswerterhalt müssen elektronische Signaturen und Zeitstempel in der durch Rechtsvorschriften geforderten Qualität sicher und zuverlässig erzeugt, geprüft, erneuert und aufbewahrt werden.

Um die beweisrechtliche Eignung elektronisch signierter Daten und Dokumente für die Dauer der Aufbewahrung zu erhalten, ist zusätzlich erforderlich:

Die für eine spätere Signaturverifikation erforderlichen Verifikationsdaten sollen unmittelbar nach der Signaturerstellung und/oder -prüfung beschafft und gemeinsam mit den zu archivierenden Dokumenten und Daten in langfristig verkehrsfähiger Form abgelegt werden.

Die Gültigkeitsprüfung der Signaturen muss in jedem Falle umfassend, vollständig und so ausgestaltet sein, dass aus dem Prüfergebnis die Erfüllung der in der europäischen Richtlinie für elektronische Signaturen wie auch im Signaturgesetz festgelegten Anforderungen an fortgeschrittene und qualifizierte elektronische Signaturen festgestellt werden kann. Sie muss sich darüber hinaus auf die gesamten Zertifikatsketten (Signaturzertifikate des Ausstellers, der Zertifizierungsstelle und der Wurzelzertifizierungsinstanz) sowie alle Verifikationsdaten und Zeitstempel beziehen und nachweislich erkennbar machen, dass die einer elektronischen Signatur zugrunde liegenden bzw. beigefügten Zertifikate zum Signaturzeitpunkt gültig und nicht gesperrt und die eingesetzten kryptographischen Algorithmen und Parameter zum Signaturzeitpunkt sicherheitsgeeignet waren. Sämtliche Prüfschritte und Prüfergebnisse müssen in übersichtlicher Weise nachvollziehbar protokolliert und angezeigt werden können.[12]

Bei der Verifikation elektronischer Signaturen soll der Signaturzeitpunkt grundsätzlich aus einem vertrauenswürdigen Zeitstempel der Signatur entnommen werden können (vgl. **[HK 06]**, S. 85). Sofern ein solcher Zeitstempel nicht vorhanden ist und die Existenz und Authentizität der Signatur zu einem früheren Zeitpunkt nicht anderweitig belegt werden kann, muss die Verifikation bezüglich des aktuellen Zeitpunkts erfolgen.

Um die Prüfbarkeit elektronisch signierter Dokumente über die gesetzlich vorgeschriebenen Aufbewahrungsfristen hin zu gewährleisten, müssen bei der Signaturerstellung standardisierte Signaturdatenformate verwendet werden. Dies betrifft neben den eigentlichen Signaturdatenformaten auch die Formate von Zertifikaten, Sperrlisten und Zertifikatsstatusabfragen sowie Zeitstempeln. Dabei muss die Kompatibilität mit den Normen und Empfehlungen der Bundesnetzagentur und des Bundesamtes für Sicherheit in der Informationstechnik sichergestellt sein (siehe hierzu **[eCard-2]**).

Elektronische Signaturen ermöglichen es nur dann, die Integrität und Authentizität elektronischer Daten nachweisbar zu machen, wenn die den Signaturen zugrunde liegenden Algorithmen mathematisch und technisch sicherheitsgeeignet sind. Fortschritte in der Entwicklung von Computern und neue Methoden der Kryptographie können jedoch dazu führen, dass die Algorithmen oder ihre Parameter im

[12] Da die Signatur selbst lediglich durch eine digitale Zeichenfolge repräsentiert wird, sind nachprüfbare und damit beweisstützende Aussagen über die Authentizität und Integrität und damit letztlich über die Echtheit der elektronischen Daten erst über eine umfassende Signaturprüfung unter Hinzuziehung der signierten Daten, geeigneter Hard- und Software zur Anzeige der Daten, der Signaturzertifikate und der Gültigkeitsabfragen und durch eine schlüssige Interpretation der Signaturprüfergebnisse möglich. Das eCard-API-Framework **[eCard-2]** unterstützt die Protokollierung und Interpretation der Signaturprüfergebnisse durch die Erzeugung eines Signaturprüfberichtes in einem standardisierten Format.

Laufe der Zeit ihre Sicherheitseignung einbüßen.[13] Ein dauerhafter und nachweisbarer Erhalt der Authentizität und Integrität elektronischer Daten erfordert deshalb den Einsatz zusätzlicher Sicherungsmittel, die den Nachweis ermöglichen, dass insbesondere elektronisch signierte Daten über die Dauer der Aufbewahrungsfristen unverfälscht aufbewahrt wurden. Elektronische Signaturen müssen daher rechtzeitig vor Ablauf der Sicherheitseignung der verwendeten kryptographischen Algorithmen und zugehörigen Parameter gemäß den Vorgaben des Signaturgesetzes erneuert werden. Die Signaturerneuerung muss entsprechend der rechtlichen Anforderungen sowie weitgehend automatisch und wirtschaftlich erfolgen können.

Vornehmliche Intention der Erneuerung von Signaturen ist der Erhalt der Nachweisbarkeit der Integrität und Authentizität der bereits signierten Dokumente. Nach geltender Rechtsauffassung ist es daher für eine erneute Signatur nach § 17 Satz 3 SigV ausreichend, wenn elektronisch signierte Daten mit einem qualifizierten Zeitstempel versehen werden, der mindestens eine qualifizierte elektronische Signatur enthält (vgl. **[SFD 06, S. 178 ff., ARO 07, S. 61 ff.]**). Die erneute elektronische Signatur kann beliebig viele Daten umschließen und auch über kryptographische Repräsentanten (Hashwerte, verschlüsselte Daten) der signierten Daten ausgeführt werden, sofern die kryptographischen Repräsentanten die signierten Daten eindeutig repräsentieren und die zur Herstellung der Repräsentation genutzten Algorithmen und zugehörigen Parameter zum Zeitpunkt der erneuten Signatur weiterhin als sicherheitsgeeignet beurteilt werden können.

Nur der Beweiswert elektronisch signierter Dokumente kann erhalten werden, der von Anfang an besteht und sich letztlich natürlich daraus bestimmt, welche Anforderungen der Aufbewahrende an die Zweckerfüllung der Beweisführung stellt bzw. zu stellen verpflichtet ist. Maßgeblich für den beweisrechtlichen Wert elektronisch signierter Dokumente ist die Qualität der eingesetzten Signaturen, Signaturerstellungseinheiten, Signaturanwendungs- und Signaturprüfkomponenten. Daraus folgt:

Für die Erstellung elektronischer Signaturen und Zeitstempel sind ausschließlich von der Bundesnetzagentur veröffentlichte und als sicherheitstechnisch unbedenklich eingestufte Schlüssellängen und Algorithmen zu verwenden.

(A4.3-1) Qualifizierte elektronische Signaturen müssen die Anforderungen an fortgeschrittene elektronische Signaturen erfüllen und gemäß § 2 Nr. 3a SigG auf einem zum Zeitpunkt ihrer Erzeugung gültigen qualifizierten Zertifikat beruhen sowie nach § 2 Nr. 3b SigG mit einer sicheren Signaturerstellungseinheit erzeugt worden sein. Qualifizierte Zeitstempel müssen die Anforderungen von § 2 Nr. 14 SigG erfüllen.

Die technische Sicherheit qualifizierter elektronischer Signaturen wird durch den Einsatz geeigneter Komponenten zur Schlüssel- und Signaturerzeugung, der Signaturanwendung und Signaturprüfung erreicht. Nach § 17 Abs. 1 SigG sind die Komponenten so zu gestalten, dass sie gegen unberechtigte Nutzung geschützt sind und sich Fälschungen von Signaturen und Manipulationen signierter Daten zuverlässig erkennen lassen. Signaturprüfkomponenten müssen nach § 17 Abs. 2 Satz 2 feststellen können, auf welche Daten sich die Signatur bezieht (Nr. 1), ob die signierten Daten unverändert sind (Nr. 2), welchem Signaturschlüssel-Inhaber die Signatur zuzuordnen ist (Nr. 3), welche Inhalte das qualifizierte Zertifikat, auf dem die Signatur beruht, und ggf. zugehörige Attributzertifikate aufweisen (Nr. 4) und zu welchem Ergebnis die Nachprüfung von Zertifikaten nach § 5 Abs. 1 Satz 2 SigG geführt hat (Nr. 5). Darüber hinaus müssen Signaturprüfkomponenten nach § 15 Abs. 2 Nr. 2 SigV die Korrektheit der Signatur zuverlässig prüfen und anzeigen sowie eindeutig erkennbar machen, ob die nachgeprüften Zertifikate zum Prüfzeitpunkt im jeweiligen Zertifikatsverzeichnis vorhanden und nicht gesperrt waren.

(A4.3-2) Die Vergabe qualifizierter Zertifikate ist nach § 2 Nr. 7 SigG Zertifizierungsdiensteanbietern vorbehalten, die mindestens die Sicherheitsanforderungen des Signaturgesetzes und der Signaturverordnung erfüllen.

Für die langfristige Sicherung und Überprüfbarkeit der Authentizität und Integrität elektronisch signierter Daten und Dokumente folgt daraus:

Die Erstellung und Prüfung qualifizierter elektronischer Signaturen für aufbewahrte signierte elektronische Daten und Dokumente sollen durch nach SigG und SigV geprüfte und bestätigte Signaturanwendungskomponenten erfolgen. Für eine Visualisierung der signierten Daten, der Zertifikate und

[13] Die jeweils als sicher angesehenen Algorithmen sind in **[ALGCAT]** aufgeführt und werden dort regelmäßig aktualisiert.

Prüfergebnisse sollen ebenfalls nach SigG und SigV geprüfte und bestätigte Anzeigekomponenten zur Verfügung stehen.

Die Integrität nicht signierter Daten kann zusätzlich ab dem Zeitpunkt der Überführung in einen ECM/Langzeitspeicher automatisch durch geeignete kryptographische Sicherungsmittel wie elektronische Archiv(eingangs)hashwerte oder -signaturen und (qualifizierte) Archiv(eingangs)zeitstempel gesichert werden.

5. Funktionen einer Middleware zum Beweiswerterhalt

Die für den Benutzer (die Geschäftsanwendung) aufrufbaren Funktionen der Middleware zum Beweiswerterhalt müssen sich selbstverständlich an den Zwecken des Archivs orientieren und darauf aufsetzen. Es müssen jedoch nicht alle Funktionalitäten eines Archivsystems abgebildet werden.

Im ersten Abschnitt dieses Kapitels werden daher die Funktionen des Archivsystems, die **aus Anwendersicht** vorhanden und nutzbar sein und daher auch von der Middleware berücksichtigt werden müssen, beschrieben. Darauf bauen die technischen Anforderungen an die Middleware auf, die in Kapitel 6 zu finden sind.

Im zweiten Abschnitt dieses Kapitels werden die wichtigsten organisatorischen Aspekte angesprochen, die eine Behörde oder ein Unternehmen zu beachten hat, um den Beweiswert der archivierten Unterlagen auch tatsächlich zu erhalten. Hierbei ist zu bedenken, dass diese Hinweise nur eine grobe Orientierung liefern können und kein umfassendes Sicherheitskonzept aller organisatorischen Belange darstellen. Hierzu sei auf Kapitel 8 verwiesen.

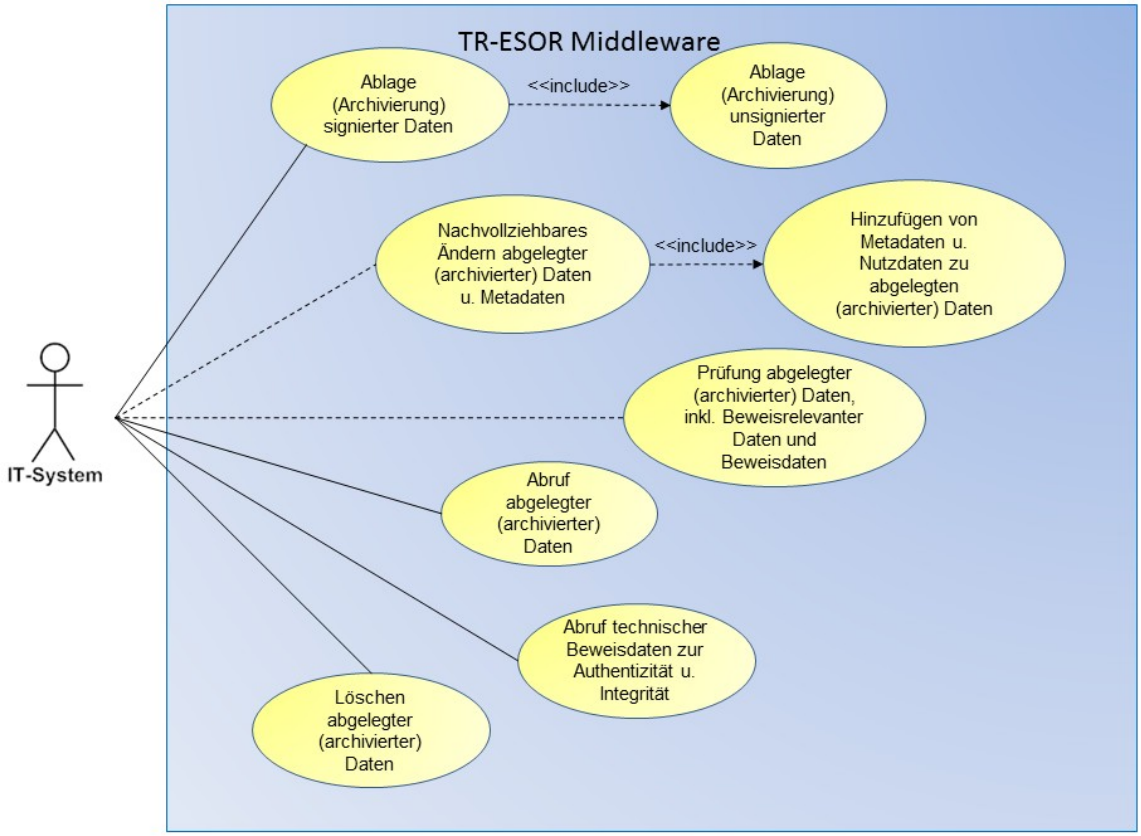


Abbildung 2: Funktionale Anforderungen

Die funktionalen Anforderungen legen fest, welche Funktionen ein Archivsystem und damit auch die Middleware für den Beweiswerterhalt aus Sicht eines Benutzers mindestens zur Verfügung stellen muss. Dabei werden, wie in Abbildung 2 dargestellt, die folgenden grundsätzlichen Anwendungsfälle unterschieden:[14]

[14] Weitere Funktionen wie z. B. „Suchen“ (auch geschäftsanwendungsübergreifend), oder „Strukturieren in Verzeichnisse“ sind sicherlich wünschenswert, für den Beweiswerterhalt jedoch nicht notwendig. Diese Technische Richtlinie beschränkt sich daher auf die oben aufgeführten verpflichtenden und optionalen Basisfunktionen.

- die Ablage (Archivierung) unsignierter und signierter Daten, ggf. inklusive bereits vorhandener zugehöriger beweisrelevanter Daten und technischer Beweisdaten (engl.: Evidence Records),
- der Abruf archivierter Daten,
- der Abruf beweisgeeigneter Nachweise über die Authentizität und Integrität der aufbewahrten Daten,
- das Löschen von Daten[15].

Es ist zu erwähnen, dass selbst diese Minimal-Funktionen nicht in jedem tatsächlichen Anwendungsfall notwendig sind. In einem klassischen Archiv[16] werden z.B. eher selten Daten geändert sondern nur abgelegt, aufgerufen und ggf. noch gelöscht. Daher wurden folgende Funktionen auch nur als mögliche Optionen festgelegt:

- das nachvollziehbare Ändern von bereits archivierten Metadaten und Nutzdaten, was auch das Hinzufügen von weiteren Metadaten und Nutzdaten zu bereits archivierten Datenstrukturen beinhaltet, und
- das Prüfen des Archivdatenobjektes samt der darin enthaltenen oder zusätzlich übergebenen beweisrelevanten Daten und Beweisdaten (engl.: Evidence Records).

Grundsätzlich gilt:

(A5.1-1) Der Zugriff auf die TR-ESOR-Middleware bzw. den ECM/Langzeitspeicher zu Zwecken der Ablage, des Änderns, des Abrufs der Daten oder des Abrufs von Beweisdaten oder auch des Löschens abgelegter Dokumente und Daten muss in jedem Falle nachweisbar (z.B. protokolliert) über definierte Schnittstellen aus den vorgelagerten IT-Anwendungen erfolgen. Diese Aktionen/Vorgänge dürfen nur von dazu autorisierten Personen vorgenommen werden. Unberechtigte Zugriffe sind zuverlässig zu verhindern. Die Nachweisführung muss in der Middleware an geeigneter Stelle, z.B. im ArchiSafe-Modul, erfolgen.

5.1 Anwendungsfälle

5.1.1 Archivierung signierter und unsignierter Daten

(A5.1-2) Eine Ablage elektronischer Dokumente und Daten (im Weiteren auch: Archivdatenobjekte) muss zu jedem Zeitpunkt aus externen IT-Anwendungen und/oder vorgelagerten Prozessen heraus über einen sicheren Kommunikationskanal[17][18] möglich sein.

(A5.1-3) Bei der Ablage der Dokumente und Daten im ECM/Langzeitspeicher muss jedem Archivdatenobjekt ein eindeutiger und in der Regel unveränderbarer Bezeichner (Archivdatenobjekt ID, AOID) zugewiesen werden. Durch die Übergabe eines AOID-Elementes bei der Archivierung signierter und unsignierter Daten kann die AOID von der aufrufenden Anwendung vergeben werden. Im Regelfall fehlt dieses Element und die AOID wird vom aufgerufenen Modul bereitgestellt. Die AOID dient der zuverlässigen Wiederauffindbarkeit der gespeicherten Dokumente und Daten und als Schlüssel für den autorisierten Zugriff auf die im ECM/Langzeitspeicher abgelegten Archivdatenobjekte.

[15] „Löschen“ meint hier „ unwiderrufliches Löschen der Daten im behördeneigenen Langzeitspeichersystem“. Die Aussonderungen gemäß den Archivgesetzen (BArchG) bleiben davon unberührt. Dabei gilt für die Behörden gemäß. § 2 Bundesarchivgesetz bzw. gemäß den entsprechenden Landesarchivgesetzen die Anbietungspflicht gegenüber dem zuständigen öffentlichen Archiv (siehe auch [TR-ESOR-B]).

[16] Gemeint ist damit ein Archiv(system), das tatsächlich ausschließlich für die Langzeitaufbewahrung von Unterlagen genutzt wird. Die sog. „frühe Archivierung“ und die damit einhergehende Anforderung an die Änderbarkeit von Unterlagen findet hier keinen Eingang.

[17] Vgl. hierzu die Ausführungen in Kapitel 8.2.

[18] Unter einem sicheren Kommunikationskanal wird dabei ein Übertragungsweg für die Daten verstanden, der die Daten vor Abhören/Mitlesen schützt, Manipulationen zumindest erkennt, wenn nicht verhindert, und bei dem das Quell- und Zielsystem hinreichend stark authentisiert sind. Die Stärke der jeweils verwendeten Mechanismen hängt vom Schutzbedarf der übertragenen Daten ab und kann daher hier nicht pauschal angegeben werden.

Um die Ablage von Daten und Dokumenten zu verhindern, deren Format nicht für eine dauerhafte und plattformübergreifende Aufbewahrung geeignet ist, ist zusätzlich zu beachten:

(A5.1-4) Die Middleware soll vor der Ablage im ECM/Langzeitspeicher die Syntax der zur Aufbewahrung übergebenen Archivdatenobjekte auf Konformität mit den für die Archivierung durch die Nutzer und Betreiber eines Archivsystems definierten und spezifizierten Datenformaten prüfen. Bei Nichtübereinstimmung muss dann die Ablage im ECM/Langzeitspeicher abgelehnt werden.

(A5.1-5) Für die Aufbewahrung signierter Daten muss die Middleware die Möglichkeit vorsehen, die Signaturen vor der Übergabe an den ECM/Langzeitspeicher umfassend zu prüfen und die Prüfergebnisse gemeinsam mit den signierten Daten abzulegen.

(A5.1-6) Für die Beweiswerterhaltung elektronischer Signaturen müssen bei einem drohenden Verlust der Sicherheitseignung der für die Signatur verwendeten Algorithmen und zugehörigen Parameter nach § 17 SigV die signierten Daten unter Einbezug aller bereits bestehenden Signaturen erneut signiert werden. Daraus folgt:

(A5.1-7) Die Middleware muss imstande sein, eine gesetzeskonforme Signaturerneuerung (vgl. § 17 SigV) über sämtliche im ECM/Langzeitspeicher aufbewahrten, elektronisch signierten Daten und Dokumente durchzuführen.[19]

(A5.1-8) Die Lösung zur Signaturerneuerung (sowohl das Verfahren als auch das Format der Beweisdaten) muss kompatibel zum „Evidence Record Syntax“- Standard der IETF **[RFC4998]** sein. Optional kann zusätzlich auch die XML Spezifikation der Evidence Record Syntax **[RFC6283]** unterstützt werden (siehe dazu auch Anlage TR-ESOR-M.3 „ArchiSig-Modul“ dieser Richtlinie).[20]

(A5.1-9) Der dauerhafte Nachweis der Integrität unsignierter Daten und Dokumente, zumindest ab dem Zeitpunkt des Übergangs in das Archivsystem, kann durch einen elektronischen Archiv-Eingangs-Hashwert, eine elektronische Archiv-Eingangs-Signatur bzw. einen elektronischen Archiv-Eingangs-Zeitstempel zusätzlich sichergestellt werden. Die benötigte Qualität des Archiv-Eingangs-Hashwerts, der Archiv-Eingangs-Signatur bzw. des Archiv-Eingangs-Zeitstempels bestimmt sich aus dem erforderlichen oder auch beabsichtigten Beweiszweck.[21]

(A5.1-10) Die Middleware soll die Möglichkeit vorsehen, dass ein ausführlicher Prüfbericht nach **[TR-ESOR-VR]** für ein XML-basierte Archivdatenobjektes (XAIP) samt der darin enthaltenen oder zusätzlich übergebenen beweisrelevanten Daten (Signaturen, Zeitstempel, Zertifikate, Sperrlisten, OCSP-Responses etc.) und Beweisdaten (Evidence Records) angefordert werden kann.

5.1.2 Ändern von bereits archivierten Daten

(A5.1-11) Ein Ändern von bereits (beweiswerterhaltend) archivierten Dokumenten und Daten einschließlich der zugehörigen Metadaten soll möglich sein. Eine im Sinne dieser TR zulässige Änderung von Archivdatenobjekten ist

(1) das Hinzufügen von weiteren Dokumenten, Daten, Metadaten, Signaturen, Signaturprüfinformationen oder anderen technischen Beweisdaten zu Archivdatenobjekten,

(2) die Änderung von Metadaten

(3) die Löschung von Daten oder Metadaten.

[19] „sämtliche im ECM/Langzeitspeicher“ meint hier alle Daten und Dokumente, die im ECM/Langzeitspeicher aufbewahrt werden und für die der Beweiswerterhalt angestrebt und über die Nutzung der TR-ESOR-Middleware umgesetzt ist. Der ECM/Langzeitspeicher kann darüber hinaus durchaus noch weitere Datenbestände halten, für die ein Beweiswerterhalt weder notwendig noch angestrebt ist.

[20] Für die rein funktionale Konformität kann von der strengen Anforderung der Kompatibilität mit **[RFC4998]** bzw. **[RFC6283]** abgewichen werden, wenn die Lösung einerseits die gesetzeskonforme Signaturerneuerung nachweisen kann und andererseits die Lösung auf nationalen oder internationalen Standards/Normen basiert.

[21] Sofern nicht signierte elektronische Dokumente in das Archiv gegeben werden, bietet es sich an, diese beim Eingang des Dokuments in das Archiv durch einen initialen Archivzeitstempel abzusichern. Zwar kann ein solcher nicht die in der Vergangenheit unterlassene Signierung ausgleichen, jedoch kann das Vorliegen des Dokumentes zu einem bestimmten Zeitpunkt nachgewiesen werden. (siehe **[ARO 07]**, S. 108).

(A5.1-12) Änderungen im obigen Sinne dürfen nur von den berechtigten IT-Anwendungen über einen sicheren Kommunikationskanal zur TR-ESOR-Middleware ausgeführt werden. In der Regel wird dies die IT-Anwendung sein, die auch die Daten ursprünglich archiviert hat.

(A5.1-13) Beim Ändern muss ein ergänzendes XML-basiertes Archivdatenobjekt (Delta-XAIP) gemäß **[TR-ESOR-F]** übergeben werden, für das die gleichen Anforderungen an das Prüfen der Datenformate und Signaturen wie beim Archivieren (vgl. (A5.1-4), (A5.1-5) und (A5.1-9)) gelten.

(A5.1-14) Sämtliche Änderungen müssen nachvollziehbar sein. Jegliche Änderung muss daher in einer neuen Version des entsprechenden Archivdatenobjektes erfolgen. Bereits archivierte Versionen von Archivdatenobjekten dürfen nicht mehr verändert werden. Die Bildung einer neuen Version soll gemäß [TR-ESOR-F], Kap. 3.2, erfolgen.[22]

(A5.1-15) Der Beweiswert darf durch Änderungen nicht kompromittiert werden. Dies gilt für alle Versionen eines geänderten Archivdatenobjektes. Weiterhin gelten die Anforderungen (A5.1-6) und (A5.1-7) auch für alle Versionen eines Archivdatenobjektes.

(A5.1-16) Die „Ändern"-Funktion muss so implementiert sein, dass ein Löschen von Daten, Metadaten oder ganzen Archivdatenobjekten nicht möglich ist, auch nicht durch Überschreiben mit leeren Datenstrukturen.[23]

(A5.1-17) Sämtliche Änderungen sollen nachvollziehbar protokolliert werden. Soweit als möglich ist der Zeitpunkt der Änderung, der Urheber und der Inhalt der Änderung zu protokollieren.

5.1.3 Abruf (Rückgabe) archivierter Daten

Beim Abruf von archivierten Daten kann es sich sowohl um komplette Aktenstrukturen, einzelne Dokumente oder nur Elemente von Dokumenten handeln. Diese Unterscheidungen werden hier nicht getroffen, sondern werden erst bei der technischen Definition in Kapitel 7 wieder aufgegriffen.

(A5.1-18) Der Abruf (die Rückgabe) archivierter Daten muss aus den vorgelagerten IT-Anwendungen über einen sicheren Kommunikationskanal erfolgen.

(A5.1-19) Für den Abruf (die Rückgabe) archivierter Daten muss eine gültige Archivdatenobjekt ID an das Archivsystem übergeben werden.

(A5.1-20) Jede Version eines geänderten Archivdatenobjektes muss einzeln abrufbar sein und auch alle Versionen eines Archivdatenobjektes müssen abrufbar sein. Beim Abruf einer bestimmten Version muss die gesuchte Version zusätzlich über einen Versions-Identifikator, im folgenden Text VersionID genannt, identifiziert werden können.

(A5.1-21) Der Abruf archivierter Daten kann durch geeignete zusätzliche Suchfunktionen unterstützt werden (siehe dazu auch TR-ESOR-M.1, Kap. 4.6). Diese Funktionen dienen jedoch nicht dem Beweiswerterhalt und brauchen daher nicht in der TR-ESOR-Middleware implementiert werden.

(A5.1-22) Der Abruf archivierter Daten kann durch eine (konfigurierbare) automatische Integritätsprüfung der abgerufenen Daten ergänzt werden. Zusammen mit den abgerufenen Daten würde die Fachanwendung ebenfalls den Nachweis der Integrität dieser Daten erhalten. Diese Funktion dient jedoch nicht dem Beweiswerterhalt und braucht daher nicht in der TR-ESOR-Middleware implementiert werden.

(A5.1-23) Beim Abruf (Rückgabe) archivierter Daten kann angefordert werden, dass das zurückgelieferte XAIP pro Version einen entsprechenden Evidence Record im angegebenen Format enthalten soll. Dieser Evidence Record muss in einem **`xaip:evidenceRecord-Element`** in die Credential Section eingefügt werden und es muss über das **`VersionID`**-Attribut auf die entsprechende Version des XAIP verwiesen werden. Falls das **`versionManifest`** nicht selbst kryptographisch geschützt ist, muss zusätzlich ein **`unprotectedObjectPointer`** eingefügt werden, der auf den Evidence Record in der Credential Section verweist.

[22] Gemäß **[TR-ESOR-F]**, Kap. 3.2, bestimmen die protectedPointer und unprotectedPointer eines versionManifests jeweils eine Version.

[23] Das Überschreiben mit anderen Inhalten kommt dem Ändern der Inhalte gleich und muss durch die Versionierung nachvollziehbar bleiben. Insbesondere müssen im ECM/Langzeitspeichersystem auch die ursprünglichen Inhalte in der vorherigen Version erhalten bleiben.

5.1.4 Abruf von Beweisdaten

(A5.1-24) Die Middleware muss imstande sein, auf Anforderung technische Belege für die Echtheit und Unverfälschtheit von Archivdatenobjekten zu erbringen. Die Archivdatenobjekte werden dabei anhand ihrer AOID identifiziert.

(A5.1-25) Beim Abruf von Nachweisen zur Echtheit und Unverfälschtheit von Archivdatenobjekten muss die Middleware sämtliche hierfür erforderlichen elektronischen Beweisdaten[24] erstellen und zurück geben. Die elektronischen Beweisdaten müssen sämtliche Informationen enthalten, die zur Verifikation der Authentizität und Integrität der gespeicherten Daten, deren Signaturen, Zertifikaten und der Signaturerneuerungen benötigt werden.

(A5.1-26) Die Middleware muss in der Lage sein, für jede Version eines Archivdatenobjektes getrennt oder für alle Versionen eines Archivdatenobjektes zusammen die elektronischen Beweisdaten zu erstellen. Im zweiten Fall muss ein lückenloser Nachweis der Integrität und Authentizität seit dem Zeitpunkt der Archivierung möglich sein, auch wenn das Archivdatenobjekt in der Zwischenzeit kontrolliert verändert (versioniert) wurde.

(A5.1-27) Der Abruf von Beweisdaten muss über einen sicheren Kommunikationskanal erfolgen.

5.1.5 Löschen archivierter Daten

Am Ende des ‚Lebenszyklus' eines Archivdatenobjektes, d. h. in der Regel nach dem Ablauf gesetzlich vorgeschriebener Aufbewahrungsfristen, kann das Objekt aus dem Archiv gelöscht werden. Da dies ein äußerst kritischer Vorgang ist, muss durch geeignete technische und organisatorische Maßnahmen eine besonders zuverlässige und nachvollziehbare Durchführung gewährleistet werden.

HINWEIS: Nach Ablauf der vorgeschriebenen Mindestaufbewahrungsfristen dürfen Archivdatenobjekte in der öffentlichen Verwaltung erst dann aus dem ECM/Langzeitspeicher gelöscht werden, wenn diese zuvor dem zuständigen Bundes- bzw. Landesarchiv angeboten und von diesem übernommen wurden bzw. von ihm die Ermächtigung zum Löschen erteilt wurde.

(A5.1-28) Das Löschen von Daten und Dokumenten **nach Ablauf** des gesetzlich vorgeschriebenen Aufbewahrungszeitraums kann durch organisatorisch berechtigte Nutzer einer technisch berechtigten vorgelagerten IT-Anwendung angestoßen werden, oder durch einen zentralen Prozess, der diese Funktion für das gesamte Archiv ausführt und entsprechend berechtigt ist.

(A5.1-29) Das Löschen von Daten und Dokumenten **vor Ablauf** des gesetzlich vorgeschriebenen Aufbewahrungszeitraums muss durch organisatorisch berechtigte Nutzer einer technisch berechtigten vorgelagerten IT-Anwendung angestoßen werden. Der Löschauftrag muss eine Begründung für das Löschen enthalten.[25]

(A5.1-30) Bei einem Löschauftrag müssen sämtliche Daten und Metadaten sowie alle Versionen eines Archivdatenobjektes gelöscht werden.

(A5.1-31) Die Beweiskraft der im ECM/Langzeitspeicher verbleibenden Dokumente muss bei Löschen anderer Archivdatenobjekte erhalten bleiben.

(A5.1-32) Um die Nachvollziehbarkeit des Handelns zu gewährleisten, muss der Löschvorgang protokolliert werden.

5.1.6 Prüfen eines Archivdatenobjektes samt der darin enthaltenen oder zusätzlich übergebenen beweisrelevanten Daten und Beweisdaten

(A5.1-33) Die Middleware soll über eine externe Schnittstelle die Möglichkeit vorsehen, XML-basierte Archivdatenobjekte (XAIP) entgegen zu nehmen und diese samt der darin enthaltenen oder zusätzlich übergebenen beweisrelevanten Daten (Signaturen, Zeitstempel, Zertifikate, Sperrlisten, OCSP-Responses etc.) und Beweisdaten (Evidence Records) zu prüfen.

[24] „Beweisdaten" meint hier den Evidence Record gemäß **[RFC4998]** oder **[RFC6283]**.

[25] Es ist hier anzumerken, dass die entsprechenden Geschäftsanwendungen eine Funktion für vorzeitiges Löschen nur dann implementieren sollen, wenn es aus fachlicher Sicht auch die Notwendigkeit für eine solche Funktion gibt.

(A5.1-34) Die Middleware soll in diesem Zusammenhang auch die Möglichkeit vorsehen, dass ein ausführlicher Prüfbericht **[TR-ESOR-VR]** bei der Übergabe eines XML-basierten Archivdatenobjektes (XAIP) samt der darin enthaltenen oder zusätzlich übergebenen beweisrelevanten Daten (Signaturen, Zeitstempel, Zertifikate, Sperrlisten, OCSP-Responses etc.) und Beweisdaten (Evidence Records) angefordert werden kann.

5.2 Organisatorische Anforderungen

Die organisatorischen Anforderungen legen die nicht-technischen Bedingungen fest, die vorzugsweise bereits vor oder bei der Einführung einer Middleware für den Beweiswerterhalt geschaffen werden müssen.

Dieses Kapitel versteht sich als Hinweis an die Benutzer einer solchen Middleware und legt keine formalen Kriterien fest.

5.2.1 Die Einrichtung der Middleware zum Beweiswerterhalt

Die gesetzlichen Vertreter eines Unternehmens oder einer Behörde tragen die Verantwortung dafür, dass im Rahmen der IT-Strategie ein langfristiges Konzept zum Einsatz von Archivierungsverfahren und dem Beweiswerterhalt aufgestellt und mit dem IT-Sicherheitskonzept abgestimmt wird.

Zum Erhalt des Beweiswertes muss über den technischen oder organisatorischen Prozess der Archivierung gewährleistet sein, dass alle relevanten Dokumente und Daten durch die TR-ESOR-Middleware erfasst werden, für welche der Beweiswerterhalt notwendig ist oder festgelegt wurde.

Ferner sind Festlegungen zur Integration der TR-ESOR-Middleware in die IT-Infrastruktur, zur Identifikation, Auswahl und Verwaltung der Daten und Dokumente mit Anforderungen an den Beweiswerterhalt sowie zur periodischen Überprüfung der erzielten Beweiskraft zu treffen.

Sämtliche durch die TR-ESOR-Middleware erstellten Protokolle sind gemäß der jeweils relevanten rechtlichen und/oder betrieblichen Vorschriften aufzubewahren.

5.2.2 Anforderungen an die Einsatzumgebung

Eine wesentliche Voraussetzung für den Beweiswerterhalt ist ein angemessenes Problembewusstsein der gesetzlichen Vertreter und der Mitarbeiter für mögliche Risiken. Dafür sind die beteiligten Mitarbeiter auf der Grundlage einer aussagekräftigen und vollständigen Verfahrensdokumentation ausreichend zu schulen und einzuweisen.

Die Beschreibung zum Prozess des Beweiswerterhaltes ist Teil der Archivierungsprozesse und muss damit verbindlich festgelegt werden. Die Verfahrens-Dokumentation dient zum Verständnis und ist damit ebenfalls aufbewahrungspflichtig.

Insbesondere sind die folgenden Bereiche bezüglich des Beweiswerterhaltes im Rahmen der Ablauforganisation zu regeln:

- Identifikation der Dokumente und Daten, für die der Beweiswert erhalten werden soll
- Festlegung des Archivierungszeitpunktes (Belegstatus);
- Festlegung der Archivierungsprozesse inkl. der Prozesse zum Beweiswerterhalt;
- zulässige/gewünschte Archivdatenformate und
- Festlegung von Aufgaben und Verantwortlichkeiten bezüglich der Prozesse zum Beweiswerterhalt.

In Organisationsanweisungen ist der Regelbetrieb der TR-ESOR-Middleware festzulegen, etwa die Aufgaben und Befugnisse von Administratoren oder Regelungen zum Change-Management.

5.2.3 Datenschutz, Datensicherheit und Vertraulichkeit

Jegliche Art der Aufbewahrung elektronischer Informationen unterliegt zwangsläufig allgemeinen und gegebenenfalls auch bereichsspezifischen datenschutzrechtlichen Regelungen und Anforderungen. Daraus folgt:

Die für die Beweiswerterhaltung notwendige Verarbeitung von Daten und Dokumenten muss den gesetzlichen und bereichsspezifischen Anforderungen an den Daten- und Geheimnisschutz genügen. Insbesondere die Verarbeitung und Speicherung personenbezogener Daten im Zusammenhang mit Signaturen und den zugehörigen Verifikationsdaten muss auf ein Minimum begrenzt werden. Dabei muss zugleich sichergestellt sein, dass Unbefugte unter keinen Umständen Zugang zu personenbezogenen oder anderweitig dem Geheimnisschutz unterliegenden Daten erhalten.

Spezielle, den Daten- und Geheimnisschutz betreffende Anforderungen müssen mit einem wirtschaftlich vertretbaren Aufwand erfüllbar sein. Es muss daher auch der Beweiswert von verschlüsselten Dokumenten und Daten erhalten werden können.

Soweit für bestimmte Zwecke, z. B. die Transformation von Daten, Signaturen des (technischen) Archivars benötigt werden, sollen diese auch unter einem Pseudonym möglich sein.

6. Abgeleitete technische Anforderungen

Der folgende Abschnitt beschreibt abgeleitete und vornehmlich technische Anforderungen, die bei der Einrichtung und dem Betrieb einer zu dieser Richtlinie konformen Middleware zum Beweiswerterhalt zu erfüllen sind.

6.1 Systemtechnische Anforderungen

(A6.1-1) Um proprietäre, d. h. produkt- oder herstellerabhängige Lösungen zu vermeiden, muss die Integrierbarkeit der Middleware in bestehende und auch in Zukunft neu beschaffte Informationssysteme sowie die Interoperabilität, Verfügbarkeit und Verkehrsfähigkeit der verwendeten Austauschformate für die Nutzdaten, die Metainformationen, Signaturen, Zeitstempel und Signaturprüfinformationen (Verifikationsdaten) mindestens für die Dauer gesetzlich vorgeschriebener Aufbewahrungsfristen gewährleistet werden können.

(A6.1-2) Die für den Beweiswerterhalt signierter elektronischer Dokumente eingesetzten Verfahren und technischen Lösungen dürfen die weitere Verwendbarkeit der elektronischen Dokumente für unterschiedliche Anwendungszwecke und in unterschiedlichen Anwendungssystemen (Fachverfahren) nicht beeinträchtigen. Durch Verfahren und technische Lösungen der Erneuerung von Signaturen dürfen insbesondere keine Behinderungen entstehen für:

- den Austausch von Dokumenten zwischen Anwendungssystemen,
- den Wechsel von Datenformaten in Anwendungssystemen,[26]
- den Austausch von Anwendungssystemen oder -komponenten.

(A6.1-3) Die TR-ESOR-Middlware soll in der Lage sein, getrennte Mandanten zu verwalten. Dies bedeutet insbesondere eine strikte (logische) Separierung der im ECM/Langzeitspeicher abgelegten Archivdatenobjekte aber auch eine Trennung der für den Beweiswerterhalt relevanten Daten (Hashbäume).

(A6.1-4) Technische Lösungen für die Middleware müssen eine sichere Administration und Konfiguration unterstützen.

6.2 Empfohlene Dokumentformate

Dieser Abschnitt beschäftigt sich mit den Formaten, die von den Fachanwendungen für die eigentlichen Nutzdaten – die Primärinformationen – verwendet werden können bzw. sollen. Der nächste Abschnitt hingegen beschreibt Datenstrukturen, die für die tatsächliche Speicherung im Archivsystem empfohlen werden und die Nutzdaten sowie die Metadaten und weitere Verwaltungsinformationen enthalten.

(A6.2-1) Im Interesse der dauerhaften Verfügbarkeit und Verkehrsfähigkeit der zu archivierenden Dokumente und Daten sollen ausschließlich Datenformate eingesetzt werden, die eine plattform- und herstellerunabhängige Archivierung in langfristig verkehrsfähiger Form ermöglichen.

Das Organisationskonzept elektronische Verwaltungsarbeit sowie DOMEA-Organisationskonzept 2.1[27] und die Standards und Architekturen für E-Government-Anwendungen (**[SAGA-5]**)[28] empfehlen, ebenso wie die von der Europäischen Kommission geförderte Anforderungsspezifikation für die elektronische Schriftgutverwaltung („Model Requirements for the Management of Electronic Records -

[26] Gemeint ist, dass das Anwendungssystem das Datenformat wechseln kann und auch mit diesem neuen Datenformat die Mechanismen des Beweiswerterhaltes funktionieren. Konkreter: die Funktionen zur Signaturerneuerung dürfen nicht auf spezielle Datenformate eingeschränkt sein.
Es wird in dieser TR davon ausgegangen, dass einmal archivierte Daten von einem Formatwechsel nicht betroffen sind und daher eine Transformation von (signierten) Daten nicht notwendig ist. Falls dies doch der Fall sein sollte, sollte auf die Ergebnisse des TransiDoc Projektes zurückgegriffen werden, siehe http://www.transidoc.de.

[27] Siehe http://www.verwaltung-innovativ.de/DE/E_Government/orgkonzept_everwaltung/orgkonzept_everwaltung_node.html

[28] Siehe http://www.cio.bund.de/Web/DE/Architekturen-und-Standards/SAGA/saga_node.html

Moreq10[29]), für die langfristige Ablage von elektronischem Schriftgut nur wenige und einheitliche Datenformate zu benutzen.

Kapitel 4 von **[TR-ESOR-F]** führt im Detail die für diese Technische Richtlinie empfohlenen Formate auf.

6.3 Empfohlene Austausch- und Speicherformate

Dieser Abschnitt beschreibt Datenstrukturen, die für die tatsächliche Speicherung von Nutzdaten (siehe vorheriger Abschnitt) sowie Metadaten und weiteren Verwaltungsinformationen im Archivsystem empfohlen werden.

Dem Programm von Bund, Ländern und Kommunen für die Standardisierung des Datenaustausches in und mit der öffentlichen Verwaltung[30] folgend, wird für die Langzeitspeicherung und insbesondere für die beweiswerterhaltende Langzeitspeicherung folgendes empfohlen:

(A6.3-1) Den Empfehlungen nationaler (**[SAGA-5]**[31], **[XÖV]**[32], **[ArchiSafe]**[33]) und internationaler (**[Moreq10]**[34], **[OAIS]**, **[OASIS]**[35]) Standardisierungsinitiativen folgend, sollen Inhaltsdaten, Metadaten und Verifikationsdaten[36] langfristig aufzubewahrender Daten und Dokumente in einem abgeschlossenen und selbst-erklärenden Archivdatenobjekt auf der Basis von XML (kurz **XAIP** für: **X**ML formatted **A**rchival **I**nformation **P**ackage[37]) und einer formalisierten Dokumenttypbeschreibung in XML-Syntax (XML-Schema) abgelegt und verwaltet werden können.[38]

(A6.3-2) Ergänzend zu Anforderung (A6.3-1) müssen bei einer Abfrage oder einem Export der aufzubewahrenden Daten und Dokumente diese in einem abgeschlossenen und selbst-erklärenden Austauschformat auf der Basis von XML und gemäß einer formalisierten Dokumenttypbeschreibung in XML-Syntax (XML-Schema) zurück geliefert werden – unabhängig vom tatsächlich verwendeten Speicherformat im ECM/Langzeitspeicher.

Die Aufbewahrung oder zumindest der Austausch von Daten und Dokumenten in einem selbst-erklärenden Archivdatenobjekt auf Basis von XML unterstützt nicht nur die Plattform- und Produktneutralität, sondern auch die beweiswerterhaltende Migration archivierter Daten.[39]

---

29 Siehe http://www.moreq.info/

30 Die gemeinsam von Bund, Ländern und Kommunen verabredete Standardisierung des Datenaustausches soll die automatisierte und medienbruchfreie Datenverbindung zwischen Kommunen, Landes- und Bundesbehörden und ihren Kunden ermöglichen. Ziel dieses Vorhabens im Rahmen des Aktionsplans Deutschland Online ist die Schaffung eines gemeinsamen, durch Bund, Länder und Kommunen getragenen Gesamtkonzepts für die Entwicklung und den bundesweiten Einsatz von einheitlichen fachlichen Datenformaten und Datenstrukturen (fachliche Standards) und technischer Schnittstellen zum elektronischen Austausch von Geschäfts- und Verwaltungsnachrichten innerhalb und mit der öffentlichen Verwaltung auf der Grundlage von XML. Mehr dazu unter http://www.it-planungsrat.de/SharedDocs/Downloads/DE/Projekte/Aktionsplan%202009.html

31 siehe http://www.cio.bund.de/Web/DE/Architekturen-und-Standards/SAGA/saga_node.html und speziell http://www.cio.bund.de/SharedDocs/Publikationen/DE/Architekturen-und-Standards/SAGA/saga_modul_tech_spez_de_bund_5_0_download.pdf , Kap. 13, S. 74ff

32 siehe http://www.it-planungsrat.de/SharedDocs/Downloads/DE/Projekte/Aktionsplan%202009.html

33 siehe http://www.archisafe.de und speziell http://www.archisafe.de/s/c/bBTTJx6K/ArchiSafe_Dokumente/Fachkonzept_V11.pdf , Kap. 5.3, S. 86ff

34 siehe http://www.moreq.info/

35 siehe http://docs.oasis-open.org/

36 Es handelt sich dabei um Signaturen und zugehörige Zertifikate sowie um die Prüfinformationen zu beiden. Im Fall einer Migration in ein neues Archivsystem können hier auch die ERS-Beweisdaten aus dem alten Archivsystem enthalten sein.

37 Die Bezeichnung folgt der Notation des Referenzmodells für Offene Archivinformationssysteme (OAIS) der Nationalen Luft- und Raumfahrtbehörde der USA. Mehr dazu unter http://public.ccsds.org/publications/archive/650x0b1.pdf

38 Es ist anzumerken, dass sich das Volumen von binären Inhaltsdaten um ca. 36% vergrößert, wenn sie für das Einbetten in ein XML-Objekt BASE64-codiert werden. Damit erhöht sich auch die Wahrscheinlichkeit, dass die Objekte eine Größe erreichen bzw. überschreiten, die eine automatische Verarbeitung verhindern.

39 Auf syntaktischer Ebene unterstützt XML als textbasierte Meta-Auszeichnungssprache nicht nur die Beschreibung, sondern vor allem die automatisierte Darstellung, Manipulation und Verarbeitung logisch strukturierter Daten und zeichnet sich darüber hinaus durch eine gute Erweiterbarkeit und eine große Flexibilität aus. Auf semantischer Ebene unterstützen Regeln und Strukturdefinitionen in XML-Syntax (XML-Schema) die Abbildung strukturierter Inhaltsmodelle. XML-Schemata erlauben nicht nur die formale und maschinenlesbare Beschreibung eines für den Datenaustausch erlaubten XML-Vokabulars, sondern darüber hinaus den Aufbau komplexer Datenstrukturen und die Formulierung von Verarbeitungsanweisungen.

Eine ausführliche Darstellung der Syntax und Semantik eines geeigneten XAIP-Dokuments findet sich in Kapitel 3 von Anlage **[TR-ESOR-F]** „Formate“ dieser Richtlinie.[40]

(A6.3-3) Den Empfehlungen nationaler (**[SAGA-5]**, **[XÖV]**[41], **[ArchiSafe]**) und internationaler (**[Moreq10]**[42], **[OAIS]**, **[OASIS]**) Standardisierungsinitiativen folgend, sollen die Schnittstellen für den Datenaustausch zwischen den Komponenten und Bestandteilen einer zu dieser Richtlinie konformen Middleware sowie zu externen Komponenten (z.B. den Fachanwendungen und dem ECM/Langzeitspeicher) grundsätzlich über XML und entsprechende Schemadefinitionen oder vergleichbare offene, standardisierte Datenformate beschrieben und realisiert werden.

In der Anlage **[TR-ESOR-E]** dieser Technischen Richtlinie sind beispielhaft die Schnittstellen der IT-Referenzarchitektur, die weiter unten eingeführt wird, entsprechend beschrieben.

6.4 IT-Infrastruktur

Die nachfolgend genannten technischen Sicherungsmaßnahmen für die TR-ESOR-Middleware und des gesamten Archivsystems dienen dem Beweiswerterhalt und umfassen physische Sicherungsmaßnahmen, logische Zugriffskontrollen sowie Datensicherungs- und Auslagerungsverfahren für den Regel- und den Notbetrieb.

Dieses Kapitel versteht sich als Hinweis an die Benutzer/Betreiber einer solchen Middleware und legt keine formalen Kriterien fest.

Der ECM/Langzeitspeicher stellt die Datensenke des elektronischen Archivs dar. Die archivierten Daten und Dokumente sind hier sicher gespeichert, inklusive aller für die langfristige Aufbewahrung und Verfügbarkeit nötigen Verkehrs- und Verwaltungsinformationen.

Es kann sich um einen Speicher handeln, der sowohl die Archivdatenobjekte als auch die Verwaltungsinformationen und die Daten zur Integritäts- und Authentizitätssicherung enthält (u.a. die Hashbäume). Die beiden Datenarten können auch in unterschiedlichen Speichern abgelegt werden.

Es kann sich um eine beliebige Art von Speichersystem (SAN, NAS, Festplattensystem mit beliebigem Dateisystem, relationale Datenbank, objektorientierte Datenbank, XML-fähige Datenbank, Archivsystem, etc.) handeln, solange dieses System alle anderen Anforderungen erfüllt.

Das Speichersystem kann physisch in mehrere Speicher aufgeteilt sein; auch in Speicher mit unterschiedlichen Schnittstellen, Kapazitäten, physischen Merkmalen wie z. B. Medien, Anbindungsart (Latenzzeit, Bandbreite), Standorten, etc.

Durch physikalische Sicherungsmaßnahmen müssen die IT-Infrastruktur zur beweiswerterhaltenden Archivierung und die entsprechenden Speichermedien vor Verlust, Zerstörung sowie unberechtigter Veränderung geschützt werden.

Neben den Zugriffsschutzmechanismen der vorgelagerten IT-Anwendungen muss zum Schutz der archivierten Daten und Dokumente auch im ECM/Langzeitspeicher ein geeignetes Berechtigungskonzept implementiert werden.

Das Gesamtsystem muss geeignete Maßnahmen vorsehen und implementieren, die eine unzulässige Manipulation oder den unzulässigen Austausch von Komponenten oder Modulen zuverlässig verhindern.

Von den Speichermedien können Sicherungs-Kopien angefertigt und an einem räumlich vom Archivierungssystem getrennten Standort ausgelagert werden.

Zur Sicherung der Lesbarkeit der Speichermedien über die gesamte Aufbewahrungsfrist sind vom Medientyp abhängige Kontrollen und Maßnahmen vorzusehen, wie etwa der regelmäßige Test auf Lesbarkeit der Speichermedien.

---

[40] Anlage **[TR-ESOR-F]** dieser Technischen Richtlinie beschreibt grundsätzliche syntaktische und semantische Strukturen für ein Archivdatenobjekt, elektronische Datenformate für die langfristige Aufbewahrung von Nutzdaten und Metadaten sowie Strukturen, Formate und Algorithmen für die Erzeugung und Interpretation kryptographischer Daten, die für den langfristigen Nachweis der Integrität und Authentizität elektronischer Dokumente (Objekte) geeignet sind.

[41] siehe http://www.deutschland-online.de/Standardisierung

[42] siehe http://www.moreq.info/

Bei redundant ausgelegten Archivierungssystemen (inkl. der Middleware) ist zu testen, ob die Funktionsübergabe bei Ausfall eines Teilsystems ordnungsgemäß erfolgt und ob bei Wiederanlauf des ausgefallenen Systems ein ordnungsgemäßer Abgleich der Daten zwischen den Systemen erfolgt.

Zur Sicherstellung des Betriebs des Archivierungssystems (inkl. der Middleware) müssen Maßnahmen, die beim Ausfall eines Archivierungssystems oder der Middleware ergriffen werden müssen, in einem Notfallkonzept festgehalten werden. Im Fall einer ungeplanten Unterbrechung ist nach Wiederanlauf sicherzustellen, dass die Konsistenz der Daten gewährleistet ist.

Dies ist insbesondere für die Daten der TR-ESOR-Middleware von Bedeutung. Bei einer auch nur kleinen Inkonsistenz kann der Nachweis der Integrität und Authentizität der archivierten Daten und Dokumente nicht mehr zuverlässig erbracht werden.

6.5 IT-Anwendungen beim Einsatz von Archivierungsverfahren

Neben Anforderungen an die IT-Infrastruktur und natürlich die TR-ESOR-Middleware müssen auch diverse Anforderungen an die vorgelagerten Fachanwendungen gestellt werden.

Dieses Kapitel versteht sich als Empfehlung an die Benutzer/Betreiber einer TR-ESOR-Middleware und legt keine formalen Kriterien fest.

Bei den zur Archivierung eingesetzten IT-Anwendungen handelt es sich im Regelfall um Softwaresysteme, die an die organisationsspezifischen Besonderheiten und Archivierungsanforderungen anzupassen sind. Eine Anwendung im Sinn dieser Richtlinie kann aus mehreren Einzelkomponenten oder Programmen bestehen. Es ist nicht notwendigerweise ein monolithisches Programm oder ein einzelnes System. In den vorgelagerten Anwendungssystemen werden die später zu archivierenden Dokumente und Daten erzeugt und bearbeitet. Bis zum Zeitpunkt der Archivierung werden sie dabei auf den zu diesen Anwendungssystemen gehörenden Datenspeichern vorgehalten.

Die zur Archivierung eingesetzten IT-Anwendungen oder IT-Services sollen folgende Mindestanforderungen erfüllen:

- Die Erzeugung der zu archivierenden Daten in definierten langfristig verkehrsfähigen und standardisierten Datenformaten (z. B. PDF oder XML, vgl. Kapitel 6.2).
- Falls aus fachlicher Sicht, d. h. durch Rechtsvorschriften oder sonstige Regelungen, geboten, muss die Anwendung bzw. der Anwender imstande sein, die zu archivierenden Nutzdaten vor der Ablage im Archivsystem mit einer elektronischen Signatur in einer durch die Rechtsvorschriften oder sonstigen Regelungen geforderten Qualität zu versehen.[43]

  Um die Gültigkeit der Signatur über die Dauer der gesetzlich vorgeschriebenen Aufbewahrungsfristen nachweisen zu können, wird empfohlen, mit der Ausführung der Signatur zugleich sämtliche für den Gültigkeitsnachweis der Signatur erforderlichen Verifikationsdaten zu beschaffen und gemeinsam mit den Signaturdaten innerhalb des Datenspeichers der Geschäftsanwendung abzulegen. Der Umfang der erforderlichen Verifikationsdaten bestimmt sich vornehmlich aus dem Ziel der erforderlichen Nachweissicherung (siehe dazu auch Kapitel 4.1).[43, 44, 45]
- Weiterhin muss die Anwendung eine Funktion zum Prüfen von Signaturen anbieten. Auch von solchen Signaturen, die nicht durch die Anwendung selbst erstellt wurde (z.B. wenn die Anwendung zwischenzeitlich durch andere abgelöst wurde).[43, 46]

[43] Es können dazu natürlich die von der TR-ESOR-Middleware angebotenen kryptographischen Funktionen genutzt werden.

[44] Verifikationsdaten müssen nach **[SFD 06]** nicht notwendigerweise beschafft und aufbewahrt werden, wenn sie vom Zertifizierungsdiensteanbieter mindestens solange vorgehalten werden, wie das signierte Dokument aufbewahrt werden muss.

[45] Hintergrund dieser Forderung ist, dass zwischen dem Zeitpunkt der Signaturerstellung und der eigentlichen Archivierung eine beträchtliche Zeitspanne liegen kann. Das Archivsystem prüft zwar laut Empfehlung die enthaltenen Signaturen bei Archiveingang, kann die Gültigkeit der dafür genutzten Zertifikate zum Signaturerstellungszeitpunkt jedoch nur dann prüfen, wenn die Zertifizierungsdiensteanbieter entsprechende Informationen noch vorhalten. Ist dies nicht (mehr) der Fall, kann die enthaltene Signatur nicht geprüft werden und die Beweiskraft der Daten ist quasi verloren.

[46] Für die Prüfung von Signaturen kann die Anwendung auch Funktionen der TR-ESOR Middleware nutzen.

- Für die Anzeige von qualifiziert signierten elektronischen Daten und Dokumenten soll die Anwendung oder die Anwendungsumgebung eine bestätigte vertrauenswürdige Anzeigekomponente (Trusted Viewer) zur Verfügung stellen. Die Bestätigung muss durch eine anerkannte Bestätigungsstelle gemäß §18 SigG erfolgen.
- Die IT-Anwendungen müssen Schnittstellenfunktionalitäten zur Ablage der zu archivierenden Dokumente und Daten besitzen.
- Die IT-Anwendungen müssen Schnittstellenfunktionalitäten zum Abruf und Löschen[47] bereits archivierter Dokumente und Daten sowie zum Abruf der technischen Beweisdaten zum Nachweis der Authentizität und Integrität von archivierten Informationen auf der Basis der vom Archivsystem bzw. der Middleware zurückgegebenen Archivdatenobjekt-IDs (AOID) und ggf. der VersionIDs besitzen und können Schnittstellenfunktionen zum Ändern bereits archivierter Daten und zum Prüfen des Archivdatenobjektes samt der darin enthaltenen oder zusätzlich übergebenen beweisrelevanten Daten und Beweisdaten besitzen.

  Der Löschvorgang wird dabei nicht vom Archivsystem initiiert, sondern nur protokolliert. Ein vollständiges und explizites Löschen (im Sinne einer unwiederbringlichen Vernichtung) von archivierten Objekten muss auch vor Ablauf der bei der Archivierung übergebenen Aufbewahrungsfrist möglich sein.
- Die Fähigkeit zur Protokollierung durchgeführter Archivoperationen.
- Die Verwaltung und Zuordnung der Archivdatenobjekt-IDs (AOID's) zu den zugehörigen Geschäftsprozessen und den Ablageorten der archivierten Daten[48].
- Die IT-Anwendungen müssen über sichere Zugriffsschutzmechanismen auf der Grundlage eines zuverlässigen und konfigurierbaren Berechtigungssystems verfügen. Die Anwendung oder die Anwendungsumgebung muss daher auch über ein eigenes zuverlässiges und sicheres Identifikations- und Authentisierungssystem verfügen. Es ist organisatorisch sicher zu stellen, dass nur die autorisierten Benutzer auch tatsächlich die notwendigen Berechtigungen innerhalb der Anwendung erhalten bzw. besitzen.

[47] Im Falle einer (Bundes-)Behörde stößt die IT-Anwendung nach Abgabe des Schriftguts an die Archivbehörde das Löschen des Schriftgutes im Langzeitspeichersystem an.

[48] Bei der Migration von Fachanwendungen ist selbstverständlich auch die Migration der AOIDs zu berücksichtigen. Nur so kann die neue Fachanwendung später auf die archivierten Daten der Altanwendung zugreifen.

7. IT-Architektur

Die IT-Architektur einer zu dieser Richtlinie konformen Middleware zum Beweiswerterhalt muss die in dieser technischen Richtlinie aufgeführten Anforderungen (insbesondere die geforderte Funktionalität aus den Kapiteln 5 und 6 und die Anforderungen aus Kapitel 4) zuverlässig umsetzen.

In diesem Abschnitt wird eine hersteller- und produktunabhängige (funktionale) IT-Referenzarchitektur empfohlen, die alle aufgeführten Anforderungen erfüllt und daher die Basis für eine entsprechende Umsetzung sein kann. Auf der Grundlage dieser IT-Referenzarchitektur werden systemlogische Komponenten und Schnittstellen grob identifiziert und beschrieben. Die weitere, ausführliche Spezifikation der anhand der IT-Referenzarchitektur identifizierten logischen Komponenten und Schnittstellen erfolgt in den Anlagen zu dieser Technischen Richtlinie.

HINWEIS: Es sei darauf hingewiesen, dass die hier beschriebene Aufteilung der Funktionen auf die Module der IT-Referenzarchitektur nicht verpflichtend ist. Eine zu dieser Technischen Richtlinie konforme Middleware muss jedoch alle Funktionen in der erforderlichen Qualität und auf dem notwendigen Sicherheitsniveau anbieten.

7.1 Empfohlene IT-Referenzarchitektur

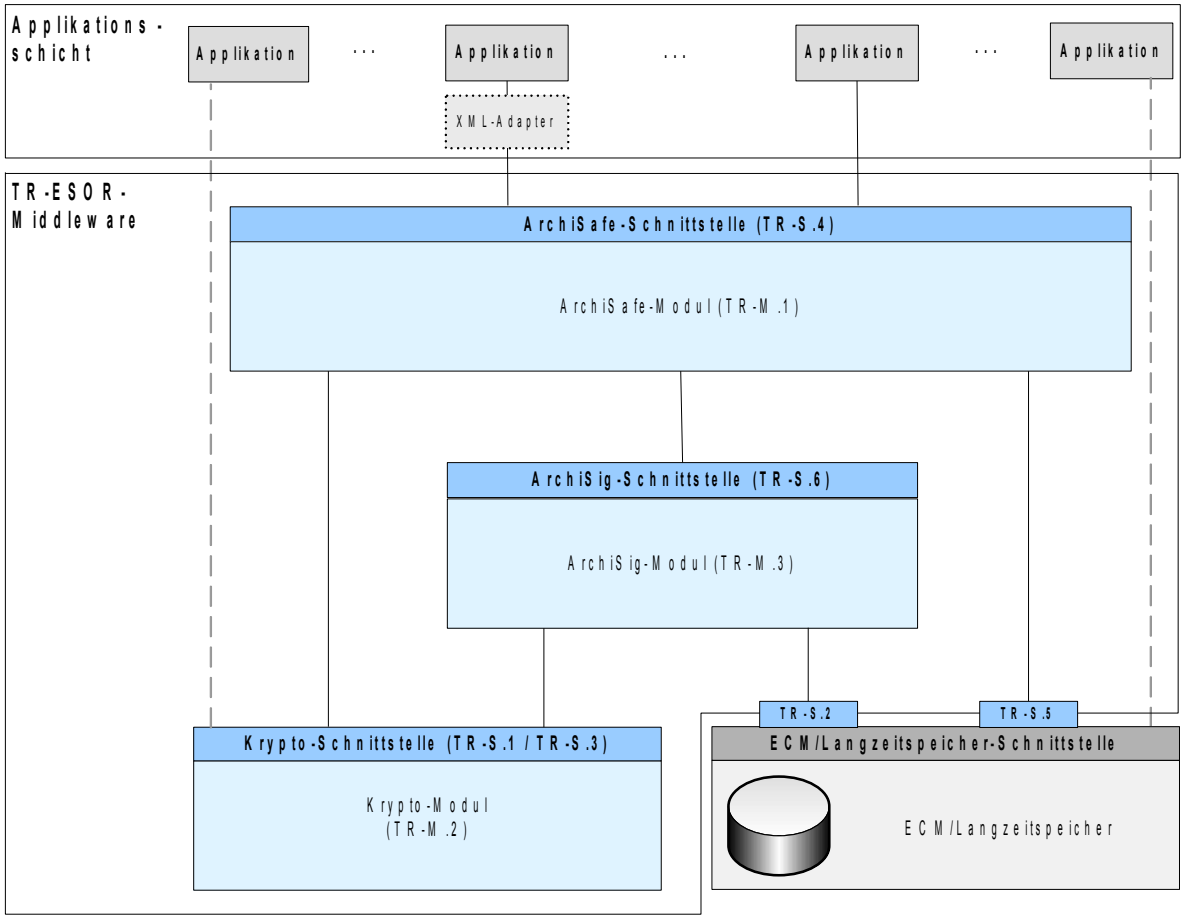


Abbildung 3: Referenzarchitektur Übersicht

Die empfohlene IT-Referenzarchitektur ist in Abb. 3 dargestellt und besteht im Wesentlichen aus den nachfolgend grob beschriebenen logischen Komponenten und Schnittstellen. Diese werden in Anhängen zur TR weiter detailliert. Die Grafik zeigt zudem die externen Komponenten und Systeme an, die das Bild vervollständigen.

Externe Komponenten und Systeme

- Vorgelagerte Anwendungen, die die Middleware und damit indirekt den ECM/Langzeitspeicher für die langfristige und beweiswerterhaltende Ablage elektronischer Daten und Dokumente nutzen.
- Ein ECM/Langzeitspeicher zur eigentlichen Datenspeicherung. Dies umfasst sowohl die Speicherung der eigentlichen Archivdatenobjekte als auch aller von der Middleware zusätzlich erzeugten und verwalteten Daten zur Beweiswertsicherung. Die Ablage der durch das ArchiSig-Modul erzeugten kryptographischen Beweisdaten soll dabei zumindest logisch getrennt in einem eigenen Speicherbereich oder besser physikalisch getrennt in einer eigenen Speichereinheit erfolgen.
- Zertifizierungs- und Zeitstempeldiensteanbieter (nicht abgebildet), die entsprechende Dienste anbieten. Es kann sich dabei um eigene Organisationen handeln, die ihre Dienste über das Internet anbieten, aber z.B. auch um selbstbetriebene zugekaufte Geräte, die eine entsprechende Zertifizierung und Zulassung besitzen.

Module und Schnittstellen der TR-ESOR-Middleware

- Das ArchiSafe-Modul (**[TR-ESOR-M.1]**), das für eine Entkopplung von Anwendungssystemen und ECM/Langzeitspeicher sowie für eine effektive und zuverlässige Zugriffskontrolle auf den ECM/Langzeitspeicher sorgen soll.
- Ein Krypto-Modul (**[TR-ESOR-M.2]**), das alle erforderlichen Funktionen zur Erstellung (optional) und Prüfung elektronischer Signaturen, zur Nachprüfung elektronischer Zertifikate und zum Einholen qualifizierter Zeitstempel für die Middleware sowie Schnittstellen zu Zertifizierungs- und Zeitstempeldiensteanbietern zur Verfügung stellt.[49]
- Ein ArchiSig-Modul (**[TR-ESOR-M.3]**), das die erforderlichen Funktionen für das Erneuern der Signaturen sowie das Erstellen kryptographischer Nachweise (bspw. einen Evidence Record gem. **[RFC 4998]** bzw. **[RFC6283]**[50]) für die Integrität archivierter Datenobjekte bereithält.
- Die Schnittstellen zwischen diesen Modulen, u. a.
  - die Schnittstelle zwischen den vorgelagerten Anwendungen und dem ArchiSafe-Modul. Der angedeutete anwendungsspezifische XML-Adapter bildet die Archivschnittstelle in eine anwendungsspezifische Schnittstelle ab.
  - Die Schnittstellen zwischen den internen und externen Komponenten der Middleware (benannt nach dem Schema **[TR-ESOR-S]**).

Der mit „TR-ESOR Middleware“ bezeichnete Rahmen in 3 zeigt den inhaltlichen Umfang dieser Technischen Richtlinie auf. Weder die Fachanwendungen, der ECM/Langzeitspeicher noch der Zertifizierungsdiensteanbieter (nicht abgebildet) sind Gegenstand dieser Technischen Richtlinie.

7.2 Alternative Architekturen

Insofern alle in den Kapiteln 4 bis 6 beschriebenen Anforderungen an die Middleware und den Beweiswerterhalt auch mit einer anderen IT-Architektur bzw. einer angepassten IT-Referenzarchitektur erfüllt werden, ist eine derartige IT-Architektur prinzipiell auch zulässig. Die weitere Beschreibung der Technischen Richtlinie, insbesondere die detaillierteren Beschreibungen in den Anhängen, bezieht sich jedoch immer auf die oben aufgeführte und empfohlene Referenzarchitektur.

[49] Dieses Modul kann auch Funktionen für das Ver- und Entschlüsseln von Archivdaten übernehmen, sollten dieses im konkreten Einsatz notwendig sein. Da dies für den reinen Beweiswerterhalt nicht notwendig ist, wird in der TR auf diesen Aspekt nicht weiter eingegangen.

[50] **[RFC4998]** muss, **[RFC6283]** kann zusätzlich unterstützt werden.

7.3 Komponenten und Module

Es folgt eine kurze Beschreibung der verschiedenen Komponenten und Module der Middleware aus der IT-Referenzarchitektur, weitergehende Beschreibungen und Detaillierungen erfolgen in den Anlagen (siehe dazu auch Kapitel 10 „Anlagen“).

7.3.1 ArchiSafe-Modul[51] (TR-ESOR-M.1)

Das ArchiSafe-Modul ist zunächst ein einheitliches und sicheres Gateway, welches den Zugriff von Geschäftsanwendungen auf den ECM/Langzeitspeicher kontrolliert.

Ziel ist die Realisierung einer strikten logischen Trennung der vorgelagerten Anwendungssysteme (den IT-Fachanwendungen) von den eigentlichen ECM/Langzeitspeichersystemen.

Unter dem Gesichtspunkt des Beweiswerterhaltes entfaltet das ArchiSafe-Modul jedoch erst dann seine Hauptfunktion, wenn ein XML-Austausch- bzw. -Speicherformat (vgl. Kapitel 6.3) genutzt wird. Das ArchiSafe-Modul ist nur in diesem Fall in der Lage, das von der Fachanwendung an die Middleware übergebene Archivdatenobjekt auf syntaktische Korrektheit zu prüfen. Des weiteren ist ein standardisiertes, sprich Archivprodukt[52]-unabhängiges ArchiSafe-Module auch nur in diesem Fall in der Lage, eingebundene Signaturen, Zertifikate, etc. prüfen zu lassen und die Ergebnisse in das Archivdatenobjekt noch vor der eigentlichen Archivierung einzutragen. Die Empfehlungen aus Kapitel 6.3 werden daher an dieser Stelle nochmals betont.

Die sicherheitstechnischen Anforderungen an ein solches ArchiSafe-Modul wurden produktunabhängig in einem Schutzprofil (Protection Profile) nach Common Criteria [CC] spezifiziert [ACMPP].

(A7.3-1) Jeder (schreibende/ändernde/löschende) Zugriff der Fachanwendungen auf den ECM/Langzeitspeicher unter Nutzung der in Kapitel 5 aufgeführten Archiv-Funktionen muss über das ArchiSafe-Modul erfolgen, eine andere Zugriffsmöglichkeit auf die Middleware oder den ECM/Langzeitspeicher durch die Fachanwendungen muss durch geeignete technische Maßnahmen ausgeschlossen werden.

Es ist jedoch durchaus zulässig, dass der ECM/Langzeitspeicher selbst Schnittstellen z.B. zum Ablegen oder Ändern anbietet, die auch von den Fachanwendungen direkt genutzt werden – allerdings dann nicht mehr mit dem Fokus des Beweiswerterhaltes und insbesondere nicht für das Ändern von (signierten) Unterlagen, die zuvor über das ArchiSafe-Modul abgelegt (gespeichert) wurden; ein reines Lesen wäre hingegen zulässig. Der ECM/Langzeitspeicher darf auch mehr Funktionen anbieten als die Middleware. Hier sind direkte Zugriffe auf den ECM/Langzeitspeicher zulässig.[53]

(A7.3-2) Das ArchiSafe-Modul muss den Anforderungen des zum Zeitpunkt der Zertifizierung gültigen und durch das Bundesamt für Sicherheit in der Informationstechnik (BSI) veröffentlichten Schutzprofils genügen. Der Nachweis darüber ist durch eine erfolgreiche Zertifizierung gemäß dieses Schutzprofils durch ein anerkanntes Common Criteria Schema (vorzugsweise durch das Deutsche) zu erbringen.

7.3.2 Krypto-Modul (TR-ESOR-M.2)

Das Krypto-Modul stellt verschiedene kryptographische Funktionen, die für den Beweiswerterhalt benötigt werden, bereit.

Dies umfasst im Wesentlichen kryptographische Verfahren, die für das Erzeugen und Verifizieren von elektronischen Signaturen benötigt werden sowie Mechanismen zum Einholen und Verifizieren von qualifizierten Zeitstempeln (vgl. auch Fußnote 49 auf Seite 39).

(A7.3-3) Das Krypto-Modul kann in verschiedenen Ausprägungen implementiert sein:

---

[51] Der Name „ArchiSafe“ bezieht sich auf das E-Government Projekt „ArchiSafe – rechts- und revisionssichere Langzeitspeicherung elektronischer Dokumente“ der Physikalisch-Technischen Bundesanstalt im Jahre 2005, das im Rahmen der E-Government Programms „BundOnline 2005“ gefördert wurde. Ziel des Projektes war die Spezifikation und Umsetzung einer service-orientierten informationstechnischen Lösung für die rechts- und revisionssichere Langzeitspeicherung elektronischer Dokumente (mehr dazu unter: http://www.archisafe.de).

[52] Gemeint ist hier ein ECM-System für die eigentliche Archivierung (Speicherung)

[53] Es wird darauf hingewiesen, dass das ArchiSafe-Konzept eine komplette logische Entkopplung von Fachanwendung und ECM/Langzeitspeicher vorsieht.

- als eigenständiges Hardware-Modul, das über spezielle Hardwareschnittstellen von anderen Modulen der Middleware angesprochen wird,
- als Mischung aus Hardware und Software; andere Module der Middleware greifen auf die Funktionen dieses Moduls ausschließlich über die angebotenen Softwareschnittstellen zu, oder
- sämtliche kryptographischen Funktionen sind komplett in Software implementiert. Das Krypto-Modul wird als Bibliothek oder Service eingebunden und von anderen Software-Paketen der Middleware genutzt.

(A7.3-4) Das Krypto-Modul muss die Anforderungen an eine Signaturanwendungskomponente nach § 17 Abs. 2 Satz 2 SigG erfüllen, da qualifizierte elektronische Signaturen mittels dieses Moduls auf ihre Gültigkeit hin überprüft werden müssen.

(A7.3-5) Ist das Modul imstande und dafür vorgesehen, qualifizierte elektronische Signaturen selbst zu erstellen, z. B. im Rahmen der Erzeugung von Zeitstempeln, müssen die dafür mit dem Modul eingesetzten Soft- oder Hardwareeinheiten die Anforderungen an eine sichere Signaturerstellungseinheit nach § 17 Abs. 1 SigG erfüllen.

(A7.3-6) Da sich die für gesetzeskonforme elektronische Signaturen zulässigen Algorithmen und Parameter zum Erzeugen von Signaturschlüsseln, zum Hashen oder zum Erzeugen und Prüfen qualifizierter elektronischer Signaturen gemäß Abschnitt I Nr. 2 SigV ändern können, muss für die Verifikation ein schneller und unkomplizierter Austausch nicht mehr sicherheitsgeeigneter oder sicherheitsgefährdeter Algorithmen und Parameter des Krypto-Moduls durch sicherheitsgeeignete Algorithmen und Parameter jederzeit möglich sein.[54]

(A7.3-7) Falls die Schnittstellen des Krypto-Moduls oder das gesamte Krypto-Modul in Software implementiert sind, sollen sie die Anforderungen der Technischen Richtlinie TR-03112 (eCard-API Framework) des BSI in der aktuell gültigen Fassung erfüllen.

7.3.3 ArchiSig-Modul[55] (TR-ESOR-M.3)

Das ArchiSig-Modul stellt vornehmlich Funktionen für den Erhalt und die Erneuerung der Beweiskraft elektronischer Signaturen sowie für die Integrität der archivierten Datenobjekte und das Erstellen von Beweisdaten (engl. Evidence Record) gemäß RFC4998/RFC6283[56] bereit (ausführlicher in der Anlage TR-ESOR-M.3 dieser Richtlinie).

Für alle kryptographischen Funktionen greift das ArchiSig-Modul auf das bereits vorgestellte Krypto-Modul zurück. Das ArchiSig-Modul muss also selbst keine kryptographischen Funktionen implementieren.

(A7.3-8) Das ArchiSig-Modul soll Modul-Charakter besitzen und damit leicht austauschbar sein.

(A7.3-9) Das ArchiSig-Modul soll in der Lage sein, in mehreren Instanzen parallel zu arbeiten, insbesondere was den Fall der Neusignatur bzw. die Erneuerung der Hashwerte aller vorhandenen Archivdatenobjekte im ECM/Langzeitspeicher angeht. In diesem Fall bedarf es jedoch noch eines steuernden Objektes, das die Arbeiten der einzelnen ArchiSig-Instanzen steuert.

(A7.3-10) Die einzelnen Instanzen sollen sowohl auf einer als auch auf unterschiedlichen Maschinen laufen können, um sowohl die Bandbreite als auch die Rechenleistung voll ausnutzen zu können.

---

[54] Ist das Krypto-Modul auch in der Lage, qualifizierte elektronische Signaturen zu erzeugen, muss auch für diese Funktion ein Austausch von Hash- und Signaturalgorithmen entsprechend möglich sein.

[55] Der Name „ArchiSig“ bezieht sich auf das Verbundprojekt „ArchiSig – Beweiskräftige und sichere Langzeitarchivierung digital signierter Dokumente“, das in den Jahren 2001 bis 2003 vom Bundesministerium für Wirtschaft und Arbeit im Rahmen des Programms „VERNET - Sichere und verlässliche Transaktionen in offenen Kommunikationsnetzen“ gefördert wurde. Ziel des Projektes war die Entwicklung einer gesetzeskonformen, wirtschaftlichen und leistungsfähigen informationstechnischen Lösung für eine beweiskräftige und sichere Langzeitarchivierung digital signierter Dokumente (mehr dazu unter: http://www.uni-kassel.de/fb07/fileadmin/datas/fb07/5-Institute/IWR/Ro%C3%9Fnagel/projekte_abgeschlossen/projekt_ArchiSig.pdf sowie https://www.teletrust.de/fileadmin/files/ag8_isis-mtt-langzeitarchiv.pdf)

[56] **[RFC4998]** muss, **[RFC6283]** kann zusätzlich unterstützt werden.

(A7.3-11) Das ArchiSig-Modul muss auch während der kompletten Neusignierung bzw. der Erneuerung der Hashwerte aller vorhandenen Archivdatenobjekte im ECM/Langzeitspeicher die laufenden Anfragen aus dem regulären Betrieb in akzeptabler Zeit bedienen können.

7.3.4 XML-Adapter zur Anbindung von Geschäftsanwendungen an die Middleware

Die **optionalen** XML-Adapter sind anwendungsspezifische oder anwendungstypspezifische Datenkonverter, die aus den (proprietären) Daten und Dokumenten der vorgelagerten Anwendungen ein einheitliches (XML basiertes) Datenformat für die Ablage erzeugen, respektive umgekehrt, den Import der XML-Daten in die vorgelagerten IT-Anwendungen unterstützen. Dies kann auch die Konvertierung von proprietären Datenformaten in offene Datenformate (z.B. PDF/A) beinhalten. Eine Ablage von offenen Datenformaten im Vergleich zu proprietären hat auf lange Sicht gesehen den Vorteil, dass ein Lesbarmachen auf jeden Fall möglich ist. Andernfalls besteht die Gefahr, dass die vorgesehene Export-Funktion (vgl. Kapitel 7.4.3) in der Zukunft gar nicht mehr in der Lage ist, eine entsprechende Konvertierung durchzuführen.

Über die XML-Adapter wird auch die standardisierte Kommunikation mit dem ArchiSafe-Modul geführt. Der XML-Adapter übernimmt dabei die Rolle eines standardisierten Konnektors.

(A7.3-12) Grundsätzlich kann ein solcher Adapter in verschiedenen Ausprägungen implementiert werden:

- als (fester) Bestandteil der Anwendung, d. h. als anwendungsintegrierte Archivierungsschnittstelle,
- als eigenständiger Dienst, der Datenstrukturen und Kommunikationsprotokoll in die standardisierten Formate des elektronischen Archivs überführt,
- als (fester) (mandantenfähiger) Bestandteil des ArchiSafe-Moduls.

Insbesondere bei der letztgenannten Variante ist jedoch sicherzustellen, dass z. B. Blockaden des XML-Adapters durch fehlerhafte Anwendungen oder sicherheitstechnische Fehlfunktionen eines einzelnen XML-Adapters nicht zu einer generellen Fehlfunktion des gesamten ArchiSafe-Moduls führt. Daher ist diese Variante (XML-Adapter ist architektonischer Bestandteil des ArchiSafe-Moduls) in der Regel nicht zu empfehlen.

Bei der zweiten Möglichkeit (eigenständiger Dienst) kann man die Möglichkeit in Betracht ziehen, mehrere gleichartige Anwendungen (z. B. mehrere Module eines SAP-Systems oder mehrere SAP-Systeme unterschiedlicher Mandanten eines Archivierungsdienstleisters) über genau einen XML-Adapter in das Archiv zu führen. Hierbei ist jedoch insbesondere aus Sicherheitssicht sicherzustellen, dass weder eine anwendungsübergreifende Kommunikation über den XML-Adapter möglich ist, noch dass eine Anwendung auf die archivierten Unterlagen einer anderen Anwendung zugreifen kann.

Die erste Möglichkeit (Bestandteil der Anwendung) kann sich wiederum in zwei Alternativen aufspalten:

- Inhärenter Teil der Anwendung. Dies bedeutet, die Geschäftsanwendung implementiert die Archivschnittstellen direkt.
- Modul für die Geschäftsanwendung. Dies bedeutet, die Archivschnittstellen sind in einem eigenständigen Modul (im Sinn einer Bibliothek) implementiert, das von der Geschäftsanwendung direkt genutzt wird. Die Geschäftsanwendung braucht also, um das Archiv nutzen zu können, selbst nicht angepasst zu werden.

(A7.3-13) Der XML-Adapter soll (sofern er vorhanden ist und genutzt wird), je nach Gesamtarchitektur des Archivs und Bedarf, mandantenfähig sein.

(A7.3-14) Der XML-Adapter muss (sofern er vorhanden ist und genutzt wird) in der Lage sein, alle Funktionen des ArchiSafe-Moduls, an das er angeschlossen ist, korrekt zu nutzen und eine sichere und zuverlässige Kommunikation in beide Richtungen (Anwendung und ArchiSafe) korrekt abzubilden.

7.3.5 Die Kommunikationskanäle und Schnittstellen

Die IT-Referenzarchitektur beinhaltet verschiedene Schnittstellen innerhalb der Middleware und auch zu den externen Komponenten (ausführlicher in der Anlage **[TR-ESOR-S]**).

Im Wesentlichen sind dabei zu unterscheiden die

- externen Schnittstellen: zu den Anwendungen, zum ECM/Langzeitspeicher oder zu den Zertifizierungsdiensteanbietern
- internen Schnittstellen: z. B. zwischen dem ArchiSafe-Modul und dem Krypto-Modul

Nicht enthalten in 3 sind notwendige administrative Schnittstellen zu den einzelnen Komponenten. Diese sind in der Regel produktspezifisch ausgeprägt (z. B. als textbasiertes interaktives Interface, als Konfigurationsdatei, als web-basierte Administrationsschnittstelle, etc.) und spielen für diese Technische Richtlinie nur eine untergeordnete Rolle.[57]

(A7.3-15) Schnittstellen zur Administration der gesamten Middleware oder einzelner Komponenten dürfen nur ausdrücklich berechtigten Personen zugänglich sein.

(A7.3-16) Schnittstellen zur Administration der gesamten Middleware oder einzelner Komponenten dürfen nicht die Sicherheitseigenschaften der Middleware oder einzelner Komponenten sowie Integrität und Authentizität der gespeicherten Daten und Dokumente kompromittieren.

7.4 Zusammenspiel der Komponenten

Der folgende Abschnitt veranschaulicht das Zusammenspiel der Komponenten in der dargestellten IT-Referenzarchitektur an den wesentlichen Anwendungsfällen (siehe 3), der Ablage elektronischer Daten, dem Ändern bereits archivierter Daten, dem Abruf archivierter Daten und technischer Beweisdaten, dem Löschen archivierter Daten und dem Prüfen von Beweisdaten und beweisrelevanten Daten.

Bei allen dargestellten Abläufen wird davon ausgegangen, dass als Speicherformat XAIP verwendet wird. Abweichungen, die sich aus dem Verwenden eines anderen Formates ergeben, sind hier nicht erwähnt.

7.4.1 Ablage elektronischer Unterlagen

Für die beweiswerterhaltende Archivierung elektronischer Unterlagen ist auf der Grundlage der IT-Referenzarchitektur folgender grundsätzlicher Ablauf vorgesehen (siehe 4). Dabei wird aus Gründen der Übersichtlichkeit hier nur der positive Fall angegeben.

An allen Entscheidungsknoten sind jedoch entsprechende Fehlerabfragen und Verzweigungen im Prozess vorzusehen. Im Fehlerfall muss der Prozess mit einer aussagekräftigen und verständlichen Fehlermeldung abgebrochen werden.

Zudem wird vorausgesetzt, dass jedem Funktionsaufruf und Transport von Daten über eine der in der IT-Referenzarchitektur benannten Schnittstellen eine erfolgreiche technische Authentisierung auf der Vermittlungs-, Transport- oder Anwendungsschicht zwischen den beteiligten Modulen vorausgegangen ist.

Schritt 1: **OPTIONAL** - Die zu archivierenden Inhaltsdaten werden innerhalb der Geschäftsan-wendung mit einer elektronischen Signatur versehen. Je nach Datenformat kann die Signatur dabei direkt in die Nutzdaten eingebettet sein oder als eigenständiges Objekt (z. B. als Datei) existieren.

Alternativ und ebenfalls optional – Die in einem anderen TR-ESOR-System bereits abgelegten Daten werden von dort zusammen mit ihren beweisrelevanten Daten und

[57] Neben den in den Anlagen zu diesem Dokument beschriebenen funktionalen und technischen Aspekten der Schnittstellen (Daten-, Aufrufformate, etc.) sind an dieser Stelle insbesondere auch Aspekte der Verfügbarkeit und Performance zu beachten. Daraus ergeben sich weitere projekt- und produktspezifische Detailarchitekturfragestellungen, wie beispielsweise nach der geeigneten Kommunikationsinfrastruktur (z. B. synchrone oder asynchrone Kommunikationsbeziehungen, Implementierung von Datenpuffern und Warteschlangen, usw.). Diese lassen sich nicht pauschal beantworten, sondern nur unter Berücksichtigung des Volumens der zu erwartenden Archivanfragen und der Größe der zu speichernden Archivdatenobjekte sowie der Anzahl und der Standorte der anzuschließenden Anwendungen.

Beweisdaten exportiert mit dem Ziel, in diesem (neuen) TR-ESOR-System weiter aufbewahrt zu werden. In diesem Fall würde man mit Schritt 4 fortsetzen.

Schritt 2: Die (signierten) Inhaltsdaten und Metainformationen[58] werden dem XML-Adapter der Geschäftsanwendung übergeben. Das hier verwendete Format hängt im Wesentlichen von der Geschäftsanwendung ab und kann daher nicht näher spezifiziert werden.

Schritt 3: Der XML-Adapter erzeugt aus den (signierten) Inhaltsdaten und den Metainformationen ein Archivdatenobjekt in XML-Syntax (XAIP-Dokument) gemäß eines definierten XML-Schemas (siehe auch Kapitel 6.3 und Anlage **[TR-ESOR-F]**).

In die Metadaten ist mindestens das Format der Nutzdaten und ein eindeutiges Identifizierungsmerkmal der zuständigen Fachanwendung einzutragen. Soweit das Ende des Aufbewahrungszeitraums bereits bekannt ist, soll dieses ebenfalls eingetragen werden. Ansonsten ist dieses Datum nachträglich über die „Ändern“ Funktion (vgl. Kapitel 7.4.2) einzubringen.

Schritt 4: Der XML-Adapter übergibt das Archivdatenobjekt an das ArchiSafe-Modul zur Archivierung über die Schnittstelle TR-ESOR-S.4.

Schritt 5: Das ArchiSafe-Modul überprüft die Zugriffsberechtigung der Geschäftsanwendung auf der Grundlage des im Aufrufs übergebenen Identifizierungsmerkmals und die Syntax des übergebenen XML-Dokuments auf Basis eines im ArchiSafe-Moduls hinterlegten und autorisierten XML-Schemas. Das XML-Schema ist kunden- und einsatzspezifisch.

Schritt 6: Beweisrelevante Daten und technische Beweisdaten sollen über die Schnittstelle TR-ESOR-S.1 an das Krypto-Modul zur Prüfung übergeben werden.

Falls das ArchiSafe-Modul so konfiguriert ist, dass enthaltene oder zusätzlich übergebene Beweisdaten geprüft werden müssen und solche Beweisdaten vorhanden sind/übergeben wurden, muss das ArchiSafe-Modul die Beweisdaten zur Verifikation an das Krypto-Modul über die Schnittstelle TR-ESOR-S.1 übergeben.

Schritt 7: Das Krypto-Modul verifiziert die mathematische Richtigkeit der Signaturen.

Schritt 8: Das Krypto-Modul validiert die Gültigkeit der zugeordneten Zertifikate über eine Abfrage beim Zertifikatsaussteller. Dazu muss ein Zertifizierungspfad bis hin zu einer, aus Sicht des Prüfenden, vertrauenswürdigen Zertifizierungsinstanz gebildet und geprüft werden.

Schritt 9: Der Zertifizierungsdiensteanbieter liefert eine Bestätigung der Gültigkeit der angefragten Zertifikate als OCSP- oder SCVP-Antwort zurück (siehe Anlage **[TR-ESOR-M.2]**).

Schritt 10: Das Krypto-Modul validiert die vorhandenen Beweisdaten und beweisrelevanten Daten, bis hin zu einer Wurzel.

Schritt 11: Das Krypto-Modul liefert je nach Fall die Ergebnisse der Signaturprüfung und einen ausführlichen Prüfbericht für die Beweisdatenverifikation in Form eines `Verification-Report`-Elementes (siehe **[TR-ESOR-VR]**) dem ArchiSafe-Modul über die Schnittstelle TR-ESOR-S.1 zurück.

Schritt 12: Die Prüfergebnisse werden vom ArchiSafe-Modul unverändert in das Archivdatenobjekt in die *CredentialSection* des XAIP-Dokuments eingetragen.

[58] Signaturen der Nutzdaten, die nicht direkt in die Nutzdaten eingebettet sind, werden hier unter dem Begriff Metadaten subsumiert. Der XML-Adapter behandelt die Signaturen jedoch etwas anders und speichert sie vor allem an einer anderen Stelle im XAIP – in der CredentialSection.

Schritt 13: Das angereicherte Archivdatenobjekt wird über die Schnittstelle TR-ESOR-S.6 dem ArchiSig-Modul zum Aufbau des initialen Archiv-Zeitstempels übergeben (siehe auch Anlage **[TR-ESOR-M.3]**)

Schritt 14: Das ArchiSig-Modul erzeugt eine neue AOID für dieses Archivdatenobjekt – falls die AOID von der aufrufenden Anwendung nicht übergeben wurde - oder lässt vom ECM/Langzeitspeicher eine AOID erzeugen und trägt diese AOID als Attribut in das XAIP-Dokument ein (siehe Anlage **[TR-ESOR-F]**).

Schritt 15: Das ArchiSig-Modul trägt im *PackageHeader* des XAIP den Kanonisierungsalgorithmus ein, mit dem das ArchiSig-Modul das XAIP anschließend kanonisiert.

Schritt 16: Unmittelbar darauf lässt das ArchiSig-Modul über die Schnittstelle TR-ESOR-S.3 vom Krypto-Modul einen Hashwert über das Archivdatenobjekt erzeugen. Details finden sich in Anhang **[TR-ESOR-M.3]**, Kapitel 2.4.1.

Schritt 17: Das Krypto-Modul liefert den Hashwert über die Schnittstelle TR-ESOR-S.3 an das ArchiSig-Modul zurück.

Schritt 18: Das ArchiSig-Modul speichert diesen Hashwert zusammen mit der AOID im Hashbaum ab (siehe Anlage **[TR-ESOR-M.3]**).

Schritt 19: Das ArchiSig-Modul übergibt das Archivdatenobjekt über die Schnittstelle TR-ESOR-S.2 an den ECM/Langzeitspeicher zur Persistierung.

Schritt 20: Der ECM/Langzeitspeicher quittiert die erfolgreiche Speicherung, z. B. durch Rückgabe der AOID.

Schritt 21: Das ArchiSig-Modul gibt an das ArchiSafe-Modul über die Schnittstelle TR-ESOR-S.6 die AOID als positive Rückmeldung zurück.

Schritt 22: Das ArchiSafe-Modul gibt die AOID über die Schnittstelle TR-ESOR-S.4 als Bestätigung für die erfolgreiche Archivierung an den aufrufenden XML-Adapter zurück.

Schritt 23: Der XML-Adapter liefert die AOID an die Geschäftsanwendung.

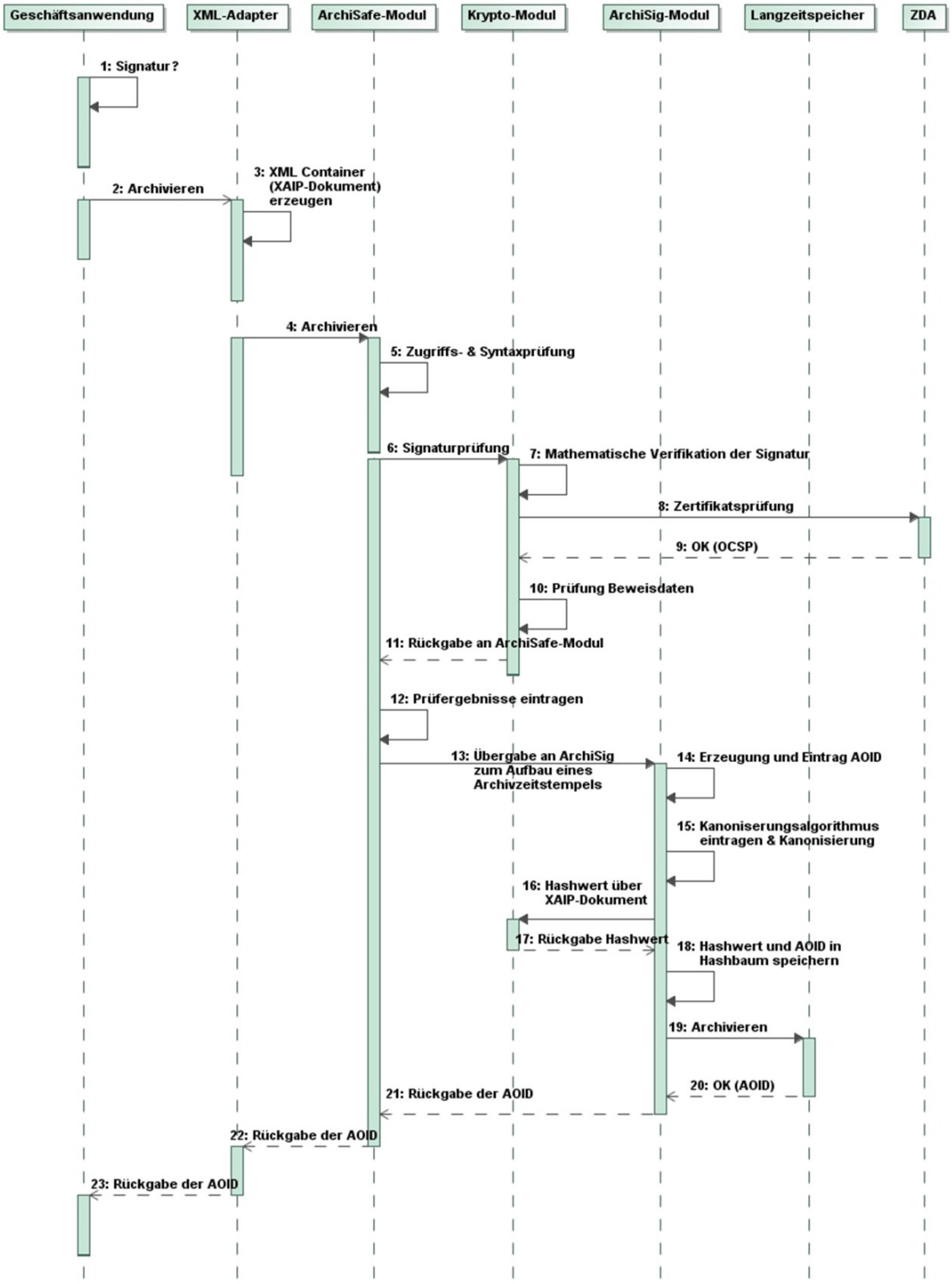


Abbildung 4: Schematischer Ablauf der Archivierung

Zu einem späteren Zeitpunkt erstellt das ArchiSig-Modul über die in letzter Zeit erzeugten Hashwerte einen initialen Archivzeitstempel und fügt diesen zusammen mit den Hashwerten dem Hashbaum hinzu. Dieser Prozess muss nicht unmittelbar bei der Archivierung erfolgen, sondern wird in der Regel periodisch und automatisiert angestoßen. Details finden sich im Anhang **[TR-ESOR-M.3]**.

7.4.2 Ändern archivierter Daten

Für die beweiswerterhaltende Änderung bereits archivierter elektronischer Unterlagen ist auf der Grundlage der IT-Referenzarchitektur folgender grundsätzlicher Ablauf vorgesehen (siehe 5). Dabei wird aus Gründen der Übersichtlichkeit hier nur der positive Fall angegeben.

An allen Entscheidungsknoten sind jedoch entsprechende Fehlerabfragen und Verzweigungen im Prozess vorzusehen. Im Fehlerfalle muss der Prozess mit einer aussagekräftigen und verständlichen Fehlermeldung abgebrochen werden.

Zudem wird vorausgesetzt, dass jedem Funktionsaufruf und Transport von Daten über eine der in der IT-Referenzarchitektur benannten Schnittstellen eine erfolgreiche technische Authentisierung auf der Vermittlungs-, Transport- oder Anwendungsschicht zwischen den beteiligten Modulen vorausgegangen ist.

Schritt 1: Auf Ebene der Geschäftsanwendung wird entschieden, welche Änderungen an einem bereits archivierten Datenobjekt vorgenommen werden bzw. welche weiteren Nutzdaten und/oder Metadaten einem bereits archivierten Datenobjekt hinzugefügt werden sollen.

Schritt 2: **OPTIONAL** - Die zusätzlich zu archivierenden Inhaltsdaten werden innerhalb der Geschäftsanwendung mit einer elektronischen Signatur versehen.
Je nach Datenformat kann die Signatur dabei direkt in die Nutzdaten eingebettet sein oder als eigenständiges Objekt (z. B. als Datei) existieren.

Schritt 3: Die zusätzlich zu archivierenden Inhaltsdaten[59] werden dem XML-Adapter samt der entsprechenden AOID von der Geschäftsanwendung übergeben. Der XML-Adapter erzeugt ein ergänzendes XML-basiertes Archivdatenobjekt (Delta-XAIP) gemäß **[TR-ESOR-F]**.

Schritt 4: Der XML-Adapter erzeugt aus den (signierten) Inhaltsdaten und/oder den Metainformationen ein Archivdatenobjekt in XML-Syntax gemäß eines definierten XML-Schemas, das ausschließlich die Änderungen enthält (Delta-XML-Dokument).

Schritt 5: Der XML-Adapter übergibt das Delta-XML-Dokument an das ArchiSafe-Modul zur Archivierung über die Schnittstelle TR-ESOR-S.4.

Schritt 6: Das ArchiSafe-Modul überprüft die Zugriffsberechtigung der Geschäftsanwendung und die Syntax des übergebenen XML-Dokuments auf Basis eines im ArchiSafe-Moduls hinterlegten und autorisierten XML-Schemas.

Schritt 7: Das ArchiSafe-Modul soll die signierten Daten und deren Signaturen zur Signaturprüfung an das Krypto-Modul über die Schnittstelle TR-ESOR-S.1 übergeben.

Schritt 8: Das Krypto-Modul verifiziert die mathematische Richtigkeit der Signaturen.

Schritt 9: Das Krypto-Modul validiert die Gültigkeit der zugeordneten Zertifikate über eine Abfrage beim Zertifikatsaussteller (i.d.R. ein Zertifizierungsdiensteanbieter). Dazu muss ein Zertifizierungspfad bis hin zu einer, aus Sicht des Prüfenden, vertrauenswürdigen Zertifizierungsinstanz gebildet und geprüft werden.

Schritt 10: Der Zertifizierungsdiensteanbieter liefert eine Bestätigung der Gültigkeit der angefragten Zertifikate als OCSP- oder SCVP-Antwort zurück (siehe Anlage **[TR-ESOR-M.2]**).

Schritt 11: Das Krypto-Modul liefert dem ArchiSafe-Modul über die Schnittstelle TR-ESOR-S.1 die Ergebnisse zurück.

[59] Signaturen der Nutzdaten, die nicht direkt in die Nutzdaten eingebettet sind, werden hier unter dem Begriff Metadaten subsumiert. Der XML-Adapter behandelt die Signaturen jedoch etwas anders und speichert sie vor allen an einer anderen Stelle im XAIP – in der CredentialSection.

Schritt 12: Die Prüfergebnisse werden vom ArchiSafe-Modul unverändert in das Delta-Archivdatenobjekt in die *CredentialSection* eingetragen.

Schritt 13: Das ArchiSafe-Modul ruft das bereits archivierte Archivdatenobjekt über die Schnittstelle TR-ESOR-S.5 aus dem ECM/Langzeitspeicher ab. Identifiziert wird das Archivdatenobjekt dabei über die AOID, die bei einer Änderungs-Funktion nicht verändert wird.

Schritt 14: Der ECM/Langzeitspeicher liefert das Archivdatenobjekt an das ArchiSafe-Modul zurück. Der ECM/Langzeitspeicher liefert dabei immer das komplette Archivdatenobjekt zurück. Dieses enthält ggf. bereits mehrere Versionen.

Schritt 15: Das ArchiSafe-Modul fügt die Änderungen aus dem Delta-Archivdatenobjekt in das vom ECM/Langzeitpeicher abgefragte Archivdatenobjekte ein und erzeugt dabei automatisch eine neue Version mit einer neuen VersionID. Wesentlich ist hier, dass das Manifest der neuen Version alle hinzugefügten Datenelemente auflistet, bei geänderten Daten auf die neueste Version des entsprechenden Datenelementes zeigt und die Datenelemente nicht mehr aufführt, die in dieser Version nicht mehr enthalten sind (weil sie durch andere/neuere Datenelemente ersetzt wurden) (Näheres siehe **[TR-ESOR-M.1]** und **[TR-ESOR-F]**).

Schritt 16: Das geänderte komplette Archivdatenobjekt wird über die Schnittstelle TR-ESOR-S.6 dem ArchiSig-Modul zum Aufbau des Archiv-Zeitstempels übergeben (siehe auch Anlage **[TR-ESOR-M.3]**)

Schritt 17: Das ArchiSig-Modul kanonisiert das Archivdatenobjekt mit dem Algorithmus, der im *PackageHeader* angegeben ist und übergibt es anschließend über die Schnittstelle TR-ESOR-S.3 an das Krypto-Modul, um über dieses Archivdatenobjekt einen Hashwert zu erzeugen.

Schritt 18: Das Krypto-Modul liefert den Hashwert über die Schnittstelle TR-ESOR-S.3 an das ArchiSig-Modul zurück.

Schritt 19: Das ArchiSig-Modul speichert diesen Hashwert zusammen mit der AOID und der VersionID im Hashbaum ab (siehe Anlage TR-ESOR-M.3).

Schritt 20: Das ArchiSig-Modul übergibt das Archivdatenobjekt über die Schnittstelle TR-ESOR-S.2 an den ECM/Langzeitspeicher zur Persistierung.

Schritt 21: Der ECM/Langzeitspeicher quittiert die erfolgreiche Speicherung.

Schritt 22: Das ArchiSig-Modul gibt an das ArchiSafe-Modul über die Schnittstelle TR-ESOR-S.6 die VersionID als positive Rückmeldung zurück.

Schritt 23: Das ArchiSafe-Modul gibt die VersionID über die Schnittstelle TR-ESOR-S.4 als Bestätigung für die erfolgreiche Änderung an den aufrufenden XML-Adapter zurück.

Schritt 24: Der XML-Adapter liefert die VersionID an die Geschäftsanwendung.

Zu einem späteren Zeitpunkt erstellt das ArchiSig-Modul über die in letzter Zeit erzeugten Hashwerte einen initialen Archivzeitstempel und fügt diesen zusammen mit den Hashwerten dem Hashbaum hinzu. Dieser Prozess muss nicht unmittelbar bei der Archivierung erfolgen, sondern wird in der Regel periodisch und automatisiert angestoßen. Details finden sich im Anhang **[TR-ESOR-M.3]**.

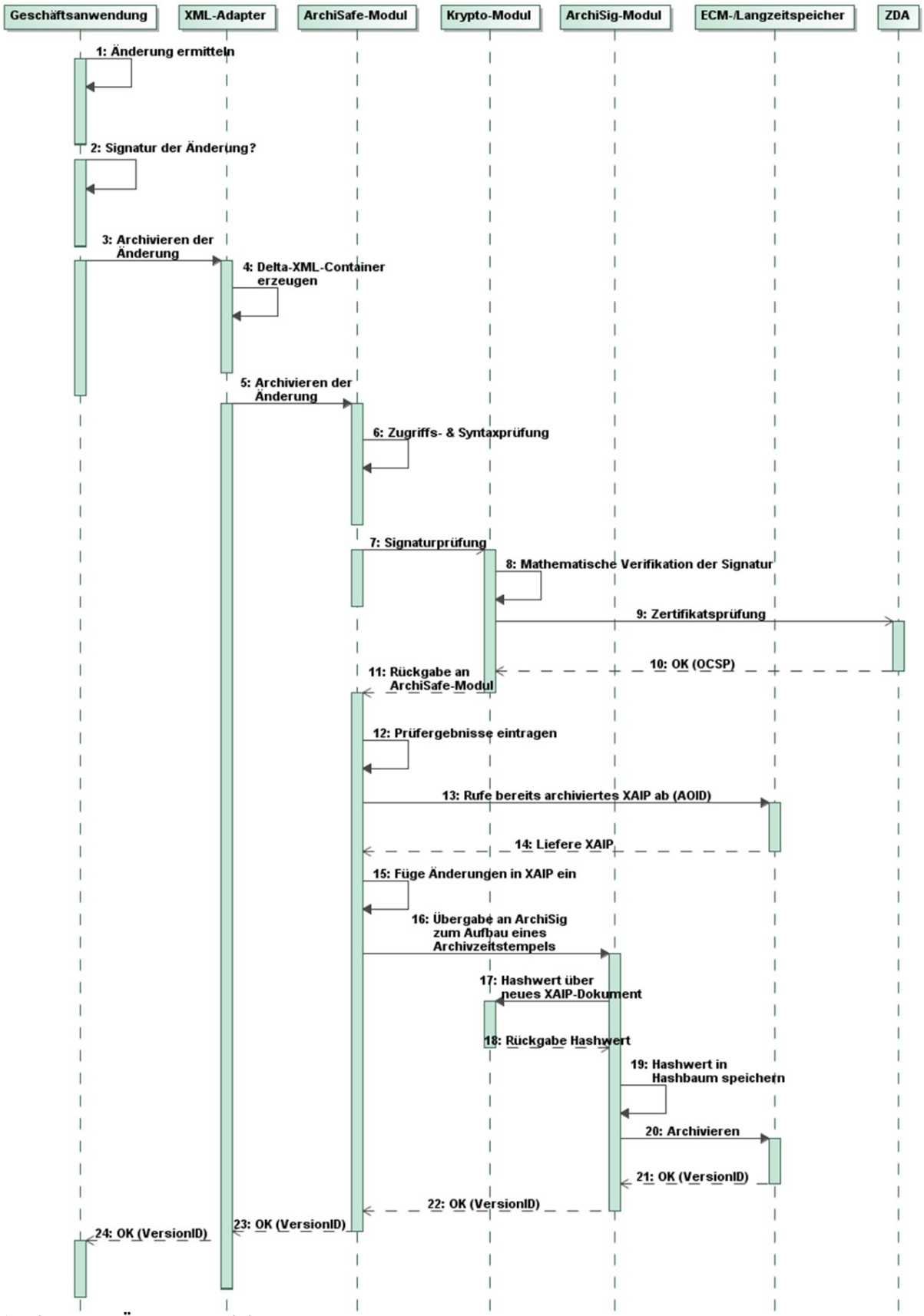


Abbildung 5: Ändern archivierter Daten

7.4.3 Abfrage archivierter Daten

Für den Abruf archivierter elektronischer Unterlagen ist auf der Grundlage der IT-Referenzarchitektur folgender grundsätzlicher Ablauf vorgesehen (siehe auch Abbildung 6). Auch hier wird vom positiven Fall ausgegangen, die notwendigen Fehlerprüfungen und Verzweigungen sind aus Gründen der Übersichtlichkeit im Ablauf nicht berücksichtigt.

An allen Entscheidungsknoten sind jedoch entsprechende Fehlerabfragen und Verzweigungen im Prozess vorzusehen. Im Fehlerfalle muss der Prozess mit einer aussagekräftigen und verständlichen Fehlermeldung abgebrochen werden.

Zudem wird vorausgesetzt, dass jedem Funktionsaufruf und Transport von Daten über eine der benannten Schnittstellen eine erfolgreiche technische Authentisierung auf der Vermittlungs-, Transport- oder Anwendungsschicht [60] zwischen den beteiligten Modulen vorausgegangen ist.

Schritt 1: Die Geschäftsanwendung stellt eine Anfrage zum Abruf archivierter Daten über den XML-Adapter an die Middleware. Das Format der Anfrage richtet sich nach der Geschäftsanwendung.[61] Es muss allerdings die AOID und ggf. die VersionID oder mehrere VersionIDs des abzufragenden Archivdatenobjektes enthalten sein. Ist keine VersionID angegebene, wird automatisch die letzte (neueste) Version angeliefert.
Die Geschäftsanwendung legt bei diesem Aufruf per Parameter fest, ob das gesamte Archivdatenobjekt mit oder ohne Beweisdaten, nur die Nutzdaten, nur die Metadaten oder eine Kombination davon zurückgeliefert werden sollen. Im weiteren Verlauf wird nicht näher auf die relevanten Unterschiede eingegangen und das Verfahren generisch beschrieben.

Schritt 2: Der XML-Adapter richtet die Anfrage zum Abruf archivierter Daten an das ArchiSafe-Modul über die Schnittstelle TR-ESOR-S.4. Die Anfrage muss die zu den archivierten Daten gehörige Archivdatenobjekt-ID (AOID), ggf. die VersionID(s) und ein eindeutiges Identifizierungsmerkmal der Fachanwendung enthalten.

Schritt 3: Das ArchiSafe-Modul überprüft die Zugriffsberechtigung der Geschäftsanwendung.

Schritt 4: Das ArchiSafe-Modul fragt das mittels AOID und ggf. VersionID(s) identifizierte Archivdatenobjekt mit oder ohne Beweisdaten bzw. die Daten eines mittels AOID und ggf. VersionID(s) identifizierten Archivdatenobjektes vom ECM/Langzeitspeicher über die Schnittstelle TR-ESOR-S.5 ab.

Schritt 5: Der ECM/Langzeitspeicher gibt das zu der AOID und ggf. VersionID(s) gehörige Archivdatenobjekt, ggf. inkl. der angefragten Beweisdaten, über die Schnittstelle TR-ESOR-S.5 an das ArchiSafe-Modul zurück. Das Archivdatenobjekt wird dabei bitgenau vom ECM/Langzeitspeicher reproduziert. ArchiSafe erhält das Archivdatenobjekt also exakt so, wie es ursprünglich archiviert wurde (siehe Kapitel 7.4.1 Schritt 17 bzw. 7.4.2 Schritt 20).[62]

Schritt 6: Das ArchiSafe-Modul gibt das Archivdatenobjekt, ggf. inkl. der angefragten Beweisdaten, über die Schnittstelle TR-ESOR-S.4 an den XML-Adapter zurück.

Schritt 7: Der XML-Adapter gibt das komplette Archivdatenobjekt (XAIP) oder die extrahierten Inhalts- und Metadaten an die Geschäftsanwendung zurück.

---

[60] Siehe dazu bspw. [BLESS 05], Seite 22

[61] Erst der XML-Adapter stellt im Schritt 2 eine äquivalente Anfrage an das ArchiSafe-Modul in der Syntax, die das ArchiSafe-Modul erwartet. Deshalb ist in diesem Schritt noch eine geschäftsanwendungs-spezifische Syntax erlaubt.

[62] Sollte das Datenobjekt ursprünglich nicht in der XAIP-Form archiviert worden sein, bedarf es an dieser Stelle noch einer Transformation in ein XAIP. Ob diese Transformation der ECM/Langzeitspeicher oder das ArchiSafe-Modul durchführt, regelt diese TR nicht. Festzuhalten bleibt nur, dass durch diese Transformation die eigentlichen Nutzdaten (z.B. eine PDF-Datei oder eine eMail im Text-Format) sowie Signaturen nicht verändert werden dürfen, um den Beweiswert dieser Daten zu erhalten.

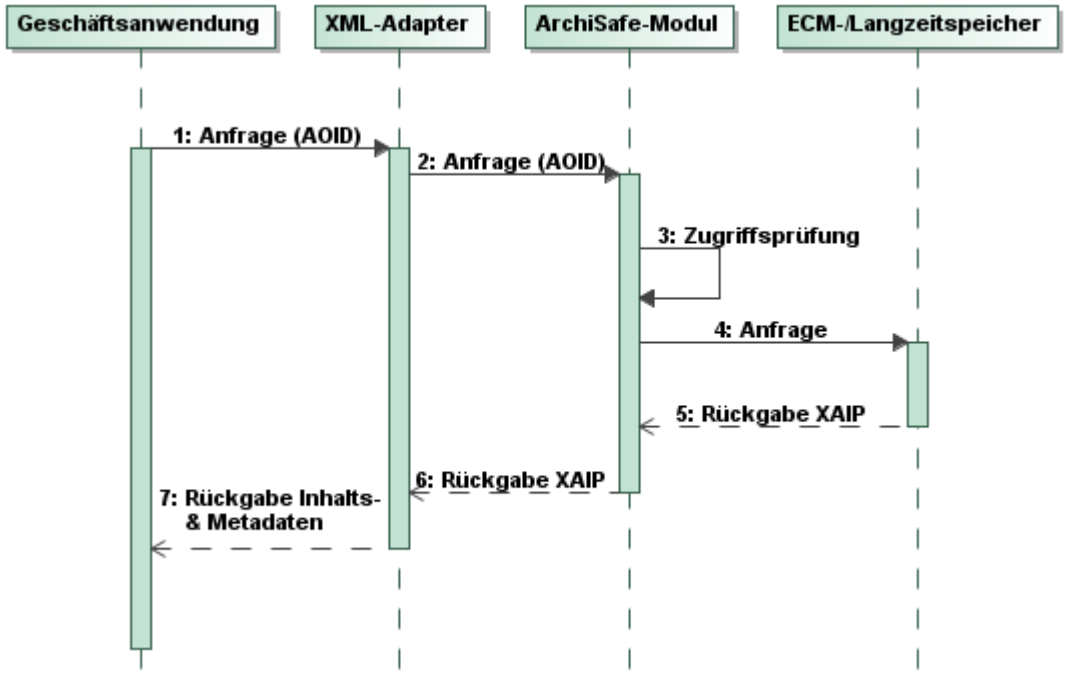


Abbildung 6: Abfrage archivierter Daten

7.4.4 Rückgabe technischer Beweisdaten

Zur Verifikation der Integrität und Authentizität der archivierten Daten können die zugehörigen Beweisdaten von der Middleware abgefragt werden. Der nachfolgend beschriebene Ablauf geht von der vorgestellten IT-Referenzarchitektur aus und beschreibt ausschließlich den positiven Fall (siehe auch Abbildung 7). Die notwendigen Fehlerprüfungen und Verzweigungen sind aus Gründen der Übersichtlichkeit im Ablauf nicht berücksichtigt.

An allen Entscheidungsknoten sind jedoch entsprechende Fehlerabfragen und Verzweigungen im Prozess vorzusehen. Im Fehlerfalle muss der Prozess mit einer aussagekräftigen und verständlichen Fehlermeldung abgebrochen werden.

Zudem wird vorausgesetzt, dass jedem Funktionsaufruf und Transport von Daten über eine der benannten Schnittstellen eine erfolgreiche technische Authentisierung auf der Vermittlungs-, Transport- oder Anwendungsschicht [63] zwischen den beteiligten Modulen vorausgegangen ist.

Schritt 1: Die Geschäftsanwendung stellt eine Anfrage bezüglich der Beweisdaten archivierter Daten an den XML-Adapter. Das Format der Anfrage richtet sich nach der Geschäftsanwendung. Es muss allerdings die AOID und ggf. die VersionID(s) des nachzuprüfenden Archivdatenobjektes enthalten sein.

Schritt 2: Der XML-Adapter richtet eine Anfrage zum Abruf der Beweisdaten über die Schnittstelle TR-ESOR-S.4 an das ArchiSafe-Modul.

Schritt 3: Das ArchiSafe-Modul überprüft die Zugriffsberechtigung der Geschäftsanwendung.

Schritt 4: Das ArchiSafe-Modul fragt die Beweisdaten des per AOID und ggf. VersionID(s) identifizierten Archivdatenobjektes über die Schnittstelle TR-ESOR-S.6 vom ArchiSig-Modul an.

[63] Siehe dazu bspw. **[BLESS 05]**, Seite 22

Schritt 5: Das ArchiSig-Modul ermittelt aus dem Hashbaum in seinem Datenspeicher[64] die technischen Beweisdaten (engl.: Evidence Record) im ERS-Format zu dem per AOID identifizierten Archivdatenobjekt.

Schritt 6: Existieren zu diesem Archivdatenobjekt mehrere Versionen im ECM/Langzeitspeicher, müssen bei Angabe von `all` im VersionID-Element die Evidence Records für alle Versionen berechnet und dem Ergebnis beigefügt werden, um die Integrität und Authentizität der Daten seit dem Zeitpunkt der ersten Archivierung nachweisen zu können.
Wurde zusätzlich zu einer AOID noch eine VersionID oder mehrere VersionIDs angegeben, muss das ArchiSig-Modul den Evidence Record für diese VersionID bzw. diese VersionIDs zurück liefern. Sofern das VersionID-Element nicht angegeben ist, wird der Beweisdatensatz für die aktuelle Version des XAIP zurückgeliefert.
Verwaltet das ArchiSig-Modul mehrere redundante Hashbäume[65], wird aus jedem Hashbaum der entsprechende reduzierte Evidence Record bzw. die Evidence Records berechnet und im Rückgabewert eingebettet.

Schritt 7: Das ArchiSig-Modul gibt den berechneten Evidence Record bzw. die Evidence Records über die Schnittstelle TR-ESOR-S.6 an das ArchiSafe-Modul zurück.

Schritt 8: Das ArchiSafe-Modul übergibt die empfangenen Beweisdaten über die Schnittstelle TR-ESOR-S.4 an den XML-Adapter.

Schritt 9: Der XML-Adapter gibt alle ermittelten Beweisdaten an die Geschäftsanwendung zurück.

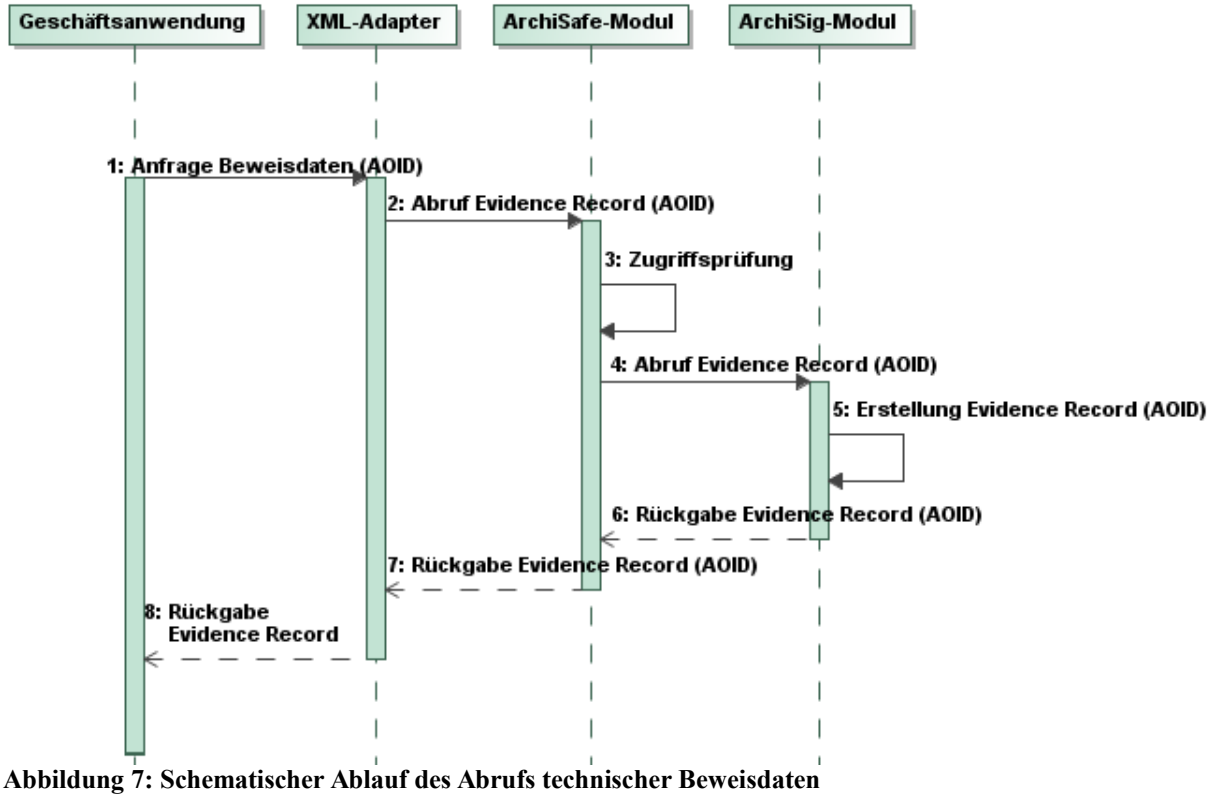


Abbildung 7: Schematischer Ablauf des Abrufs technischer Beweisdaten

[64] Gemäß der empfohlenen IT-Referenzarchitektur in Kapitel 7.1 verwaltet ArchiSig seine Daten in einem mindestens logisch von den eigentlichen Archivdaten separierten Speicher. Die Schnittstelle TR-ESOR-S.2 formuliert die entsprechenden Zugriffsfunktionen nicht aus, weshalb hier nicht Bezug auf diese Schnittstelle und auch nicht auf den ECM/Langzeitspeicher genommen wird.

[65] vgl. **[TR-ESOR-M.3]** und auch **[RFC4998]** bzw. **[RFC6283]**

7.4.5 Löschen von Archivdaten

Selbstverständlich müssen auch in einem Archiv Daten grundsätzlich gelöscht werden können. Dabei ist jedoch zu unterscheiden, ob die Daten vor oder nach ihrer festgelegten Mindestaufbewahrungsfrist gelöscht werden sollen. Ein vorzeitiges Löschen kann z. B. dann notwendig werden, wenn personenbezogene Daten gespeichert sind und die betreffende Person der Speicherung nicht mehr zustimmt bzw. widerspricht. In jedem Falle muss das Löschen archivierter Daten aus den vorgelagerten IT-Anwendungen heraus nur von ausdrücklich autorisierten Personen erlaubt sein. Die entsprechenden Sicherheitsmerkmale müssen durch die vorgelagerten IT-Anwendungen durchgesetzt werden. Für Behörden ist vor dem Löschen auf die Anbietungspflicht zu achten (vgl. Kapitel 5.1.5).

Voraussetzung für diese Funktion ist natürlich, dass der verwendete ECM/Langzeitspeicher bzw. dessen Medien ein Löschen überhaupt zulassen. Ist dies nicht der Fall, hat der ECM/Langzeitspeicher bzw. die Middleware den Aufruf dieser Lösch-Funktion mit einem Fehler zu quittieren.

Der nachfolgend beschriebene Ablauf (siehe auch Abbildung 8) geht von der in Kapitel 7.1 vorgestellten IT-Referenzarchitektur aus und beschreibt ausschließlich den positiven Fall. Die notwendigen Fehlerprüfungen und Verzweigungen sind aus Gründen der Übersichtlichkeit im Ablauf nicht berücksichtigt.

An allen Entscheidungsknoten sind jedoch entsprechende Fehlerabfragen und Verzweigungen im Prozess vorzusehen. Im Fehlerfalle muss der Prozess mit einer aussagekräftigen und verständlichen Fehlermeldung abgebrochen werden.

Zudem wird vorausgesetzt, dass jedem Funktionsaufruf und Transport von Daten über eine der in der IT-Referenzarchitektur benannten Schnittstellen eine erfolgreiche technische Authentisierung auf der Vermittlungs-, Transport- oder Anwendungsschicht des TCP/IP-Schichtenmodells[66] zwischen den beteiligten Modulen vorausgegangen ist.

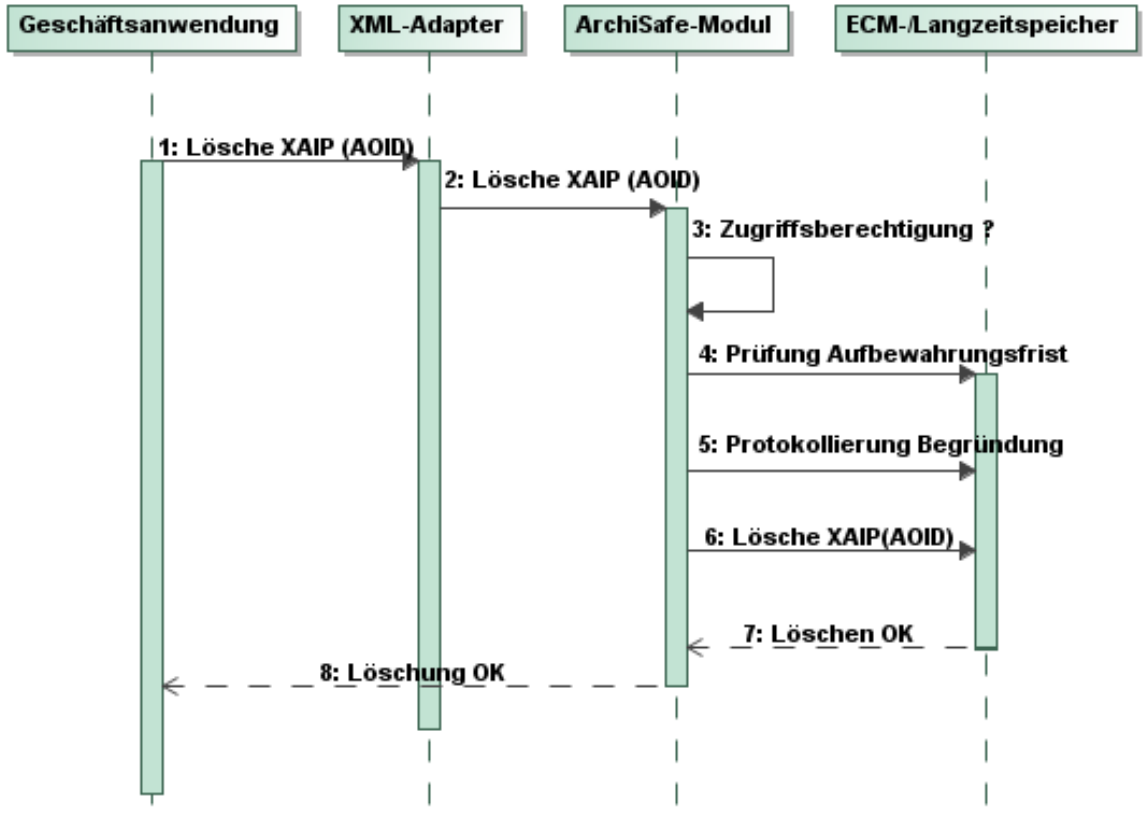


Abbildung 8: Schematischer Ablauf des Löschens von Archivdatenobjekten

Schritt 1: Die Geschäftsanwendung stellt eine Anfrage zum Löschen archivierter Daten an den XML-Adapter. Das Format der Anfrage richtet sich nach der Geschäftsanwendung. Es

[66] Siehe dazu bspw. **[BLESS 05]**, Seite 22

muss allerdings die AOID des zu löschenden Archivdatenobjektes enthalten sein. Handelt es sich um ein Löschen vor Ablauf der Mindestaufbewahrungsfrist, muss der Aufruf zusätzlich eine protokollierbare Begründung für das vorzeitige Löschen beinhalten.

Schritt 2: Der XML-Adapter richtet eine Anfrage zum Löschen archivierter Daten an das ArchiSafe-Modul (über Schnittstelle TR-ESOR-S.4). Die Anfrage muss die AOID des zu löschenden Archivdatenobjektes enthalten. Handelt es sich um ein Löschen vor Ablauf der Mindestaufbewahrungsfrist, muss der Aufruf zusätzlich die protokollierbare Begründung für das vorzeitige Löschen beinhalten.

Schritt 3: Das ArchiSafe-Modul überprüft die Zugriffsberechtigung der Geschäftsanwendung.

Schritt 4: Das ArchiSafe-Modul prüft, ob die Mindestaufbewahrungsfrist bereits erreicht wurde. Hierzu fragt das ArchiSafe-Modul die entsprechenden Metadaten aus dem XAIP aus dem ECM/Langzeitspeicher über die Schnittstelle TR-ESOR-S.5 ab.[67]Falls die Mindestaufbewahrungsfrist noch nicht abgelaufen ist, prüft das ArchiSafe-Modul, ob die Löschanfrage eine Begründung für das vorzeitige Löschen enthält.

Schritt 5: Im Fall eines vorzeitigen Löschens protokolliert das ArchiSafe-Modul den übergebenen Begründungstext gemeinsam mit der AOID.[68]

Schritt 6: Das ArchiSafe-Modul fordert den ECM/Langzeitspeicher über die Schnittstelle TR-ESOR-S.5 auf, das per AOID identifizierte Archivdatenobjekt zu löschen.

Schritt 7: Der ECM/Langzeitspeicher löscht das Archivdatenobjekt[69].Der ECM / Langzeitspeicher quittiert über die Schnittstelle TR-ESOR-S.5 den Erfolg der Löschaktion an das ArchiSafe-Modul.

Da alle Versionen eines Archivdatenobjektes technisch innerhalb dieses Archivdatenobjektes enthalten sind, werden bei einem Löschen automatisch alle Versionen eines Archivdatenobjektes gelöscht. Dies ist ein beabsichtigtes Verhalten!

Schritt 8: Das ArchiSafe-Modul quittiert das erfolgte Löschen über den XML-Adapter an die Fachanwendung, die die Löschaktion ausgelöst hat.[70]

7.4.6 Prüfen von beweisrelevanten Daten und Beweisdaten

Die TR-ESOR Middleware soll die Möglichkeit anbieten, Archivdatenobjekte samt der darin enthaltenen oder zusätzlich übergebenen beweisrelevanten Daten (Signaturen, Zeitstempel, Zertifikate, Sperrlisten, OCSP-Responses usw.) und technische Beweisdaten (Evidence Records gemäß RFC4998) zu prüfen. Dafür ist der nachfolgend beschrieben Ablauf (siehe auch 9) vorgesehen.

Schritt 1: Übergabe des XML-Dokuments an das ArchiSafe-Modul

Schritt 2: Das ArchiSafe-Modul überprüft die Zugriffsberechtigung der Geschäftsanwendung auf der Grundlage des im Aufruf übergebenen Identifizierungsmerkmals und die Syntax des übergebenen XML-Dokuments auf Basis eines im ArchiSafe-Moduls hinterlegten und autorisierten XML-Schemas. Das XML-Schema ist kunden- und einsatzspezifisch..

---

[67] Falls das entsprechende Archivdatenobjekt in mehreren Versionen existiert, ist die Mindestaufbewahrungsfrist der letzten (neuesten) Version ausschlaggebend.

[68] Dieser Schritt sollte immer vor dem eigentlichen Löschen erfolgen, so dass sichergestellt ist, dass der Begründungstext immer vorhanden ist, auch wenn der ECM/Langzeitspeicher beim eigentlichen Löschen ausfällt.

[69] Dabei ist sicher zu stellen, dass die zu löschenden Daten im ECM/Langzeitspeicher unwiederbringlich gelöscht, d. h. auf dem Speichermedium irreversibel unkenntlich gemacht werden.

[70] Falls auch das ArchiSig-Modul Kenntnis von einem gelöschten Archivdatenobjekt erhalten soll, kann dies an dieser Stelle vom ArchiSafe-Modul angestoßen werden.

Schritt 3: Das ArchiSafe-Modul übergibt die signierten Daten und deren Signaturen sowie ggf. dazu gehörige Beweisdaten zur Signaturprüfung an das Krypto-Modul über die Schnittstelle TR-ESOR-S.1.

Schritt 4: Das Krypto-Modul verifiziert die mathematische Richtigkeit der Signaturen.

Schritt 5: Das Krypto-Modul validiert die Gültigkeit der zugeordneten Zertifikate über eine Abfrage beim Zertifikatsaussteller (z.B. OCSP Anfrage). Dazu muss ein Zertifizierungspfad bis hin zu einer, aus Sicht des Prüfenden, vertrauenswürdigen Zertifizierungsinstanz gebildet und geprüft werden.

Schritt 6: Der Zertifizierungsdiensteanbieter liefert eine Bestätigung der Gültigkeit der angefragten Zertifikate zum Beispiel als OCSP- oder SCVP-Antwort zurück (siehe Anlage **[TR-ESOR-M.2]**).

Schritt 7: Das Krypto-Modul liefert die Ergebnisse der Signaturprüfung und ggf. einen ausführlichen Prüfbericht in Form eines VerificationReport-Elementes für das Archivdatenobjekt und/oder Beweisdaten (siehe **[TR-ESOR-VR]**) dem ArchiSafe-Modul über die Schnittstelle TR-ESOR-S.1 zurück.

Schritt 8: Die Prüfergebnisse werden vom ArchiSafe-Modul unverändert in das Archivdatenobjekt in die *CredentialSection* des XAIP-Dokuments eingetragen.

Schritt 9: Das ArchiSafe-Modul gibt die Returncodes über die Schnittstelle TR-ESOR-S.4 als Bestätigung für die erfolgreiche Prüfung an die aufrufende Geschäftsanwendung zurück.

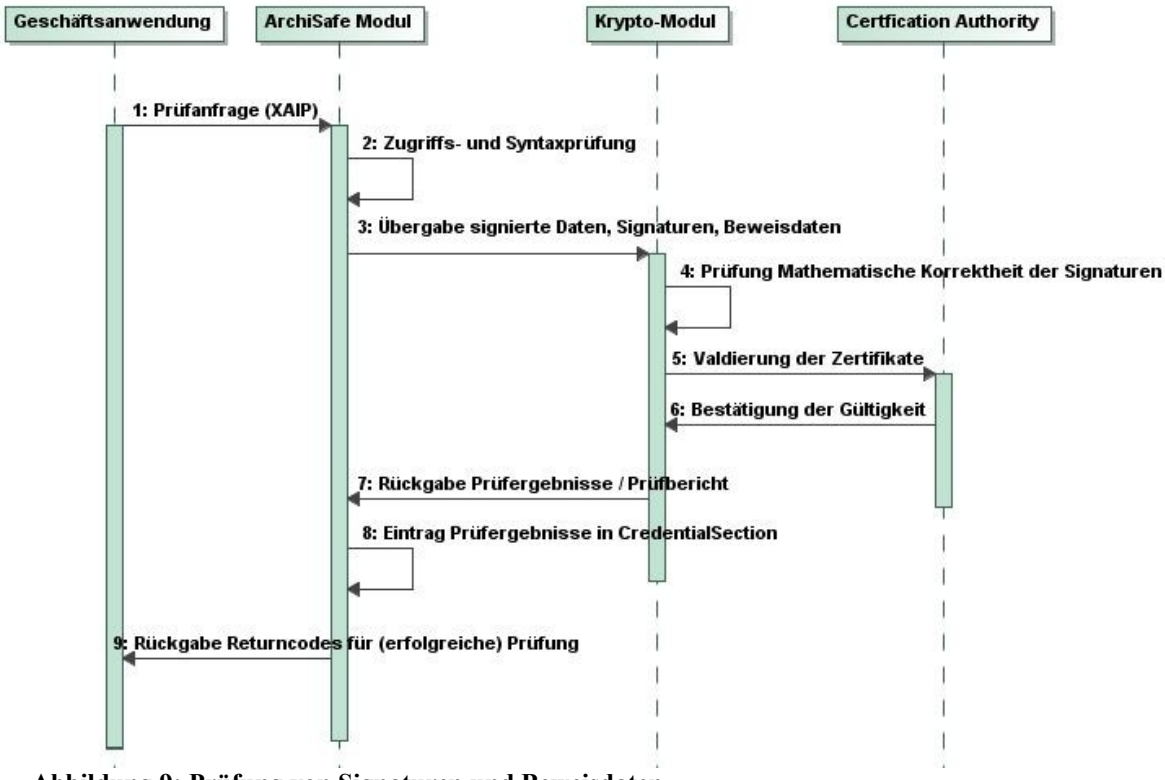


Abbildung 9: Prüfung von Signaturen und Beweisdaten

8. IT-Sicherheitskonzept

In diesem Abschnitt wird auf der Grundlage der in Kapitel 4 beschriebenen allgemeinen Anforderungen sowie der in Kapitel 7 empfohlenen IT-Referenzarchitektur ein generisches Sicherheitskonzept mit Blick auf das Gesamtsystem entwickelt.

Neben Anforderungen an die Middleware für die Beweiswerterhaltung von kryptographisch signierten Dokumenten sind dabei auch Forderungen an die Einsatzumgebung, zu der auch die Fachanwendungen und die ECM/Langzeitspeicher gehören, unumgänglich. Keine Komponente der Einsatzumgebung ist jedoch möglicher Gegenstand einer Konformitätsprüfung gegen diese Technische Richtlinie; die hier angegebenen Eigenschaften werden lediglich als gegeben vorausgesetzt und sind rein informeller Natur.

8.1 Sicherheitsziele

Voraussetzung für eine beweiswerterhaltende elektronische Ablage aufbewahrungspflichtiger Unterlagen sind hinreichend sichere Archivierungsverfahren. Die hierfür erforderlichen organisatorischen und technischen Maßnahmen und Vorkehrungen sind Bestandteil eines organisationsspezifischen Sicherheitskonzepts, das zur Gewährleistung des erforderlichen Grades an Informationssicherheit entwickelt und umgesetzt werden muss. Bestandteil eines solchen Sicherheitskonzeptes sind insbesondere Maßnahmen und Vorkehrungen zur Gewährleistung der folgenden Sicherheitsziele:

- **Vertraulichkeit**

  Das Kriterium Vertraulichkeit verlangt, dass Daten nicht unberechtigt eingesehen, weitergegeben oder veröffentlicht werden können. Dieser Anforderung ist auch beim Einsatz von Archivierungssystemen Rechnung zu tragen, indem die Middlewarekomponenten, das eigentliche ECM/Langzeitspeichersystem, die Speichermedien, etwaige Sicherheitskopien und die Kommunikationsverbindungen mittels physischer und/oder logischer Zugangs- und Zugriffskontrollen vor unberechtigter Kenntnisnahme geschützt werden.

- **Integrität**

  Die Integrität eines elektronischen Archivierungssystems ist gegeben, wenn die zu archivierenden Dokumente und Daten nachweislich vollständig und unverfälscht aufbewahrt werden. Um die Integrität sicherzustellen, sind der ECM/Langzeitspeicher insgesamt und die gespeicherten Dokumente und Daten vor Manipulation und ungewollten oder fehlerhaften Änderungen zu schützen. Manipulationen und ungewollte oder fehlerhafte Änderungen müssen immer entdeckt werden können.

- **Verfügbarkeit**

  Das Sicherheitsziel der Verfügbarkeit gibt an, dass die zur Aufbewahrung bestimmten Daten und Dokumente bei Bedarf (jederzeit) in einer angemessenen Zeitspanne vollständig und unverfälscht aus dem ECM/Langzeitspeicher ausgelesen werden können müssen. Das betrifft auch die zum Nachweis der Authentizität und Integrität erzeugten und gespeicherten Verifikationsdaten.

Aus diesen grundsätzlichen Zielen der IT-Sicherheit können für den Beweiswerterhalt noch weitere Sicherheitsziele abgeleitet werden:

- **Authentizität**

  Für den Beweiswerterhalt archivierter Dokumente oder Daten ist neben der Unverfälschtheit die nachprüfbare Authentizität der Dokumente und Daten von entscheidender Bedeutung. Es muss zweifelsfrei nachweisbar sein und bleiben, dass eine bestimmte (natürliche) Person ein bestimmtes Datum zu einer bestimmten Zeit mit dem vorliegenden Inhalt und in der vorliegenden Form erzeugt oder zur Kenntnis genommen hat. Dieser Nachweis muss im Fall des Langzeitarchivs auch nach mehreren Jahrzehnten noch möglich sein. Zur Authentizität archivierter Dokumente und Daten gehört auch, dass die im elektronischen ECM/Langzeitspeicher aufbewahrten Informationen vollständig sind (vgl. Integrität) und zweifelsfrei einem bestimmten Geschäftsvorfall zugeordnet werden können. Dieses Sicherheitsziel stützt sich auf das Sicherheitsziel der Integrität ab, stellt jedoch noch deutlich höhere Anforderungen.

- **Verbindlichkeit**

  Unter Verbindlichkeit wird die Eigenschaft verstanden, gewollte Rechtsfolgen dauerhaft zu gewährleisten.

  Elektronische Daten sind grundsätzlich geeignet, im Geschäftsverkehr Beweiskraft für gewollte Rechtsfolgen zu erbringen. Der beweisrechtliche Wert elektronischer Daten hängt dabei maßgeblich davon ab, wie es gelingt, nachzuweisen, dass die Dokumente seit ihrer Erstellung oder Aufbewahrung nicht mehr verändert worden sind (Integrität) und in Form und Inhalt vom bezeichneten Aussteller herrühren (Authentizität).

  Im Sinne des Beweiswerterhaltes bedeutet Verbindlichkeit zudem, dass jegliche Operation auf den Archivdatenobjekten während der Aufbewahrung nachvollziehbar dokumentiert werden kann. Dies bezieht sich insbesondere auf die Überarbeitung von Metainformation und das vorzeitige Löschen von Archivdatenobjekten.

8.2 Maßnahmen

Um die oben angegebenen Sicherheitsziele für die Middleware und den ECM/Langzeitspeicher in der Ausprägung der empfohlenen Referenzarchitektur zu erfüllen, sind die folgenden Maßnahmen erforderlich.

Dieses Kapitel versteht sich als Hinweis an die Benutzer einer solchen Middleware bzw. eines ECM/Langzeitspeichers und legt keine formalen Kriterien fest.

HINWEIS: Es ist zu beachten, dass dieser generische Maßnahmenkatalog auf keinen Fall ein konkretes Sicherheitskonzept gemäß bspw. den IT-Grundschutz-Katalogen des BSI ersetzen kann, das den lokalen und organisationsspezifischen Bedürfnissen und Gegebenheiten angepasst ist.

8.2.1 Übergreifende Maßnahmen

Vor dem Einrichten eines elektronischen Archivsystems mit dem Fokus auf dem Beweiswerterhalt muss ein die technischen Systeme und sämtliche relevanten Prozesse abdeckendes IT-Sicherheitskonzept basierend auf einer standardisierten Methodik (z. B. BSI-100 Standard) erstellt und mit der Inbetriebnahme umgesetzt werden.

Das IT-Sicherheitskonzept muss regelmäßig (z. B. einmal pro Jahr) auf den aktuellen Stand gebracht werden.

Die Maßnahmen, die sich aus dem IT-Sicherheitskonzept und dessen Überarbeitung ergeben, müssen - soweit wirtschaftlich vertretbar - zeitnah umgesetzt werden. Dies gilt insbesondere für die Definition und Umsetzung der Verantwortlichkeiten und Kompetenzen, der fachlichen Prozesse sowie sicherer Administrations- und Kontrollprozesse.

Insbesondere für Einrichtungen, Organisationen und Unternehmen der öffentlichen Verwaltung soll das Einrichten und der Betrieb eines Archivsystems mit einer Middleware zum Beweiswerterhalt einem IT-Grundschutz-Audit mit dem Ziel der Zertifizierung unterzogen werden, um auch die jeweiligen Prozesse und Organisationen in der Einsatzumgebung nachweislich zielgerichtet definiert zu haben.

8.2.2 Maßnahmen zum Schutz der Vertraulichkeit

Das ECM/Langzeitspeichersystem und dessen Medien muss in Räumen betrieben werden, die zutrittsgesichert sind. Zutritt zu diesen Räumen ist nur sehr restriktiv zu gewähren. Dies gilt auch für eventuell vorhandene redundante Systeme und Backup-Systeme und dessen Medien.

Die Handhabung und Verwaltung (Transport, Lagerung, Entsorgung) von Wechseldatenträgern (hier insbesondere Backup-Medien) muss exakt definiert und sehr restriktiv gehandhabt werden. Über die Backup-Medien darf der Zugriff nicht vereinfacht und der Kreis der Zugriffsfähigen (nicht deckungsgleich mit den Berechtigten) nur soweit als unbedingt notwendig ausgeweitet werden.

Der Zutritt von Personen zu diesen Räumen soll protokolliert und stichprobenartig überprüft werden. Optional kann eine unabhängige Überwachung der Räume, z. B. per Videoanlage, erfolgen.

Jegliche Aktion im Zusammenhang mit Backupmedien (Auslagerung, Einlagerung, Umschichtung, Prüfung der Lesbarkeit, Entsorgung, etc.) soll protokolliert werden. Die Protokolle sollen mindestens aufzeigen, welche Person wann aus welchem Grund welche Aktion mit welchen Medien durchgeführt hat.

Sämtliche Archivdaten im ECM/Langzeitspeicher können verschlüsselt werden. In einem solchen Fall ist jedoch besonderes Augenmerk auf das sichere Schlüsselmanagement und die Wiederherstellbarkeit sämtlicher Daten im Fehlerfall zu legen. Aus Gründen der Wirtschaftlichkeit wird daher empfohlen, bei Bedarf die erforderlichen Ver- und Entschlüsselungsprozesse und die damit verbundene Administrationsinfrastruktur auf externe, vorgelagerte IT-Anwendungen zu verlagern. Eine Verschlüsselung ersetzt jedoch nicht die generell notwendigen Zugriffskontrollmechanismen.

Der ECM/Langzeitspeicher kann für die Wiederherstellung verloren gegangener oder beschädigter Daten Backupsysteme nutzen, die die Daten während der Aufbewahrung auf den Backupmedien verschlüsseln. Auch hier ist in diesem Fall besonderes Augenmerk auf die Wiederherstellbarkeit der Daten im Fehlerfall zu legen.

Sofern Kommunikationsverbindungen zwischen einzelnen Komponenten des Gesamtsystems nicht durch anderweitige Maßnahmen geschützt sind (vgl. Kapitel 7.3.5), müssen die physischen Kommunikationsverbindungen in gesicherten Räumen und/oder in gesicherten Leitungsführungen untergebracht sein. Ein unerlaubter Zugriff auf die Leitungen muss sehr zeitnah erkannt werden können.

Jegliche Kommunikation zwischen den Komponenten der Middleware und mit externen Komponenten[71] darf erst nach einer erfolgreichen Authentisierung dieser Komponenten aufgenommen werden. Hierbei müssen unterschiedliche Authentisierungsstufen berücksichtigt werden:

- Die Authentisierungsverfahren müssen so ausgelegt sein, dass keine Komponente der Middleware oder des ECM/Langzeitspeichers unbemerkt ausgetauscht oder umgangen werden kann.
- Die Authentisierungsverfahren müssen hinreichend stark sein. Dabei ist insbesondere zu beachten, ob die Kommunikationsbeziehungen und Komponenten physisch geschützt sind oder nicht.
- Die Authentisierung von den von der Middleware genutzten externen Dienstleistern (z. B. den Zertifizierungsdiensteanbietern) kann nur in dem Maße genutzt werden, wie die Dienstleister dies anbieten. Die angebotenen Möglichkeiten müssen genutzt werden.
- Die Authentisierung von externen Dienstleistern, die auf die Middleware und deren Komponenten zugreifen möchten (z.B. zur Fernwartung), muss eine hinreichende Stärke aufweisen, damit kein unerlaubter Zugang und Zugriff von diesen Systemen zur Middleware oder zum ECM/Langzeitspeicher und dessen Daten möglich ist.
- Die Authentisierung externer Systeme (hier insbesondere die Geschäftsanwendungen) muss ebenfalls eine hinreichende Stärke aufweisen, damit kein unerlaubter Zugang und Zugriff von diesen Systemen zur Middleware oder zum ECM/Langzeitspeicher und dessen Daten möglich ist.[72]
- Die an die Middleware angebundenen Geschäftsanwendungen müssen eine personenbezogene Authentisierung und Autorisierung durchsetzen. Ausschließlich den fachlich autorisierten Personen soll so der Zugriff auf die Middleware möglich sein.

Fehlgeschlagene Authentifizierungsversuche sind zu protokollieren. Es ist aus fachlicher Sicht abzuwägen, ob Zugänge nach mehrfachen fehlerhaften Authentifizierungsversuchen gesperrt werden, da dies auch relativ leicht für Denial-of-Service Attacken genutzt werden kann.

Erfolgreiche Authentifizierungen können protokolliert werden.

[71] z. B. die Fachanwendung oder ein Zertifizierungsdiensteanbieter

[72] Der XML-Adapter wird in diesem Zusammenhang, obwohl durch diese Technische Richtlinie definiert, als eine externe Komponente betrachtet. Es bedarf also einer Authentisierung zwischen XML-Adapter und Middleware. Weiterhin muss sichergestellt sein, dass der XML-Adapter nicht von unautorisierten Geschäftsanwendungen genutzt werden kann.

Jegliche Kommunikation zwischen den Komponenten der Middleware und externen Anwendungen oder Dienstleistern (bspw. Zertifizierungsdiensteanbietern) soll verschlüsselt werden. Sollte eine physische Absicherung einer Kommunikationsbeziehung nicht möglich sein, muss die Kommunikation verschlüsselt werden.

Sollte ein externer Dienstleister keine Verschlüsselungsoption für die Kommunikation anbieten, muss geprüft werden, ob ein anderer Dienstleister, der eine Verschlüsselungsoption anbietet, diese Dienstleistungen gleichwertig erbringen kann.

Für die Kommunikationsverschlüsselung sind hinreichend starke Verschlüsselungsverfahren und Schlüssellängen einzusetzen. Eine Aushandlung einer unzureichenden oder nicht vorhandenen Verschlüsselungsstärke bei Sitzungsaufbau muss verhindert werden. Es darf keine Kommunikation mit zu schwacher Verschlüsselung stattfinden. Das Ereignis ist zu protokollieren.

Jede Kommunikation wird nur bei Bedarf und nur von der dafür eingerichteten Komponente oder den dazu autorisierten Personen initiiert. Unbegründete bzw. unerwartete Kommunikationsverbindungsanfragen sind von allen Komponenten abzulehnen.

Der Zugriff auf Protokolldaten der Middleware ist ebenso möglichst restriktiv zu halten.

Sollte die TR-ESOR-Middleware einen mandantenfähigen Betrieb anbieten, muss die TR-ESOR-Middleware einen mandatenübergreifenden Zugriff auf die Archivdatenobjekte zuverlässig verhindern. Bei sehr hohen Anforderungen an die Vertraulichkeit sollte die TR-ESOR-Middleware auch nach Covered Channels und anderen Angriffsvektoren bezüglich Vertraulichkeitsverletzungen untersucht werden.

Sollte ein mandantenfähiger Betrieb der TR-ESOR-Middleware erforderlich sein, sollten diese Mandanten sich auch im verwendeten ECM-/Langzeitspeicher konsistent fortsetzen.

8.2.3 Maßnahmen zum Schutz der Authentizität, Integrität und Verbindlichkeit

Sofern die Sicherung der Authentizität und Integrität elektronischer Daten mit Hilfe elektronischer Signaturen normiert oder gewünscht ist, müssen elektronische Signaturen von Daten und Dokumenten in hinreichender Qualität grundsätzlich durch die Anwendungen und vor der Ablage im ECM/Langzeitspeicher realisiert werden.

Um sicherzustellen, dass es bei der Hashwertbildung und auch bei der Signatur von Inhaltsdaten in XML-Notation zu keinen Mehrdeutigkeiten kommt, wird vor der Hashwertbildung bzw. Signatur eine Kanonisierung der Inhaltsdaten empfohlen, ausführlicher dazu in Anlage TR-ESOR-M.2 Krypto-Modul (insbesondere zu Signaturen) und TR-ESOR-M.3 ArchiSig-Modul (insbesondere zur Hashwertbildung).

Die Signaturen sind so mit den signierten Daten zu verbinden, dass der Zusammenhang zwischen den Signaturen und den signierten Daten jederzeit und zweifelsfrei auch durch Dritte reproduziert werden kann.

Darüber hinaus sollen die für eine vollständige Prüfung der Gültigkeit der Signaturen erforderlichen Prüfdaten bei oder unmittelbar nach der Erstellung der Signatur beschafft und ebenfalls vor der Ablage im ECM/Langzeitspeicher so mit den Signaturen und signierten Daten verbunden werden, dass der Zusammenhang jederzeit und auch durch Dritte reproduziert werden kann. Diese Verifikationsdaten müssen spätestens bei der Ablage im Archivsystem durch das ArchiSafe-Modul beschafft werden.

Es wird deshalb empfohlen, die Signaturdaten gemeinsam mit den Signaturverifikationsdaten und den Inhaltsdaten in einem XML-basierten Archivdatenobjekt (siehe Anlage **[TR-ESOR-F], [TR-ESOR-VR]** und **[TR-ESOR-ERS]**) abzulegen.

(A8.2-1) Um die langfristige Nachprüfbarkeit der Signaturen zu gewährleisten, müssen die Signaturen und Signaturprüfdaten (Zertifikate und Statusabfragen/-informationen) in standardisierten Datenformaten abgelegt werden. Details dazu finden sich in **[TR-ESOR-F]** bzw. **[TR-ESOR-ERS]**.

(A8.2-2) Liegt das zu archivierende Datenobjekt in einem XML-Format vor, muss dieses Archivdatenobjekt durch das ArchiSafe-Modul gegen eine in dieser Komponente hinterlegte und durch die Fachanwendung autorisierte XML Schemadatei auf syntaktische Richtigkeit geprüft werden. Schlägt die Überprüfung fehl, darf das Objekt nicht weiter verarbeitet werden.

(A8.2-3) Enthält das zu archivierende Archivdatenobjekt elektronische Signaturen und ggf. Beweisdaten, muss das ArchiSafe-Modul die Gültigkeit der Signaturen und Beweisdaten prüfen (lassen) und die Prüfergebnisse in standardisierter Form in das Archivdatenobjekt eintragen. Schlägt die Prüfung fehl, darf das Objekt nicht weiter verarbeitet werden.

(A8.2-4) Ist die Prüfung erfolgreich, kann das ArchiSafe-Modul das gesamte Archivdatenobjekt zusätzlich mit einer fortgeschrittenen elektronischen Signatur oder einem elektronischen Zeitstempel versehen.

(A8.2-5) Alle noch nicht integritätsgeschützten Hashwerte in der ArchiSig-Datenbasis müssen regelmäßig durch einen qualifizierten „Archivzeitstempel“, der eine qualifizierte elektronische Signatur enthält, nach dem in der Anlage **[TR-ESOR-M.3]** „ArchiSig-Modul“ näher beschriebenen ERS-Standard der IETF gesichert werden.[73]

- Empfehlung: mindestens einmal pro Tag.

(A8.2-6) Rechtzeitig vor dem Auslaufen der Sicherheitseignung oder bei Bekanntwerden[74] einer (realistischen) Angreifbarkeit der für den Archivzeitstempel verwendeten Algorithmen und Parameter[75] muss der Inhalt des Zeitstempelfeldes des letzten (zeitlich vorangegangenen) Archivzeitstempels neu gehashed und ein neuer Archivzeitstempel errechnet werden. Dieser neue Zeitstempel basiert auf sicherheitsgeeigneten Algorithmen und ist ebenfalls der ArchiSig-Datenbasis hinzuzufügen.

(A8.2-7) Rechtzeitig vor dem Auslaufen der Sicherheitseignung oder dem Bekanntwerden einer (theoretischen) Angreifbarkeit der für die Berechnung der Hashwerte der Archivdatenobjekte verwendeten Algorithmen und Parameter müssen für alle diese Archivdatenobjekte im ECM/Langzeitspeicher neue Hashwerte auf Basis sicherheitsgeeigneter Algorithmen und Parameter berechnet und mit neuen Archivzeitstempeln nach dem ERS-Standard der IETF gesichert werden. Der ECM/Langzeitspeicher muss für diese Operation dem ArchiSig-Modul einen performanten, sicheren und zuverlässigen Zugriff zur Verfügung stellen.

Da diese Operation abhängig vom Volumen der gespeicherten Daten möglicherweise einen nicht unerheblichen Zeitraum beanspruchen wird, soll die Middleware als Fallback-Lösung zusätzlich eine sekundäre ArchiSig-Datenbasis parallel zur primären Datenbasis pflegen. Diese sekundäre Datenbasis muss auf anderen kryptographischen Algorithmen und Parametern als die primäre Datenbasis aufsetzen. Die sekundäre Datenbasis muss genau die gleichen Datenobjekte wie die primäre Datenbasis absichern und jederzeit parallel zur primären Datenbasis in Betrieb genommen werden können.

ArchiSig-Datenbestände dürfen nicht gelöscht werden oder durch sonstige Umstände verloren gehen. Dies gilt auch dann, wenn einzelne Archivdatenobjekte schon gelöscht oder wenn die verwendeten Algorithmen ausgelaufen sind oder gebrochen wurden.

Die ArchiSig-Datenbestände müssen auf bzw. in Speichern[76] gehalten werden, die grundlegende integritätssichernde Mechanismen zur Verfügung stellen. Dies bezieht sich nicht nur auf die Zeitstempel und Hashwerte sowie die Archivdatenobjekt ID’s selbst sondern auch auf die Verknüpfungen zwischen diesen Datenelementen.

Der ECM/Langzeitspeicher muss derart gewählt werden, dass eine bitgenaue Reproduktion der gespeicherten Archivdatenobjekte (XAIP) und der ArchiSig-Datenbestände garantiert werden kann.

---

[73] Ein „Archivzeitstempel“ kann auf Datenobjekte oder Gruppen von Datenobjekten angewendet werden. Die kryptographischen Repräsentanten (Hashwerte) der Datenobjekte bzw. Datenobjektgruppen werden zunächst in einem so genannten Merkle-Hashbaum **[MER 1980]** zusammengefasst und der letzte Hashwert des Baums wird dann zunächst mit einem initialen Zeitstempel versehen. Auf diese Weise sind alle unter einem Hashbaum subsumierten Hashwerte mit zunächst nur einem initialen Zeitstempel kryptographisch geschützt (siehe auch TR-ESOR-M.3 und unter http://www.ietf.org/rfc/rfc4998.txt).

[74] Der Zeitpunkt des Bekanntwerdens ist ein entsprechender Eintrag in den Algorithmenkatalog der Bundesnetzagentur.

[75] Dies schließt sowohl das Hash-Verfahren als auch das Signaturverfahren ein.

[76] Es wird nicht gefordert, dass das Langzeitspeichersystem diese Mechanismen zur Verfügung stellt. Das ArchiSig-Modul könnte diese auch selbst realisieren.

Alle im ECM/Langzeitspeicher gehaltenen Medien (auch Backup-Medien) sowie die darauf gespeicherten Daten müssen regelmäßig auf ihre Lesbarkeit hin überprüft werden. Selbst bei Identifikation nur geringfügiger Fehler (z. B. Bit-Fehler auf Medium) muss das entsprechende Medium ersetzt bzw. die betroffenen Datenbestände von integren Backup-Medien zurückgesichert werden.

Alle Komponenten der Middleware und des ECM/Langzeitspeichers müssen derart ausgelegt sein, dass der parallele Zugriff einer oder mehrerer unterschiedlicher Geschäftsanwendungen, auch mit unterschiedlicher Rechenkapazitäts- und Bandbreitenausnutzung, nicht zu unerwünschten Verfälschungen an den übertragenen oder gespeicherten Daten führt.

Die kryptographischen Beweisdaten im Speichersystem müssen gegen unautorisierten (schreibenden) Zugriff geschützt werden. Insbesondere ist auch sicherzustellen, dass Administratoren- und Anwenderaccounts für die Archivdatenobjekt-Datenbestände keinen Zugriff auf die Beweisdaten-Datenbestände besitzen. Es empfiehlt sich dazu, eine mindestens logische Trennung dieser beiden Datenbestände einzuhalten.

8.2.4 Maßnahmen zum Schutz der Verfügbarkeit

Archivdatenobjekte dürfen nur gelöscht werden, wenn die definierte Mindestaufbewahrungsdauer abgelaufen ist und ein Löschauftrag im Falle einer vorzeitigen Löschung eine Begründung für ein vorzeitiges Löschen enthält. Die Begründung ist im Falle eines vorzeitigen Löschens nachweislich durch den ECM/Langzeitspeicher zu protokollieren und für die Dauer der Aufbewahrungsfristen (die sich auf das Löschprotokoll bezieht, nicht auf das Original-Dokument) unverfälscht vorzuhalten. Es ist zu empfehlen, dass für das (vorzeitige) Löschen innerhalb der Geschäftsanwendung ein 4-Augen-Prinzip oder ein anderes Berechtigungs- und Kontrollmodell durchgesetzt wird.[77]

Der ECM/Langzeitspeicher soll sämtliche Daten redundant speichern. In welchem Grad dies notwendig ist, muss das konkrete IT-Sicherheitskonzept aufzeigen. Dies gilt sowohl für die eigentlichen Archivdatenobjekte als auch für die ArchiSig-Datenbasis.

Die Infrastruktur und die technischen Komponenten des gesamten Archivsystems sowie die Anbindungen an externe Komponenten müssen hinreichend verfügbar und ggf. redundant ausgelegt werden. In welchem Grad dies notwendig ist, muss das konkrete IT-Sicherheitskonzept aufzeigen.

Alle Komponenten der Middleware müssen derart ausgelegt sein, dass keine der angeschlossenen Geschäftsanwendungen den Zugriff auf die Middleware oder den ECM/Langzeitspeicher blockieren kann.

Alle Komponenten der Middleware müssen derart ausgelegt sein, dass keine middleware-internen Aktionen den zeitnahen Zugriff für die Geschäftsanwendungen blockieren können.

8.2.5 Maßnahmen zur Autorisierung

Die an der Middleware angeschlossenen Geschäftsanwendungen müssen ein zuverlässiges Authentisierungs- und Autorisierungssystem implementieren, das den Zugriff auf die Middleware nur berechtigten Personen ermöglicht.

Das ArchiSafe-Modul muss bei jeder Archivanfrage überprüfen können, ob die anfragende Geschäftsanwendung für einen Zugriff (Ablage, Ändern, Rückgabe, Prüfung beweisrelevanter Daten und Beweisdaten oder Löschen) auf die Middleware autorisiert ist.

Das ArchiSafe-Modul muss überprüfen können, ob die anfragende Geschäftsanwendung für den Zugriff (Ändern, Rückgabe, Prüfung beweisrelevanter Daten und technischer Beweisdaten oder Löschen) auf das durch eine AOID identifiziertes Archivdatenobjekt autorisiert ist.

Das ArchiSafe-Modul muss überprüfen können, ob eine Archivanfrage (z. B. Ablage, Ändere, Suchen, Löschen, etc.) ein zulässiger Befehl ist.

[77] Im behördlichen Umfeld sind weitere Vorschriften vorhanden.

9. Konformität und Interoperabilität

Dieses Kapitel erläutert die vorgesehenen Stufen der Konformität zu dieser TR und das Verfahren zum Nachweis dieser Konformität.

9.1 Konformität und Konformitätsprüfung

Es sind drei aufeinander aufbauende Stufen für die Konformitätsprüfung von einzelnen Modulen oder ganzen Systemen (siehe [HKS 12]) vorgesehen.

Diese drei Konformitätsstufen unterscheiden sich in technischen Detailspezifikationen der Schnittstellen und Formate.

Produkte und Systeme, die gemäß der Technischen Richtlinie 03125 TR-ESOR zertifiziert werden möchten, haben ihre Konformität gemäß den entsprechenden vorliegenden Testspezifikationen nachzuweisen.

Um entsprechend der angestrebten Konformitätsstufe zertifiziert zu werden, muss ein Produkt oder System alle Muss-Konformitätskriterien (Muss-Testfälle) für diese Konformitätsstufe und für alle tieferen Konformitätsstufen erfüllen.

Eine Komponente oder ein System ist konform gemäß der TR, wenn die Komponente bzw. das System die erforderliche Konformitätsprüfung ohne Abweichung von der für die Konformitätsstufe geltenden Spezifikationen durchlaufen hat.

Eine bestandene Konformitätsprüfung ist der Nachweis, dass die Komponente oder das System die technischen Anforderungen der TR erfüllt.

Ein zu prüfendes System kann komplett konform sein oder nur die Anforderungen einzelner Module implementieren.

Bzgl. der Konformitätsstufen ist das Folgende festzuhalten:

9.1.1 Konformitätsstufe 1 - Funktionale Konformität

Ein System oder eine Komponente ist funktional konform zu dieser Technischen Richtlinie, wenn das System oder die Komponente funktional auf die in dieser Richtlinie beschriebene Systemkomposition oder auf einzelne (auch mehrere) Module dieser Systemkomposition abgebildet werden kann und die Übereinstimmung zu den Anforderungen (Ax.y-z) an das Gesamtsystem oder an einzelne Module festgestellt wird.

Funktional konform im Sinne dieser TR bedeutet, dass die Komponenten die in dieser TR definierten funktionalen und sicherheitstechnischen Anforderungen erfüllen, die logische Abbildung der funktionalen Anforderungen nachvollziehbar dargestellt wird und die Komponenten zweckmäßig auf der Basis der in dieser TR aufgeführten Ziele und Standards miteinander arbeiten können.

Funktional komform im Sinne dieser TR bedeutet nicht, dass für die Ablage im ECM/Langzeitspeicher ausschließlich XML-basiert Archivdatenobjekte verwendet werden müssen.

Funktional konform im Sinne dieser TR bedeutet nicht, dass die Schnittstellen der Komponente bzw. des Systems den ASN.1- oder XML- Spezifikationen exakt entsprechen müssen.

Wesentliches Ziel dieser Konformitätsprüfung ist der Nachweis, dass das Modul bzw. das Gesamtsystem den entsprechenden Anteil für die Beweiswerterhaltung, funktional umsetzt. Die entsprechenden Testspezifikationen für die logisch-funktionale Konformitätsstufe 1 befinden sich in **([TR-ESOR-C.1])**.

9.1.2 Konformitätsstufe 2 - Technische Konformität ([TR-ESOR-C.2])

Ein System oder eine Komponente ist technisch konform, wenn zusätzlich zum Nachweis der funktionalen Konformität auch die oberste externe betreffende Schnittstelle S.x gemäß der Referenzarchitektur (siehe **[TR-ESOR-E]**, Abbildung 2) auf Basis der eCard-API, wie in **[TR-ESOR-E]** beschrieben,

umgesetzt ist sowie ein definiertes XML-Datenformat (z.B. XAIP), Beweisdatenformat[78] und VerificationReport-Format[79] für die Kommunikation und das Speichern verwendet wird.[80]

Wesentliches Ziel dieser zusätzlichen Prüfung ist der Nachweis, dass eine technische Interoperabilität auf Basis eines wohldefinierten Standards erreicht werden kann. Dies ist insbesondere dann relevant, wenn generell der Einsatz offener, interoperabler und standardisierter Datenformate und herstellerunabhängiger Schnittstellen entsprechend nationaler[81] und internationaler[82] Standards angestrebt wird oder wenn nur einzelne Module geprüft werden, die als eigenständige Produkte vertrieben werden und damit mit anderen Modulen/Systemen zusammen arbeiten müssen.

Die Prüfung der technischen Konformität umfasst dabei insbesondere:

1. die Prüfung der in **[TR-ESOR-E]** spezifizierten relevanten oberen externen Webservice-Schnittstelle,
2. die Prüfung der syntaktischen und semantischen Korrektheit der Evidence Records gemäß **[RFC4998]** bzw. **[RFC6283]**[83] und **[TR-ESOR-ERS]**,
3. die Prüfung der syntaktischen und semantischen Korrektheit der XAIP-Container,
4. die Prüfung des Prüfberichtes in Form eines VerificationReport-Elementes gemäß **[TR-ESOR-VR]**.

Als XML-Datenformat soll XAIP bzw. Delta-XAIP aus **[TR-ESOR-F]** verwendet werden. Abweichungen im verwendeten XML-Datenformat sind zulässig, allerdings muss dann erläutert werden, dass gleichwertige Funktionalität unterstützt wird. Insbesondere ist zu erläutern, wie eine Transformation in das XAIP Format aus **[TR-ESOR-F]** erfolgen kann.

Die entsprechenden Testspezifikationen für die technischeKonformitätsstufe 2 befinden sich in **([TR-ESOR-C.2])**.

9.1.3 Konformitätsstufe 3 - Konformität gemäß der Profilierung für Bundesbehörden

Die Testfälle der Konformitätsstufe 3 basieren auf den zusätzlichen Anforderungen gemäß Anhang **[TR-ESOR-B]**.

Die entsprechenden Testspezifikationen für die Konformitätsstufe 3 gemäß der Profilierung für Bundesbehörden befinden sich in **([TR-ESOR-C.3])**.

9.2 Beteiligte Instanzen bei der Konformitätsprüfung

Die folgenden Instanzen sind an einer Konformitätsprüfung beteiligt:

Antragsteller	Hersteller, Vertreiber oder Betreiber einer Komponente/eines Systems im Sinne dieser TR.
Prüfgegenstand	Komponente/System nach dieser TR, die/das zur Konformitätsprüfung bereitgestellt wird.
Prüfstelle	Vom BSI zugelassene Stelle oder Einrichtung, welche die Konformitätsprüfung durchführt.
Bestätigungsstelle	Konformitätsbestätigungsstelle des BSI.

9.2.1 Antragsteller

Der Antragsteller möchte die Konformität seines Systems oder seiner Komponente(n) gemäß einer der beiden oben angegebenen Stufen der TR prüfen und bestätigen lassen.

[78] RFC 4998 muss, RFC 6283 kann unterstützt werden.
[79] Siehe [TR-ESOR-VR]
[80] Es ist hier zu beachten, dass triviale XML-Datenformate, die lediglich ein proprietäres Format kapseln, nicht zulässig sind. Als XML-Datenformat soll XAIP aus Anhang F verwendet werden. Abweichungen im verwendeten XML-Datenformat sind zulässig, allerdings muss dann erläutert werden, dass gleichwertige Funktionalität unterstützt wird. Insbesondere ist zu erläutern, wie eine Transformation in das XAIP Format aus Anhang F erfolgen kann.
[81] SAGA, XÖV, ArchiSafe
[82] Moreq2, OASIS,
[83] RFC 4998 muss, RFC 6283 kann unterstützt werden.

Dazu stellt er beim BSI einen Antrag auf Bestätigung der Konformität seines Systems oder seiner Komponente(n). Das offizielle Antragsdatum ist für die Reihenfolge der Bearbeitung der verschiedenen Bestätigungsverfahren beim BSI maßgebend. Es wird dem Antragsteller vom BSI mitgeteilt, wenn der Antrag vollständig eingegangen ist und die Verfahrensnummer vergeben wurde.

Der Antragsteller schließt mit der Prüfstelle einen Vertrag zur Durchführung der Konformitätsprüfung.

Der Antragsteller verpflichtet sich, alle für die Durchführung der Konformitätsprüfung nötigen Informationen, den Prüfgegenstand selbst und ggf. erforderliche Testwerkzeuge und Schulungen zur Verfügung zu stellen. Er ist für die Richtigkeit seiner Angaben zu seinem System oder seiner Komponente verantwortlich.

9.2.2 Prüfgegenstand

Das System oder die Komponente, deren Konformität bestätigt werden soll, wird als Prüfgegenstand bezeichnet.

Dabei kann es sich um Software handeln, die auf einer bestimmten Plattform zur Ausführung kommt und in einer bestimmten Einsatzumgebung zu verwenden ist. Ebenso kann es sich um Hardwareprodukte handeln oder eine Kombinationen aus Software und Hardware.

Zum Zeitpunkt der Durchführung der Konformitätsprüfung muss der Prüfgegenstand vollständig vorliegen und die Entwicklung für den zur Prüfung eingereichten Versionsstand abgeschlossen sein. Der Versionsstand des Prüfgegenstandes wird bei Antragstellung festgehalten.

Nachbesserungen am Prüfgegenstand während der Konformitätsprüfung sind nur in Absprache mit dem BSI möglich.

9.2.3 Prüfstelle

Konformitätsprüfungen mit dem Ziel der Bestätigung durch das BSI werden von den durch das BSI zugelassenen Prüfstellen durchgeführt.

Eine Voraussetzung für die Zulassung ist die Einhaltung der DIN EN ISO/IEC 17025.

Die Prüfstelle ist für die Richtigkeit ihrer Prüfergebnisse verantwortlich und dokumentiert diese Ergebnisse in einem Prüfbericht. Die Durchführung der Konformitätsprüfung erfolgt erst, nachdem ein Antrag auf Konformität offiziell vom BSI angenommen wurde. Dazu stimmt die Prüfstelle die Planung und Durchführung der Konformitätsprüfung mit der Bestätigungsstelle des BSI aktiv ab. Diese Abstimmung beinhaltet die zeitliche Planung, die Planung der technischen Durchführung und Angaben zu den im Verfahren eingesetzten Prüfern.

Der Prüfbericht dokumentiert den Prüfablauf und die Ergebnisse. Er wird der Bestätigungsstelle zur Prüfung und Abnahme zur Verfügung gestellt. Den abschließenden Prüfbericht erhält der Antragsteller nach Abnahme durch die Bestätigungsstelle von der Prüfstelle.

Die durch das BSI zugelassenen Prüfstellen und das BSI haben einen Vertrag geschlossen, der ihre gegenseitigen Rechte und Pflichten regelt.

Die akkreditierte Prüfstelle ist verpflichtet, Herstellerinformationen und Prüfgegenstände sowie die Ergebnisse der Prüfungen vertraulich zu handhaben und sie vor unbefugter Kenntnisnahme zu schützen. Das need-to-know Prinzip ist anzuwenden. In der Kommunikation mit der Bestätigungsstelle ist die Vertraulichkeit zu wahren. Alle Prüfunterlagen sind als firmenvertraulich zu kennzeichnen.

Herstellerinformationen und Prüfberichte müssen in der Prüfstelle einem Konfigurationsmanagement unterliegen.

Die Dienstleistung der Prüfstelle muss in ein Qualitätsmanagementsystem der Prüfstelle eingegliedert sein.

Zugelassene Prüfstellen werden vom BSI in regelmäßig aktualisierten Publikationen veröffentlicht und können auf der BSI Webseite eingesehen werden.

9.2.4 Bestätigungsstelle

Aufgabe der Bestätigungsstelle ist es, den Ablauf der Konformitätsprüfung zu überwachen (Prüfbegleitung) und nach erfolgreich durchgeführter Prüfung den Konformitätsreport und den Konformitätsbescheid zu erstellen.

Die Bestätigungsstelle prüft den Antrag auf Bestätigung der Konformität. Bei der Abstimmung der Durchführung der Prüfung durch die im Antrag angegebene Prüfstelle werden die Angaben der Prüfstelle zur zeitlichen Planung, zur Planung der technischen Durchführung der Prüfung und ggf. die Angaben zur Kompetenz der genannten Prüfer geprüft. Lizenz- und Kompetenzfragen werden ggf. mit der Akkreditierungsstelle des BSI abgestimmt.

Nachdem die Antragsprüfung abgeschlossen ist, wird dem Antragsteller und der Prüfstelle das offizielle Antragsdatum und eine Verfahrensnummer mitgeteilt. Die Verfahrensnummer ist die Vorgangskennung beim BSI. Sie wird bei jedem Schriftwechsel zur Kennzeichnung der Dokumente und der Bestätigungsurkunde verwendet.

Die Bestätigungsstelle des BSI oder ein von ihr beauftragter BSI Mitarbeiter nimmt ggf. an Teilen der Durchführung der technischen Konformitätsprüfung teil. Der von der Prüfstelle vorgelegte Prüfbericht wird geprüft, ggf. kommentiert und abgenommen.

Zum Abschluss des Prüfverfahrens erstellt die Bestätigungsstelle ein Zertifikat sowie den zugehörigen Konformitätsbescheid.

Bestätigte Produkte und Systeme werden vom BSI – sofern der Antragsteller dem zustimmt – durch die Bestätigungsstelle veröffentlicht.

9.3 Abwicklung der Konformitätsprüfung

Konformitätsprüfungen werden von einer Prüfstelle durchgeführt. Die Prüfgegenstände durchlaufen bei der Konformitätsprüfung nacheinander die folgende drei Phasen:

1. Vorphase
2. Durchführung der Konformitätsprüfung
3. Konformitätsbestätigung

9.3.1 Vorphase

Die erste Phase besteht aus den Schritten:

- Beantragung durch den Antragsteller mit Angabe der Konformitätsstufe
- Antragsprüfung durch die Bestätigungsstelle
- offizielle Annahme des Antrags durch das BSI
- Abstimmung der Durchführung der Prüfung zwischen den Parteien
- Bereitstellung des Prüfgegenstands und der nach der TR notwendigen Unterlagen durch den Hersteller/Betreiber

9.3.2 Durchführung der Konformitätsprüfung

In der zweiten Phase wird die ausgewählte und parametrisierte Prüffolge durch die Prüfstelle abgearbeitet. Je nach Prüfmethode werden verschiedene Prüfverfahren oder Prüfwerkzeuge eingesetzt. Die während der Prüfung anfallenden Prüfresultate werden gesammelt und geeignet archiviert. Außerdem werden die während der Durchführung der Prüfung erzielten und beobachteten Prüfresultate analysiert und dokumentiert und es wird ein Prüfbericht erstellt. Dabei besteht die Konformitätsprüfung aus folgenden Schritten:

- Durchführung der technischen Prüfung durch die Prüfstelle entsprechend den Spezifikationen der TR und entsprechend der mit der Bestätigungsstelle abgestimmten Planung und Durchführung; ggf. beobachtende Begleitung der Prüfung vor Ort durch das BSI, um eine einheitliche Vorgehensweise und Methodik und ggf. vergleichbare Bewertungen sicherzustellen.
- Dokumentation der Teilschritte der Durchführung und der Ergebnisse der Prüfung in einem Prüfbericht durch die Prüfstelle.
- Prüfung, ggf. Kommentierung und Abnahme des Prüfberichtes durch das BSI.

Bei der Prüfung werden alle muss[84]-Anforderungen auf ihre uneingeschränkte Umsetzung hin überprüft. Eine Abweichung von den muss-Anforderungen ist nicht zulässig.

Ebenso werden alle soll-Anforderungen geprüft. Ihre Nichteinhaltung muss durch den Antragsteller, schlüssig und nachvollziehbar, schriftlich begründet werden.

kann-Anforderungen sind nicht Gegenstand der Prüfung.

9.3.3 Konformitätsbestätigung

Diese Phase umfasst:

- Erstellung des Konformitätsreportes, des Zertifikates und Erteilung des Konformitätsbescheides durch das BSI.
- Veröffentlichung des Ergebnisses, sofern dem der Antragsteller zugestimmt hat.

9.4 Interoperabilität

Während durch die funktionale Konformitätsprüfung die Übereinstimmung von implementierten Komponenten zu den eher funktionalen Anforderungen der TR festgestellt wird, bedeutet Interoperabilität zwischen konformen Komponenten, dass diese Komponenten auf einer technischen Ebene zusammenwirken können.

Die funktionale Konformität ist daher Voraussetzung für die Interoperabilität, aber nicht immer hinreichend. Wenn funktional konforme Komponenten jeweils verschiedene Anforderungen einer Spezifikation erfüllen, welche keine gemeinsame Schnittmenge haben, dann sind die Komponenten jeweils einzeln funktional konform zur Spezifikation, aber nicht miteinander interoperabel.

Im Rahmen dieser TR werden für die funktionale Konformitätsprüfung keine eigenen Interoperabilitätsprüfungen durchgeführt, sondern es wird durch geeignete Festlegungen der Konformitätskriterien erreicht, dass die Komponenten logisch und funktionell interoperabel gestaltet sind.

Für die technische Interoperabilitätsprüfung muss ein nachvollziehbarer technischer Nachweis erbracht werden, dass die geprüften Komponenten oder Module die mit Hilfe der eCard-API spezifizierten Schnittstellen korrekt implementiert haben.

[84] Diese Prüfungen beziehen sich natürlich auch auf alle Forderungen mit dem Wortlauf „ist“, „darf nicht“, etc.

10. Anlagen

Diese Technische Richtlinie umfasst dieses Hauptdokument und gemäß der empfohlenen Referenzarchitektur aus Kapitel 7 die folgenden Anlagen zu den in der Referenzarchitektur definierten Modulen (Komponenten) und Schnittstellen.

10.1 TR-ESOR-M.1 ArchiSafe-Modul

Die Anlage mit der Bezeichnung „TR-ESOR-M.1 ArchiSafe Modul“ spezifiziert und erläutert die funktionalen und sicherheitstechnischen Anforderungen an ein sicheres Gateway, welches den Informationsfluss innerhalb der Middleware und damit zusammenhängend auch den Zugriff auf den ECM/Langzeitspeicher für folgende Operationen regelt:

- die Ablage von Datenobjekten,
- das Ändern von Archivdatenobjekten (optional),
- den Abruf von Archivdatenobjekten (ganz oder teilweise),
- die Abfrage von Beweisdaten,
- das Prüfen von beweisrelevanten Daten und Beweisdaten (optional) und
- das Löschen von Archivdatenobjekten.

Ziel des ArchiSafe-Moduls ist die Realisierung einer strikten logischen Trennung der vorgelagerten IT-Fachanwendungen von den eigentlichen ECM-/Langzeitspeichersystemen. Bei der Ablage elektronisch signierter Daten und Dokumente sichert das ArchiSafe-Modul zudem die beweisrechtliche Qualität der zu archivierenden Informationen, indem

1) elektronische Signaturen auf Gültigkeit geprüft und die Prüfergebnisse in standardisierter Form in die XML-Dokumente eingebettet bzw. anderweitig abgelegt werden. Die Signaturprüfung wird durch kryptographische Module realisiert, die den in der Anlage TR-ESOR-M.2 beschriebenen Anforderungen genügen müssen. Die Schnittstelle zwischen dem ArchiSafe-Modul und den kryptographischen Einheiten ist in Anlage TR-ESOR-S (dort S.1) spezifiziert.

2) das für die Signaturerneuerung verantwortliche ArchiSig-Modul (siehe Anlage TR-ESOR-M.3) die Archivdatenobjekt ID (AOID) nach der dort durchgeführten Hashwertberechnung zurück gibt. Nur mittels dieser AOID wird ein späterer Zugriff auf das Archivdatenobjekt möglich.

Darüber hinaus bietet dieses Modul einheitliche Schnittstellen zur Kommunikation mit den kryptographischen Komponenten (TR-ESOR-M.2 und TR-ESOR-M.3), die den Erhalt des Beweiswertes der gespeicherten elektronischen Unterlagen unterstützen.

Jeder Archivaufruf von einer vorgelagerten, externen IT-Anwendung zur Ablage, zum Ändern oder zum Abruf archivierter Daten und Dokumente in bzw. aus dem ECM/Langzeitspeicher mit dem Nebenziel des Beweiswerterhaltes muss über das ArchiSafe-Modul erfolgen.

Die externe IT-Anwendung öffnet zu diesem Zweck einen sicheren Kommunikationskanal mit dem ArchiSafe-Modul und versendet eine Archivanfrage. Das ArchiSafe-Modul identifiziert und authentifiziert die aufrufende Anwendung und überprüft die syntaktische Gültigkeit der von der aufrufenden Anwendung übermittelten Archivanfrage anhand der im ArchiSafe-Modul abgelegten Konfigurationsdaten (z.B. XML-Schemata, Kommunikations- und Verarbeitungsregeln).

10.2 TR-ESOR-M.2 Krypto-Modul

Die Anlage mit der Bezeichnung „TR-ESOR-M.2 Krypto-Modul“ spezifiziert und erläutert die funktionalen und sicherheitstechnischen Anforderungen an kryptographische Module zur Erstellung und Prüfung elektronischer Signaturen und zur Einholung von qualifizierten Zeitstempeln.

Das Krypto-Modul stellt benötigte kryptographische Funktionen zentral bereit, die für den Beweiswerterhalt benötigt werden. Im Wesentlichen umfasst dies kryptographische Verfahren, die für das Erzeugen und Verifizieren von elektronischen Signaturen bzw. Zeitstempeln und die Hashwert-Erzeugung benötigt werden.

Das Krypto-Modul besitzt folgende kryptographischen Funktionen, es implementiert keine fachlichen Prozesse:

- Kryptographische Funktionen:
  - Erzeugung einer digitalen Signatur (optional)
  - Verifikation von digitalen Signaturen; insbesondere von signierten Archivdatenobjekten und von darin eingebetteten signierten Nutzdatenobjekten und ggf. Beweisdaten
  - Validierung von Zertifikaten
  - Erzeugung eines Hashwertes
  - Anforderung eines qualifizierten Zeitstempels
  - Verifikation eines qualifizierten Zeitstempels

Des Weiteren beschreibt diese Anlage grundlegende Anforderungen an eingesetzte Algorithmen sowie an erforderliche Sicherheitsfunktionalitäten und die Konfiguration des Krypto-Moduls.

10.3 TR-ESOR-M.3 ArchiSig-Modul

Die Anlage mit der Bezeichnung „TR-ESOR-M.3 ArchiSig-Modul“ spezifiziert und erläutert die funktionalen und sicherheitstechnischen Anforderungen an ein kryptographisches Modul zum Erhalt und der Erneuerung der Beweiskraft elektronischer Signaturen nach dem ERS-Standard der IETF ([RFC4998] bzw. [RFC6283])[85].

Kryptographische Operationen wie elektronische Signaturen ermöglichen es nur dann, die Integrität und Authentizität elektronischer Daten nachweisbar zu machen, wenn die den Signaturen zugrunde liegenden Algorithmen mathematisch und technisch sicherheitsgeeignet sind. Ein dauerhafter und nachweisbarer Erhalt der Authentizität und Integrität elektronischer Daten erfordert deshalb den Einsatz zusätzlicher Sicherungsmittel, die den Nachweis ermöglichen, dass insbesondere elektronisch signierte Daten über die Dauer der Aufbewahrungsfristen unverfälscht aufbewahrt wurden.

Aufgabe des ArchiSig-Moduls ist der Erhalt des Beweiswertes durch zusätzliche kryptographische Sicherungsmittel und die Erzeugung und Rückgabe von Beweisdaten.

Das ArchiSig-Modul implementiert für diesen Zweck eine kryptographische Lösung, die insbesondere sicherstellt, dass das durch § 17 Signaturverordnung (SigV) normierte Verfahren zur Aufrechterhaltung der Sicherheit und Vertrauenswürdigkeit elektronischer Signaturen durch eine erneute Signatur zuverlässig und wirtschaftlich, d. h. auch für große Datenmengen, erfüllt werden kann. Die erneute elektronische Signatur muss die Daten und frühere Signaturen einschließen und mit sicherheitsgeeigneten kryptographischen Algorithmen und Parametern erzeugt werden. Für die erneute elektronische Signatur ist zumindest ein qualifizierter Zeitstempel notwendig, der eine qualifizierte elektronische Signatur trägt. Das Erneuerungsverfahren kann automatisiert und so eingerichtet werden, dass viele Dokumente gemeinsam elektronisch neu signiert werden. Bei elektronischen Signaturen auf Basis von qualifizierten Zertifikaten, herausgegeben von Zertifizierungsdiensteanbietern mit Anbieterakkreditierung, müssen qualifizierte Zeitstempel akkreditierter Zertifizierungsdiensteanbieter verwendet werden.

Grundlage des ArchiSig-Moduls ist die informationstechnische Umsetzung des Evidence Record Syntax (kurz: ERS) Standards der IETF ([RFC4998] bzw. [RFC6283]). ERS definiert im Detail, wie Signaturerneuerungen für große Dokumentenmengen automatisch durchgeführt werden können. Darüber hinaus legt der Standard die Datenformate fest, in denen die Beweisdaten über einen unbegrenzten Zeitraum bereitgestellt und ausgetauscht werden. Datenschutz-technische Aspekte werden ebenso berücksichtigt, da mit demERS-Standard auch Teile aus dem Dokumentenbestand gelöscht werden können, ohne die Beweiskraft der übrigen Teile zu beeinträchtigen.

Technisch basiert der ERS-Standard auf dem Ansatz, dass kryptographische Prüfsummen (Hashwerte) der Archivdatenobjekte als kryptographisch eindeutige Repräsentanten der aufzubewahrenden Daten bei der Ablage im ECM/Langzeitspeicher zusätzlich mit einem qualifizierten Archivzeitstempel gesichert werden.

[85] RFC 4998 muss, RFC 6283 kann unterstützt werden.

10.4 TR-ESOR-S Schnittstellen

Die Anlage mit der Bezeichnung „TR-ESOR-S“ spezifiziert und erläutert die funktionalen und sicherheitstechnischen Anforderungen an die Schnittstellen zwischen den einzelnen Komponenten der TR-ESOR-Middleware und auch zwischen der Middleware und den externen Systemen.

Die Schnittstellen wurden möglichst generisch festgelegt und in ASN.1-Notation spezifiziert. Daraus ergeben sich jedoch keine Anforderungen an spezielle Codierungsverfahren oder einfache Datentypen, wenn diese nicht explizit angegeben sind.

Dieser Anhang gibt wesentliche Kriterien für die ***funktionale Konformitätsprüfung*** vor.

10.5 TR-ESOR-ERS Profilierung der Evidence Records gemäß RFC4998 und RFC6283

Der Anhang ERS “Evidence Record Syntax” spezifiziert ein Interoperabilitätsprofil für technischen Beweisdaten (Evidence Record) gemäß **[RFC4998]** bzw. **[RFC6283]**. Dieses Profil soll eine langfristige und weitgehend system- und plattformunabhängige Interpretierbarkeit technischer Beweisdaten zwischen unterschiedlichen TR-ESOR-Implementierungen sicher stellen.

Dieser Anhang gibt wesentliche Kriterien für die Prüfung der technischen *Konformität* vor.

10.6 TR-ESOR-VR Verification Reports for Selected Data Structures

Der Anhang VR “Verification Reports for Selected Data Structures” beschreibt und spezifiziert die Prüfberichte für ein Archivdatenobjekt und ggf. auch für die dazugehörigen Beweisdaten. Dieser Anhang steht gegenwärtig nur in englischer Fassung zur Verfügung. Die deutsche Übersetzung ist geplant.

Dieser Anhang gibt wesentliche Kriterien für die Prüfung der technischen *Konformität* vor.

10.7 TR-ESOR-F Formate

Die Anlage mit der Bezeichnung „TR-ESOR-F Formate“ (**[TR-ESOR-F]**) spezifiziert mit dem `<XAIP>`-Element ein XML-basiertes Containerformat für Archivdatenobjekte (XAIP), das von TR-konformen Middlewarekomponenten erzeugt und verarbeitet wird, sowie mit dem `<DXAIP>`-Element eine beim `ArchiveUpdateRequest` (vgl. TR-ESOR-E) übergebene Delta-XAIP-Struktur.

Darüber hinaus spezifiziert und erläutert die Anlage F (**[TR-ESOR-F]**) die funktionalen und sicherheitstechnischen Anforderungen an Datenformate für die Ablage der Nutzdaten, Metainformationen und Signaturdaten (Archivdatenobjekte). Weiterhin werden in diesem Dokument die empfohlenen Formate für die Kommunikation mit externen Systemen und Partnern, wie bspw. den Zertifizierungsdiensteanbietern, erläutert.

10.8 TR-ESOR-B Profilierung für Bundesbehörden

Die Anlage B **„**Profilierung für Bundesbehörden**”** konkretisiert Anforderungen, Datenformate und Protokolle für die beweiserhaltende Aufbewahrung kryptografisch signierter Daten und Dokumente speziell für die Belange in der Bundesverwaltung.

„Dieses Profil sollte von Bundesbehörden mindestens dann angewendet werden, wenn die Neubeschaffung oder die Aktualisierung eines Archivsystems oder einer Archiv-Middleware für die Aufbewahrung von kryptographisch signierten Unterlagen ansteht. Für bestehende Installationen, mit denen kryptographisch signierte Unterlagen für lange Zeit aufbewahrt werden sollen, wird die Anwendung dieses Profiles nachdrücklich empfohlen“ (siehe **[TR-ESOR-B]**).

10.9 TR-ESOR-E Konkretisierung der Schnittstellen auf Basis des eCard-API-Frameworks

Die genannte Anlage E (**[TR-ESOR-E]**) beinhaltet eine XML-basierte Spezifikation der verschiedenen in **[TR-ESOR-S]** eingeführten Funktionen zur Beweiswerterhaltung kryptographisch signierter Dokumente.

Dieser Anhang stellt die Basis für die Prüfung der ***technischen Konformität*** dar. Für die Stufe „Funktionale Konformität“ ist dieses Dokument nicht von Belang.

10.10 TR-ESOR-C.1 Conformity Test Specification (Level 1 - Functional Conformity)

Der Anhang C.1 “Conformity Test Specification (Level 1 - Functional Conformity)” beschreibt und spezifiziert die Konformitätstestfälle bezüglich des Konformitätslevels 1 “Funktionale Konformität”. Dieser Anhang steht gegenwärtig nur in englischer Fassung zur Verfügung. Die deutsche Übersetzung ist geplant.

10.11 TR-ESOR-C.2 Conformity Test Specification (Level 2 - Technical Conformity)

Der Anhang C.2 “Conformity Test Specification (Level 2 - Technical Conformity)” beschreibt und spezifiziert die Konformitätstestfälle bezüglich des Konformitätslevels 2 “Technische Konformität”. Dieser Anhang steht gegenwärtig nur in englischer Fassung zur Verfügung. Die deutsche Übersetzung ist geplant.

10.12 TR-ESOR-C.3 Conformity Test Specification (Level 3 - Conformity with Federal Agency Profile)

Der Anhang C.3 “Conformity Test Specification (Level 3 - Technical Conformity)” beschreibt und spezifiziert die Konformitätstestfälle bezüglich des Konformitätslevels 3 “Technische Konformität gemäß der Profilierung für Bundesbehörden”.

Dieser Anhang steht gegenwärtig nur in englischer Fassung zur Verfügung. Die deutsche Übersetzung ist geplant.

11. Abkürzungsverzeichnis

AIP	Archival Information Package
AOID	Archive Object ID (Identifier)
API	Application Programming Interface
ARS	ArchiSafe Recordkeeping Strategy
ASCII	American Standard Code for Information Interchange
ASN.1	Abstract Syntax Notation One
ATS	Archive Timestamp
BaFin	Bundesanstalt für Finanzdienstleistungsaufsicht
BArchG	Bundesarchivgesetz
BDSG	Bundesdatenschutzgesetz
BFH	Bundesfinanzhof
BGB	Bürgerliches Gesetzbuch
BGBl	Bundesgesetzblatt
BGH	Bundegerichtshof
BMF	Bundesministerium für Finanzen
BMI	Bundesministerium des Innern
BMWi	Bundesministerium für Wirtschaft und Technologie
BNetzA	Bundesnetzagentur für Elektrizität, Gas, Telekommunikation, Post u. Eisenbahnen
BSI	Bundesamt für Sicherheit in der Informationstechnik
BStBl	Bundesteuerblatt
CA	Certification Authority
CC	Common Criteria for Information Technology Security Evaluation
CCITT	Comité Consultatif International Téléphonique et Télégraphique
CMS	Cryptographic Message Syntax
CRL	Certificate Revocation List (Zertifikatsperrliste)
DIN	Deutsches Institut für Normung
DOMEA	Dokumentenmanagement und elektronische Archivierung im IT-gestützten Geschäftsgang
DSS	Digital Signature Standard
DSSC	Data Structure for Security Suitability's of Cryptographic Algorithms
DTD	Document Type Definition
ECM	Enterprise Content Management
ERS	Evidence Record Syntax
ETSI	European Telecommunications Standards Institute
EuGH	Europäischer Gerichtshof
GDPdU	Grundsätze zum Datenzugriff und zur Prüfbarkeit digitaler Unterlagen
GoB	Grundsätze ordnungsgemäßer Buchführung
GoBS	Grundsätze ordnungsgemäßer DV gestützter Buchführungssysteme
HSM	Hardware Security Module
HTTP	Hypertext Transfer Protocol
IETF	Internet Engineering Task Force
IPSec	Internet Protocol Security
ISIS-MTT	Industrial Signature Interoperability Specification-Mailshot
ISO	International Organization for Standardization
IT	Informationstechnologie

ITSEC	Information Technology Security Evaluation Criteria
JPEG	Joint Photographic Experts Group
LDAP	Lightweight Directory Access Protocol
MIME	Multipurpose Internet Mail Extension
NIST	National Institute of Standards and Technology (USA)
OAIS	Open Archival Information System
OCSP	Online Certificate Status Protocol
ODF	Open Document Format
OSCI	Online Service Computer Interface
PDF	Portable Document Format
PK-DML	Prüfkriterien für Dokumentenmanagement-Lösungen
PKCS	Public Key Cryptography Standard
PKI	Public Key Infrastructure
PKIX	PKI-Arbeitsgruppe der IETF
PNG	Portabe Network Graphics Format
PP	Protection Profile
RFC	Request for Comments
S/MIME	Secure Multipurpose Internet Mail Extension
SAGA	Standards und Architekturen für E-Government-Anwendungen
SASL	Simple Authentication and Security Layer
SCVP	Server-Based Certificate Validation Protocol
SigG	Gesetz über Rahmenbedingungen für elektronische Signaturen-(deutsches) Signaturgesetz
SigV	Verordnung zur elektronischen Signatur-(deutsche) Signaturverordnung
SMTP	Simple Mail Transfer Protocol
SNIA	Storage Network Industry Association
SSL	Secure Sockets Layer (Protocol)
ST	Security Target
TAP	Trustworthy Archival Protocol
TC	Trust Center
TCP/IP	Transmission Control Protocol / Internet Protocol
TIFF	Tagged Image File Format
TLS	Transport Layer Security
TS	Time Stamping
TSP	Time Stamp Protocol
UML	Unified Modelling Language
URI	Uniform Resource Identifier
URL	Uniform Resource Locator
USB	Universal Serial Bus
WWW	Word Wide Web
XAIP	XML formatted Archival Information Package
XML	eXtensible Markup Language
XSD	XML Schema Definition
ZDA	Zertifizierungsdiensteanbieter
ZPO	Zivilprozessordnung

12. Glossar

Absender	Eine externe (vorgelagerte) IT-Anwendung (Client Software), die Daten zur Archivierung an das Archivsystem übergibt.
Abstract Syntax Notation One (ASN.1)	Die Abstract Syntax Notation One (ASN.1) ermöglicht es, die Syntax von Daten präzise und unabhängig von der tatsächlichen Codierung zu beschreiben. Sie wurde im Rahmen des [X.408]-Standards entwickelt und dann in [X.680] standardisiert.
Akkreditierung	Die Akkreditierung ist gemäß § 2 Nr. 15 SigG ein freiwilliges „Verfahren zur Erteilung einer Erlaubnis für den Betrieb eines Zertifizierungsdienstes, mit der besondere Rechte und Pflichten verbunden sind“. Zu den Pflichten des akkreditierten Zertifizierungsdiensteanbieters gehört bspw., dass er geprüfte und bestätigte Produkte einsetzen muss (§ 15 Abs. 7 SigG), dass er, sofern er Zertifikate ausstellt, diese mindestens 30 Jahre nach Ablauf der Gültigkeit des Zertifikates nachprüfbar halten muss, und dass er sein Sicherheitskonzept von einer von der Bundesnetzagentur anerkannten Stelle auf seine Eignung und praktische Umsetzung hin prüfen und bestätigen lassen muss.
Anscheinsbeweis	Ein Anscheinsbeweis liegt vor, wenn ein erwiesener Sachverhalt der Lebenserfahrung nach auf einen bestimmten (typischen) Ablauf eines damit zusammenhängenden Sachverhalts hinweist, dieser also indirekt dem Anschein nach bewiesen wird. Anscheinsbeweis (prima-facie-Beweis) ist möglich bei typischen Geschehensabläufen. Steht ein Sachverhalt fest, der nach aller Lebenserfahrung auf einen bestimmten Geschehensablauf hinweist, kann dieser Ablauf als bewiesen angesehen werden. Der Anscheinsbeweis ist gesetzlich nicht geregelt. Das Gesetz nimmt aber vereinzelt auf den Anscheinsbeweis Bezug (so etwa § 371a der deutschen Zivilprozessordnung für qualifizierte elektronische Signaturen).
ArchiSafe	Im Rahmen des E-Government Projektes des Bundes "ArchiSafe Rechtssichere Langzeitarchivierung elektronischer Dokumente" wurden die Grundlagen für eine kostengünstige und skalierbare elektronische Archivlösung definiert und in Form eines Pilotsystems realisiert. Die während des Projektes erarbeiteten informationstechnischen Konzepte ermöglichen die dauerhafte sichere elektronische Ablage digitaler Unterlagen. Das Projekt knüpft bewusst an die Ergebnisse des Projektes "ArchiSig – Beweiskräftige und sichere Langzeitarchivierung digital signierter Dokumente" an, in dem wesentliche Grundlagen der die Beweiskraft erhaltende Archivierung elektronisch signierter Dokumente erarbeitet wurden. Mehr dazu unter http://www.archisafe.de Im Rahmen der Technischen Richtlinie bezeichnet der Begriff „ArchiSafe-Modul“ eine einheitliche, funktionale Archivschnittstellenkomponente, die ein strikte logische Trennung vorgelagerter IT-Fachanwendungen von den eigentlichen Langzeitspeichersystemen gewährleistet und so imstande ist, unberechtigte Zugriffe auf das Langzeitspeichersystem zuverlässig zu verhindern.

ArchiSig

ArchiSig ist ein vom Bundesministerium für Wirtschaft und Technologie (BMWi) im Rahmen des Programms „VERNET – Sichere und verlässliche Transaktionen in offenen Kommunikationsnetzen“ gefördertes Verbundprojekt zur beweiskräftigen und sicheren Langzeitspeicherung digital signierter Dokumente. Im Rahmen des Projektes ArchiSig wurden aus den allgemeinen gesetzlichen Regelungen konkrete rechtliche Anforderungen an Systeme zur langfristigen Aufbewahrung elektronisch signierter Dokumente abgleitet und prototypisch implementiert. Es konnte erstmalig gezeigt werden, dass die Langzeitaufbewahrung elektronisch signierter Dokumente gesetzeskonform, performant und akzeptabel umgesetzt werden kann.

Mehr dazu unter: http://www.archisig.de

Im Rahmen der Technischen Richtlinie bezeichnet der Begriff „ArchiSig-Modul“ eine kryptographische Lösung, welche die Nachweisbarkeit von Authentizität, Integrität und damit des beweisrechtlichen Werts vor allem elektronisch signierter Dokumente durch zusätzliche kryptographische Sicherungsmittel entsprechend der gesetzlichen Anforderungen gewährleistet. Das ArchiSig-Modul implementiert für diesen Zweck eine kryptographische Lösung, die insbesondere sicherstellt, dass das durch § 17 SigV skizzierte Verfahren zur Aufrechterhaltung der Sicherheit und Vertrauenswürdigkeit elektronischer Signaturen durch eine erneute Signatur zuverlässig und wirtschaftlich, d. h. auch für große Datenmengen, erfüllt werden kann.

Archivanfrage
(Archive Request)

Eine XML-basierte Nachricht, die von einer autorisierten externen Anwendung (Client Software) zum ArchiSafe-Modul übertragen wird und eine →Archivoperation auslöst.

Archivdatenobjekt
(Archival Information Packages, AIP)

Ein Archivdatenobjekt im Sinne dieser Richtlinie ist ein selbst-beschreibendes und wohlgeformtes XML-Dokument, das gegen ein gültiges und autorisiertes XML-Schema geprüft werden kann.

Archivierung, elektronische A.

Die dauerhafte und unveränderbare Aufbewahrung (Speicherung) von elektronischen Dokumenten und anderen Daten wird im informationstechnischen Sprachgebrauch allgemein als „elektronische Archivierung“ bezeichnet. Der mit dem Begriff „dauerhaft“ bezeichnete Zeithorizont ist dabei aus informationstechnischer Sicht die Umschreibung eines nicht näher fixierten Zeitraums, in dem wesentliche, im Allgemeinen aber kaum vorhersehbare technische oder technologische Veränderungen eintreten können, die u. U. dazu führen, dass die informationstechnischen Systeme, mit denen Dokumente ursprünglich erfasst, erstellt und gespeichert wurden, nicht mehr zur Verfügung stehen. Hierfür wird im deutschen Sprachgebrauch mitunter auch der Begriff der „elektronischen (digitalen) Langzeitspeicherung“ verwendet, um den Unterschied zur kurzzeitigen „lebenden Schriftgutablage“ bzw. zum Backup hervorzuheben.

Aus rechtlicher Sicht ist der Begriff der Archivierung durch die Archivgesetze des Bundes und der Länder konkretisiert und belegt und daher von der zeitlich beschränkten Aufbewahrung zu unterscheiden. „Archivierung“ im juristisch korrekten Sinne betrifft allein Unterlagen der öffentlichen Verwaltung und bezieht sich darauf, dass Unterlagen einer Behörde, sobald sie für die Zwecke der Behörde nicht mehr benötigt werden, ausgesondert und durch eine zuständige staatliche Einrichtung (Archiv) auf unbegrenzte Zeit verwahrt werden sollen (vgl. §§ 1 und 2 BArchG).

Archivoperation

Eine Archivoperation ist zunächst eine Ausführung definierter Funktionen (Operationen) in der TR-ESOR-Middleware. Das Ausführen dieser Funktionen zieht i.d.R. eine Funktion im Langzeitspeicher nach sich.

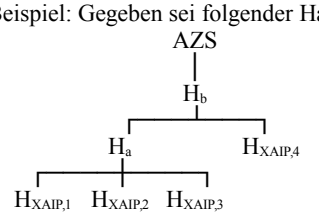
Archivzeitstempel

Ein Archivzeitstempel ist ein Zeitstempel, der in Verbindung mit einer elektronischen Signatur bestätigt, dass bestimmte zur Ablage im Archiv vorgesehene Daten zu einem bestimmten Zeitpunkt vorgelegen haben. Dies wird dadurch erreicht, dass der Zeitstempel sich auf die →Hashwerte der entsprechenden Daten bezieht.

Nach dem ArchiSig-Konzept muss nicht jedes Dokument einzeln zeitgestempelt werden. Vielmehr genügt es, →Hashbäume, die viele Dokumente repräsentieren, mit einer Signatur oder mit einem Zeitstempel, der eine Signatur enthält, an der Wurzel zu versehen.

Der sog. „reduzierte Hashbaum“ umfasst genau die Menge an Einträgen dieses Hashbaumes, die für den Nachweis der Integrität eines Dokumentes notwendig sind.

Beispiel: Gegeben sei folgender Hashbaum:



Der „reduzierte Hashbaum“ für $H_{XAIP,2}$ besteht aus $H_{XAIP,1}$, $H_{XAIP,3}$ und $H_{XAIP,4}$. H_a und H_b können über die gelieferten Werte erschlossen und mit AZS der Integritätsnachweis geführt werden.

Asymmetrische Kryptoalgorithmen

Für asymmetrische kryptographische Algorithmen existiert ein komplementäres Schlüsselpaar (privater und öffentlicher Schlüssel), das zur Realisierung digitaler Signaturen, zur Vereinbarung geheimer Schlüssel oder zur Verschlüsselung verwendet werden kann. Das Konzept asymmetrischer Kryptoalgorithmen geht zurück auf W. Diffie und M. Hellman [DiHe 76]. Der heute gebräuchlichste asymmetrische Algorithmus ist der RSA-Algorithmus.

Authentifikation, Authentifizierung

Dient dem Nachweis der Identität eines Benutzers oder eines Kommunikationspartners bzw. der Quelle einer Nachricht. Bei der Authentifizierung werden zur Feststellung der Identität Zertifikate einer vertrauenswürdigen Instanz verwendet. Zur Überprüfung der Unversehrtheit (und der Quelle) einer Nachricht dienen Funktionen, die einen kryptographisch gesicherten (signierten) „Fingerabdruck“ der unkodierten Originalnachricht erstellen und mit versenden.

Authentizität

Elektronische →Daten sind authentisch, wenn sie mit den Ursprungsdaten übereinstimmen und ihnen zweifelsfrei die Identität eines Ausstellers (Verfassers, Erstellers und/oder Absenders) zugeordnet werden kann.

BArchG

Das **Bundesarchivgesetz** oder Gesetz über die Sicherung und Nutzung von Archivgut des Bundes in Deutschland bestimmt, wie das Archivgut des Bundes durch das Bundesarchiv auf Dauer zu sichern, nutzbar zu machen und wissenschaftlich zu verwerten ist.

Archive in diesem Zusammenhang sind (staatliche) Einrichtungen, die die Unterlagen aller Behörden ihres Zuständigkeitsbereichs - im Falle des Bundesarchivs (= Staatsarchiv der Bundesregierung und Bundesverwaltung) also aller Bundesbehörden - übernehmen, bewerten und für die spätere Nutzung im Archiv erschließen und bereitstellen, sobald diese für die Zwecke der Behörde, bei der sie entstanden sind, nicht mehr benötigt werden (§§1 und 2 BArchG). Die Archivierung erfolgt hier nicht auf lange, sondern auf unbegrenzte Zeit (dauerhaft „für die Ewigkeit“. Vgl. Bundesarchivgesetz, Handkommentar, Baden-Baden 2006, § 1 Rz 18).

BASE64

Base64 ist ein Begriff zur Kodierung von Binärdaten in eine Zeichenfolge, die nur aus wenigen, Codepage-unabhängigen ASCII-Zeichen besteht. Das Verfahren findet vor allem im Internet-Standard MIME (Multipurpose Internet Mail Extensions) Anwendung und wird damit z. B. beim Versenden von E-Mail-Anhängen verwendet. Nötig ist dies, um den problemlosen Transport von beliebigen Binärdaten zu gewährleisten, da SMTP in seiner ursprünglichen Fassung nur für den Versand von 7-Bit ASCII-Zeichen ausgelegt war.

Zur Kodierung werden jeweils drei Byte des Bytestroms (=24 bit) in vier 6-bit-Blöcke aufgeteilt. Jeder dieser 6-bit-Blöcke bildet eine Zahl zwischen 0 und 63, woraus sich auch der Name des Algorithmus erklärt. Diese Zahlen werden anhand einer Umsetzungstabelle in „druckbare ASCII-Zeichen“ umgewandelt und ausgegeben.

Durch diese Kodierung steigt der Platzbedarf um ca. 36% an (33% durch die Kodierung an sich, weitere 3% durch Zeilenumbrüche).

Beweisdaten, technische

Technische Beweisdaten (engl. Evidence Records) dienen dem Nachweis der Unversehrtheit der Integrität und Authentizität der archivierten Datenobjekte. In Übereinstimmung mit den Spezifikationen des ERS-Standards der IETF enthält ein technischer Beweisdatensatz Archivzeitstempel ausreichender Qualität über die gespeicherten (signierten) →Archivdatenobjekte, die die Unversehrtheit der Daten nachweisen, und zusätzlich Informationen, welche die Richtigkeit und die Gültigkeit elektronischer Signaturen zum Signaturzeitpunkt sowie die rechtzeitige Signaturerneuerung entsprechend der rechtlichen Anforderungen belegen.

Beweisrelevante Daten

Beweisrelevante →Daten sind Signaturen bzw. Zeitstempel zu genau einem Datenobjekt bzw. Dokument und enthalten auch die für die Prüfung der Signatur bzw. Zeitstempelsignatur notwendigen Prüfdaten wie z. B. Zertifikate sowie CRL-Listen und OCSP-Responses zu diesen Zertifikaten.

Die →Beweisdaten belegen, dass das Dokument ab dem Zeitpunkt der Archivierung nicht mehr verändert wurde. Die beweisrelevanten Daten belegen, dass die ggf. außerhalb des Archives erzeugten Signaturen und Zeitstempel gültig sind bzw. zum Erstellungszeitpunkt gültig waren.

Beweiswerterhalt

Beweiswerterhalt im Sinne dieser technischen Richtlinie bedeutet, dass ein zu dieser Richtlinie konformes System imstande ist, den beweisrechtlichen Wert der in ihm aufbewahrten elektronischen Informationen über die Dauer des Aufbewahrungszeitraumes zu erhalten und so die mit der Aufbewahrung bezweckten Rechtsfolgen elektronischer Unterlagen mindestens für die Dauer der gesetzlich vorgeschriebenen Aufbewahrungs-zeiträume zu gewährleisten. Technisch wird dies durch →Beweisdaten und →beweisrelevante Daten realisiert.

Client Software

Eine externe (vorgelagerte) IT-Anwendung, die imstande und autorisiert ist, über das →ArchiSafe-Modul Daten im Langzeitspeicher zu archivieren, archivierte Daten zu suchen, abzurufen oder zu löschen.

Common Criteria (CC)

Mit den Common Criteria for Information Technology Security Evaluation (kurz. Common Criteria [CC]) wurde ein internationaler Standard (ISO 15408) für die Bewertung und Zertifizierung der Sicherheit von Computersystemen geschaffen. Die CC sehen verschiedene Vertrauenswürdigkeitsstufen (Evaluation Assurance Level) vor, von den Stufen „EAL 1“ (funktionell getestet) bis „EAL 7“ (formal verifizierter Entwurf und getestet).

Cryptographic Message Syntax (CMS) **RFC 5652**	Die Cryptographic Message Syntax (CMS) ist eine durch die Internet Engineering Task Force (IETF) veröffentlichte Spezifikation, die in ASN.1 Syntax beschreibt, wie Daten durch kryptographische Maßnahmen wie digitale Signaturen oder Verschlüsselung geschützt, respektive Signaturdaten über das Internet ausgetauscht werden können. Sie basiert auf dem ursprünglich durch die RSA Laboratories veröffentlichten PKCS#7 (Public Key Cryptography Standard) Dokument in der Version 1.5, das eine allgemeine Syntax für Daten darstellt, auf die kryptographische Operationen wie digitale Signaturen oder digitale Umschläge angewendet wurden. Der PKCS#7v1.5 Standard ist Grundlage des S/MIME Protokolls und der in PDF-Dokumenten eingebetteten elektronischen Signaturen sowie der Authentizitätssicherung von ausführbaren Software-Dateien. Die Syntax ist rekursiv, so dass Daten und Umschläge verschachtelt oder bereits chiffrierte Daten unterschrieben werden können. Die Syntax ermöglicht zudem, dass weitere Attribute, wie z. B. Zeitstempel, mit den Daten oder dem Nachrichteninhalt authentifiziert werden können und unterstützt eine Vielzahl von Architekturen für die Schlüsselverwaltung auf der Basis von elektronischen Zertifikaten.
Daten	Oberbegriff für alle Informationen, die von elektronischen Medien gelesen, elektronisch verarbeitet oder auf elektronischen Medien gespeichert werden. In der Informationstechnik werden häufig Daten von Dokumenten unterschieden. Siehe auch →Datenmodell
Datenmodell	beschreibt innere Strukturen und Beziehungen von → Daten untereinander. Die Beschreibung des Modells erfolgt in der Regel durch eine formale Darstellung, bspw. durch ein UML-Klassendiagramm und zusätzliche textuelle Beschreibung.
Deterministischer Algorithmus	ein Algorithmus, der zu einer bestimmten Eingabe immer die gleiche Folge von Operationen ausführt, d. h. zu jedem Zeitpunkt ist die folgende Operation des Algorithmus eindeutig festgelegt.
Dokument, elektronisch	ist ein Text, eine Zahlentabelle, ein Bild oder eine Folge oder Kombination von Texten, Tabellen oder Bildern, die durch Digitalisieren (Umwandlung in einen Binärcode) in Dateiform angelegt oder überführt wurden. Im weiteren Sinne bezieht sich der Begriff auf alle Arten von schwach strukturierten oder unstrukturierten Informationen, die als geschlossene Einheit in einem EDV-System als Datei vorliegen. (Quelle: Wikipedia)
DOMEA	DOMEA steht für „Dokumentenmanagement und elektronische Archivierung im IT-gestützten Geschäftsgang“ und ist ein Konzept für Dokumentenmanagement und elektronische Archivierung in der öffentlichen Verwaltung. Wesentliches Ziel des DOMEA-Konzeptes ist die Einführung der elektronischen Akte als Weiterentwicklung des Konzeptes „Papierarmes Büro“ aus dem Jahr 1996. Da für die elektronische Akte die gleichen Gesetze, Geschäftsordnungen, Richtlinien und Vorschriften wie für Papierakten gelten, müssen behördliche Geschäftsprozesse, Vorgangsbearbeitung und Archivierung vollständig in konforme IT-Prozesse überführt werden. Das DOMEA-Konzept liefert dafür Richtlinien, ist aber trotz seiner weiten Verbreitung und der Möglichkeit der Zertifizierung kein genormter Standard. Das Konzept liegt seit November 2005 in der Version 2.1 vor.
Eigentümer	Der Eigner (Eigentümer) eines →Archivdatenobjektes ist i.d.R. die Client Software, die das →Archivdatenobjekt zur Ablage im Langzeitspeicher über das →ArchiSafe-Modul übergeben hat.

Evidence Record **Evidence Record Syntax**	Siehe →Beweisdaten, technische und auch →[RFC4998] bzw. →[RFC6283]
Hashbaum	Von Merkle [MER 1990] stammt der Vorschlag, gleichzeitig mehrere Datensätze mit Hilfe eines so genannten Authentifizierungsbaums (engl. Authentication Tree, Hash Tree, Merkle Tree) durch eine einzige, an der Wurzel dieses Baums getätigte Signatur zu signieren. Merkle hat für einen solchen Authentifizierungsbaum eine binäre Baumstruktur vorgesehen. Die Blätter dieses Baums werden durch die →Hashwerte der zu schützenden Datenobjekte gebildet. In den Knoten des binären Authentifizierungsbaums wird jeweils ein →Hashwert der beiden Kinder dieses Knotens abgelegt. In jedem Blatt wird der →Hashwert eines bestimmten Datums aus der Gesamtmenge der mittels dieses Baums signierten Daten gespeichert. Die Daten selbst sind nicht Bestandteil des Baums, sie werden ausschließlich durch ihre digitalen „Fingerabdrücke“ (Hashwerte) repräsentiert. Die von Merkle vorgeschlagene binäre Struktur ist ein Spezialfall. Es sind durchaus Authentifizierungsbäume denkbar, deren Knoten maximal k ($k > 2$) statt maximal 2 Kinder haben.
Hashfunktion	Eine Hashfunktion ist ein kryptographischer Algorithmus, bei dem (elektronische) Nachrichten beliebiger Länge auf einen →Hashwert fester Länge (z. B. 160 Bit) abgebildet werden. Bei kryptographisch geeigneten Hashfunktionen ist es praktisch unmöglich zwei Nachrichten mit dem gleichen →Hashwert zu finden (Kollisionsresistenz) und für einen gegebenen Hashwert eine Nachricht zu finden, die durch die Hashfunktion auf den →Hashwert abgebildet werden kann (Einwegeigenschaft).
Hashwert	Ein Hashwert ist eine eindeutige Repräsentation elektronischer Daten und wird auch als Message Digest oder digitaler „Fingerabdruck“ der Daten bezeichnet. Eine →Hashfunktion zur Berechnung des Hashwertes ist eine mathematisch oder anderweitig definierte Funktion, die ein Eingabedatum variabler Länge aus einem Urbildbereich (auch als „Universum“ bezeichnet) auf ein (in der Regel kürzeres) Ausgabedatum fester Länge (den Hashwert) in einem Bildbereich abbildet. Das Ziel ist, einen „Fingerabdruck“ der Eingabe zu erzeugen, die eine Aussage darüber erlaubt, ob eine bestimmte Eingabe aller Wahrscheinlichkeit nach mit dem Original übereinstimmt. Hashwerte werden im Kontext elektronischer Signaturen und Zeitstempel als eindeutige digitale Repräsentanten der zu signierenden Daten benutzt.
IETF	Internet Engineering Task Force, eine offene, technisch orientierte internationale Gemeinschaft von Netzwerkdesignern, professionellen Anwendern und Herstellern, die sich mit den technischen Grundlagen des Internets sowie mit Netzwerkmanagement befasst.
Information	Für die Aneignung, Übermittlung und Verarbeitung „in Form“ gebrachte Kenntnisse oder Tatsachen, wie Mitteilungen, Nachrichten, Daten oder Messwerte. In der Informatik werden Informationen betrachtet, die Gegenstand von maschineller Speicherung, Verarbeitung und Übertragung sind, überwiegend als Folge von Zeichen aus einem bestimmten Zeichenvorrat (bspw. einem Alphabet).
Inhaltsdaten	Inhaltsdaten (synonym: Primärdaten) ist ein Satz an Information (Texte, Dokumente, Vorgänge oder Akten bzw. Aktenteile), der das eigentliche Ziel der Erhaltung (Langzeitspeicherung) ist.
Integrität	Elektronische Daten sind integer, wenn sie vollständig sind und nachweislich keine Veränderungen oder Manipulationen an den Daten festgestellt werden können.

Interoperabilität	Interoperabilität bezeichnet im weiteren Sinne die Fähigkeit verschiedener Geräte- oder Softwarekomponenten, direkt miteinander kommunizieren, d. h. insbesondere Daten austauschen zu können. Im engeren Sinne ist I. die Fähigkeit von IT-Systemen, direkt mit anderen Systemen zu kommunizieren, wenn sie über ein Netz verbunden sind.
ISO 15498	ISO 15489 ist ein internationaler Standard, der in Deutschland unverändert als DIN-Norm übernommen wurde. Er bietet Leitlinien zur Verwaltung von Schriftgut von öffentlichen und privaten Organisationen. Schlüsselbegriffe sind 'Aktenführung', 'Schriftgutverwaltung' oder Records Management. Die Zielsetzung der Norm besteht darin, für die Verwaltung und Aufbewahrung von Unterlagen - unabhängig von ihrer physischen Beschaffenheit und der logischen Struktur - einen Rahmen zu schaffen.
Kanonisieren	Die Kanonisierung oder auch Normalisierung eines XML Dokumentes beschreibt den Vorgang, ein XML Dokument in eine eindeutige physische Repräsentation zu bringen (Leerzeichen, Zeilenumbrüche, etc.). Hintergrund ist die eindeutige bitgenaue Darstellung des XML Dokument, so dass insbesondere eine reproduzierbare Berechnung des →Hashwerts möglich wird.
Konfigurationsdaten	Dazu zählen alle Modul-internen Daten, die für eine korrekte Ausführung der sicherheitsrelevanten Funktionen, insbesondere die korrekte und zuverlässige Identifizierung und Authentifzierung der externen Anwendungen, sowie der internen Module des Archivsystems sowie die Überprüfung und Ausführung der Archivanfrage benötigt werden.
Konformität	Konformität bedeutet die Übereinstimmung eines Systems oder Komponente mit den für diese Art von Systemen oder Komponenten (System- bzw. Komponentenklasse) definierten Anforderungen.
Konkatenieren	Beschreibt den Vorgang, zwei oder mehrere Bit- oder Zeichenketten aneinander zu fügen und als eine Bit- oder Zeichenkette zurückzuliefern. Bei Bedarf werden die Bit-/Zeichenketten vor der Verküpfung sortiert, um eine Reproduzierbarkeit der Ergebnisse zu ermöglichen.
Kryptographisch signierte Dokumente	Mit dem Begriff der „kryptographisch signierten Dokumente“ sind dabei in dieser TR neben den qualifiziert signierten Dokumenten (im Sinne der deutschen Signaturgesetzgebung) auch Dokumente mit einer fortgeschrittenen Signatur erfasst, wie sie oft in der internen Kommunikation von Behörden entstehen. Nicht gemeint sind hier Dokumente mit einfachen Signaturen basierend auf anderen (kryptographischen) Verfahren.
Langzeitarchivierung	Siehe →Archivierung
Langzeitspeicherung	Siehe →Archivierung
Mandantenfähig	Als mandantenfähig (auch mandantentauglich) wird Informationstechnik bezeichnet, die auf demselben Server oder demselben Software-System mehrere Mandanten, also Kunden oder Auftraggeber, bedienen kann, ohne dass diese gegenseitigen Einblick in ihre Daten, Benutzerverwaltung und ähnliches haben. Ein IT-System, das dieser Eigenschaft genügt, bietet die Möglichkeit der disjunkten, mandantenorientierten Datenhaltung, Präsentation (GUI) und Konfiguration (Customizing). Jeder Kunde kann nur seine Daten sehen und ändern. (Quelle: Wikipedia)
Metadaten	Metadaten sind im weitesten Sinne Daten, die andere Daten beschreiben. Metadaten sind i. d. R. Daten, die die Strukturen und den Zusammenhang von Daten bei der Verarbeitung der Daten durch die IT-Systeme beschreiben, die die Daten erzeugen, bearbeiten, verwalten und speichern. Metadaten eines →Archivdatenobjektes sind i. d. R. text- oder XML-basierte Metadaten zur Identifikation und Rekonstruktion des Verwaltungs- oder Geschäftkontextes der Nutzdaten.

Middleware

Middleware (deutsch etwa „Zwischenanwendung“) bezeichnet in der Informatik anwendungsneutrale Programme, die so zwischen Anwendungen vermitteln, dass die Komplexität dieser Applikationen und ihrer Infrastruktur verborgen wird. Man kann Middleware auch als eine Verteilungsplattform, d. h. als ein Protokoll (oder Protokollbündel) auf einer höheren Schicht als die der gewöhnlichen Rechnerkommunikation auffassen. Im Gegensatz zu niveautieferen Netzwerkdiensten, welche die einfache Kommunikation zwischen Rechnern handhaben, unterstützt Middleware die Kommunikation zwischen Prozessen. (Quelle: Wikipedia)

Migration

Der Begriff Migration bezeichnet in der Informationstechnik die Transformation von Daten auf ein anderes Betriebs- oder Speichersystem oder in ein anderes Datenformat. Für die vertrauenswürdige Langzeitaufbewahrung elektronischer Daten von besonderer Bedeutung ist dabei die Tatsache, dass bei einem solchen Vorgang die Authentizität und Integrität der Daten nicht beeinträchtigt werden darf. Wie das zu bewerkstelligen ist, ist Gegenstand des Projektes TransiDoc.

MoReq10

MoReq (Model Requirements for the Management of Electronic Documents and Records) ist der europäische Standard für das elektronische Records Management. Er wurde im Rahmen des IDA-Programmes der Europäischen Kommission entwickelt und vom DLM-Forum veröffentlicht. Ursprünglich sollte MoReq zur Vereinheitlichung des Dokumentenaustauschs zwischen der europäischen Kommission und den Regierungen der Mitgliedsstaaten beitragen. Inzwischen hat sich MoReq als Grundlage für verschiedene Standards für das elektronische Dokumenten-, Archiv- und Records-Management etabliert. An MoReq orientieren sich z. B. die Standards für das Records Management in der öffentlichen Verwaltung in England (TNA), in den Niederlanden (ReMano), in Norwegen (NOARK) und Luxemburg (SEL ECM). MoReq liefert im Gegensatz zu anderen Standards (wie z. B. ISO 15489) eine sehr detaillierte Anforderungsliste sowohl für funktionale Anforderungen an ein elektronisches und papierbasiertes Records Management System, als auch für die dazugehörigen elektronischen Vorgangsbearbeitungs- und Dokumenten-Management-Systeme. MoReq schließt auch Richtlinien zur Betrachtung von operationalen Systemen und Managementsystemen ein und erstellt nicht nur Anforderungen für eine Aufbewahrung von elektronischen Aufzeichnungen, sondern auch für die Anforderungen anderer elektronischer dokumentenbezogener Funktionen wie Workflow, E-Mail und Elektronische Signaturen. MoReq10 ist die aktuelle und umfassendste Spezifikation für Records Management.

Nachsignatur

Die für die elektronische Signatur eingesetzten Algorithmen und Parameter können mit wachsender Rechenleistung oder der Verfügbarkeit verbesserter Algorithmen ihre Sicherheitseignung verlieren, so dass die Beweiskraft elektronisch signierter Daten abnehmen würde. Deshalb sieht § 17 [SigV] vor, dass Daten mit einer qualifizierten elektronischen Signatur neu zu signieren sind, „*wenn diese für längere Zeit in signierter Form benötigt werden, als die für ihre Erzeugung und Prüfung eingesetzten Algorithmen und zugehörigen Parameter als geeignet beurteilt sind. In diesem Falle sind die Daten vor dem Zeitpunkt des Ablaufs der Eignung der Algorithmen oder der zugehörigen Parameter mit einer neuen qualifizierten elektronischen Signatur zu versehen. Diese muss mit geeigneten neuen Algorithmen oder zugehörigen Parametern erfolgen, frühere Signaturen einschließen und einen qualifizierten Zeitstempel tragen.*“

Nichtabstreitbarkeit

Unter Nichtabstreitbarkeit (eng. non-repudiation) versteht man, dass die Urheberschaft, der Versand oder der Empfang von Daten und Informationen nicht in Abrede gestellt werden können.

Nutzdaten	Als Nutzdaten (Englisch: *payload*) werden üblicherweise diejenigen während einer Kommunikation zwischen zwei Kommunikationsend-punkten transportierten Daten eines Datenpakets bezeichnet, die *keine* Steuer- oder Protokollinformationen enthalten. Die Nutzdaten eines Archivdatenobjekts umfassen die → Inhaltsdaten (synonym: Primärinformationen), → Repräsentationsinformationen und → beweisrelevante Daten.
OAIS	OAIS steht für Open Archival Information System bzw. Offenes Archiv-Informations-System (ISO-Standard 14721:2012). Der Grund für die Entwicklung dieses Modells bestand in der Einsicht, dass elektronisch archivierte Dokumente nach längerer Zeit aus vielfältigen Gründen nicht mehr lesbar sein könnten. Das Referenzmodell beschreibt ein Archiv als Organisation, in dem Menschen und Systeme zusammenwirken, um einer definierten Nutzergemeinde Archivgut verfügbar zu machen. Die Implementierung eines OAIS-konformen Archivs ist dabei jedoch nicht festgelegt. Die Entwicklung des Standards wurde von der NASA initiiert und gemeinsam mit der Raumfahrtorganisation ESA und Weltraum-forschungszentren in Großbritannien, Kanada, Frankreich, Deutschland, Brasilien, Japan und Russland vorangetrieben. Im Mai 1999 legte das Beratungskomitee für Weltraumdatensysteme (CCSDS) den Entwurf "Referenzmodell für ein offenes Archiv-Informationssystem (OAIS)" vor.
OCSP (RFC 2560)	Das Online Certificate Status Protocol [RFC 2560] ist ein Protokoll für die Online-Statusabfrage eines elektronischen Zertifikats bei einem Zertifizierungsdiensteanbieter.
Öffentlicher Schlüssel	Ein öffentlicher Schlüssel ist jener Teil eines kryptographischen Schlüsselpaares, der öffentlich bekannt und frei zugänglich ist. Er kann in einem Zertifikat enthalten sein und wird neben der Prüfung digitaler Signaturen auch verwendet, um Daten zu verschlüsseln.
Personal Security Environment (PSE)	Eine PSE ist ein Aufbewahrungsmedium für private Schlüssel und vertrauenswürdige Zertifikate. Eine PSE kann entweder als Software-Lösung, z. B. als eine mittels Passwort geschützte Datei im PKCS#12 Format oder als Hardware-Lösung, beispielsweise in Form einer Smart Card (Chipkarte) realisiert sein.
Privater Schlüssel	Der private Schlüssel ist jener Teil eines kryptographischen Schlüsselpaares, auf das nur der Inhaber des Schlüsselpaares zugreifen kann. Er wird verwendet, um Daten zu signieren und um verschlüsselte Daten zu entschlüsseln.
Protokolldaten	Protokolldaten sind Log-Informationen, die durch ein Modul erzeugt und für einen konfigurierbaren Zeitraum aufbewahrt oder dem → Archivdatenobjekt hinzugefügt werden.

Public Key Cryptography Standards (PKCS)

PKCS ist eine von der US amerikanischen Firma RSA Security Inc. entwickelte Reihe von Standards für Technologien auf Basis von asymmetrischen Kryptoalgorithmen. Zu den wichtigsten Standards in dieser Reihe gehören:

- PKCS#1: RSA Cryptography Standard, ein sehr häufig eingesetztes Low-Level-Signaturformat auf der Basis des RSA-Algorithmus. Die aktuelle Version ist PKCS#1, V. 2.1 [RFC3447]
- PKCS#7: Cryptographic Message Syntax Standard, ein sehr weit verbreitetes High-Level-Signaturformat, das von vielen Standard-Softwarekomponenten unterstützt wird. Die CMS-Spezifikation der IETF [RFC2630, RFC3369, RFC3852, RFC5652] basiert auf diesem Standard.
- PKCS#11: Cryptographic Token Interface Standard, eine Programmierschnittstelle für den standardisierten Zugriff auf Chipkartenfunktionen.
- PKCS#12: Personal Information Exchange Syntax Standard, ein Datenformat für den Austausch von mittels Passwort verschlüsselten privaten Schlüsseln.

Public Key Infrastructure (PKI)

Eine PKI ist eine technische und organisatorische Infrastruktur, die es ermöglicht, auf asymmetrischen Kryptoverfahren basierende digitale Zertifikate auszustellen, zu verteilen, zu verwalten und zu prüfen.

Qualifizierte elektronische Signatur

Eine qualifizierte elektronische Signatur ist gemäß § 2 Nr.3 SigG eine fortgeschrittene elektronische Signatur, die unter Verwendung einer sicheren Signaturerstellungseinheit erzeugt wurde und zum Zeitpunkt der Signaturerstellung auf einem gültigen qualifizierten Zertifikat beruht.

Qualifizierter Zeitstempel

Ein qualifizierter Zeitstempel ist gemäß § 2 Nr.14 SigG ein Zeitstempel, der von einem Zertifizierungsdiensteanbieter gemäß Signaturgesetz ausgestellt wird.

Qualifiziertes Zertifikat

Ein qualifiziertes Zertifikat ist gemäß § 2 Nr.7 SigG ein Zertifikat, das von einem Zertifizierungsdiensteanbieter für natürliche Personen ausgestellt wird. Die detaillierten Inhalte eines qualifizierten Zertifikats ergeben sich aus § 7 SigG.

Relax NG

Regular Language Description for XML New Generation (RELAX NG) ist eine einfache Schemasprache für XML. Ein RELAX-NG-Schema spezifiziert Muster für die Struktur und den Inhalt eines XML-Dokuments. Dabei ist ein RELAX-NG-Schema selbst ein XML-Dokument, jedoch bietet es auch eine kompakte Nicht-XML-Syntax an.

RELAX NG ist beschrieben in einem Dokument der OASIS RELAX NG Technical Committee und darüber hinaus als internationaler Standard ISO/IEC 19757-2 innerhalb der Document Schema Definition Languages (DSDL).In der Komplexität steht Relax NG etwa zwischen DTD und XML-Schema. Gegenüber der einfachen DTD hat Relax NG vor allem den Vorteil, (wahlweise) XML-Syntax zu verwenden und auch ungeordnete Inhalte zu unterstützen. Darüber hinaus kennt es Datentypen und Namespaces.

Siehe auch unter http://relaxng.org/

RSA-Algorithmus

Der nach seinen Erfindern (Rivest, Shamir und Adleman) benannte RSA-Algorithmus ist ein asymmetrischer Kryptoalgorithmus, der zur Verschlüsselung und zur Erzeugung digitaler Signaturen verwendet werden kann. Die Sicherheit des Verfahrens beruht auf der Annahme, dass das dem Algorithmus zugrunde liegende Faktorisierungsproblem für große Zahlen nicht effizient gelöst werden kann.

Repräsentationsinformationen	Informationen über Datenformate oder Informationen über Softwareapplikationen, die für eine maschinenlesbare Darstellung der Inhaltsdaten zum Zeitpunkt der Ablage im Langzeitspeicher verwendet wurden.
SAGA **Standards und Architekturen für E-Government-Anwendungen**	Die Richtlinie „Standards und Architekturen für E-Government-Anwendungen (SAGA)“ definiert Empfehlungen zum Einsatz von IT-Standards und IT-Architekturen in E-Government-Projekten der Bundesverwaltung. Ziel ist, die Interoperabilität, die Offenheit und Skalierbarkeit, Wiederverwendbarkeit und die Investitionssicherheit von E-Government Anwendungen zu fördern.
SASL	*Simple Authentication and Security Layer* (SASL) ist ein Framework, das von verschiedenen Protokollen zur Authentifizierung verwendet wird. Es wurde im Oktober 1997 als RFC 2222 definiert und im Juni 2006 durch [RFC4422] ersetzt. SASL bietet dem Applikationsprotokoll eine standardisierte Möglichkeit der Aushandlung von Kommunikationsparametern. Im Regelfall wird nur eine Authentifizierungsmethode ausgehandelt, es kann aber auch vereinbart werden, dass zuerst auf ein verschlüsseltes Transportprotokoll, wie beispielsweise TLS, gewechselt wird. Die SASL-Implementierungen auf beiden Seiten der Kommunikationspartner einigen sich auf ein Verfahren und dieses kann dann von der Applikation transparent benutzt werden.
Schema, XML	Ein Schema beschreibt die syntaktische Struktur einer XML-Datei und definiert damit einen Dokumententyp von XML-Dokumenten. Verbreitete Sprachen für die Erstellung von Schemata sind XML-Schema (XSD) und Relax NG.
Schnittstelle (Interface)	Verbindungs- oder Berührungspunkte von Systemen oder Komponenten, die miteinander kommunizieren oder zusammenarbeiten. Die Informationstechnik unterscheidet Hardware, Software- und Benutzerschnittstellen. Software-Schnittstellen dienen dem Datenaustausch von Anwendungen oder Komponenten untereinander bzw. mit dem Betriebssystem.
SCVP	Server-Based Certificate Validation Protocol (SCVP) ist ein Internet-Protokoll, das es Clients ermöglicht, den Aufbau einer X.509-Zertifikatskette und deren Validierung auszulagern. Dies wird vor allem bei Clients, die mit dem Kettenaufbau und der Validierung 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 unterstützten Validation Policies, die bestimmen für welche Anwendungen der Server konfiguriert wurde. Danach schickt der Client dem Server die Zertifikats-IDs und gibt an, welche Aktionen durchzuführen sind, die der Server signiert beantwortet. SCVP ist noch sehr neu und wird bisher nur von wenigen Anwendungen unterstützt.
Semantik	Die Semantik definiert – im Gegensatz zur Syntax – die Bedeutung der gültigen Zeichen, Wörter und Sätze einer Sprache.

Sichere Signaturerstellungseinheit (SSEE)

Eine sichere Signaturerstellungseinheit ist gemäß § 2 Nr.10 SigG eine Signaturerstellungseinheit, die den Anforderungen des SigG, insbesondere § 17 Abs. 1 SigG und § 15 Abs. 1 SigV genügt. Dazu gehört bspw., dass selbst der Signaturschlüssel-Inhaber seinen privaten Schlüssel nicht aus der Signaturerstellungseinheit auslesen und veröffentlichen kann. I. d. R. wird dies in Form einer Chipkarte realisiert. Die Erfüllung der Anforderungen muss durch anspruchsvolle Prüfungen nach international anerkannten Sicherheitskriterien und eine Bestätigung gemäß Signaturgesetz nachgewiesen werden.

Sicherungsmittel

Sicherungsmittel sind technische und organisatorische Maßnahmen (Vorkehrungen) mit dem Ziel, eine langfristige und unveränderbare Aufbewahrung elektronischer Dokumente sicherzustellen.

Systembezogene Sicherungsmittel beschränken durch eine individuelle Konfiguration des jeweiligen Systems oder der auf dieses zugreifenden Komponenten den Zugriff auf die Daten, z. B. durch Berechtigungssysteme.

Datenträgerbezogene Sicherungsmittel sind Speichermedien, die ein Überschreiben oder Verändern der auf ihnen abgelegten Informationen ausschließen.

Dokumentbezogene Sicherungsmittel sind solche, die die elektronischen Dokumente selbst gegen unbemerkte Veränderungen und unberechtigte Kenntnisnahme zu schützen imstande sind, z. B. Verschlüsselungstechnologien.

Signatur, elektronische S.

Elektronische Signaturen sind gemäß Signaturgesetz „Daten in elektronischer Form, die anderen elektronischen Daten beigefügt oder logisch mit ihnen verknüpft sind und die zur Authentifizierung“ im elektronischen Rechts- und Geschäftsverkehr dienen. Ihre Aufgabe ist die Identifizierung des Urhebers der Daten, d. h. der Nachweis, dass die Daten tatsächlich vom Urheber herrühren (Echtheitsfunktion) und dies vom Empfänger der Daten auch geprüft werden kann (Verifikationsfunktion). Beides lässt sich nach dem heutigen Stand der Technik zuverlässig am ehesten auf der Grundlage kryptographischer Authentifizierungssysteme, bestehend aus sicheren Signaturalgorithmen sowie dazu passenden und personifizierten Signaturschlüsseln realisieren.

Technisch bezeichnet eine elektronische (digitale) Signatur den mit einem privaten Signaturschlüssel „signierten“ →Hashwert einer Information (Dokumentes oder Nachricht). Da der →Hashwert in diesem Fall als eindeutiger elektronischer Repräsentant der Information angesehen werden kann, bezeugt der „signierte“ →Hashwert die Authentizität der Information. Die Überprüfung der elektronischen Signatur erfolgt mit Hilfe des öffentlichen Schlüssels des Ausstellers der Information, der entweder in der Signatur selbst enthalten ist oder über die in der Signatur enthaltenen Zertifikatsinformationen beschafft werden kann.

Signaturanwendungskomponente

Signaturanwendungskomponenten sind gemäß § 2 Nr.11 SigG Software- oder Hardwareprodukte, die dazu bestimmt sind, Daten dem Prozess der Erzeugung oder Prüfung qualifizierter elektronischer Signaturen zuzuführen oder qualifizierte elektronische Signaturen zu prüfen oder qualifizierte Zertifikate nachzuprüfen und die Ergebnisse anzuzeigen.

Signaturprüfung	Die Signaturprüfung umfasst zwei Prüfungsschritte. Beim ersten Schritt wird die mathematische Gültigkeit der Signatur zum Nachweis der Integrität geprüft. Im zweiten Schritt wird für den Nachweis der Authentizität die Gültigkeit der gesamten Signatur im Hinblick auf das zugrunde liegende Gültigkeitsmodell geprüft. Dies umfasst die Prüfung, ob das zur Signaturerstellung verwendete →Zertifikat zum Referenzzeitpunkt, d. h. bei einer qualifizierten elektronischen Signatur der Zeitpunkt der Signaturerstellung und bei einer zur Authentifizierung verwendeten Signatur der aktuelle Zeitpunkt, gültig ist. Für die Gültigkeit eines Zertifikats wird geprüft, ob die durch den Aussteller der Zertifikats gesetzte Signatur gültig ist, ob Zertifikatserweiterungen richtig gesetzt wurden und ob ein Zertifikatspfad zu einem vertrauenswürdigen Wurzelzertifikat gebildet werden kann und ob das Zertifikat nicht gesperrt wurde.
Standard	Ein Standard bezweckt die Vereinheitlichung von Gütern, Leistungen oder Prozessen nach bestimmten Mustern. In der Informationstechnik dienen Standards bspw. dem Ziel, für eine Gruppe von Anwendern und für einen gewissen Zeitraum allgemein akzeptierte und öffentlich zugängliche Regeln aufzustellen, die es ermöglichen, verschiedenartige IT-Systeme im Verbund einzusetzen. Absicht einer derartigen Standardisierung ist ein technisches oder logisches Muster für die Harmonisierung des Datenaustausches zwischen den IT-Systemen mit dem Ziel, die Transaktionskosten der Datenaustauschprozesse zu senken und die Qualität zu erhöhen.
Syntax	Die Syntax definiert, wie gültige Sätze einer Sprache aufgebaut werden. So besteht eine Sprache aus einer Menge gültiger Symbole (Zeichen, Wörter) und einem Regelwerk (Grammatik), das besagt, wie die einzelnen Zeichen oder Wörter miteinander kombiniert werden, um gültige Sätze zu formen. Die Syntax trifft aber keine Aussage über die Bedeutung (Semantik) der gebildeten Sätze.
Time-Stamp Protocol (TSP)	TSP ist ein in [RFC3161] von der IETF standardisiertes Client-Server-Protokoll zur Ausstellung von Zeitstempeln.
TransiDoc	TransiDoc (Transformation signierter Dokumente) ist ein vom BMWi gefördertes Forschungsprojekt mit dem Ziel, Anforderungen und Regeln (Normen) für die rechtssichere Transformation elektronisch signierter Dokumente zu spezifizieren.
TR-ESOR-Middleware	Die in dieser TR als Referenzarchitektur vorgeschlagene TR-ESOR-Middlware ist eine →Middlware zwischen den Client-Anwendungen und dem eigentlichem Speichersystem, die vor allem Funktionen für den langfristigen Beweiswerterhalt elektronisch signierter Dokumente sowie Funktionen zum Ausgeben der beweisrelevanten Daten (siehe → Beweisdaten, technische) besitzt.
UML **Unified Modeling Language**	Die Unified Modelling Language (UML) ist eine seit Ende der 1990er Jahre entwickelte grafische Modellierungssprache für die einheitliche Beschreibung und Darstellung von Geschäftsprozessen sowie der Funktionalität und Kommunikation komponentenbasierter IT-Systeme. Sie hat sich nach der Standardisierung durch die Object Management Group (OMG) weltweit zum Standard für Analyse und Designnotationen entwickelt. UML liegt seit August 2003 in der Version UML 2 vor und wird im Software Engineering besonders in der Frühphase der Anforderungsdefinition und der Systemkonzeption eingesetzt und stellt Diagramme und Notationselemente zur Verfügung, mit deren Hilfe statische und dynamische Aspekte beliebiger Anwendungsgebiete modelliert werden können.

Verbindlichkeit	Unter Verbindlichkeit versteht man, dass ein Rechtsgeschäft seine beabsichtigte rechtliche Wirkung entfaltet. Voraussetzung ist teilweise die Einhaltung von Formerfordernissen (bspw. Schriftform) und das Vorhandensein von Beweismitteln.
Verfügbarkeit	Elektronische Informationen sind verfügbar, wenn auf sie in einer angemessenen Zeit zugegriffen werden kann, und wenn sie auf den zum Zeitpunkt des Zugriffs eingesetzten IT-Systemen für menschliche Benutzer lesbar dargestellt werden können.
Verifikationsdaten	Verifikationsdaten sind Daten, die dem Nachweis des Übereinstimmens von Ist-Eigenschaften mit den durch ein Ziel, einen Zweck oder eine Spezifikation definierten Soll-Eigenschaften eines Systems, einer Komponente oder von Daten oder Datengruppen dienen. Die Art und der Umfang der für einen solchen Nachweis erforderlichen Verfikationsdaten bestimmt sich daher immer auch aus den ziel- oder zweckbestimmmten Soll-Eigenschaften.
Verkehrsfähigkeit	Daten / Dokumente sind "verkehrsfähig", wenn sie (und die zugehörigen Signaturen und Verifikationsdaten) in Formaten vorliegen, die ein typischer Benutzer zum Zeitpunkt der Verwendung (also hier mindestens bis zum Ende der Aufbewahrungsfrist) mit üblicher Standard-IT-Ausstattung lesen und interpretieren kann, wobei die Übereinstimmung mit dem Original gewährleistet ist. Danach wäre z.B. PDF/A oder XML aus heutiger Sicht verkehrsfähig, eine MS-Word-Datei (.doc) aber nicht.
Vertraulichkeit	Schutz vor unbefugter Kenntnisnahme zur Sicherung personenbezogener Daten und betriebs- oder berufsbezogener Geheimnisse. Die Vertraulichkeit ist die einzige bei der Aufbewahrung elektronischer Dokumente zu berücksichtigende Anforderung zur IT-Sicherheit, die sich nicht aus den Aufbewahrungszwecken, sondern aus anderen zu schützenden Rechtsgütern ergibt.
W3C **World Wide Web Consortium**	Das W3C ist ein Zusammenschluss von Wirtschaft und Wissenschaft mit dem Ziel, interoperable Technologien zu entwickeln, um das gesamte Potenzial des World Wide Web ausschöpfen zu können. Es erstellt seine Standards als Empfehlungen und hat sich verpflichtet, ausschließlich Technologien zu verwenden, die frei von Patent-Gebühren sind.
X.509	[X.509] ist ein internationales Standardformat für die Ausstellung digitaler PKI Zertifikate über die Identität des Zertifikatinhabers.
XML **Extensible Markup Language**	Die Extensible Markup Language (XML) ist eine vor allem für das Internet entwickelte Formatbeschreibungssprache für den Austausch strukturierter Daten und wurde 1997 vom Word Wide Web Consortium (W3C) standardisiert (mehr unter: http://www.w3c.org/XML/).
XML Schema Definition	XML-Schema Definition (XSD) ist eine Empfehlung des W3C zur Spezifikation syntaktischer Regeln für den Aufbau von XML-Dokument-strukturen. Anders als bei einer klassischen XML-DTD wird die Struktur in Form eines XML-Dokuments, d. h. in XML-Syntax, beschrieben. Neben der Definition von Elementen, Attributen und Verarbeitungsanweisungen erlauben XML-Schemata die Formulierung von Bedingungen und Beschränkungen für den Zugriff auf diese.

XML-DSig

Die XML Signatur Spezifikation (auch XML-DSig, RFC3275) definiert eine XML Syntax für digitale Signaturen. In ihrer Funktion ähnelt sie dem PKCS#7 Standard, ist aber leichter zu erweitern und auf das Signieren von XML Dokumenten spezialisiert. Sie findet Einsatz in vielen weiterführenden Web-Standards wie etwa SOAP, SAML oder dem deutschen OSCI.

Mit XML Signaturen können Daten jeden Typs signiert werden. Dabei kann die XML-Signatur Bestandteil des XML Datenpakets sein (enveloped signature), die Daten können aber auch in die XML-Signatur selbst eingebettet sein (enveloping signature) oder mit einer URL adressiert werden (detached signature).

Eine XML Signatur ist immer mindestens einer Ressource zugeordnet, dass heißt ein XML Baum oder beliebige Binärdaten, auf die ein XML-Link verweist. Beim XML Baum muss sichergestellt sein, dass es zu keinen Mehrdeutigkeiten kommt. Um dies erreichen zu können, ist eine so genannte Kanonisierung des Inhalts erforderlich. Dabei werden nach Maßgabe des Standards alle Elemente in der Reihenfolge ihres Auftretens aneinander gereiht und alle Attribute alphabetisch geordnet, so dass sich ein längerer UTF-8 String ergibt. Aus diesem wird dann der eigentliche Hashwert für die Signatur gebildet.

Da die Signatur eine binäre Zeichenfolge ist, lässt sie sich nicht direkt in ein XML Dokument einbetten. Man codiert die binären Werte im Base64-Format [RFC 1521], um so aus ihnen ASCII lesbare Zeichen zu gewinnen.

Im Rahmen der Struktur eines XML Dokuments lassen sich Subelemente explizit vom Signieren ausschließen, so auch die Signatur selbst. Umgekehrt lassen sich beliebig viele Referenzen auflisten, die als Gesamtheit zu signieren sind.

Zeitstempel, elektronischer

Ein Zeitstempel ist eine von einem vertrauenswürdigen Dritten zuverlässig bescheinigte elektronische Angabe von Zeit und Datum. Ein Zeitstempel dient dazu, verlässlich und nachweislich zu belegen, dass digitale Daten eines bestimmten Inhalts zu einem bestimmten Zeitpunkt bei dem Aussteller des Zeitstempels (i. d. R. ein Zertifizierungsdiensteanbieter) vorgelegen haben.

Zertifikat

Nach § 2 Nr. 6 SigG sind Zertifikate elektronische Bescheinigungen, mit denen Signaturschlüssel einer Person zugeordnet werden und die Identität einer Person bescheinigt wird. Für die Anwendung von Signaturverfahren von besonderer Bedeutung ist die Feststellung, dass „qualifizierte Zertifikate“ nur auf natürliche Personen ausgestellt werden dürfen.

Das Zertifikat enthält neben dem öffentlichen Signaturschlüssel insbesondere Angaben zur Person, die von der ausstellenden Instanz zum Zeitpunkt der Zertifikatserstellung geprüft wurden, sowie zum Gültigkeitszeitraum.

Zertifizierungsdiensteanbieter

Ein Zertifizierungsdiensteanbieter ist gemäß § 2 Nr. 8 SigG eine natürliche oder juristische Person, die qualifizierte Zertifikate oder qualifizierte Zeitstempel ausstellt.

Zertifikatsperrliste

Eine Zertifikatsperrliste (engl. Certificate Revocation List – CRL) ist eine Liste, die die Ungültigkeit von Zertifikaten beschreibt. Sie ermöglicht es, festzustellen, ob ein Zertifikat gesperrt oder widerrufen wurde und warum.

13. Quellenverzeichnis

[ACMPP] Physikalisch-Technische Bundesanstalt (PTB): *Common Criteria Protection Profile for an ArchiSafe Compliant Middleware for Enabling the Legally compliant Long-Term Preservation of Electronic Documents (ACM_PP)*, jeweils aktuell gültige Fassung

[AIS 20] BSI: *Anwendungshinweise und Interpretationen zum Schema (AIS), Funktionalitätsklassen und Evaluationsmethodologie für deterministische Zufallszahlengeneratoren*, Version 1
siehe unter

https://www.bsi.bund.de/cln_165/DE/Themen/ZertifizierungundAnerkennung/ZertifizierungnachCCundITSEC/AnwendungshinweiseundInterpretationen/anwendungshinweiseundinterpretationen_node.html

[AIS 31] BSI: *Anwendungshinweise und Interpretationen zum Schema (AIS)*, Funktionalitätsklassen und Evaluationsmethodologie für physikalische Zufallszahlengeneratoren,Version 1
siehe unter

https://www.bsi.bund.de/cln_165/DE/Themen/ZertifizierungundAnerkennung/ZertifizierungnachCCundITSEC/AnwendungshinweiseundInterpretationen/anwendungshinweiseundinterpretationen_node.html

[ALGCAT] *Geeignete Kryptoalgorithmen 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*, jeweils aktuell gültige Fassung, siehe

http://www.bundesnetzagentur.de/cln_1912/DE/Service-Funktionen/QualifizierteelektronischeSignatur/WelcheAufgabenhatdieBundesnetzagentur/GeeigneteAlgorithmenfestlegen/geeignetealgorithmenfestlegen-node.html

[ANSI X3.4] ANSI X3.4 Information Systems – *Coded Character Sets – 7-Bit American National Standard Code for Information Interchange (7-Bit ASCII)*

[ANSI X9.62] Public Key Cryptography for the Financial Services Industry, The Elliptic Curve Digital Signature Algorithm (ECDSA)

[ArchiSig] A. Rossnagel, P. Schmücker (Hrsg.): *Beweiskräftige elektronische Archivierung*. Ergebnisse des Forschungsprojektes „ArchiSig – Beweiskräftige und sichere Langzeitarchivierung digital signierter Dokumente“, Economica Verlag, 2006

[ARO 07] A. Rossnagel, S. Fischer-Dieskau, S. Jandt, M. Knopp: *Langfristige Aufbewahrung elektronischer Dokumente*, Band 17 der Reihe „Der elektronische Rechtsverkehr“, 1. Auflage, Nomos-Verlag, 2007.

[ASN.1] O. Dubuisson, ASN.1 – *Communication between heterogeneous systems*, Academic Press, 2001

[BArchG] *Gesetz über die Sicherung und Nutzung von Archivgut des Bundes (Bundesarchivgesetz – BArchG) vom 06.01.1988*, zuletzt geändert durch § 13 Abs. 2 G vom 05.09.2005 I 2722, siehe unter
http://www.gesetze-im-internet.de/bundesrecht/barchg/gesamt.pdf

[BASE64] Freed, N, Borenstein, N.: *Multipurpose Internet Mail Extensions (MIME) Part One: Format of Internet Message Bodies*, section 6.8, Base64 Content-Transfer-Encoding, IETF RFC 2045, November 1996.

[BDSG] *Bundesdatenschutzgesetz*, vom 20. Dezember 1990, BGBl I 1990, 2954, 2955; zuletzt geändert durch G. Vom 5.9. 2005, BGBl I 2722; siehe unter http://bundesrecht.juris.de/bundesrecht/bdsg_1990/, 1990

[BGB] *Bürgerliches Gesetzbuch*, in der Fassung der Bekanntmachung vom 2. Januar 2002 (BGBl. I S. 42, 2909; 2003 I S. 738), zuletzt geändert durch Artikel 1 des Gesetzes vom 4. Juli 2008 (BGBl. I S. 1188) siehe unter www.gesetze-im-internet.de/bundesrecht/bgb/gesamt.pdf

[BLESS 05] Bless, R., et al.: *Sichere Netzwerkkommunikation. Grundlagen, Protokolle und Architekturen*, Springer Verlag, Berlin Heidelberg, 2005

[BORG 03] Borghoff, C., et al.: *Long-Term Preservation of Digital Documents, Principles and Practices*, Springer, 2003

[BT 01] Bröhl, G. M., Tettenborn, A., *Das neue Recht der elektronischen Signaturen*, Bundesanzeigerverlag, 2001

[C14N] *Canonical XML*, Version 1.0, W3C Recommendation, Mai 2001, siehe unter http://www.w3.org/TR/xml-c14n

[C14N11] *Canonical XML*, Version 1.1, W3C Recommendation, 2 May 2008, siehe unter http://www.w3.org/TR/xml-c14n11

[C14N20] *Canonical XML*, Version 2.0, W3C Working Draft, 22 October 2009, siehe unter http://www.w3.org/TR/2009/WD-xml-c14n2-20091022

[CAdES] ETSI: *CMS Advanced Electronic Signatures (CAdES)*. ETSI Technical Specification TS 101 733, Version 2.2.1 , April 2013, siehe unter http://www.etsi.org

[CC] *Common Criteria for Information Technology Security Evaluation (CC)*, Version 3.1, siehe unter http://www.commoncriteriaportal.org

[Common-PKI] T7 e.V. und TeleTrusT e.V.: *Common PKI Specification*, Version 2.0, Januar 2009, siehe unter http://www.common-pki.org/uploads/media/Common-PKI_v2.0.pdf

[CRYPTO3N2] CryptoBytes, Volume 3, Number 2. *The Cryptographic Hash Function RIPEMD-160*. RSA Laboratories. Autumn 1997.

[DOL02] Dollar, C. M., Authentic Electronic Records: *Strategies for Long-Term Access*, Cohasset Associates , Inc., 2002

[DSSC] T. Kunz, S. Okunick, U. Pordesch: IETF RFC5698 - *Data Structure for Security Suitabilities of Cryptographic Algorithms (DSSC)*, siehe unter http://www.ietf.org/rfc/rfc5698.txt

[EBU-BWF] European Broadcasting Union (EBU): *EBU Broadcast Wave Format – a format for audio data files in broadcasting*, Version 1, July 2001, http://tech.ebu.ch/docs/tech/tech3285.pdf

[EC14N] *Exclusive XML Canonicalization*, Version 1.0, W3C Recommendation, Juli 2002, siehe unter http://www.w3.org/TR/xml-exc-c14n

[eCard-1] BSI: *eCard-API-Framework – Part 1 – Overview and general definitions*, BSI TR-03112-1, Version 1.1**.2** vom 27.02.2012, siehe https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/TechnischeRichtlinien/TR03112/api1_teil1_pdf.pdf

[eCard-2] BSI: *eCard-API-Framework – Part 2 – eCard-Interface, BSI TR-03112-2* , Version 1.1.2 vom 27.02.2012; siehe unter https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/TechnischeRichtlinien/TR03112/api1_teil2_pdf.pdf

[eCard-3] BSI: *eCard-API-Framework – Part 3 – Management-Interface*, BSI TR-03112-3 , Version 1.1.2 vom 27.02.2012, siehe unterhttps://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/TechnischeRichtlinien/TR03112/api1_teil3_pdf.pdf

[eCard-4] BSI: *eCard-API-Framework – Part 4 – ISO24727-3-Interface*, BSI TR-03112-4 , Version 1.1.2 vom 27.02.2012, siehe unter https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/TechnischeRichtlinien/TR03112/api1_teil4_pdf.pdf

[eCard-7] BSI, eCard-API-Framework – Part 7 – Protokols, BSI TR-03112-7 , Version 1.1.2 vom 27.02.2012, siehe unter https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/TechnischeRichtlinien/TR03112/api1_teil7_pdf.pdf

[eGov-Org] Die Bundesregierung: *Organisationskonzept elektronsiche Verwaltungsarbeit*, siehe unter http://www.verwaltung-innovativ.de/DE/E_Government/orgkonzept_everwaltung/orgkonzept_everwaltung

[ETSI 101 733] ETSI: *CMS Advanced Electronic Signatures (CadES),* ETSI Technical Specification TS 101 733, Version 2.2.1 , April 2013, siehe unter http://www.etsi.org

[ETSI 101 903] ETSI: *XML Advanced Electronic Signatures (XAdES)*, ETSI Technical Specification TS 101 903, Version 1.4.2, , Dezember 2010, siehe unter http://www.etsi.org

[ETSI 103 171] ETSI: Electronic Signatures and Infrastructures (ESI), *XAdES Baseline Profile,* V2.1.1 (2012-03)

[ETSI 103 173] ETSI: Electronic Signatures and Infrastructures (ESI); *CAdES Baseline Profile*, V2.2.1 (2013-04)

[ETSI 101 733] ETSI: *CMS Advanced Electronic Signatures (CAdES)*. ETSI Technical Specification TS 101 733, Version 2.2.1. http://www.etsi.org/deliver/etsi_ts/101700_101799/101733/02.02.01_60/ts_101733v020201p.pdf, April 2013.

[ETSI EN 319122-1] ETSI: *CMS Advanced Electronic Signatures (CAdES); Part 1: Core Specification,* ETSI Technical Specification TS 319 122-1, Version 0.0.3 DRAFT, November 2013

[ETSI EN 319122-2] ETSI: *CMS Advanced Electronic Signatures (CAdES); Part 2: Baseline Profile,* ETSI Technical Specification TS 319 122-2, Version 0.0.3 DRAFT, November 2013

[ETSI EN 319132-1] ETSI: *XML Advanced Electronic Signatures (XAdES); Part 1: Core Specification*, ETSI Technical Specification TS 319 132-1, Version 0.0.4 DRAFT, November 2013

[ETSI EN 319132-2] ETSI: *XML Advanced Electronic Signaures (XAdES); Part 2: XAdES Baseline Profile*, ETSI Technical Specification TS 319 132-2, Version 0.0.4 DRAFT, November 2013

[ETSI-TSP] ETSI: *Time stamping profile*, , TS 101 861 V 1.4.1, Juli 2011, siehe unter http://www.etsi.org

[FC 07] F. Cohen: *FastSOA*, Elsevier Inc., 2007

[FIPS180-2] United States of America National Institute for Standards and Technology (NIST): *Secure Hash Standard (SHS)*, Federal Information Processing Standard (FIPS), Publication 180-4, März 2012, siehe unter http://csrc.nist.gov/publications/fips/fips180-4/fips-180-4.pdf

[GDPdU] *Grundsätze zum Datenzugriff und zur Prüfbarkeit digitaler Unterlagen (GDPdU)* (BMF-Schreiben vom 16. Juli 2001 - IV D 2 - S 0316 - 136/01 -), siehe unter www.zdh.de/fileadmin/user_upload/themen/Steuerinfo/BMF-Schreiben_16-07-01_GdPDU.pdf

[GLAD 07] Gladney, H. M.: *Preserving Digital Information*, Springer Publ., 2007

[GoBS] *Grundsätze ordnungsmäßiger DV-gestützter Buchführungssysteme (GoBS)*, Schreiben des Bundesministeriums der Finanzen an die obersten Finanzbehörden der Länder vom November 1995 - IV A 8 - S 0316 - 52/95- BStBl 1995 I S. 738 siehe unter www.bundesfinanzministerium.de/

[GON 07] Gondrom, T.: *Evidence Record Syntax,* in: N. Pohlmann et al.: ISSE/SECURE 2007 Securing Electronic Business Processes: Highlights of the Information Security Solutions Europe/SECURE 2007 Conference, Vieweg + Teubner, 2007, 367 ff.

[HGB] *Handelsgesetzbuch*, vom 10. Mai 1897, RGBl 1987, 219, zuletzt geändert druch Art. 1 G. v. 3.8.2005 I 2267, siehe unter http://bundesrecht.juris.de/bundesrecht/hgb

[HIGGINS 2010] Higgins, S.: *Standards Watch Papers ISO15498*, abgerufen unter: http://www.dcc.ac.uk/resources/briefing-papers/standards-watch-papers/iso-15489

[HK 06] Hühnlein, D., Korte, U.: *Grundlagen der elektronischen Signatur*, Bundesamt für Sicherheit in der Informationstechnik und Secu Media Verlag, Bonn / Ingelheim, 2006

[HK 06b] Hühnlein, D., Korte, _U.: *Signaturformate für elektronische Rechnungen*, in Horster P. (Hrsg.): Tagungsband „D•A•CH Security“, 2006, IT-Verlag, ISBN 3-00-018166-0, 2006 Seiten 1-14, http://www.ecsec.de/pub/2006_DACH_Signaturformate.pdf

[HKS 12] Hühnlein, D., Korte, U., Schumacher, A.: *Die BSI-Richtlinien TR-ESOR und TR-RESISCAN*, in Schartner, P., Taeger, J. (Hrsg.): „D•A•CH Security“, 2012, Syssec, ISBN 978-3-00-039221-4, S. 409-420, 2012.

[HORN 04] Hornung, G.: *Der zukünftige Einsatz von Chipkarten im deutschen Gesundheitswesen*, in: Horster p. (Hrsg.), D·A·CH Security 2004, 226

[HORN 05] Hornung, G.: *Die digitale Identität. Rechtsprobleme von Chipkartenausweisen: digitaler Personalausweis, elektronische Gesundheitskarte, Job-Card-Verfahren*, Baden-Baden, 2005

[HUE 04] Hühnlein, D.: *Intervall-Qualifizierte Zeitstempel*, in: P. Horster (Hrsg), Elektronische Geschäftsprozesse, S. 341, IT-Verlag, 2005, siehe auch.: http://www.ecsec.de/pub/2004_EGP_IQZeitstempel.pdf

[INHE 1995] Inhester, M.: *Rechtliche Konsequenzen des Einsatzes von Bildarchivierungs- und Kommunikationssystemen (PACS)*, NJW 1995, 685

[ISO 14533-1] ISO 14533-1:2012 Processes, data elements and documents in commerce, industry and administration – Long term signature profiles Part 1: Long signature profiles for CMS Advanced Electronic Signatures (CaDES), siehe unter http://www.iso.org/

[ISO 14533-2] ISO 14533-2:2012 Processes, data elements and documents in commerce, industry and administration – Long term signature profiles – Part 2: Long term signature profiles for XML Advanced Electronic Signatures (XaDES), siehe unter http://www.iso.org/

[ISO 19005-3] ISO 19005-3:2012: *Document management – Electronic document file format for lang-term preservation – Part 3: Use of ISO 32000-1 with support for embedded files (PFD/A-3),* 2012, siehe unter http://www.iso.org/iso/iso_catalogue/catalogue_tc/catalogue_detail.htm%3Fcsnumber%3D57229

[ISO-Latin-1] ISO/IEC 8859-1:1998: *Information technology -8-bit single-byte coded graphic character sets, Part 1: Latin alphabet No. 1*, siehe unter: http://www.iso.org/

[KAMPFF 97] Kampffmeyer, U., Rogalla, J.:*Grundsätze der elektronischen Archivierung,* VOI Kompendium Band 3. VOI Verband Organisations- und Informationssysteme e. V., Darmstadt 1997, ISBN 3-932898-03-6.

[KNAACK 2003] Knaack, I.: *Handbuch IT-gestützte Vorgangsbearbeitung in der öffentlichen Verwaltung*, Nomos Verlag 2003.

[KUSSEL 03] Kussel, S., Die Digitalisierung der Verwaltungsgerichtsbarkeit, Berlin, 2003

[LAZ 01] Lazinger, S. S.: *Digital Preservation and Metadata*, Greenwood Publishing, 2001

[LTAP] A. Jerman Blazic, P. Sylvester, C. Wallace: *Long-term Archive Protocol (LTAP)* – draft-ietf-ltans-ltap-08, siehe unter http://tools.ietf.org/html/draft-ietf-ltans-ltap-08

[MER 1980] Merkle, R. C.: *Protocols for Public Key Cryptosystems*, Proceedings of the 1980 IEEE Symposium on Security and Privacy (Oakland, CA, USA), pages 122-134, April 1980.

[MER 1990] Merkle, R. C.: *A Certified Digital Signature*, Advances in Cryptology; CRYPTO `89, LNCS, Bd. 0435, S. 218-238, Springer Verlag, 1990

[METS] *Metadata Encoding and Transmission Standards*, siehe unter http://www.loc.gov/standards/mets/

[Moreq10] *„Model Requirements for the Management of Electronic Records – Moreq10, Modular Requirements for Records Systems, Version 1.1 (englisch),* ISBN: 978-92-79-18519-9, siehe unter http://www.moreq.info/index.php

[NATARCHUK2002] *Generische Anforderungen zur langzeitlichen Erhaltung elektronischer Informationen*, abgerufen unter: http://www.nationalarchives.gov.uk/documents/de_generic_requirements_vol1.pdf

[OAIS] ISO 14721:2012 Space Data and Information Transfer Systems – *Open Archival Information System (OAIS) – Reference Model. (2012)*, siehe unter http://www.iso.org/iso/iso_catalogue/catalogue_tc/catalogue_detail.htm%3Fcsnumber%3D57284

[OASIS VR] Hühnlein, D., *OASIS DSS v1.0 Profile for Comprehensive Multi-Signature Verification Reports Version 1.0*, Committee Specification 01, 12 November 2010, http://docs.oasis-open.org/dss-x/profiles/verificationreport/oasis-dssx-1.0-profiles-vr-cs01.pdf

[OASIS VR XSD] http://docs.oasis-open.org/dss-x/profiles/verificationreport/oasis-dssx-1.0-profiles-vr-cs01.html

[OASIS-Async] Kuehne, A.: *Asynchronous Processing Abstract Profile of the OASIS Digital Signature Services Version 1.0*, OASIS Standard, 11 April 2007, http://docs.oasis-open.org/dss/v1.0/oasis-dss-profiles-asynchronous_processing-spec-v1.0-os.pdf

[OASIS-DSS] OASIS: *Digital Signature Service Core Protocols, Elements, and Bindings, Version 1.0*, OASIS Standard, via http://docs.oasis-open.org/dss/v1.0/oasis-dss-core-spec-v1.0-os.pdf

[PDF 1.4] Adobe Systems Inc., *PDF – Reference – Third Edition – Adobe Portable Document Format Version 1.4*, Addison Wesley, ISBN 0-201-75839-3, siehe unter http://partners.adobe.com/public/developer/en/pdf/PDFReference.pdf, November 2001

[PDF 1.7] Adobe Systems Inc., *PDF – Reference – Sixt Edition – Adobe Portable Document Format Version 1.7*, November 2006, siehe unter http://www.adobe.com/content/dam/Adobe/en/devnet/acrobat/pdfs/pdf_reference_1-7.pdf

[PDF/A-3] ISO 19005-3:2012: *Document management – Electronic document file format for lang-term preservation – Part 3: Use of ISO 32000-1 with support for embedded files (PFD/A-3),* 2012, siehe unter http://www.iso.org/iso/iso_catalogue/catalogue_tc/catalogue_detail.htm%3Fcsnumber%3D57229

[PK-DML] *Prüfkriterien für Dokumentenmanagement-Lösungen*, VOI Verband Organisations- und Informationssysteme e.V., Bonn, 2. Auflage 2004

[PKCS#12] RSA Laboratories: *PKCS#12: Personal Information Exchange Syntax Standard*, Version 1.0, Juni 1999, siehe unter http://www.rsa.com/

[PKCS#7] RSA Laboratories: *PKCS#7: Cryptographic Message Syntax Standard*, Version 1.5, November 1993, siehe unter http://www.rsa.com/

[PREMIS] Library of Congress: *Preservation Metadata Maintenance Activity*, http://www.loc.gov/standards/premis/

[PTB 05] Physikalisch-Technische Bundesanstalt: *ArchiSafe-Webseite*, siehe unter http://www.archisafe.de

[RegR] *Richtlinie für das Bearbeiten und Verwalten von Schriftgut (Akten und Dokumenten) in Bundesministerien (RegR)*, siehe unter www.bmi.bund.de

[RFC1521] Borenstein, N., Freed, N.: IETF RFC 1521 – *MIME (Multipurpose Internet Mail Extensions) Part One: Mechanisms for Specifying and Describing the Format of Internet Message Bodies*, siehe unter http://www.ietf.org/rfc/rfc1521.txt

[RFC1945] Berners-Lee, T., Fielding, R., Frystyk, H.: IETF RFC 1945 – *Hypertext Transfer Protocol - HTTP/1.0*, siehe unter http://www.ietf.org/rfc/rfc1945.txt

[RFC2119] Bradner, S.: IETF RFC 2119 – *Key words for use in RFCs to Indicate Requirement Levels*, siehe unter http://www.ietf.org/rfc/rfc2119.txt

[RFC2401] Kent, S., Atkinson, R.: IETF RFC 2401 – *Security Architecture for the Internet Protocol (IPSec)*, siehe unter http://www.ietf.org/rfc/rfc2401.txt

[RFC2459] Housley, R., Ford, W.: IETF RFC 2459 – *Internet X.509 Public Key Infrastructure Certificate and CRL Profile*, siehe unter http://www.ietf.org/rfc/rfc2459.txt

[RFC2560] Myers, M., Ankney, A., Malpani, A, Galperin, S., Adams, C.: IETF RFC 2560 – *X.509 Internet Public Key Infrastructure - Online Certificate Status Protocol – OCSP*, siehe unter http://www.ietf.org/rfc/rfc2560.txt

obsolet, ersetzt durch [RFC6960]

[RFC2616] Fielding, R., Gettys, J., Mogul, J., Frystyk, H., Masinter, P., Leach, P., Berneres-Lee, T.: IETF RFC 2616 – *Hypertext Transfer Protocol - HTTP/1.1*, siehe unter http://www.ietf.org/rfc/rfc2616.txt

[RFC2634] Hoffman, P., Editor, *Enhanced Security Services for S/MIME*, RFC 2634, June 1999, http://www.ietf.org/rfc/rfc2634.txt

[RFC3161] Adams, C., Cain, P., Pinkas, D., Zuccherrato, R.: IETF RFC 3161 – *Internet X.509 Public-Key Infrastructure – Time Stamp Protocol (TSP)*, siehe unter http://www.ietf.org/rfc/rfc3161.txt

[RFC3275] Eastlake, D., Reagle, J., Solo, D.: IETF RFC 3275 – *(Extensible Markup Language) XML –Signature Syntax and Processing*, siehe unter http://www.ietf.org/rfc/rfc3275.txt

[RFC3280] Housley, R., Polk, W., Ford, W., Solo, D.: IETF RFC 3280 – *Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile*, siehe unter http://www.ietf.org/rfc/rfc3280.txt

obsolet, ersetzt durch [RFC5280]

[RFC3281] Farrell. S., Housley, R.: IETF RFC3281 – *An Internet Attribute Certificate Profile for Authorization,* siehe unter http://www.ietf.org/rfc/rfc3281.txt, April 2002

obsolet, ersetzt durch [RFC5755]

[RFC3447] Jonsson, J., Kaliski, B.: IETF RFC 3447 – Public-Key Cryptography Standards (PKCS)#1: RSA Cryptography Specifications Version 2.1, siehe unter http://www.ietf.org/rfc/rfc3447.txt, 2003

[RFC3533] Pfeiffer, S.: IETF RFC 3533 – *The Ogg Encapsulation Format Version 0*, siehe unter http://www.ietf.org/rfc/rfc3533.txt, 2003

[RFC3852] Housley, R.: IETF RFC 3852 – *Cryptographic Message Syntax (CMS)*, siehe unter http://www.ietf.org/rfc/rfc3852.txt, siehe auch RFC5652

obsolet, ersetzt durch [RFC5652]

[RFC4346] Dierks, T., Rescorla, E.: IETF RFC 4346 - *The Transport Layer Security (TLS) Protocol*, Version 1.1, siehe unter http://www.ietf.org/rfc/rfc4346.txt

[RFC4422] Melnikov, A., Zeilenga, K.: IETF RFC 4422 – *Simple Authentication and Security Layer (SASL)*, siehe unter http://www.ietf.org/rfc/rfc4422.txt

[RFC4510] Zeilenga, K., Ed.: IETF RFC 4510 – *Lightweight Directory Access Protocol (LDAP): Technical Specification Road Map*, siehe unter http://www.ietf.org/rfc/rfc4510.txt

[RFC4514] Zeilenga K., *Lightweight Directory Access Protocol (LDAP): String Representation of Distinguished Names*, RFC 4514, June 2006, http://www.ietf.org/rfc/rfc4514.txt

[RFC4648] Josefsson, S., SJD: IETF RFC 4510 – *The Base16, Base32, and Base64 Data Encodings*, siehe unter http://www.ietf.org/rfc/rfc4648.txt

[RFC4810] Wallace, C., Pordesch, U., Brandner, R.: IETF RFC 4810 – *Long-Term Archive Service Requirements*, siehe unter http://www.ietf.org/rfc/rfc4810.txt

[RFC4998] Gondrom, T., Brandner, R., Pordesch, u.: IETF RFC 4998 – *Evidence Record Syntax (ERS)*, siehe unter http://www.ietf.org/rfc/rfc4998.txt

[RFC5019] Deacon, A., Hurst, R.: IETF RFC5019 – *The Lightweight Online Certificate Status Protocol (OCSP) Profile for High-Volume Environments*, http://www.ietf.org/rfc/rfc5019.txt , September 2007

[RFC5035] Schaad, J., *Enhanced Security Services (ESS) Update: Adding CertID Algorithm Agility*, August 2007, http://tools.ietf.org/html/rfc5035

[RFC5055] Freeman, T., Housley, R., Malpani, A., Cooper, D., Polk, W.: IETF RFC 5055 – *Server-Based Certification Validation Protocol*, siehe unter http://www.ietf.org/rfc/rfc5055.txt

[RFC5126] Pinkas, D.,Ross, J., und Pope, N.: IETF RFC5126– *CMS Advanced Electronic Signatures (CAdES)*, Request For Comments, http://www.ietf.org/rfc/rfc5126.txt , Februar 2008

[RFC5276] Wallace, C.: IETF RFC5276 – *Using the Server-Based Certificate Validation Protocol (SCVP) to Convey Long-Term Evidence Records* http://www.ietf.org/rfc/rfc5276.txt, August 2008

[RFC5280] Cooper, D., Santesson, S., Farrell, S., Boeyen, S., Housley, R., Polk, W.: IETF RFC 5280 – *Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile*, siehe unter http://www.ietf.org/rfc/rfc5280.txt

[RFC5652] Housley, R.: IETF RFC 5652 – *Cryptographic Message Syntax (CMS)*, http://www.ietf.org/rfc/rfc5652.txt , September 2009

[RFC5755] Farrell. S., Housley, R., Turner, S.: IETF RFC5755 – An Internet Attribute Certificate Profile for Authorization, http://www.ietf.org/rfc/rfc5755.txt, Januar 2010

[RFC5816] Santesson, S., Pope, N., *ESSCertIDv2 Update for* RFC 3161, März 2010, siehe unter http://tools.ietf.org/html/rfc5816

[RFC6283] Blazic, A. J., Saljic, S., SETCCE, Gondrom, T.: *Extensible Markup Language Evidence Record Syntax (XMLERS)*, IETF Proposed Standard , siehe unter http://tools.ietf.org/html/rfc6283, July 2011

[RFC6818] Yee, P.: *Updates to the Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile,* siehe unter http://tools.ietf.org/html/rfc6818, Januar 2013.

[RFC6960] Santesson, S., Myers, M., Ankney, R., Malpani, A., Galperin, S., Adams, C.: *X.509 Internet Public Key Infrastructure Online Certificate Status Protokcol – OCSP,* siehe unter http://tools.ietf.org/html/rfc6960, Juni 2013

[RoSc05] Alexander Rossnagel und Paul Schmücker (Herausgeber). *Beweiskräftige und sichere Langzeitarchivierung elektronisch signierter Dokumente / Ergebnisse des Forschungsvorhabens ArchiSig* (Verlagsgruppe Huthig, Jehle, Rehm, 2005)

[SAGA-5] IT-Rat der Bundesregierung: SAGA 5, November 2011, siehe unter http://www.cio.bund.de/Web/DE/Architekturen-und-Standards/SAGA/saga_node.html

[SAMLv2] Cantor, S., Kemp, J., Philpott, R., Maler, E.: *Assertions and Protocol for the OASIS Security Assertion Markup Language (SAML) V2.0,* OASIS Standard, 15.03.2005

[SBJ 1991] Schmidt-Beck, J. R.:*Rechtliche Aspekte der EDV-gestützten ärztlichen Dokumentation*, NJW 1991, 2335

[SBR 04] Brumme, S, Gustmann, U, Krebs, F.:*Erfolgreiche Einführung elektronischer Archive*, Deutscher Sparkassen Verlag, Stuttgart, 2004

[SCHNEIER] Schneier, B.: *Angewandte Kryptographie*, Addison-Wesley, München 1996

[SFD 06] Fischer-Dieskau, S.: *Das elektronisch signierte Dokument als Mittel zur Beweissicherung*, Band 12 der Reihe *„Der elektronische Rechtsverkehr“*, 1. Auflage 2006, Nomos-Verlag.

[SigG] *Gesetz über die Rahmenbedingungen für elektronische Signaturen und zur Änderung weiterer Vorschriften (SigG)*, vom 16.5.2001, BGBl. 2001, Teil I Nr. 22, S. 876 ff., geändert durch Art 1 G v. 4.1.2005 I 2 , zuletzt durch Art. 4 G v. 17.07.2009

http://www.bundesnetzagentur.de/SharedDocs/Downloads/DE/Sachgebiete/QES/Rechtsgrundlagen/SignaturGesetz16052001Id2247pdf.pdf

[SigV] *Verordnung zur elektronischen Signatur (Signaturverordnung – SigV),* vom 16.11.2001, BGBl. 2001, Teil I Nr. 59, S. 3075 ff., geändert durch Art 2 G v. 4.1.2005 I 2, zuletzt durch Art. 1 ÄndVO v. 15.11.2010

http://www.bundesnetzagentur.de/SharedDocs/Downloads/DE/Sachgebiete/QES/Rechtsgrundlagen/SignaturVerordnungId18198pdf.pd

[SNIA 08] SNIA - Information Management – *Extensible Access Method (XAM) – Part 1: Architecture*, Version 1.0 , Working Draft, April, 2008, siehe unter http://www.snia.org

[sRGB] *Bilingual Multimedia systems and equipment - Colour measurement and management - Part 2-1: Colour management - Default RGB colour space - sRGB*, siehe unter: http://www.srgb.com/srgb.html bzw. als IEC-Standard: IEC 61966-2-1 – Ed. 1.0 – http://webstore.iec.ch/webstore/webstore.nsf/

http://webstore.iec.ch/webstore/webstore.nsf/artnum/025408

[TAP 03] Wallace, C., Chokani, S.: *Trusted Archive Protocol (TAP)*, Internet Draft , draft-ietf-pkix-tap-00.txt, February 2003, siehe unter http://tools.ietf.org/id/draft-ietf-pkix-tap-00.txt

[TIFF6] Adobe Systems Inc., *TIFF – Revision 6.0*, vom 3. Juni 1992, siehe unter http://partners.adobe.com/public/developer/en/tiff/TIFF6.pdf

[TR 02102] BSI TR-02102: *Kryptographische Verfahren: Empfehlungen und Schlüssellängen*, Version 1.0, 20.06.2008

[TR-ESOR-B] BSI TR 03125: Beweiswerterhaltung kryptographisch signierter Dokumente: *Anlage TR-ESOR-B: Profilierung für Bundesbehörden*

[TR-ESOR-C.1] BSI TR 03125: Preservation of Evidence of Cryptographically Signed Documents: *Annex TR-ESOR-C.1: Conformity Test Specification (Level 1 - Functional Conformity)*

[TR-ESOR-C.2] BSI TR 03125: Preservation of Evidence of Cryptographically Signed Documents: *Annex TR-ESOR-C.2: Conformity Test Specification (Level 2 - Technical Conformity)*

[TR-ESOR-C.3] BSI TR 03125: Preservation of Evidence of Cryptographically Signed Documents: *Annex TR-ESOR-C.3: Conformity Test Specification (Level 3 - Conformity with the German Federal Agency Profiling)*

[TR-ESOR-E] BSI TR 03125: Beweiswerterhaltung kryptographisch signierter Dokumente: *Anlage TR-ESOR-E Konkretisierung der Schnittstellen auf Basis des eCard-API-Frameworks*

[TR-ESOR-ERS] BSI TR 03125: Beweiswerterhaltung kryptographisch signierter Dokumente: *Anlage TR-ESOR-ERS Evidence Record gemäß RFC4998 und RFC6283*

[TR-ESOR-F] BSI TR 03125: Beweiswerterhaltung kryptographisch signierter Dokumente: *Anlage TR-ESOR-F Formate und Protokolle*

[TR-ESOR-M.1] BSI TR 03125: Beweiswerterhaltung kryptographisch signierter Dokumente: *Anlage TR-ESOR-M.1 ArchiSafe Modul*

[TR-ESOR-M.2] BSI TR 03125: Beweiswerterhaltung kryptographisch signierter Dokumente: *Anlage TR-ESOR-M.2 Krypto-Modul*

[TR-ESOR-M.3] BSI TR 03125: Beweiswerterhaltung kryptographisch signierter Dokumente: *Anlage TR-ESOR-M.3 ArchiSig-Modul*

[TR-ESOR-S] BSI TR 03125: Beweiswerterhaltung kryptographisch signierter Dokumente: *Anlage TR-ESOR-S Schnittstellenspezifikation*

[TR-ESOR] BSI TR 03125: Beweiswerterhaltung kryptographisch signierter Dokumente, *Hauptdokument,* dieses Dokument

[TR-ESOR-VR] BSI TR 03125: Preservation of Evidence of Cryptographically Signed Documents: Annex TR-ESOR-VR: *Verification Reports for Selected Data Structures*

[UNICODE] Unicode Consortium: *Unicode Standard* (ISBN 0-201-61633-5), siehe unter http://unicode.org/versions/Unicode4.1.0/dies ist funktional äquivalent zu ISO/IEC 10646:2003 – *Information technology – Universal Multiple-Octet Coded Character Set (UCS)*. siehe unter http://www.iso.org/

[VERS] *Victorian Electronic Records Strategy*, siehe unter http://www.prov.vic.gov.au/vers

[VOI 05] VOI – Verband Organisation und Informationssysteme e.V.: *Dokumenten-Management Vom Archiv zum Enterprise-Content-Management*, , Bonn, 2005

[WSDL] W3C Recommendation: *Web Services Description Language (WSDL)* Version 1.1, siehe unter http://www.w3.org/TR/wsdl

[X.408] ITU-T: *ITU-T Recommendation X.408, Message Handling Systems : Encoded Information Type Conversion Rules*, 1988

[X.509] ITU-T: *ITU-T Recommendation X.509 (2012) - ISO/IEC 9594-8:Information Technology – Open Systems Interconnection – The Directory: Public-key and attribute certicate frameworks,* 2012, siehe unterhttp://www.itu.int/rec/T-REC-X.509/en

[X.680] ITU-T: *ITU-T Recommendation X.680(2002) – ISO/IEC 8824-1:2002. Information Technology – Abstract Syntax One (ASN.1): Specification of Basic Notation*, 2002

[XAdES] ETSI: *XML Advanced Electronic Signatures (XAdES)*, ETSI Technical Specification TS 101 903, Version 1.4.2, , Dezember 2010, siehe unter http://www.etsi.org

XBARCH https://www.bundesarchiv.de/fachinformationen/00895/index.html.de, Version 1.4.3

XDOMEA	https://www.xrepository.de/Inhalt/urn:uuid:0e13664e-6df5-4d1f-8397-elee-d87a0d4a.xhtml, Version 2.2.0
[XFDU]	Nikhinson, S., Reich, L.: *XML formatted Data Unit (XFDU), Structure and construction rules*, CCSDS 661.0-R-1, January 2007, siehe unter http://sindbad.gsfc.nasa.gov/xfdu
[XML Name]	W3C: *Namespaces in XML 1.1 (Second Edition)*, W3C Recommendation 16 August 2006 siehe unter http://www.w3.org/TR/REC-xml-names/
[XML]	Bray, T. et al.: *Extensible Markup Language (XML) 1.1*, second edition, W3C Recommendation, 16.August 2006, siehe unter http://www.w3.org/TR/xml
[XMLDSIG]	Eastlake, D. , et al.: *XML Signature Syntax and Processing (Second Edition)*, W3C Recommendation 10 June 2008 siehe unter http://www.w3.org/TR/2008/REC-xmldsig-core-20080610/
[XMLENC]	Imamura, T. et al.: *XML Encryption Syntax and Processing,* W3C Recommendation 10 December 2002 siehe unter http://www.w3.org/TR/2002/REC-xmlenc-core-20021210/
[XMLENC 12]	Imamura, T. et al.: *XML Encryption Syntax and Processing Version 1.1,* Working Draft 18 October 2012 siehe unter http://www.w3.org/TR/xmlenc-core1/
[XMLENTRUST]	EnTrust XML Schema, http://www.si-tsa.gov.si/dokumenti/timestamp-protocol-20020207.xsd
[XMLERS]	Blazic, A. J., Saljic, S., SETCCE, Gondrom, T.: *Extensible Markup Language Evidence Record Syntax (XMLERS)*, IETF Proposed Standard , July 2011 siehe unter http://tools.ietf.org/html/rfc6283
[XMLSACR]	World Wide Web Consortium (W3C): *XML Security Algorithm Cross-Reference*. W3C Working Draft 05 January 2012 siehe unter http://www.w3.org/TR/2012/WD-xmlsec-algorithms-20120105/
[XML-SRC]	World Wide Web Consortium (W3C): *XML Security Algorithm Cross-Reference*, W3C Working Group Note 11 April 2013, http://www.w3.org/TR/xmlsec-algorithms/
[XSD]	Fallside, D. C., et al.: (Ed.): *XML Schema*, W3C Recommendation, 28. October 2004 siehe unter http://www.w3.org/TR/xmlschema-0/ (Primer) siehe unter http://www.w3.org/TR/xmlschema-1/ (Structures) siehe unter http://www.w3.org/TR/xmlschema-2/ (Datatypes)
[XSD2012]	W3C, *W3C XML Schema Definition Language (XSD) 1.1 Part 2: Datatypes*, Version 1.1, http://www.w3.org/TR/xmlschema11-2, April 2012
[ZPO]	*Zivilprozessordnung*, siehe unter www.gesetze-im-internet.de/zpo