Standards und Lösungen zur langfristigen Beweiswerterhaltung

Steffen Schwalm[1] · Ulrike Korte[2] · Detlef Hühnlein[3] · Tomasz Kusber[1]

[1]BearingPoint
{steffen.schwalm | tomasz.kusber}@bearingpoint.com

[2]Bundesamt für Sicherheit in Informationstechnik (BSI)
ulrike.korte@bsi.bund.de

[3]ecsec GmbH
detlef.huehnlein@ecsec.de

Zusammenfassung

Die Geschäftsprozesse in der öffentlichen Verwaltung und Wirtschaft werden zunehmend digitalisiert. Besondere Herausforderungen existieren dabei insbesondere beim dauerhaften Erhalt der Beweiskraft der elektronisch signierten Dokumente. Vor diesem Hintergrund wurden internationale Standards wie ISO 14721, RFC 4998/RFC 6283, deutschen Standards wie die DIN-Standards DIN 31644 und DIN 31647 und europäische ETSI-Standards für die Signaturformate CAdES, XAdES und den Container ASiC entstellt. Auf dieser Basis entwickelt das Bundesamt für Sicherheit in der Informationstechnik (BSI) die entsprechende Technische Richtlinien TR-ESOR mit Lösungsansätzen und Empfehlungen, die auch in § 6 EGovG (Elektronische Aktenführung) ihren Niederschlag fanden [EGovG-RE]). Der vorliegende Beitrag erläutert die wesentlichen Inhalte der vorgenannten Standards und stellt das mögliche Zusammenspiel dieser Standards in kompakter Weise vor.

1 Einleitung

Die Nutzung der Informationstechnologie zur Abbildung durchgängig elektronischer Geschäftsprozesse ist in der Wirtschaft und der öffentlichen Verwaltung etabliert. Dabei bestehen weiterhin umfassende Dokumentations- und Nachweispflichten zur Nachvollziehbarkeit der Entscheidungsprozesse gegenüber Dritten, so z. B. Gerichten oder Prüfbehörden. Manifestiert wird dies u. a. durch die Aktenführungspflicht der öffentlichen Verwaltung oder handels- und steuerrechtliche sowie spezialgesetzliche (z. B. Pharmaindustrie, Bauwesen, Banken/Versicherungen etc.) Rahmenbedingungen. Elementare Grundlage zur Erfüllung dieser Nachweispflichten bildet gem. der rechtlichen wie fachlichen Anforderungen die Wahrung der:

- Authentizität (Echtheit des Ausstellers oder Absenders eines Dokuments)
- Integrität (Unveränderlichkeit abgeschlossener Dokumente)
- Nutzbarkeit
- Verlässlichkeit (Nachvollziehbarkeit und damit Vollständigkeit zum Nachweis des jeweiligen Entscheidungsprozesses notwendigen Unterlagen)

P. Schartner · P. Lipp (Hrsg.) · D•A•CH Security 2014 · syssec (2014) 46-58.

der elektronischen Unterlagen bis zum Ablauf der geltenden Aufbewahrungsfristen sowie der eindeutige Nachweis dessen gegenüber Gerichten oder Prüfinstitutionen (z. B. Rechnungshof). Realisiert wird dies vor allem durch eine ganzheitliches Records Management, welches den gesamten Lebenszyklus elektronischer Unterlagen einbezieht. Records Management beschreibt die notwendigen organisatorischen Regularien und hieraus abgeleiteten Maßnahmen und Verantwortlichkeiten nachhaltiger elektronischer Geschäftsprozesse unter Beachtung der geltenden rechtlichen Rahmenbedingungen sowie der Anforderungen der jeweiligen externen Stakeholder einer öffentlichen wie private Organisation. Hinzu kommen die eingesetzten technischen Verfahren, um eine anforderungskonforme Erzeugung, Strukturierung, Aufbewahrung und einen Zugriff auf geschäftsrelevante Unterlagen zu ermöglichen und so die Erfüllung geltender Dokumentationspflichten, so der Nachvollziehbarkeit der Entscheidungsprozesse gegenüber Dritten z. B. Gerichte, Prüfbehörden, sicherzustellen. Wesentliche Grundlage zur Nachweisführung ist dabei die Gewährleistung der Verkehrsfähigkeit der Daten, also die Möglichkeit, die Wahrung der o. g. Anforderungen an den Unterlagen selbst nachzuweisen, da im Streitfall diese und nicht die jeweils eingesetzte Hard- oder Software als Beweisdokumente dienen.

Die Nutzung kryptographischer Sicherungsmittel, wie fortgeschrittene oder qualifizierte elektronischer Signaturen (QES) und qualifizierte Zeitstempel (QZS), ermöglicht nach geltendem Recht sowie dem aktuellen Stand der Technik die Erhaltung des für die Nachweisführung notwendigen Beweiswerts, ohne die Verkehrsfähigkeit einzuschränken (siehe [Fish06, Ross07, [BMWi07]). Qualifizierte elektronische Signaturen ermöglichen durch zugrundeliegende Zertifikate die nichtabstreitbare Zuordnung elektronischer Dokumente zum Aussteller bzw. Absender sowie durch die eingesetzten Hashwerte den eindeutigen Nachweis der Integrität und so die maßgeblichen Voraussetzungen zur Beweisführung gegenüber Dritten. Qualifizierte Zeitstempel, die technisch eine QES beinhalten, beweisen, dass der Hashwert eines elektronischen Dokuments zu der angegebenen Zeit dem Aussteller des Zeitstempels im Sinne eines „proof of existence (PoE)“ vorgelegen hat. Archive können so den Zeitpunkt eindeutig nachweisen, ab dem das jeweilige Dokument nicht mehr verändert wurde.

Diese Entwicklung vollzieht sich vor dem Hintergrund geltender Aufbewahrungsfristen zwischen 2 und 100 Jahren oder dauernd. Im Kontext der technischen Innovation der IT unterliegen sowohl die eingesetzten Dateiformate der geschäftsrelevanten Unterlagen als auch die zum Nachweis von Authentizität und Integrität eingesetzten kryptographischen Signaturen und Zeitstempel der technischen Alterung. Dies bedeutet im Falle dieser kryptographischen Sicherungsmittel, dass die eingesetzten Signatur- und Hashalgorithmen kompromittiert werden können und somit die Beweissicherheit der Unterlagen, auf die sie sich beziehen, nach einiger Zeit gefährdet sein kann.

Insofern gilt es, neben der Erhaltung der elektronischen Unterlagen selbst, Maßnahmen und Verantwortlichkeiten zu treffen, um den Beweiswert elektronischer Unterlagen bis zum Ablauf der geltenden Aufbewahrungsfristen zu sichern, um eine langfristige, gerichtsfeste Nachweisbarkeit von Authentizität und Integrität und damit eine nachhaltige elektronische Geschäftsführung zu ermöglichen. Der Beweiswert ist wie beschrieben eine inhärente Eigenschaft der jeweiligen elektronischen Unterlagen. Dementsprechend müssen Maßnahmen zur Beweiswerterhaltung auch direkt an den elektronischen Unterlagen ansetzen. Dies erfolgt durch eine Nachsignatur (gem. § 17 SigV), also der Anbringung einer neuen qualifizierten elektronischen Signatur sowie eines qualifizierten Zeitstempels an den aufzubewahrenden Unterlagen, bevor die bislang eingesetzten kryptographischen Algorithmen ihre Sicherheits-

eignung verlieren. Hierbei genügt die Erstellung von qualifizierten Zeitstempeln, sofern diese mittels einer qualifizierten elektronischen Signatur erzeugt wurden.

Mit dem in ISO 14721 genormten OAIS-Modell (vgl. [OAIS]), der DIN 31644 (vgl. [DIN 31644:2012-04]) und DIN 31645 (vgl. [DIN 31645:2011-11]) stehen etablierte Normen zur Verfügung, welche die notwendigen Maßnahmen zur Erhaltung der elektronischen Unterlagen (Informationserhaltung) umfassend beschreiben. Im Kontext der Erzeugung und Aufbewahrung geschäftsrelevanter Unterlagen sind diese Standards durch Lösungswege zur Beweiswerterhaltung gezielt zu ergänzen In Bezug auf die Beweiswerterhaltung werden diese Standards zur Informationserhaltung durch die DIN 31647 (draft) (vgl. [DIN-31647]) sowie die TR-03125 des BSI (vgl. [BSI-TR-03125]) ergänzt.

Dieser Beitrag liefert auf Basis einer zielgerichteten Verknüpfung der Standards zur Informations- und Beweiswerterhaltung einen Vorschlag zur langfristigen Nachweisfähigkeit der Authentizität und Integrität elektronischer Unterlagen bei gleichzeitiger Wahrung von deren Verkehrsfähigkeit. Wesentliche Maßgabe ist die Unabhängigkeit von einer bestimmten Hard- oder Softwareumgebung, deren Existenz über die Aufbewahrungsdauer erfahrungsgemäß nicht gesichert werden kann. Hierauf aufbauend stellt der Beitrag die neusten im Rahmen der Fortschreibung der zur Beweiswerterhaltung unter Verwendung kryptographischer Methoden maßgeblichen Technischen Richtlinie 3125 des BSI (vgl. [BSI-TR03125]) erarbeiteten technischen Ansatz im Kontext der Verwendung von Evidence Record gem. [RFC4998] bzw. [RFC6283] vor und diskutiert die Möglichkeiten zur Integration der europäischen Entwicklung zur Thema interoperablen Signatur-Container - Associated Signature Containers (ASiC) (vgl. [ETSI319162-{1,2}]).

2 Standards zur Langzeitspeicherung

2.1 ISO-14721

Das in ISO-14721 genormte OAIS-Modell (vgl. [OAIS]) beschreibt grundlegend die notwendigen Funktionen und Informationspakete zur langfristigen Aufbewahrung elektronischer Unterlagen. Abbildung 1zeigt das OAIS-Modell im Überblick.

Das OAIS-Modell geht dabei von der Aufbewahrung der elektronischen Unterlagen in selbsttragenden Archivinformationspaketen (AIP) aus, also Datenpaketen, die alle zur Erfüllung des Aufbewahrungszwecks notwendigen Informationen bis zum Ablauf der geltenden Aufbewahrungsfristen in einer hard- und softwareneutralen Form beinhalten. Es handelt es sich dabei um:

- Metadaten
- Inhaltsdaten (die aufzubewahrenden Daten selbst)[1]
- Zum Nachweis von Authentizität und Integrität notwendige Daten.

[1] Z.B. PDF/A für dokumentbasierte Unterlagen, SIARD für Datenbanken etc.

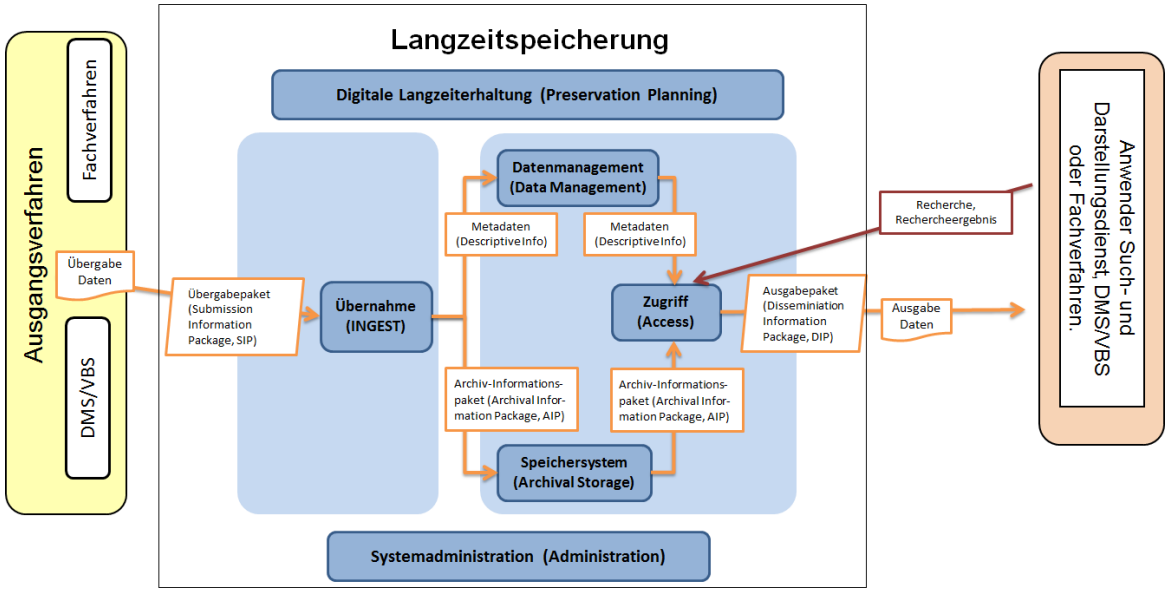

Abb. 1: Open Archival Information System (OAIS) – Überblick

Dabei ist es z.B. für die öffentliche Verwaltung nicht ausreichend, einzelne Dokumente oder Daten aufzubewahren. Vielmehr muss die Langzeitspeicherung den Entstehungskontext bzw. den Aktenzusammenhang wahren. Es gilt, Verwaltungsentscheidungen für die gesamte Dauer der Aufbewahrungsfristen nachvollziehbar und beweissicher zu halten. Nur so kann der bestehende Beweiswert erhalten und Kosten für die aufwändige Rekonstruktion der Unterlagen vermieden werden. Dementsprechend müssen die fachlichen Metadaten den Aktenzusammenhang nachweisen. Die Beweiswerterhaltung setzt hier also schon bei den Metadaten und nicht erst bei den kryptographischen Sicherungsmitteln an.

2.2 DIN 31644 und DIN 31647

Die DIN 31644 (vgl. [DIN 31644:2012-04]) untersetzt das allgemeingültige OAIS-Modell durch Anforderungen an ein vertrauenswürdiges digitales Langzeitarchiv (dLZA), welches als organisatorisches (Rollen, Verantwortlichkeiten Ziele) wie technisches System (funktionale Anforderungen) zu betrachten. Hierzu gehört neben der Benennung des Anwendungszwecks (z. B. beweissichere Aufbewahrung bis zum Ablauf der geltenden Aufbewahrungsfristen) und Zielen des dLZA, die hieraus abgeleitete Festlegung verbindlicher Verantwortlichkeiten, die Detaillierung der Prozesse und Informationspaketen gem. OAIS-Modell für das dLZA. Die DIN 31644 fokussiert dabei, äquivalent dem OAIS-Modell, auf die Informationserhaltung für die jeweilige Aufbewahrungsdauer.

Die DIN 31647 (vgl. [DIN 31647]) formuliert fachliche und funktionale Anforderungen an ein generisches System zur Beweiswerterhaltung kryptographisch signierter Dokumente unter Wahrung der Authentizität , Integrität , Nachvollziehbarkeit, Verfügbarkeit, Verkehrs- und Austauschfähigkeit der Dokumente bis zum Ablauf der geltenden Aufbewahrungsfristen. Die Archivierung in Gedächtnisorganisationen ist kein Anwendungsfeld der DIN 31647. Als kryptographisch signierte Dokumente gelten dabei alle Unterlagen, deren Beweiswert mit Hilfe kryptographischer Sicherungsmittel erhalten werden soll.

Die in der Norm 31647 beschriebenen Funktionen zur Beweiswerterhaltung kryptographisch signierter Dokumente stellen dabei kein eigenes System dar. Sie ergänzen vielmehr ein vertrauenswürdiges dLZA gem. dem OAIS-Modell sowie der DIN 31644 um die notwendigen

Funktionen zur Beweiswerterhaltung der elektronischen Unterlagen. Ein generisches System zur Beweiswerterhaltung beinhaltet daneben z. B. folgende Funktionen:

- Hashen von AIP,
- Einholung und Prüfung der beweisrelevanten Daten:
  - Signaturprüfung, Einholung beweisrelevanter Daten (z.B. Zertifikatsinformationen, Sperrdaten [CRL-Listen, OCSP-Antworten] und Einlagerung im AIP,
- Erzeugen von technischen Beweisdaten des AIP:
  - Evidence Record gem. RFC 4998 bzw. RFC 6283 einschl. Archivzeitstempel und Nachweis über Gültigkeit elektronischer Signaturen zum Signaturzeitpunkt sowie die rechtzeitige Signaturerneuerung / Hasherneuerung,
- Abruf der technischen Beweisdaten und beweisrelevanten Daten des AIP,
- Prüfung der technischen Beweisdaten,
- Erhaltung durch Erneuerung der technischen Beweisdaten des AIP,
- Nachsignatur und Hasherneuerung:
  - Einschluss aller alle vorhergehenden Signaturen und Zeitstempel.

Ein vertrauenswürdiges dLZA, welches den Beweiswert der aufbewahrten Unterlagen und so deren langfristigen Nachweis der Authentizität und Integrität sichert, beinhaltet damit Funktionen zur:

- Informationserhaltung (Aufnahme und/oder Erzeugung der notwendigen Metadaten, Formatkonvertierung etc. Migrationsfunktionen etc.)

und

- Beweiswerterhaltung.

Die AIPs beinhalten also die notwendigen Informationen für beide Zwecke in selbsttragender und damit herstellerneutraler Form.

2.3 TR 03125 mit RFC 4998 und RFC 6283

Die TR-03125 (vgl. [BSI-TR-03125]) beschreibt in einer Referenzarchitektur notwendige Module und Funktionen zur Beweiswerterhaltung kryptographisch signierter Dokumente und damit eine mögliche Umsetzungsform der DIN 31647. Konkret beinhaltet die Richtlinie:

- Daten- und Dokumentenformate,
- Austauschformate für Archivdatenobjekte und Beweisdaten,
- Empfehlungen zu einer Referenzarchitektur, zu ihren Prozessen, Modulen und Schnittstellen als Konzept einer Middleware,
- zusätzliche Anforderungen für Bundesbehörden sowie
- Konformitätsregeln für die folgende Konformitätsstufen:
  - Konformitätsstufe 1: „logisch-funktional“ (vgl. [BSI-TR-03125-C.1]),
  - Konformitätsstufe 2: „technisch-interoperabel“ (vgl. [BSI-TR-03125-C.2]),
  - Konformitätsstufe 3: „Bundesbehördenprofil“ (vgl. [BSI-TR-03125-C.3]).

Sie setzt hinsichtlich der Module und Funktionen auf den Erfahrungen des ArchiSafe- (vgl. [ArchiSafe]) und ArchiSig-Projekts (vgl. [RoSc06]) auf und greift auf Standards wie ISO-14721 etc. zurück. Hinsichtlich der Beweiswerterhaltung basiert die TR auf der Nutzung von

Merkle-Hashbäume und der Erzeugung von Evidence Records gem. [RFC4998] bzw. [RFC6283] mit Archivzeitstempeln gem. RFC 3161. Hinsichtlich des Formats der AIP wird mit dem auf XFDU (vgl. [XFDU]) basierenden XAIP eine XML-Struktur empfohlen, welche die Erzeugung selbsttragender AIP gem. OAIS-Modell ermöglicht, ergänzt um eine Sektion für die beweisrelevanten Daten und technischen Beweisdaten – also die zur Beweiswerterhaltung notwendigen Credentials. Der Erhalt der Integrität und Authentizität eines solchen selbsttragenden XAIPs über einen langen Zeitraum wird gem. TR 03125 durch den Einsatz von Zeitstempeln gem. [RFC4998] bzw. [RFC6283] erreicht, die erneuert werden, bevor die bis dahin genutzten Signatur- und Hashalgorithmen ihre Sicherheitseignung verlieren.

Um die Anzahl der erforderlichen qualifizierten Zeitstempel bei der Zeitstempelerneuerung zu minimieren, beschreiben die Standards [RFC4998] bzw. [RFC6283] Prozesse und CMS- bzw. XML-basierte Datenstrukturen, um zahlreiche Archivdatenobjekte mit einem einzigen Prozessschritt und mit nur einem einzigen Zeitstempel unter Nutzung von Merkle Hashbäume (vgl. [Merk80]) zu schützen bzw. gem. SigV § 17 überzusignieren. Dabei stellen die unteren Blätter des Hashbaumes die Hashwerte der zu schützenden Datenobjekte dar, und der Zeitstempel wird für den obersten alleinigen Hashwert des Hashbaumes errechnet.

Um die Existenz eines speziellen Datenobjekts oder einer speziellen Datengruppe zu einem bestimmten Zeitpunkt zu beweisen, kann der Hashbaum auf eine kleine Menge von Hashwerten reduziert werden, die auch als reduzierter Hashbaum oder technische Beweisdaten (engl.: Evidence Record) bezeichnet werden. Dieser Evidence Record reicht aus, die Existenz sowie Integrität und Authentizität eines Datenobjektes oder einer Datengruppe zu einem bestimmten Zeitpunkt zu beweisen.

Die nachstehende Graphik (vgl. Abbildung 2) zeigt beispielhaft das Prinzip des Merkle-Hashbaums, der die Hashwerte einer Vielzahl an AIPs unter einem Archivzeitstempel beinhalten kann und so eine wirtschaftliche Beweiswerterhaltung ermöglicht.

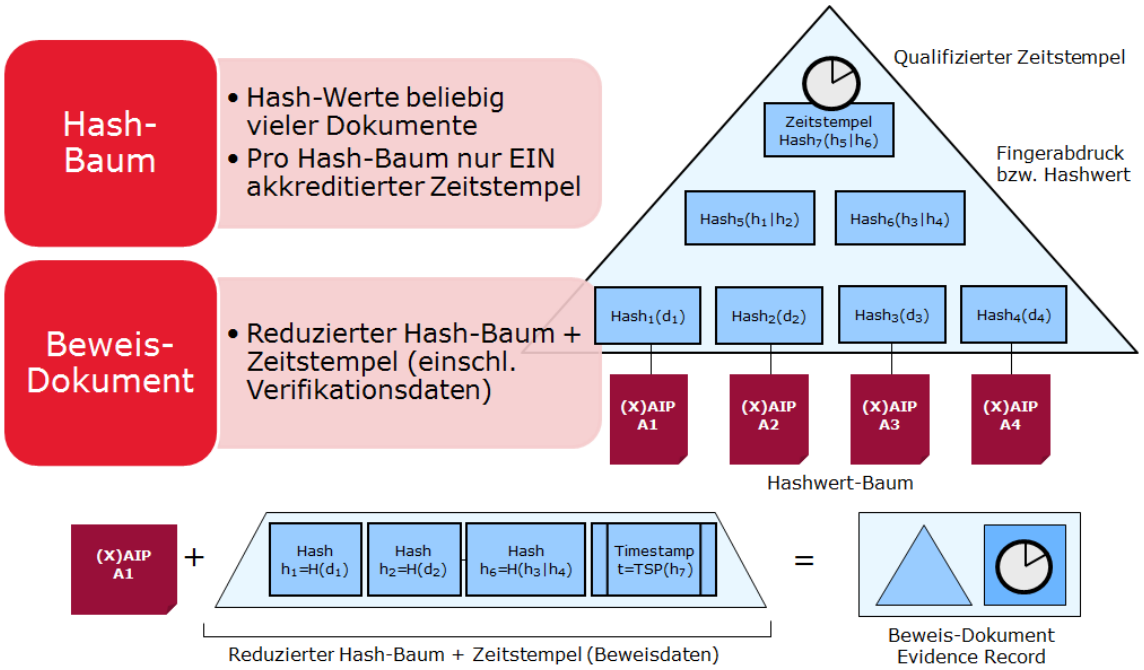

Abb. 2: Merkle-Hashbaum

Falls der Signaturalgorithmus droht, seine Sicherheitseignung zu verlieren, wird über dem vorhandenen Zeitstempel ein neuer Zeitstempel mit einem zum Zeitpunkt der Erstellung sicheren Signaturalgorithmus erzeugt. Die daraus resultierende Datenstruktur wird Zeitstempelkette genannt. Falls der Hashalgorithmus in absehbarer Zeit droht, seine Sicherheitseignung zu verlieren, wird mit einem zum Zeitpunkt der Erstellung sicheren Hashalgorithmus auf Basis der bislang archivierten Daten und dem vorhandenen zuletzt erstellten Archivzeitstempel ein neuer Hashbaum erstellt. Diese neu gewonnene Datenstruktur wird Archivzeitstempelsequenz genannt.

2.4 Beweiswerterhaltung gem. ETSI

Ein alternativer Ansatz für die Beweiswerterhaltung bis zum Ablauf der geltenden Aufbewahrungsfristen ist in [ETSI101733] oder [ETSI319122-{1,2}] bzw. [ETSI101903] oder [ETSI319122-{1,2}] vorgestellt.

In diesen Standards werden aktuell unter der Bezeichnung {C/X}AdES verschiedene Signaturprofile für {CMS/XML}-basierte fortgeschrittene elektronische Signaturen definiert.

Ziel der Profile {C/X}AdES-A ist die beweiswerterhaltende Archivierung von elektronischen Signaturen über einen langen Zeitraum. Dieser Ansatz benutzt direkt die Mechanismen, die von der Signaturen gem. CAdES-A bzw. XAdES-A angeboten werden. Dementsprechend wird eine CMS-Signatur zu einer CAdES-A Signatur ausgebaut und z. B. mithilfe von sog. Archive-Timestamp-V3 (ATSv3) Attribut geschützt (vgl. [ETSI101733], Kap. 6.4.3). Eine XML-Signatur kann entsprechend zu einer XAdES-A-Signatur ausgebaut werden und mithilfe des sog. *<xadesv141:ArchiveTimeStamp>* Element versiegelt (vgl. [ETSI101903], Kap. 8.2) werden.

Ein ATSv3 wird als nichtsigniertes Attribut innerhalb der Signatur abgelegt, und es ist erlaubt, dass es mehrmals vorkommt. Die Erneuerung besteht darin, dass ein neuer ATSv3 bezogen wird, der u. A. alle bereits vorhandenen relevanten nichtsignierten Attribute[2] der vorausgegangenen Signatur oder des vorausgegangenen Zeitstempels schützt (vgl. [ETSI101733], Kap. 6.4).

Die XAdES-A-Signaturen beinhalten den Archivzeitstempel als Teil der die Signatur qualifizierenden nichtsignierten Eigenschaften. Die Zeitstempelerneuerung besteht darin, dass ein neuer Zeitstempel erzeugt wird und als zusätzliches Element innerhalb der nichtsignierten Eigenschaften abgelegt wird. Der Vorgängerzeitstempel kann mit geschützt werden, sofern im unsignedAttrsHashIndex-Attribut des ATSHashIndex ein Hashwert bzgl. des vorausgegangenen Zeitstempels abgelegt wird (vgl. [ETSI101903], Kap. 8.2).

Im Allgemeinen benötigt eine Zeitstempelerneuerung gemäß {C/X}AdES jeweils einen neuen Zeitstempel pro Archivdatenobjekt. Allerdings ist es gegenwärtig in CAdES auch möglich, Evidence Records in ein unsigniertes Attribut beizufügen, die sich auf mehrere Archivdatenobjekte beziehen können.

[2] Sogenannte unsigned attributes

2.5 Associated Signature Container (ASIC)

Ein weiterer Ansatz zur Beweiswerterhaltung elektronischer Unterlagen unter Verwendung kryptographischer Methoden bildet die Nutzung von Associated Signature Container (vgl. [ETSI319162-1]), einem weiteren derzeit sich in Entwicklung befindenden ETSI-Standard.

Kryptographische elektronische Signaturen können unterschiedlich mit den signierten Daten gebunden werden. Man unterscheidet:

- verbundene Signaturen (attached signature), die entweder die signierten Daten umhüllen (enveloping signature) oder von den signierten Daten umhüllt werden (enveloped signature),
- abgesetzte Signaturen (detached signature), die die signierten Daten referenzieren.

Der Ansatz von abgesetzten Signaturen bringt den Vorteil mit sich, dass die signierten Daten nicht verändert werden. Andererseits können die Signatur und die signierten Daten leicht voneinander getrennt werden und so der Beweiswert, z.B. im Rahmen der zur Datenerhaltung notwendigen Migrationen, verlorengehen. Um dieser Problematik entgegen zu kommen, werden die vordefinierten Container benötigt, die in einer definierten Art und Weise sowohl die Daten als auch die dazugehörenden Signaturen beinhalten können. Gem. [ETSI319162-1], Kap. 4.1 werden folgende Signaturobjekte unterstützt:

- CAdES, gem. [ETSI319122-{1,2}],
- XAdES, gem. [ETSI319132-{1,2}],
- Zeitstempeltoken, gem. [RFC3161].

Ein ASiC-Container basiert jeweils auf CAdES oder XAdES.

Der Aufbau des Containers orientiert sich dabei an einem ZIP-Container, wie von vielen Anwendungen bereits benutzt[3], schreibt jedoch keine konkrete Zusammenstellungsstruktur vor. Grundsätzlich unterscheidet man zwei Typen von Container:

- ASiC-S – Simple Associated Signature Container, der nur ein signiertes Objekt beinhaltet,
- ASiC-E – Extended ASiC – beinhaltet ein oder mehrere signierte Objekte, jeweils mit möglichen mehrerer Signaturen und/oder Zeitstempeln.

3 Bewertungen und Lösungsvorschläge

3.1 Vergleich der ERS- und {C/X}-AdES-basierten Ansätze

Die beiden zuvor vorgestellten Ansätze für die Beweiswerterhaltung in einem vertrauenswürdigen digitalen Langzeitarchiv gem. [BSI-TR03125] bzw. [ETSI101733] oder [ETSI319122-{1,2}] bzw. [ETSI101903] oder [ETSI319122-{1,2}] werden unter Aspekten der Überschaubarkeit und Wirtschaftlichkeit untersucht und die Ergebnisse zusammengestellt. Wünschenswert im Sinne der technischen Interoperabilität ist eine Entwicklung, die weder einen noch den anderen Ansatz verhindert und darüber hinaus die Möglichkeit anbietet, eine möglichst nahtlose Übernahme der Daten aus einem gem. Paradigma A funktionierenden dLZA in ein gem. Paradigma B funktionierenden dLZA zu gewährleisten, ohne den Beweiswert zu

[3] Beispielsweise Open Document Format (ODF) oder OEBPS Container Format (OCF) u.Ä.

verlieren. Der mögliche Weg, der mit ETSI bereits diskutiert wurde, ist die Aufnahme der optionalen Profile CAdES-A und XAdES-A als Zeitstempelformat für Evidence Records in [BSI-TR03125] einerseits und die optionale Benutzung eines gem. [RFC4889] bzw. [RFC6283] erzeugten Evidence Records als sog. „proof of evidence“ innerhalb der ETSI-Signatur-Standards andererseits.

Die alleinige Nutzung eines ATSv3 gemäß [ETSI101733] oder [ETSI319122-{1,2}] zur Beweiswerterhaltung bedingt die Zeitstempelung jedes Archivdatenobjekts, was im Hinblick auf die permanent steigende Datenmenge aufzubewahrender elektronischer Unterlagen allein aus wirtschaftlicher Sicht kritisch zu betrachten ist. Im Gegensatz dazu impliziert der auf Merkle Hashbäumen beruhende Ansatz gemäß [RFC4998] und [RFC6283] die Einbindung einer beliebigen Anzahl von Archivdatenobjekte innerhalb eines Hashbaums mit der daraus folgenden objektbezogenen Erzeugung der zur Nachweisführung notwendigen Evidence Records und ist daher performanter und wirtschaftlicher.

Auch ist der Prüfvorgang eines Evidence Records auf Basis der zeitlich und kaskadierend auf einander aufbauenden Sequenzen von Beweisdatenketten deutlich einfacher und übersichtlicher als die Validierung einer {C/X}-AdES-Signatur ([ETSI 319 102]).

3.2 Erweiterung des ASiC-Containers um Evidence Records

Im Rahmen des Reviews zu [ETSI319162-{1,2}] im Dezember 2013 wurde eine Erweiterung der in ASiC möglichen Signatur-/ und Zeitstempelobjekt- Typen um den Evidence Records gem. [RFC4998] bzw. [RFC6283] vorgeschlagen, wie im folgenden Text dargestellt wird. Beim Exportieren eines durch einen Evidence Records geschützten Datenobjekts, z. B. XAIP, aus einem Archiv ist in diesem Fall der entsprechende Evidence Record auch aus dem Archiv zu extrahieren und im ASiC-Container zusammen mit den zugehörigen Nutz- und Signaturdaten abzulegen (als Erweiterung zu [ETSI319162-1], Kap. 5.4 und Kap. 6.5).

Die Referenzierung zwischen den Nutzdaten und dem Evidence Record erfolgt mittels eines Manifests, sofern im Evidence Record selbst keine Referenz- Datenelemente enthalten sind.

Das Ergebnis sieht dann folgendermaßen aus (vgl. Abbildung 3):

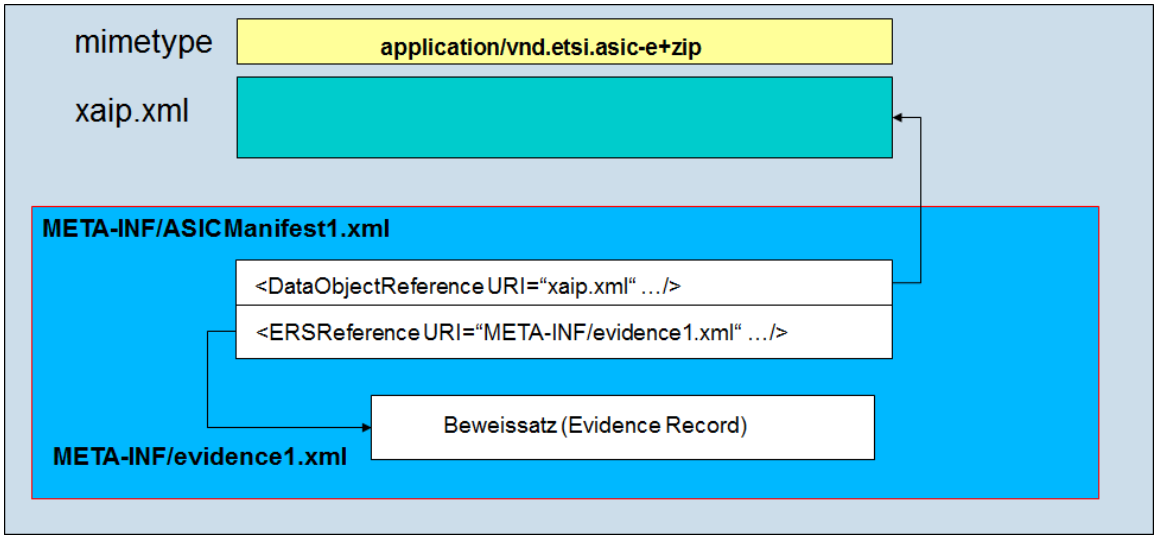

Abb. 3: ASiC-Container mit Evidence Records

Alle ASiC-Container–Typen erlauben auch eine Verschachtelung von ASiC-Containern und Containern anderer Arten (vgl. [ETSI 319 162-1], S. 16). Das Manifest kann zusätzlich zum Archivdatenobjekt, z. B. xaip.xml, auch noch auf weitere externe Datenobjekte außerhalb des XAIPs zeigen. In diesem Fall stellen die unteren Blätter des Hashbaumes des dazu gehörigen Evidence Records einerseits den Hashwert des zu schützenden Archivdatenobjektes und zusätzlich die Hashwerte der externen Dateien dar. Das Manifest des ASiC-Containers darf allerdings keine Referenzen zu Datenobjekten außerhalb des Containers enthalten.

So gesehen ist der auf ZIP beruhende ASiC-Container ein selbsttragendes Archivdatenobjekt, der es potentiell ermöglichen kann, umfangreiche Datenobjekte neben ERS, z. B. auch XAIP-konforme AIPs, in einem Objekt abzulegen und zwischen XAIP und weiteren Datenobjekten zu verweisen.

3.3 Interoperabilität der Signaturen der Beweisdaten

Um im Kontext der geltenden Aufbewahrungsfristen ein Höchstmaß an Softwareneutralität zu ermöglichen ist es notwendig, zu spezifizieren, wie der Evidence Record zu erzeugen ist, welche Daten der dem ERS zugrundeliegende Archivzeitstempel beinhaltet und welche jeweils in die Signatur des ERS eingeschlossen werden, um so deren Interoperabilität z. B. zur Nachweisführung in Drittsystemen zu unterstützen. Diese Aspekte wurden im Rahmen der Fortschreibung der TR-03125 aufgegriffen. Im Rahmen dieser Weiterentwicklung wurde zudem die internationale Entwicklung der aktuellen ETSI-Standards {C/X}AdES, so z. B. der Nutzung von Archivzeitstempeln v3 (ATS v3) zur Beweiswerterhaltung, untersucht und Vorschläge entwickelt, beide Ansätze zu verknüpfen.

In [BSI-TR03125] ist detailliert dargestellt, wie die Beweiswerterhaltung der in einem vertrauenswürdigen digitalen Langzeitarchiv aufbewahrten Dokumenten einschließlich der notwendigen beweisrelevanten wie technischen Beweisdaten bis zum Ablauf der geltenden Aufbewahrungsfristen sichergestellt wird.

Die Schlüsselrolle spielt dabei der in einem Evidence Record enthaltende qualifizierte Archivzeitstempel, üblicherweise gem. [RFC3161] (vgl. [BSI-TR03125], Anlage M-2, Kap. 5.3.1), mit Hilfe dessen die in einem Merkle Hashbaum gesammelten Hashwerte der aufzubewahrenden Archivdatenobjekte versiegelt werden (vgl. [BSI-TR03125], Anlage M-3, Kap. 2.4.1). Die periodische Erneuerung des Archivzeitstempels, gem. [RFC4998] resp. [RFC6283], oder bedarfsgesteuerte Erneuerung des darunterliegenden Hashbaumes, gem. [RFC4998] resp. [RFC6283] sobald die Sicherheitseignung der zugrundeliegenden Signatur- oder Hashalgorithmen entsprechend der technischen Entwicklung nicht mehr gegeben ist, führen zur Anforderung eines neuen qualifizierten Archivzeitstempels. Der Schutz des neuen Archivzeitstempel erstreckt sich nicht nur über die bereits von dessen Vorgänger geschützten Dokumenten, sondern betrifft auch den Vorgängerarchivzeitstempel selbst (vgl. [BSI-TR03125], Anlage M-3, Kap. 2.4.2).

Die Aspekte der nachhaltigen Erhaltung des Beweiswerts werden ausführlich in [ETSI101733] und [ETSI319122-1] bzw. [ETSI319122-2] für die CMS-Signaturen sowie in [ETSI101903] und [ETSI319132-1] bzw. [ETSI319132-2] für XML-Signaturen dargestellt. Um die Prüfbarkeit des angeforderten Archivzeitstempels zu vereinfachen und auch langfristig zu bewahren, ist (direkt im Anschluss der Erstellung oder spätestens unmittelbar vor dem Ablauf der sog. „Grace-Period“ (vgl. [ETSI101733], Abschnitt 4.4.2) notwendig, die für die Prüfung benötigte Zertifikate und dazugehörige Sperrinformation zusammen mit der Signatur des

Zeitstempels abzulegen (vgl. [BSI-TR03125], Anhang-F, Kap. 5.4). In [BSI03125] wird zu diesem Zweck eine Empfehlung ausgesprochen, womit die Zeitstempeltoken gem. [RFC3161], die eine CMS-Signatur beinhalten, zu einer CAdES-X Long Signatur (vgl. [ETSI101733] bzw. [ETSI319122-{1,2}]) ausgebaut werden sollen. Die XML-Signaturen werden analog zu einer XAdES-X Long Signatur (vgl. [ETSI101903] bzw. [ETSI319122-{1,2}]) ausgebaut. Gem. [RFC3161] weist ein Zeitstempeltoken sowie dessen Signatur einen besonderen Aufbau auf (z. B. nur eine digitale Signatur ist gestattet etc.).

Um den Besonderheiten des verwendeten Zeitstempeltoken und deren Signatur gerecht zu werden und deren Aufbau aus den Interoperabilitätszwecken wohldefiniert zu halten, wurden im Rahmen von [BSI-TR3125] die entsprechenden Profilierungen der Signatur des Zeitstempels definiert. In [BSI-TR03125], Anhang ERS werden folgende vier Profilierungen angeboten:

- CAdES-XL-Profilierung – ein an die Ausgestaltung der CAdES-X Long–Signatur angelegtes Profil gem. [ETSI101733] bzw. [ETSI319122-{1,2}],
- CAdES-A-Profilierung –ein an CAdES-A Signatur angelegtes Profil (vgl. [ETSI101733] bzw. [ETSI319122-{1,2}]),
- XAdES-XL-Profilierung – ein an XAdES-X Long Signatur sich orientierendes Profil (vgl. [ETSI101903] oder [ETSI319122-{1,2}],
- XAdES-A-Profilierung – ein XAdES-A Signatur Profil (vgl. [ETSI101903] oder [ETSI319122-{1,2}]).

Die verstärkte Bedeutung der erstellten Profilierungen wird insbesondere im Hinblick auf den in [BSI-TR03125], Anhang E, Kap. 5 beschriebenen Prozess des übergangslosen Imports von Evidence Records ersichtlich, was die Notwendigkeit einer weitgehenden Interoperabilität der Archivierungssysteme anspricht.

3.4 Zusammenfassung und Ausblick

Es wurde ein Überblick über internationale und nationale Standards zum Beweiswerterhalt kryptographisch signierter Dokumente gegeben.

Die Integrität und Authentizität der Archivdatenobjekte über einen langen Zeitraum wird durch Zeitstempel oder in Evidence Records eingebettete Zeitstempel sichergestellt. Es wurde gezeigt, dass der Evidence Record Ansatz als „Proof of Existence“ (PoE) gleichzeitig über mehrere signierte Datenobjekte oder Datenobjektgruppen und den dazu gehörenden Signaturen und signaturrelevanten Daten errechnet werden kann, und so skalierbarer und kosteneffektiver ist als der {C/X}-AdES-Ansatz von ETSI. Durch Einsatz von ETSI-Signatur-Profilen für die Zeitstempel selbst im Evidence Record ist aber dennoch ein Mindestmaß an Interoperabilität zwischen Evidence Record-basierten und ETSI-basierten Archivsystemen möglich.

Gleichzeitig wurde die Möglichkeit zur Verknüpfung von ASiC-Containern und Evidence Records im folgenden Text dargestellt. Dabei könnte die Dateigröße des AIP potenziell optimiert werden und gleichzeitig, in anwendungsgerechter Verbindung von Standards zur Informationserhaltung einerseits und Erhaltung kryptographischer Sicherungsmittel und damit Beweiswerterhaltung andererseits, ein international gültiges Austauschformat für beweissicher aufzubewahrende elektronische Unterlagen mit allen notwendigen Informationen geschaffen werden.

Literatur

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

[BMWi 07] BMWI: Handlungsleitfaden zur Aufbewahrung elektronischer und elektronisch signierter Dokumente. Bundesministerium für Wirtschaft und Technologie (Hrsg.), Berlin 2007.

[BSI-TR-03125] Bundesamt für Sicherheit in der Informationstechnik (BSI): Beweiswerterhaltung kryptographisch signierter Dokumente (TR-ESOR), TR 03125, Version 1.1, https://www.bsi.bund.de/ContentBSI/Publikationen/TechnischeRichtlinien/tr03125/index_htm.html, 2011.

[BSI-TR-03125-B] Bundesamt für Sicherheit in der Informationstechnik (BSI): Anlage B zu [BSI-TR-03125], Profilierung für Bundesbehörden, 2011

[BSI-TR-03125-C.1] Bundesamt für Sicherheit in der Informationstechnik (BSI): Anlage C.1 zu [BSI-TR-03125], Conformity Test Specification (Level 1 – Functional Conformity), geplant für 2012

[BSI-TR-03125-C.2] Bundesamt für Sicherheit in der Informationstechnik (BSI): Anlage C.2 zu [BSI-TR-03125], Conformity Test Specification (Level 2 – Technical Conformity), geplant für 2014

[BSI-TR-03125-C.3] Bundesamt für Sicherheit in der Informationstechnik (BSI): Anlage C.3, zu [BSI-TR-03125], Conformity Test Specification (Level 3 – Conformity with the German Federal Agency Profiling), geplant für 2014

[BSI-TR-03125-E] Bundesamt für Sicherheit in der Informationstechnik (BSI): Anlage E zu [BSI-TR-03125]: Konkretisierung der Schnittstellen auf Basis des eCard-API-Frameworks, TR 03125 Version 1.1, 2011

[BSI-TR-03125-F] Bundesamt für Sicherheit in der Informationstechnik (BSI): Anlage F zu [BSI-TR-03125], Formate und Protokolle, 2011

[DIN 31644:2012-04] DIN 31644: Information und Dokumentation – Kriterien für vertrauenswürdige digitale Langzeitarchive, 2012

[DIN 31645:2011-11] DIN 31645: Information und Dokumentation – Leitfaden zur Informationsübernahme in digitale Langzeitarchive, 2011

[DIN 31646:2013-01] DIN 31646:Information und Dokumentation – Anforderungen an die langfristige Handhabung persistenter Identifikatoren (Persistent Identifier), 2013

[DIN-31647] DIN 31645:2013-Entwurf: Beweiswerterhalt kryptografisch signierter Dokumente (Entwurf).

[EGovG-RE] Referentenentwurf der Bundesregierung: Gesetz zur Förderung der elektronischen Verwaltung sowie zur Änderung weiterer Vorschriften, BGBL. I Nr. 43, S. 2749, 2013.

[ETSI 101 733] ETSI TS 101 733: CMS Advanced Electronic Signatures (CAdES), (2013-04)

[ETSI 101 903] ETSI TS 101 903: XML Advanced Electronic Signatures (XAdES), (2010-12)

[ETSI 319 102] ETSI prEN 319 102: Electronic Signatures and Infrastructures (ESI); Procedures for Signature Creation and Validation, V0.2.1, Draft (2013-11)

[ETSI 319 122] ETSI prEN 319 122: CMS Advanced Electronic Signatures (CAdES), Part 1: Core Specification, Draft, über http://docbox.etsi.org/ESI/Open/Latest_Drafts/prEN-319122-1v003-CAdES-core, (2013); Part 2: Baseline Profile, Draft, über http://docbox.etsi.org/ESI/Open/Latest_Drafts/prEN-319122-2v003-CAdES-base, (2013)

[ETSI 319 132] ETSI prEN 319 132: XML Advanced Electronic Signatures (XAdES), Part 1: Core Specification, V0.0.4, Draft, über http://docbox.etsi.org/ESI/Open/Latest_Drafts/prEN-319132-1v004-XAdES-core, (2013); Part 2: Baseline Profile, V0.0.4, Draft, über http://docbox.etsi.org/ESI/Open/Latest_Drafts/prEN-319132-2v004-XAdES-base, (2013)

[ETSI 319 162-1] ETSI prEN 319 162-1: Electronic Signatures and Infrastructures (ESI); Associated Signature Containers (ASiC); Part 1: Core Specification, V0.0.3, Draft (2013-11)

[Fish06] S. Fischer-Dieskau: Das elektronisch signierte Dokument als Mittel zur Beweissicherung. Baden-Baden 2006.

[Merk80] R. Merkle: Protocols for Public Key Cryptosystems, Proceedings of the 1980 IEEE Symposium on Security and Privacy (Oakland, CA, USA), SS. 122-134

[OAIS] ISO 14721:2012, Space data and information transfer systems – Open archival information system (OAIS) – Reference model, (2012)

[RFC3161] C. Adams, P. Cain, D. Pinkas, R. Zuccherato: Internet X.509 Public Key Infrastructure – Time-Stamp Protocol (TSP), IETF RFC 3161, http://www.ietf.org/rfc/rfc3161.txt, 2001

[RFC4998] T. Gondrom, R. Brandner, U. Pordesch: Evidence Record Syntax (ERS), IETF RFC 4998, http://www.ietf.org/rfc/rfc4998.txt, August 2007

[RFC6283] A. J. Blazic, S. Saljic, T. Gondrom: Extensible Markup Language Evidence Record Syntax (XMLERS), IETF RFC 6283, http://www.ietf.org/rfc/rfc6283.txt, Juli 2011.

[RoSc06] A. Rossnagel, P. Schmücker (Hrsg.): Beweiskräftige elektronische Archivierung. Ergebnisse des Forschungsprojektes „ArchiSig – Beweiskräftige und sichere Langzeitarchivierung digital signierter Dokumente“, Economica Verlag, 2006

[Ross07] A. Rossnagel: Langfristige Aufbewahrung elektronischer Dokumente, Anforderungen und Trends, Baden-Baden, 2007.

[SGHJ12] A. Schumacher, O. Grigorjew, D. Hühnlein, S. Jandt: *Die Entwicklung der BSI-Richtlinie für das rechtssichere ersetzende Scannen*, in Tagungs-band FTVI 2012, GI, LNI, 2012, http://www.ftvi.de/

[XFDU] The Consultative Committee for Space Data Systems: *XML FORMATTED DATA UNIT (XFDU)*, CCSDS 661.0-B-1, September 2008, http://public.ccsds.org/publications/archive/661x0b1.pdf