Informations- und Beweiswerterhaltung in a Nutshell – Übersicht über Lösungsoptionen für Archivinformationspakete.

Tomasz Kusber, Fraunhofer FOKUS, tomasz.kusber@fokus.fraunhofer.de

Steffen Schwalm, Fraunhofer FOKUS, steffen.schwalm@fokus.fraunhofer.de

Dr. Ulrike Korte, BSI, ulrike.korte@bsi.bund.de

1 Einführung

Die Nutzung der Informationstechnologie zur Abbildung elektronischer Geschäftsprozesse ist in Wirtschaft und Verwaltung etabliert. In der Folge liegen geschäftsrelevante Aufzeichnungen zunehmend ausschließlich elektronisch vor. Gleichzeitig sind gesetzliche Vorgaben bzgl. Zeitpunkt sowie Art und Weise der vollständigen Umsetzung digitaler Transaktionen oder elektronischer Akten einzuhalten. Digitale Daten sind aus sich selbst heraus jedoch weder wahrnehmbar, lesbar oder liefern Hinweise für ihre Integrität, Authentizität oder Ordnungsmäßigkeit im elektronischen Rechts- und Geschäftsverkehr. Dies erfolgt vor dem Hintergrund geltender Dokumentations- und Nachweispflichten, die zum einen für Fristen zwischen zwei und 110 Jahren zu erfüllen sind, die teilweise erst Jahrzehnte nach dem Abschluss des zugrundeliegenden Geschäftsvorfalls beginnen. Während dieser Zeit muss es möglich sein, gegenüber Prüfbehörden, Gerichten den Nachweis von Authentizität, Integrität und Nachvollziehbarkeit der geschäftsrelevanten Aufzeichnungen zu führen. Dies bedingt sowohl eine langfristige Verfügbarkeit und Verkehrsfähigkeit der Aufzeichnungen, um diese zum Nachweis vorlegen zu können [Ko13], [KuSc16], [Ro07], [Fi06], [EUDSGVO].

Die Verwendung kryptographischer Sicherungsmittel wie mindestens fortgeschrittener elektronischer Signaturen, Siegel und Zeitstempel ermöglicht nach geltendem Recht die Erhaltung des zur Nachweisführung notwendigen Beweiswerts direkt an den aufzubewahrenden Aufzeichnungen und damit ohne deren Verkehrsfähigkeit einzuschränken (Beweiswerterhaltung). Darüber hinaus ist es notwendig, die Interpretierbarkeit der Aufzeichnungen zu gewährleisten, sie also entsprechend dem Aufbewahrungszweck und –vorgaben verfügbar zu halten (Informationserhaltung) [Ko13] [Ro07], [EIDAS], [VDG], [SR019510].

Die Umsetzung erfolgt in Praxis auf Basis geltender Standards und Normen zur beweissicheren Langzeitspeicherung, die es ermöglichen, die zur Beweiswert- und Informationserhaltung notwendigen Information, gemeinsam mit den aufzubewahrenden Aufzeichnungen in selbsttragenden Archivinformationspaketen (AIP) in einem digitalen Langzeitarchiv auf Basis [ISO14721], [DIN31647], [TR-03125-F]. Abhängig von der Datenmenge und –größe gilt es, machbare technische Lösungen für AIP zu finden, die neben der Aufbewahrung auch einen performanten Betrieb und Nutzung der Aufzeichnungen ermöglichen.

Hierzu ist es notwendig, zunächst die regulatorischen (Kap. 2.1) und fachlichen Anforderungen an die Informations- und Beweiswerterhaltung elektronischer Aufzeichnungen (Kap. 2.2) sowie den Stand der Technik (Kap. 2.3) zu beschreiben sowie die Anforderungen an Formate für selbsttragende Archivinformationspakete zu benennen (Kap. 2.4).

Im nächsten Schritt werden die verschiedenen, in der Praxis relevanten Optionen möglicher Formate beschrieben (Kap. 3) und schlussendlich die vorgestellten Formate anhand der Anforderungen an AIP bewertet (Kap. 4) sowie ein Fazit für die praktische Anwendung gezogen (Kap.5).

2 Informations- und Beweiswerterhaltung im Überblick

2.1 Regulatorischer Rahmen in Deutschland und Europa

Die eIDAS-Verordnung [EIDAS] schuf im EWR einheitliche Vorgaben für vertrauenswürdige digitale Transaktionen auf Basis elektronischer Identifizierungsmittel sowie elektronischer Vertrauensdienste im Binnenmarkt. Als Identifizierungsmittel gilt hierbei z.B. der neue Personalausweis, die Vertrauensdienste umfassen elektronische Signaturen, Siegel, Zeitstempel, Verifikationsdienste (Prüfung von Signaturen, Siegeln etc.), Bewahrungsdienste (Beweiswerterhaltung), Einschreib- und Zustelldienste (z.B. De-Mail) sowie Websitezertifikate. Durch die Zulassung z.B. von Server- und Fernsignaturen ohne Signaturkarte sowie von Siegeln (Signaturen für Organisationen) ebenso wie die Pflicht zur Anerkennung jeder qualifizierten elektronischen Signatur bzw. Siegel bzw. Zeitstempel (Art. 25, 35, 41 [EIDAS]) jedes qualifizierten europäischen Vertrauensdienstes, ist ein deutlicher Anstieg signierter Dokumente in Deutschland absehbar, wie dies auch in den europäischen Nachbarstaaten bereits erfolgt [VS18], [KSDV15]. Die [EIDAS] umfasst insbesondere auch Anforderungen für die beweiswerterhaltende Aufbewahrung gemäß Artikel 34 [EIDAS].

Im Zuge der Umsetzung der [EIDAS] werden „beim Erlass von delegierten Rechtsakten bzw. Durchführungsrechtsakten die von europäischen und internationalen Normungs-organisationen und -einrichtungen, insbesondere dem Europäischen Komitee für Normung (CEN), dem Europäischen Institut für Telekommunikationsnormen (ETSI), der Internationalen Normungsorganisation (ISO) und der Internationalen Fernmeldeunion (ITU), festgelegten Normen und technischen Spezifikationen gebührend berücksichtigt“ [EIDAS]. Die genannten Standardisierungsgremien haben mit Mandat M416 der Europäischen Kommission die explizite Aufgabe, die rechtlichen Regelungen der [EIDAS] durch konkrete technische Standards untersetzen und so die Umsetzung durch Interoperabilität und Harmonisierung von Vertrauensdiensten und elektronischen Identifizierungsmitteln zu erleichtern [Ko17]. Diese technischen Standards werden zudem zunehmend weltweit angewandt, was deren Bedeutung hervorhebt [KSDV15].

In Deutschland wird die wirksame Durchführung von [EIDAS] durch das Vertrauensdienstegesetz [VDG] geregelt. Dieses sieht die Beweiswerterhaltung signierter Dokumente in § 15 [VDG] vor.

Die Umsetzung vertrauenswürdige digitaler Transaktionen sowie deren Nachweis wird durch weitere EU-Vorgaben [EUDLR], [EUDSGVO] einerseits sowie durch branchenspezifische Vorgaben anderseits, so z.B. [EASA], [FDA], [GXP] in Luftfahrt, Gesundheitswesen und Pharma, [EuroSOX], [PSD2] in der Finanzindustrie, oder Maßgaben zum Haftungsrecht [BGB] andererseits untersetzt [Ko16], [We18].

Eine weitgehende Digitalisierung der deutschen Bundesbehörden (z. B. Einführung einer führenden E-Akte, Umsetzung vom rechtssicheren ersetzenden Scannen oder Implementierung von beweiswerterhaltenden Aufbewahrungsdienste ist bis 2020 vorgesehen, der Justiz bis 2022 [EGOVG], [eJusticeG]. Grundlage hierfür bildet das E-Government-Gesetz aus 2013 [eGovG]. Entsprechende Pendants liegen in nahezu allen Bundesländern vor. Parallel besteht die Verpflichtung, behördlicher Entscheidungen nachweisbar und damit gerichtsfest zu halten bis zum Ablauf der geltenden Aufbewahrungsfristen, zum anderen gilt die BSI Technische Richtlinie TR-3125 TR-ESOR [TR3125] gem. [EGOVG] als Stand der Technik zur Beweiswerterhaltung [MiniKeGovG], [We18], [Ko16].

2.2 Fachliche Anforderungen

Um den geltenden Dokumentations- und Nachweispflichten (Kap. 2.1) nachzukommen, muss es möglich sein, Authentizität, Integrität und Nachvollziehbarkeit geschäftsrelevanter Aufzeichnungen jederzeit und verlustfrei gegenüber Gerichten, Prüfbehörden, Dritten nachzuweisen, was deren Verkehrsfähigkeit bedingt. Das bloße Speichern auf einem Datenträger ist also nicht ausreichend [Ko13], [KuSc16], [Ko17]. Dies würde zudem nicht den Erfordernissen der Informationssicherheit an eine ordnungsgemäße Aufbewahrung entsprechen [BSIGS].

Der Nachweis wird dabei anhand der Aufzeichnungen geführt, ebenso beziehen sich Aufbewahrungserfordernisse auf die Unterlagen selbst. Es wird nicht das IT-Verfahren bewahrt, sondern die Aufzeichnungen. Der Beweiswert ist also eine inhärente Eigenschaft der Aufzeichnungen selbst. Um insofern die beschriebenen regulatorischen wie fachlichen Anforderungen zu erfüllen, muss eine beweissichere Langzeitspeicherung die Informationserhaltung und Beweiswerterhaltung ermöglichen [Ko13], [Ko16], [Sc15].

Eine wesentliche Grundlage zur Umsetzung bildet ein ordnungsgemäßes Records Management, welches auf Basis klarer Richtlinien, Verantwortlichkeiten und Prozess die Identifikation sowie strukturierte und anforderungsgerechte Ablage geschäftsrelevanter Aufzeichnungen ermöglicht [Wi15], [To07], [We18]. Ziel ist es dabei, dass die Unterlagen als eindeutiger Nachweis geschäftlicher Transaktionen und Entscheidungen gegenüber Dritten dienen können und damit die Vertrauenswürdigkeit von Prozess und Aufzeichnungen gewährleistet wird [ISO30301], [ISO15489], [Ko14], [KuSc16], [Sc17].

Wie in der Einleitung beschrieben, ermöglicht die Nutzung kryptographischer Sicherungsmittel die Erhaltung des Beweiswerts direkt an den Aufzeichnungen, ohne deren, zur Nachweisführung notwendige, Verkehrsfähigkeit einzuschränken. Diese kryptographischen Mittel (Signaturen, Siegel, Zeitstempel etc.) werden direkt am Dokument/Daten angebracht. Der Beweiswert, ebenso wie das Dateiformat oder die Metadaten zur inhaltlichen Beschreibung eines Dokuments, bildet eine signifikante Eigenschaft im Sinne [ISO14721]. Ebenso wie Datenformate unterliegen auch kryptographische Sicherungsmittel der Überholung durch den technischen Fortschritt. Die Beweiswerterhaltung erfolgt hierzu durch eine erneute Signierung/Versiegelung/Zeitstempelung bzw. Neuverhashung [VDG], [EIDAS], [SR010510], [TR-03125], [DIN31647], also der Anbringung einer neuen qualifizierten elektronischen Signatur/einem neuen qualifizierten elektronischen Siegel oder eines qualifizierten elektronischen Zeitstempels, bevor die Sicherheitseignung der Signatur-/Hashalgorithmen ausläuft. Um dies wirtschaftlich durchzuführen, werden sog. Merkle-Hashbäume [RFC4998], [RFC6283] verwendet, wie in der nachstehenden Grafik dargestellt.

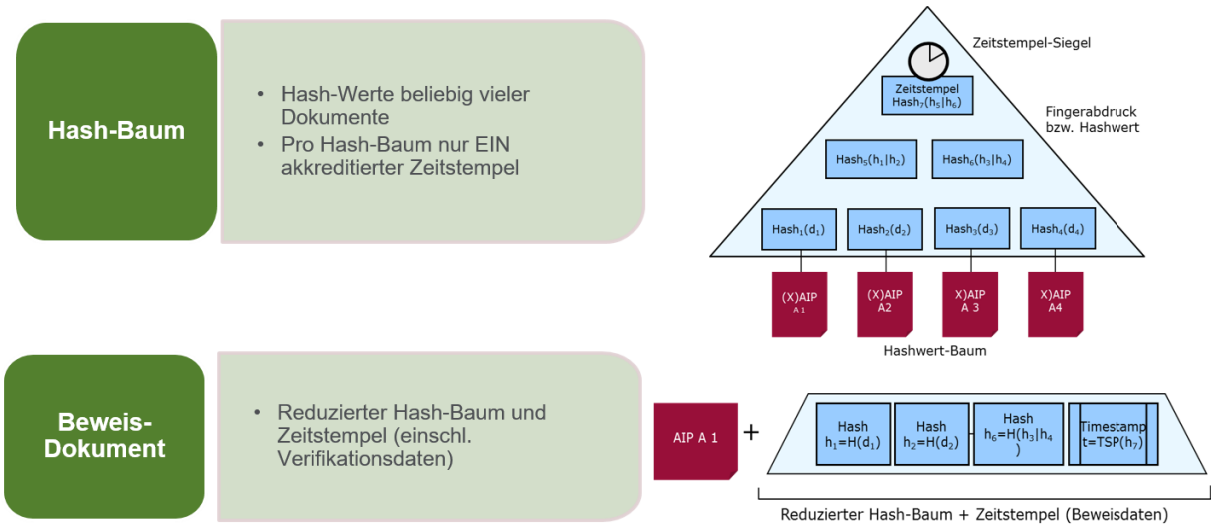

Abbildung 1: Hashbaum und Evidence Record gem. RFC 4998/6283

Der reduzierte Hashbaum incl. Zeitstempel je AIP wird als Evidence Record bezeichnet und ermöglicht den eindeutigen wie gerichtsfesten Nachweis der Integrität sowie implizit der Authentizität der Aufzeichnungen. Neben der Neusignierung/Neuversiegelung/Neuzeitstempelung bzw. Neuverhashung werden die zur Beweiswerterhaltung notwendigen Daten im untrennbaren Zusammenhang mit den zugehörigen Aufzeichnungen selbst aufbewahrt. Hierzu zählen beweisrelevante Daten (Signaturen, Siegel, Zeitstempel, Zertifikatsinformation, Prüfdaten, Sperrinformationen) sowie technische Beweisdaten (Evidence Record) [DIN31647], [TR-3125]. Beide Arten zusammen werden auch als Credentials bezeichnet und entsprechen den sog. Fixity Information im OAIS-Datenmodell [ISO14721], [DIN31647].

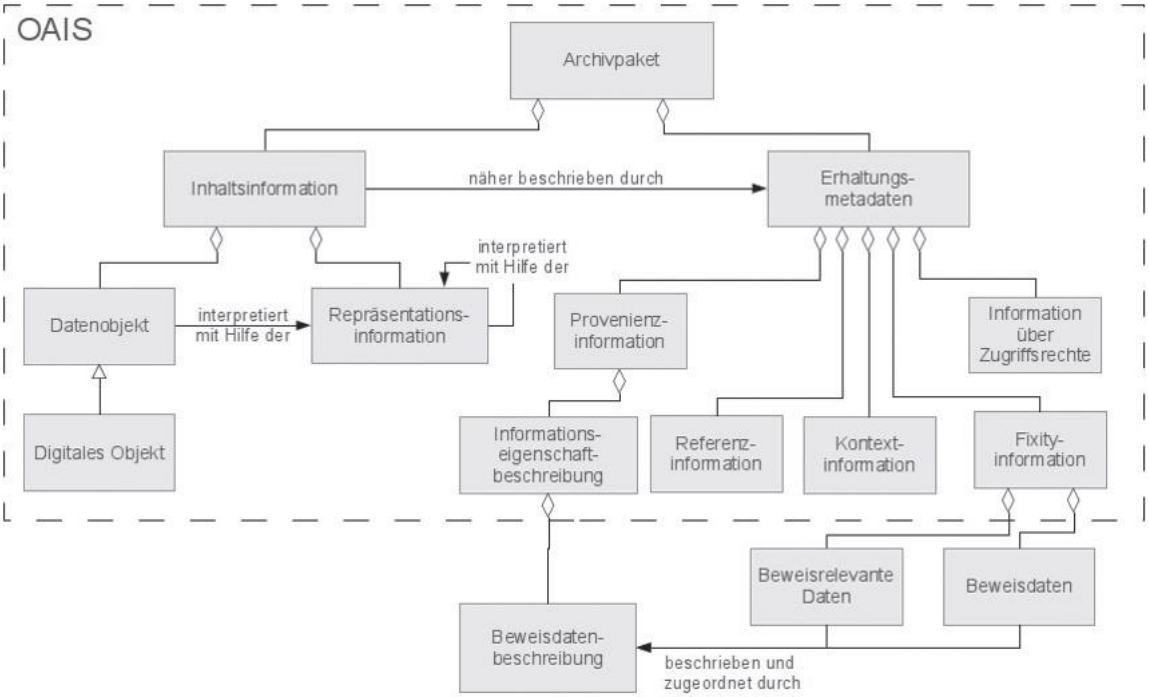

Abbildung 2: Archivinformationspaket mit beweisrelevanten und technischen Beweisdaten gem. DIN 31647:2015

Darüber hinaus gilt es, die Aufzeichnungen selbst zu bewahren durch die Verwendung stabiler Datenformate sowie die Beschreibung entsprechend geltender Standards und Normen (Kap. 2.3). Es muss also die Verfügbarkeit und damit Lesbarkeit der Aufzeichnungen bis zum Ablauf der Aufbewahrungsfrist gewährleistet werden, um diese visualisieren und nutzen zu können, wozu bspw. auch deren Auswertbarkeit oder die Reproduzierung eines wissenschaftlichen Forschungsergebnisses (z.B. Medizin, Toxikologie, Pharma) gehören kann.

Praktisch erfolgen Beweis- und Informationserhaltung mit Hilfe sog. selbsttragenden Archivinformationspaketen, welche die Inhaltsdaten, also die Dokumente selbst, einschließlich der zugehörigen beschreibenden Informationen, wie auch die zur Beweiswerterhaltung notwendigen Information in zusammenhängender Form (Container) beinhalten [Ko13], [Ko14], [DIN31647], [Gia11]. Dabei umfassen die beschreibenden Metadaten auch Informationen insbesondere zum Geschäftskontext oder zur technischen Umgebung (Formatidentifikation, Softwareumgebung etc.).

Dieses Vorgehen hat sich in der Praxis branchenübergreifend in zahlreichen Projekten bewährt, in denen sowohl Einzelinstallationen als auch komplexe Dienste zur beweissicheren Langzeitspeicherung im SOA-Sinne umgesetzt wurden. Praktisch werden dabei, aus wirtschaftlichen Gründen, kryptographische Sicherungsmittel sowohl für signierte als auch unsignierte Aufzeichnungen verwendet [Ko17], [KuSc16], [Sc17].

2.3 Wesentliche Standards und Normen

Als wesentliche Standards und Normen zur Umsetzung einer beweissicheren Langzeitspeicherung sind zu benennen [Ko13], [Ko14], [Sc17]:

- [ISO14721] – Beschreibung der notwendigen Prozesse, Funktionen und Informationspaket für die langfristige Aufbewahrung elektronischer Aufzeichnungen,
- [ISO14533]-{1,2,3} – Aufbau von Langzeitaufbewahrungsformate für CAdES, XAdES und PAdES Signaturen,
- [SR019510] – Darstellung der maßgeblichen Verfahren zur Beweiswerterhaltung im Kontext [EIDAS] in Europa,
- [DIN31644] – Beschreibung der Kriterien für ein vertrauenswürdiges digitales Langzeitarchiv (dLZA),
- [DIN31647] – Beschreibung der notwendigen Funktionen und Daten an ein generisches System zur Beweiswerterhaltung kryptographisch signierter Unterlagen innerhalb eines dLZA gem. [DIN31644] und [ISO14721],
- [RFC4998], [RFC6283] sowie [TR-03125] – speziell die TR beschreibt, basierend auf den beiden RFC, eine Referenzarchitektur, notwendige Funktionen und Module sowie Zertifizierungsverfahren und Maßgaben zur Interoperabilität für die Umsetzung von Beweiswerterhaltung.

2.4 Herausforderungen bei Erzeugung und Nutzung von AIP

Derzeit werden selbsttragende AIP vielfach als XML-Informationspakete technisch realisiert, wie dies z.B. auch die [TR-03125] vorsieht. Die Aufbewahrung eingebetteter Binärdaten in XML-Strukturen erfolgt dabei i.d.R. durch Base64-Codierung, was eine Steigerung der Datenmenge um ca. 33 % nach sich zieht. Die Verarbeitung solcher XML-basierter, selbsttragender Archivinformationspakete (AIP) hat sich in der Praxis bewährt, sofern keine Anforderungen an eine sehr hohe Performanz für sehr große Datenvolumina oder für hochfrequente Lese- wie Schreibvorgänge vorliegen. In einigen Fällen, so z.B. Geodaten, übersteigt das Datenvolumen bei einem selbsttragenden AIP in Form eines XML-Containers die Kapazitäten marktüblicher Schnittstellen, so dass weitere Lösungen in die Betrachtungen einzubeziehen sind [Ko17].

Eine mögliche Alternative ist die Verwendung logischer XML-basierter Container, bei denen die Inhaltsdaten nicht direkt im Objekt gespeichert, sondern mittels einer eindeutigen Referenz verlinkt werden. Eine weitere Option ist der Einsatz standardisierter Containerformate, die binäre Daten ohne zusätzliche Kodierung aufnehmen können oder diese verlustfrei komprimieren können. Hier bieten sich derzeit das PDF/A-3 (vgl. [ISO19005-3]) oder das auf dem ZIP-Format basierende ASiC (vgl. [EN319162]) an.

Um im Anwendungsfall eine gezielte Auswahl treffen zu können, gilt es, zunächst die Anforderungen an Formate für selbsttragende Archivinformationspakete zu benennen.

2.5 Anforderungen an Archivinformationspakete

Es haben sich folgende Anforderungen herausgestellt [Ko17]. Ein Archivinformationspaket soll

1. beliebig viele, verschiedene Inhaltsdaten, Metadaten und beweisrelevante Daten/ technische Beweisdaten enthalten;
2. signierte/ zeitgestempelte und un-signierte/ un-zeitgestempelte Daten parallel enthalten;
3. verschiedene digitale Signaturtechniken (z.B. (AdES) Signaturen, Zeitstempel, Evidence Records) unterstützen;
4. parallele und zusätzliche Signaturen unterstützen;
5. nachträgliches Einspielen von Sperrmaterial etc. ohne Zerstörung der vorausgegangenen Signatur ermöglichen;
6. verschiedene Versionen von Inhalts-/ Meta- und Beweisdaten enthalten, die nach und nach in das Paket eingestellt werden können;
7. eine Referenzmöglichkeit (z.B. ein Manifest-Objekt oder ein Indexobjekt) enthalten können, dass entsprechende Nutzdaten-, Metadaten- und beweisrelevanten Daten/ Beweisdaten verknüpft, die durch ein spezielles Objekt der digitalen Signaturtechnik (z.B. digitale Signatur im AdES-Format, Zeitstempel, Evidence Record) geschützt werden;
8. unterstützen, dass Versionen oder spezielle Elemente des AIP gezielt ausgelesen werden können;
9. performant auch bei großen Datenmengen/ Dateien (z.B. Geodaten) sein;
10. eine wirtschaftliche Realisierung (z.B. auf Basis von Open Source-Softwarekomponenten, serviceorientierten Architekturen oder Softwarekomponenten mit kostengünstigen Lizenz- und Servicemodellen) ermöglichen;
11. selbsttragend sein, also alle zur Informations- und Beweiswerterhaltung, also dem Aufbewahrungszweck, notwendigen Daten in standardisierter Form enthalten;
12. auf weit verbreiteten, offenen Standards weithin anerkannter, unabhängiger Standardisierungsgremien beruhen

3 Lösungsoptionen für AIP zur Informations- und Beweiswerterhaltung

3.1 XAIP in TR-ESOR

3.1.1 TR-ESOR Referenzarchitektur

Aus den für den Erhalt des Beweiswerts notwendigen funktionalen Anforderungen wurde in der [TR-03125] eine modulare Referenzarchitektur abgeleitet, die im folgenden Text kurz vorgestellt wird. Die Erfüllung dieser Anforderungen kann im Rahmen eines TR-spezifischen Zertifizierungsverfahrens nachgewiesen werden.

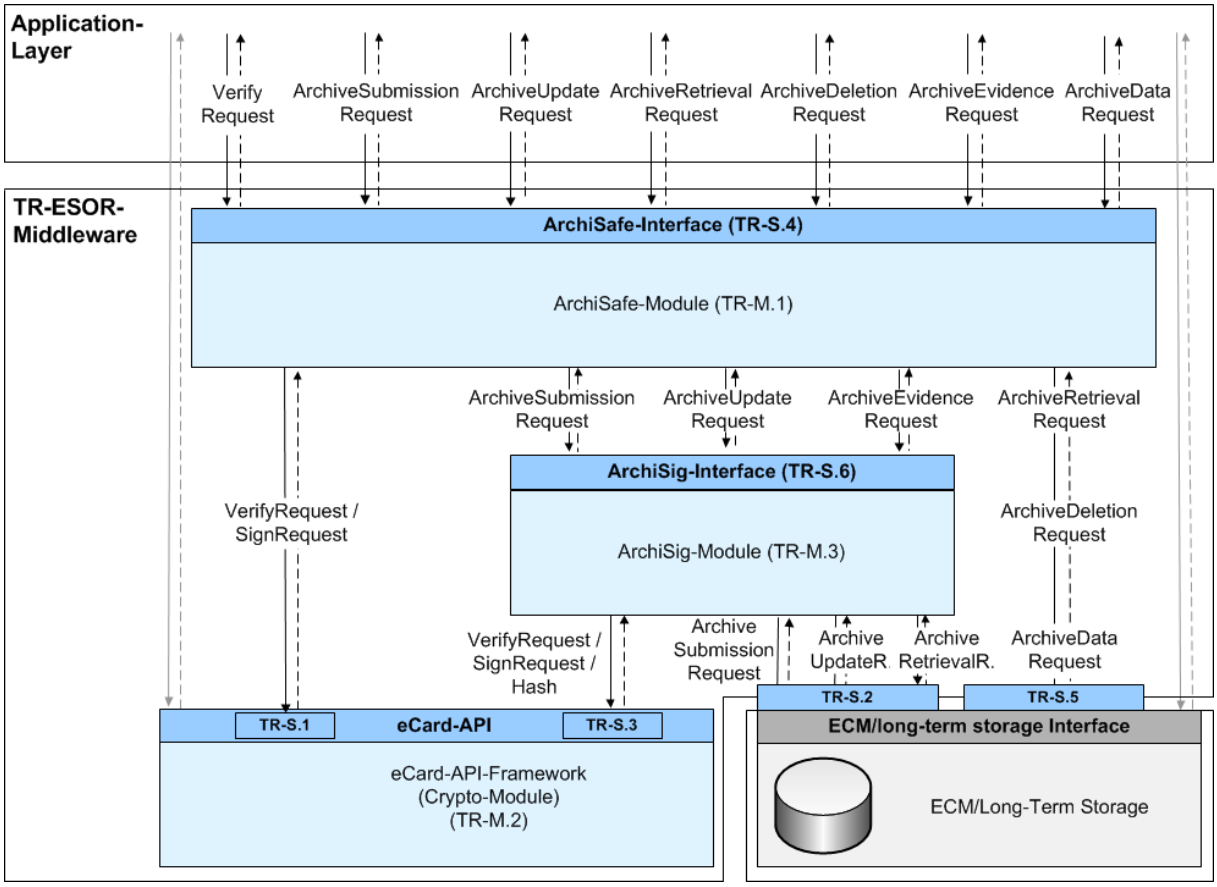

Abbildung 3: TR-ESOR Referenzarchitektur incl. Schnittstellen

Die in der TR-ESOR für Zwecke des Beweiswerterhalts kryptographisch signierter Daten entwickelte Referenzarchitektur (vgl. Abb. 3) besteht aus den folgenden funktionalen und logischen Einheiten [HüKS12]:

Das „ArchiSafe-Interface“ (TR-S. 4) bildet die Eingangs-Schnittstelle zur TR-ESOR-Middleware und bettet diese in die bestehende IT- und Infrastrukturlandschaft ein.

Das „ArchiSafe-Modul“ (TR-M.1) regelt den Informationsfluss in der Middleware, sorgt dafür, dass die Sicherheitsanforderungen an die Schnittstellen zu den Geschäftsanwendungen umgesetzt werden und gewährleistet eine Entkopplung von Geschäftsanwendungen, weiteren Modulen in einem OAIS-konformen dLZA (z.B. Module zur Konvertierung/Validierung von Inhaltsdaten) und Archivspeicher.

Das „Krypto-Modul“ (TR-M.2) mit den Eingangsschnittstellen TR-S.1 und TR-S.3 stellt die kryptographischen Funktionen bereit, welche für den Beweiswerterhalt kryptographisch signierter Dokumente wesentlich sind. Das Krypto-Modul stellt Funktionen zur Berechnung von Hashwerten und Prüfung elektronischer Signaturen, zur Nachprüfung elektronischer Zertifikate und zum Einholen qualifizierter Zeitstempel sowie optional elektronischer Signaturen bzw. Siegel, für die Middleware zur Verfügung. Die Aufrufschnittstellen des Krypto-Moduls sollen nach dem eCard-API-Framework [TR-03112], [OASIS-DSS] und [TR-03125-E]. gestaltet sein, um die Integration und Austauschbarkeit kryptographischer Funktionen zu erleichtern.

Das „ArchiSig-Modul“ (TR-M.3) mit der Schnittstelle TR-S. 6 stellt die erforderlichen Funktionen für die Beweiswerterhaltung der digital signierten Unterlagen gemäß [RoSc06] zur Verfügung. Auf diese Weise wird gewährleistet, dass die u.a. in § 15 [VDG] geforderte Signatur-/Siegel-/Zeitstempelerneuerung einerseits gesetzeskonform und anderseits performant und wirtschaftlich durchgeführt werden kann und somit dauerhafte Beweissicherheit gegeben ist.

Der Archivspeicher (Long-Term Storage), der von der TR-ESOR-Middleware über die Schnittstellen TR-S. 2 und TR-S. 5 angesprochen wird, ist nicht mehr Teil der Technischen Richtlinie 03125 TR-ESOR und sorgt für die physische Speicherung der aufzubewahrenden Daten.

Die in Abb. 3 dargestellte IT-Referenzarchitektur orientiert sich an der ArchiSafe-Referenzarchitektur [ArchiSafe] und soll die logische (funktionale) und technische Interoperabilität künftiger Produkte mit den Zielen und Anforderungen der Technischen Richtlinie ermöglichen und unterstützen [TR-03125-C.1] und [TR-03125-C.2]. Die Middleware nach [TR-03125] kann dabei auch für unsignierte Daten verwendet werden, wie dies in der Praxis häufig gewählt wird, um nicht mehrere parallele Archivierungslösungen aufzubauen oder bspw. die Integrität der unsignierten Daten ab Ablage über die Middleware schützen wie nachweisen zu können.

3.1.2 XAIP

Das XML-formatierte Archivinformationspaket, kurz XAIP genannt, ist ein in [TR-3125-F] spezifiziertes, selbstbeschreibendes Archivinformationspaket im Sinne des OAIS-Modells [ISO14721]. Das Format selbst beruht auf dem XFDU-Standard [ISO13527] sowie Victorian Electronic Record Strategy aus Australien [VERS]. In [VERS] wurde die XFDU-native *Behaviour-Section* durch eine *CredentialSection* für die beweisrelevanten und technischen Beweisdaten [DIN31647], also die Fixity Information gem. [ISO14721], ersetzt, um die Beweiswerterhaltung auf Basis selbsttragender AIP zu ermöglichen. Die [TR-3125-F] entwickelte [VERS] zu XAIP weiter.

Das XAIP beinhaltet einerseits einen Kopfbereich (*PackageHeader*) zur Beschreibung des gesamten Pakets und dessen Aufbau. Hierzu gehören z.B. die eindeutige ArchivObjekt-ID (AOID), Angaben zum XML-Schema, zum Ende der Aufbewahrungsfrist oder zum Absender des XAIP. Hinzu kommen versionsspezifische Inhaltsverzeichnisse mittels XML-basierter Manifeste. Zum Nachweis vertrauenswürdiger Transaktionen kann es notwendig sein, bestimmte schützenswerte Dokumente bereits vor Schließung des zugehörigen übergeordneten logischen Objekts, z.B. des Vorgangs, ins dLZA zu überführen, um die Beweiswerterhaltung zu gewährleisten. Hierzu gehört beispielsweise das ersetzende Scannen gem. [TR-03138], signierte Dokumente oder elektronische Anträge. Gleiches gilt für Verfahren, deren Fristen erst mit einem Ereignis in der Zukunft beginnen, wie dies in komplexen Zulassungsverfahren im Pharmabereich, in der Chemieindustrie oder der Luftfahrt der Fall ist. Hierfür bietet die [TR-03125] die Möglichkeit einer Versionierung des XAIP. Dabei handelt es sich technisch um XML-Versionen, die ebenso eindeutig identifiziert und beschrieben sind wie alle anderen Versionen des XAIP, und darüber hinaus dezidiert abrufbar und mit einem eigenen Evidence Record geschützt sind *(ArchiveRetrievalRequest*). Damit ermöglicht die [TR-03125] ein kontinuierliches Anwachsen der XAIP entsprechend dem Nutzungszweck des Anwenders. Durch die Aufbewahrung aller Versionen eines XAIP in einem Datenpaket wird die Interoperabilität der Daten und Erhaltung logischer Zusammenhänge (z.B. Aktenzusammenhang) in herstellerneutraler Form erleichtert sowie der Aufwand für Datenmanagement und Migrationsrisiken begrenzt.

Neben dem Header beinhaltet das XAIP andererseits eine beliebige Anzahl aufzubewahrenden Daten in der sog. *DataObjectSection*. Die Inhaltsdaten selbst können als Base64-kodierte Binärdaten oder als XML-Struktur abgelegt werden. Dabei wird für jedes Inhaltsdatenobjekt ein eindeutiges Identifikationsmerkmal vergeben [TR-03125-F]. Außerdem ist es möglich, eine Prüfsumme und Informationen über Transformierungen eines Datenobjektes hinzuzufügen [TR-03125-F] Hinzu kommen die je Datenobjekt notwendigen fachliche, technischer oder sonstigen Metadaten (*MetaDataSection*) sowie die zugehörigen beweisrelevanten Daten und technischen Beweisdaten (*CredentialSection*) in jeweils eigenen Sektionen. Dabei ist es u.a. auch möglich, die in [ISO13527] definierten „category"- und „classification"-Attribute zu nutzen oder fachspezifische bzw. technische Metadaten gemäß [XBARCH], [XDOMEA] und [PREMIS] zu integrieren.

Der letzte Abschnitt des XAIP-Paketes ist der Beweisdaten-Abschnitt (CredentialSection), der beweisrelevante Daten, wie z.B. digitale Signaturen, elektronische Zeitstempel, Zertifikate, Zertifikat-Statusinformationen, „Verification Reports" gemäß [OASIS-VR], und/ oder technische Beweisdaten in Form von einem oder mehreren Evidence Record(s) [RFC4998/RFC6283] beinhalten kann.. Diese beweisrelevanten Daten und technischen Beweisdaten dienen dem Nachweis der Unversehrtheit (Integrität), der Authentizität (sofern die Inhaltsdaten signiert sind) und des „Proof of Existence" der im XAIP enthaltenden archivierten Datenobjekte [Ko17].

Jeder dieser Bereiche enthält spezifische Datenelemente, die innerhalb des XAIP eindeutig über eine ID referenziert werden können (Bsp.: die *dataObjectID* eines *DataObjects* in der *DataObjectSection*). Zum Auslesen eines XAIP sind die *VersionManifest*-Elemente im *packageHeader* wichtig, die jeweils ein versionsspezifisches Inhaltsverzeichnis darstellen. Die *VersionManifest*-Elemente verweisen auf die zu einer Version gehörenden Datenelemente des *XAIPs* und legen fest, welche Datenelemente in die Bildung der Hashwerte einfließen [Ko17]. Dabei darf nur auf die direkt in diesem XAIP enthaltenen Datenelemente verwiesen werden. Der Verweis auf die einer Version zugehörigen Datenelemente im *VersionManifest* kann mittels zweier Pointer-Typen vorgenommen werden:

- protectedObjectPointers:

  „Durch die Menge der hier angegebenen *<protectedInfoPointer>*-Elemente wird definiert, welche Teile des Archivdatenobjektes in die Hashwertbildung einfließen und deshalb vom entsprechenden Evidence Record geschützt werden." ([TR-03125-F], S. 14).
- unprotectedObjectPointers:

  "Durch einen hier angegebenen *<unprotectedInfoPointer>* wird klargestellt, dass das Objekt auf das hier verwiesen wird, logisch zur angegebenen *XAIP*-Version gehört. Allerdings fließt dieses Objekt *nicht* in die Hashwertbildung ein und es ist deshalb nicht von einem Evidence Record umfasst und kryptographisch geschützt." ([TR-03125-F], S. 14). Dies ermöglicht eine spätere Änderung der Daten dieser Version ohne vorhandene Evidence-Records zu zerstören [Ko17].

Die nachstehende Grafik zeigt ein XAIP im Überblick. Die Metadaten und Datenobjekte sind aus Platzgründen nur beispielhaft dargestellt.

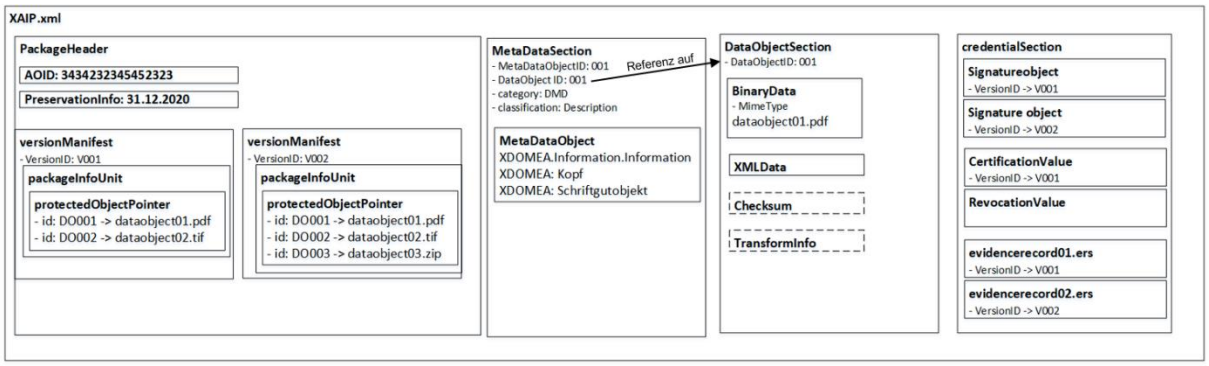

Abbildung 4: Überblicksdarstellung XAIP

3.2 Logisches XAIP in TR-ESOR

Das logische XAIP spezifiziert ein selbsttragendes Archivinformationspaket auf Basis des Formats XAIP der [TR-03125-F], bei welchem die Inhaltsdaten nicht innerhalb des AIP-Containers an Beweiswerterhaltungkomponente, z.B. eine Middleware gem. [TR-03125], innerhalb eines dLZA, übergeben, sondern erst während des Middleware-internen Ablageprozesses (*ArchiveSubmissionRequest*) oder der Versionierung (*ArchiveUpdateRequest*) von der Middleware on demand (*RetrievalRequests*) von dem Archivspeicher angefordert werden. Dieses Vorgehen ermöglicht es, große Datenmengen performant beweiswerterhaltend aufzubewahren, ohne die Inhaltsdaten mittels der webservicebasierten Zugangsschnittstellen der Beweiswerterhaltungskomponenten abzulegen und so die physikalischen Grenzen aktueller Webservices (z.B. SOAP, REST/JSON) zu überschreiten.

Um nun große Datenmengen zu übergeben, muss es möglich sein, die Inhaltsdaten in einem definierten Prozess, bspw. unter Verwendung eines dezidierten Upload-Modules und mindestens geschützt durch eine Prüfsumme[1], an den Archivspeicher zu übergeben. Der Archivspeicher erzeugt eine eindeutige Referenz auf den Speicherort sowie die eindeutige *ArchivObjekt-ID* (AOID), wobei letztere auch herstellerneutral vom Upload-Modul erzeugt werden könnte.

Die AOID sowie die Referenz auf den Speicherort der Inhaltsdaten wird nun dem logischen XAIP hinzugefügt (*ApplicationLayer*). Der nachstehende Text verdeutlicht die mögliche Erweiterung der Referenzarchitektur.

Ausgehend von der [TR-03125]-Referenzarchitektur lässt sich der Ansatz eines logischen XAIPs wie folgt beschreiben:

Die Datenobjekte können vor dem Absetzen des A*rchiveSubmissionRequest* über ein Upload-Service in dem Archive-Storage abgelegt werden. Im Gegenzug bekommt der uploadende Client eindeutige Referenzen als eindeutige *ArchivObjekt-IDs* für die hochgeladenen Datenobjekte. Die erhaltenen Referenzen (begleitet durch z.B. Hashwerte der Inhalte und Angabe zum Speicherort) werden in das XAIP an der Stelle des Inhalts der Datenobjekte *(DataObjectSection*) abgelegt, was das XAIP zu einem logischen XAIP (LXAIP) macht. Das LXAIP wird über die S.4 mit Hilfe des Prozesses *ArchiveSubmissionRequest* an die Middleware übertragen.

Im Rahmen eines *Verify- oder SignRequests* kann das Krypto-Modul über die S.2 –Schnittstelle des Archivspeichers (Long-Term-Storage) im Bedarfsfall auf die Datenobjekte mit Hilfe der

1 Es könnten, abhängig vom Schutzbedarf, zur Integritätssicherung unsignierter Inhaltsdaten auch fortgeschrittene Signaturen verwendet werden

AOID zugreifen. Das ArchiSig-Modul erzeugt die erforderlichen Beweisdaten und übergibt dann das LXAIP auch dem Archivspeichers (Long-Term-Storage).

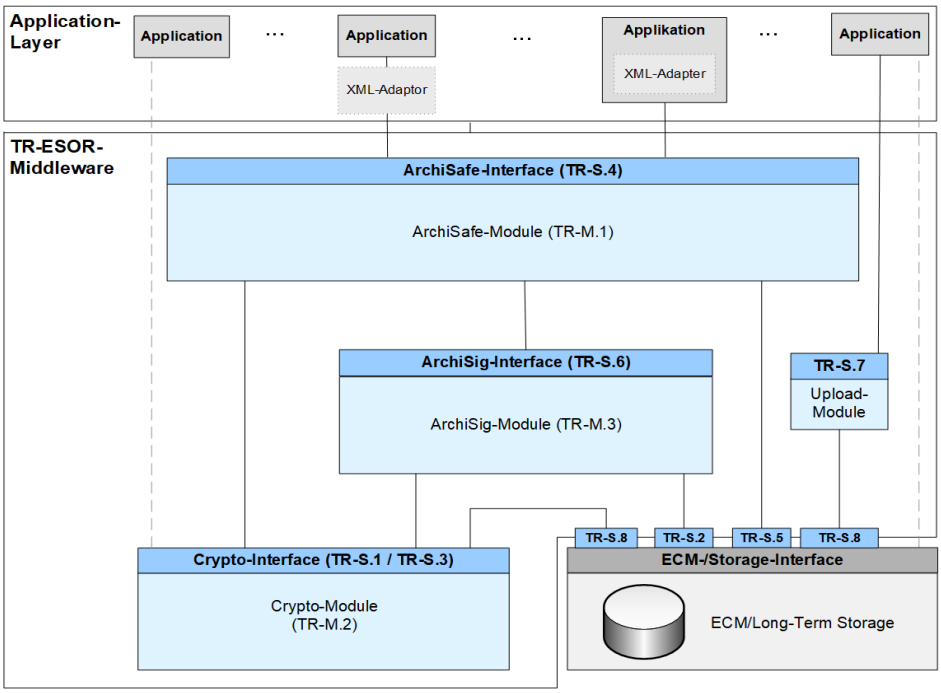

Abbildung 5: Mögliche Erweiterung der Referenzarchitektur [TR-03125] für ein logisches XAIP

Hinsichtlich des XAIP-Formats muss also die Möglichkeit geschaffen werden, eine Referenz auf einen externen Speicherort sowie eine kryptographische Sicherung für die, vor der Übergabe an die Beweiswerterhaltungskomponente, im Archivspeicher abgelegten Inhaltsdaten, zu integrieren. Um den Umsetzungsaufwand für die Produktanbieter zu begrenzen, ist zu prüfen, ob diese zusätzlichen Elemente ohne Änderung des XAIP-Schemas ergänzt werden können, z.B. im Rahmen der bestehenden Erweiterungsoptionen in der relevanten *DataObjectSection*.

Hierfür bietet sich das Element *XMLData* (vgl. Abb. 6) an, welches in der aktuellen Spezifikation einen any-type aufweist, also die beliebige, schemakonforme Nutzung ermöglicht. So könnte ein neues Element *DataObjectReference-Type* (vgl. Abb. 7) eingefügt werden, der wiederum eine eindeutige Identifikation sowie eine Referenz auf den Speicherort der Inhaltsdaten sowie die Prüfsumme oder kryptographische Signatur zur Integritätsprüfung trägt.

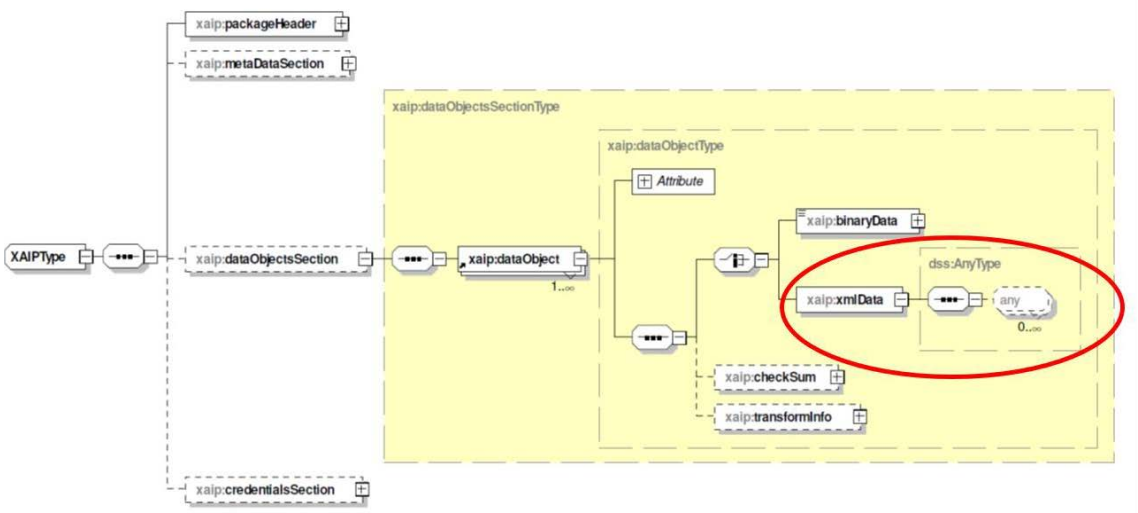

Abbildung 6: Element XML-Data in XAIP zur Aufnahme der Referenzen für ein logisches XAIP

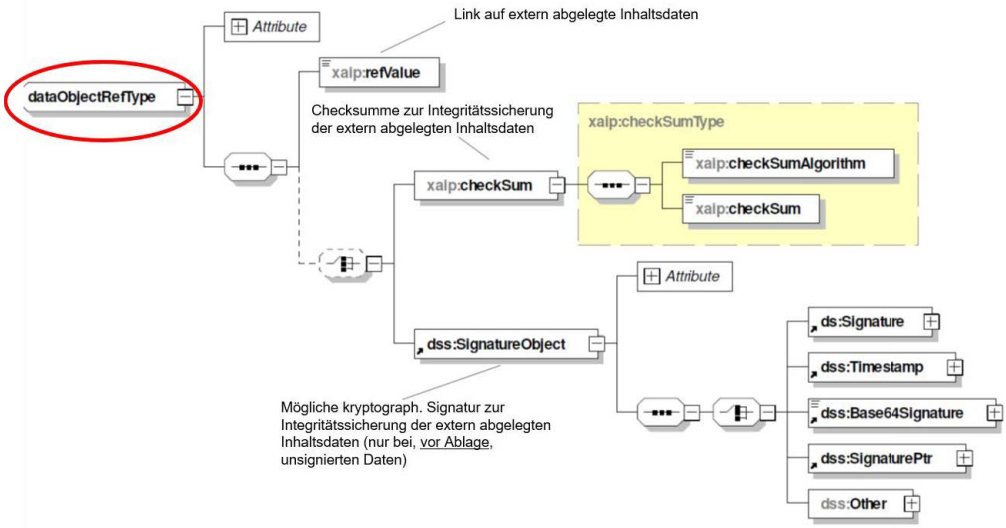

Abbildung 7: Möglicher Aufbau logisches XAIP

Während des Ablageprozesses (*ArchiveSubmissionRequest*) oder der Versionierung (*ArchiveUpdateRequest*) würden Inhaltsdaten, unter Verwendung der o.g. Referenz, on demand ins Krypto-Modul entspr. der Referenzarchitektur in Abb. 5 geladen und die Integritätsprüfung vorgenommen. Nach deren erfolgreicher Durchführung werden die weiteren Schritte durchgeführt, so z.B. Einholung der beweisrelevanten Daten sowie Verhashung der anhand der ProtectedPointer des XAIP zu schützenden Daten zwecks Erzeugung des Hashbaums zur Beweiswerterhaltung gem. [RFC4998] bzw. [RFC6283]. Gemäß [RFC4998] bzw. [RFC6283] können aus dem Hashbaum Evidence Records abgeleitet werden, die in die nichtverhashten Teile des XAIP abgelegt werden, als zusätzliche Sicherheit. Daneben könnten die Inhaltsdaten im Rahmen eines *ArchiveRetrievalRequests* im Bedarfsfall in ein selbsttragendes XAIP wieder hinzugefügt und so ein vollständig selbttragendes AIP erzeugt werden, das im Rahmen eines *ArchiveRetrievalResponse* dem aufrufenden Client-/Geschäftsanwendung zurückgegeben werden kann.

3.3 ASiC

Der Associated Signature Container (ASiC) ist in [EN319162] spezifiziert und gilt gem. [EIDAS] als einer der zu unterstützenden Signaturformate [EIDAS], [2015/1506/EU]: Es handelt sich dabei um einen Binärcontainer, deren Inhalte mit Hilfe des ZIP-Algorithmus (vgl. [ISO21320-1]) platzsparend komprimiert sind. Je nach Anzahl der aufzubewahren Signaturen wird dabei zwischen zwei Varianten des ASiC unterschieden:

- Einfacher Container - ASiC-S,
- Erweiterter Container – ASiC-E.

Da ASiC-S über eine Einschränkung verfügt, die die Ablage von nur einem Signatur- oder *time assertion*-Objekt erlaubt, ist dieses Format für weitere Untersuchungen ungeeignet.

Eine kurze Darstellung der Kerneigenschaften von ASiC-E, sowie einen Vorschlag für dessen Einsatz als AIP innerhalb der Langzeitspeicherung sind dem nachkommenden Kapitel zu entnehmen.

3.3.1 ASiC-E

Die erweiterte Variante von ASiC, ASiC-E, erlaubt grundsätzlich die Ablage einer beliebigen Anzahl von Signatur- oder Zeitstempel bzw. Evidence Records (*time assertions*-Objekte) sowie von zugehörigen Datenobjekte direkt im Wurzelverzeichnis der Container-Datei. Die Signatur- oder Zeitstempel bzw. Evidence Records (*time assertion*-Objekte) sowie (bei Bedarf) weitere anwendungsrelevante Dateien werden in einem dedizierten Verzeichnis *META-INF* abgelegt, Datenobjekte dagegen sind direkt im Wurzelverzeichnis platziert. Die logische Verbindung zwischen einem Signaturobjekt und den zugehörigen Datenobjekten wird explizit in einer Manifest-Datei (ASiCManifest.xml) innerhalb des *META-INF*-Verzeichnis abgelegt (vgl. Teil 1, Kap. 4.4.2 [EN319162], Abbildung 8).

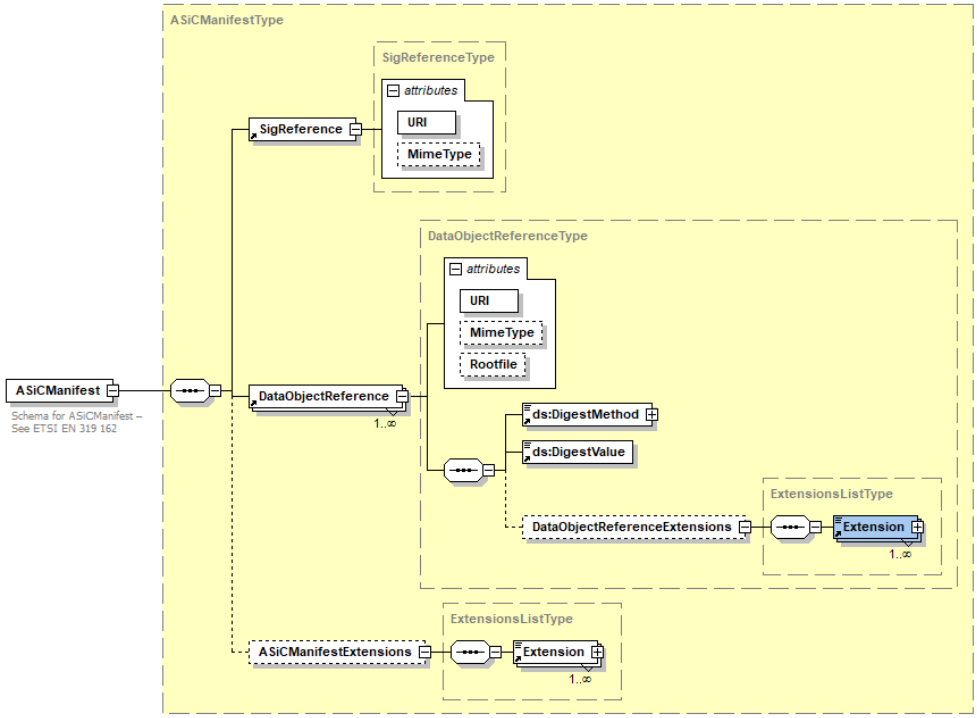

Abbildung 8: Struktur des ASiCManifest-Elementes

Angelegt an die Bedürfnisse eines AIP und unter Berücksichtigung der Regeln zum Aufbau eines ASiC-E, wurde ein Vorschlag erarbeitet, der das bereits vorgestellte logische XAIP mit einem ASiC-E verknüpft und somit ein ASiC-E-AIP definiert. Die nachkommende Abbildung stellt ein Beispiel eines ASiC-E-AIP dar.

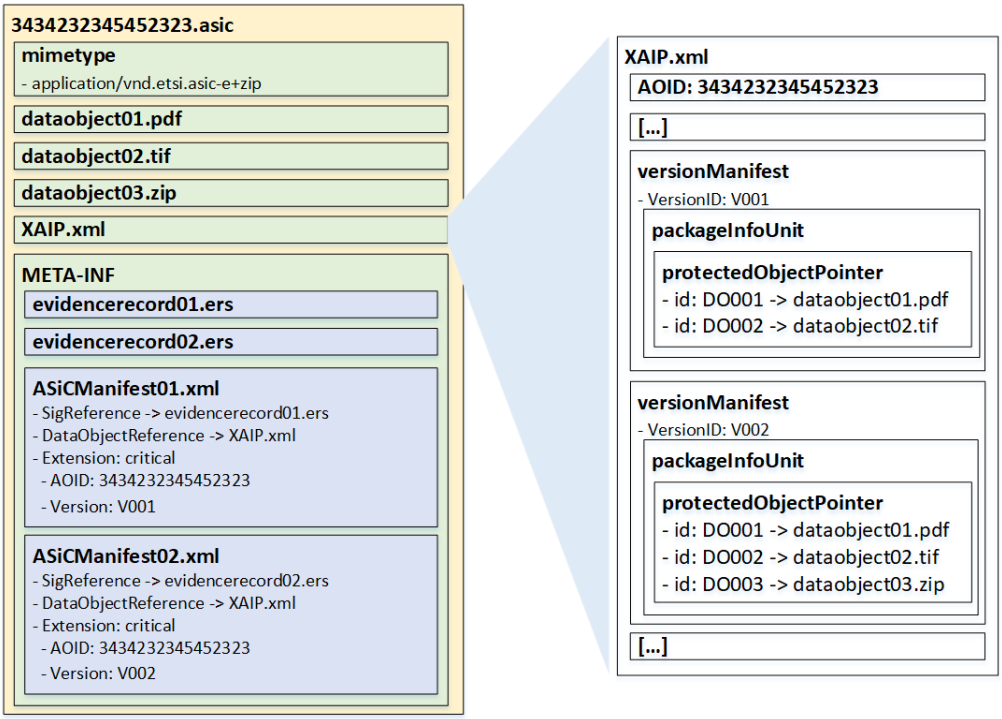

Abbildung 9: AIP basierend auf ASiC-E

Der Container beinhaltet die Mime-Type-Definition (*mimetype*) und vier Datenobjekte im Wurzelverzeichnis: dataobject01.pdf, dataobject02.tif, dataobject03.zip, XAIP.xml. Die Datei XAIP.xml stellt eine Instanz vom logischen XAIP, das die drei vorgenannten Datenobjekte aus der *DataObjectSection* heraus referenziert. Das XAIP beinhaltet zwei Versionen die jeweils durch einen Evidence-Record geschützt werden. Diese Evidence-Records wurden entsprechend ASiC-E-Regeln im *META-INF*-Verzeichnis abgelegt (evidencerecord01.ers, evidencerecord02.ers). Weiterhin beinhaltet das *META-INF*-Verzeichnis zwei Manifest-Dateien (ASiCManifest01.xml ASiCManifest02.xml), die entsprechend jeweils ein Evidence-Record (z. B. im Falle von ASiCManifest01.xml den evidencerecord01.ers) mit dem zugehörigen XAIP (XAIP.xml) und der darin enthaltenen korrespondierenden Version (Version: V001) in Verbindung bringen und somit im weiteren Zuge auf die mit der Version korrelierenden Datenobjekte (dataobject01.pdf, dataobject02.tif) verweisen. Die für die Interpretation eines auf dieser Weise aufgebauten Containers notwendige Semantik ist durch die Eingabe einer kritischen Erweiterung (critical extension) innerhalb von ASiCManifest gegeben (vgl. Abbildung 10).

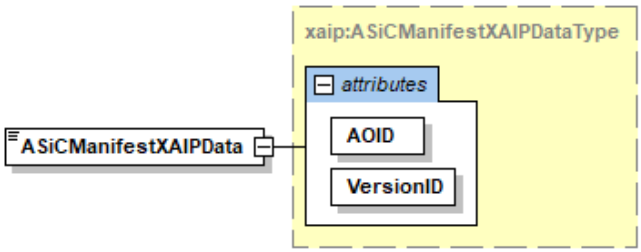

Abbildung 10: XML-Schema für die kritische Erweiterung von ASiCManifest im Falle eines ASiC-E-AIP

3.4 PDF/A-3

PDF/A definiert Konformitätsstufen des zugrundeliegenden Dokumentenformats PDF [ISO32000-1], die insbesondere die Anforderungen der Langzeitspeicherung und –archivierung berücksichtigen. Die erste Ausprägung, PDF/A-1, wurde im Jahre 1995 als ISO-Standard veröffentlicht [ISO19005-1] und hat die Eingeschalten definiert, die ein PDF Dokument aufweisen muss um als langzeitstabil zu gelten (z. B. keine aktiven oder dynamischen Inhalte, keine ausführbaren Objekte etc.). Die im Jahre 2012 verabschiedete Konformitätsstufe PDF/A-3 [ISO19005-3] wurde eine entscheidende Einschränkung der vorrausgegangenen Stufen A-1 und A-2 aufgehoben, nämlich das Verbot der Einbettung von fremden Formaten. Auf dieser Weise kann ein PDF/A-3 Dokument auch als ein Container betrachtet werden, der beliebige Dateien in Form sog. Anhänge (file attachements[2]) beinhalten kann. Die eingebetteten Dateien können mit einer Information zum *mimetype*. versehen werden und platzsparend (Verwendung des ZIP-Algorithmus) abgelegt werden. Die Beziehung der einzelnen Dateien zu dem eigentlichen PDF/A-3 Dokument muss dabei definiert werden: Alternative, Source, Data oder Supplement. Eine weitere zwingende Voraussetzung eines PDF/A-3-konformes Dokuments ist das Vorhandensein von sog. Metadaten, die im XMP-Format verfasst [ISO16684-1] die wichtigsten Informationen über das Dokument beinhalten. Neben den standardmäßig zugelassenen Metadaten-Schemata in XMP (z.B. Dublin-Core etc.) besteht die Möglichkeit, eigene Metadaten-Format zu verwenden, soweit ein PDF/A-Erweiterungsschema dafür definiert wurde. Dabei ist jedoch zu beachten, dass marktübliche PDF-Viewer im Standard nur das PDF-hauptdokument, nicht jedoch etwaige Erweiterungsschemata visualisieren.

Hinsichtlich signierter Dokumente können PAdES-Signaturen (PDF-Signaturen) inkl. der zugehörigen Long-Term-Archive (LTA)-Profiles verwendet werden. Allerdings bezieht sich die Signatur des Archivzeitstempels immer auf den gesamten PDF/A-3-Container. Für die Integration von Versionen sowie Protected Pointern, wie dies in XAIP, LXAIP sowie ASiC auf Basis XAIP möglich ist, bestehen in PDF/A-3 bislang keine Ansatzpunkte, was die Praktikabilität des Containerformats für die beweiswerterhaltende Langzeitspeicherung derzeit erheblich einschränkt. Darüber hinaus beschränkt sich PDF/A-3 auf die Prüfung von Signaturen im PAdES-Format [EN319142]. Gleiches gilt für eine derzeit fehlende Versionierung, wie dies XAIP, LXAIP und ASiC-E zulassen. Nähere Angaben zu den Nutzungsmöglichkeiten von PDF/A-3 als AIP-Container sind in [Ko17] zu finden.

Hier erscheinen weitere Forschungsarbeiten u.a. zur Lösung dieser offenen Punkte sinnvoll.

---

[2] Auch im kommenden ISO-Standard PDF 2.0 bzw. [ISO32000] soll diese Datenstruktur für denselben Zweck verwendet werden.

4 Bewertung der einzelnen Lösungsoptionen

Anforderung	XAIP	Logisches XAIP (LXAIP)	ASiC
Beliebige viele Nutzdaten, Metadaten, beweisrelevante Daten/ Beweisdaten,	**Ja;** als Objekte in der jeweiligen Sektion des XAIP	**Ja;** Metadaten physisch im LXAIP enthalten, Inhaltsdaten physisch ausgelagert und dafür eine entsprechende Referenz in der jeweiligen Sektion des XAIP	**Ja,** als Dateien, jedoch nur ASiC-E
Signierte/zeitgestempelte und unsignierte/nicht zeitgestempelte Daten	**Ja** Herstellung Zusammenhalt zwischen den Daten und genutzten Signaturtechniken mittels eines Version-Manifest	**Ja** Herstellung Zusammenhalt zwischen den Daten und genutzten Signaturtechniken mittels eines VersionManifest und geeigneter Referenzen	**Ja** Herstellung Zusammenhalt zwischen den Daten und genutzten Signaturtechniken mittels ASiC-Manifest Nur ASiC-E
Verschiedene Signaturtechniken erzeugen und verifzieren können	**Ja,** AdES-Signaturen, - Zeitstempel, Evidence Recordes	**Ja, wie XAIP**	**Ja,** AdES-Signaturen, -Zeitstempel, Evidence Records
Parallele Signaturen	**Ja**	**Ja**	**Ja**

Anforderung	**XAIP**	**Logisches XAIP (LXAIP)**	**ASiC**
nachträgliches Einspielen von Sperrmaterial ohne Verletzung Beweiswert	**Ja**	**Ja**	**Ja**
Versionierung Nutz-, Meta- und Beweisdaten	**Ja** Herstellung eines versionierten Zusammenhalts zwischen Daten und genutzten Signaturtechniken mittels jeweils einem VersionManifest pro Version. Unter Verwendung von mehreren VersionManifesten können mehrere Zusammenhalte mit einer erkennbaren Reihenfolge in einem XAIP Container abgelegt werden,	**ja, wie XAIP**	**Eingeschränkt:** Nicht-versionierte Herstellung eines Zusammenhalts zwischen Daten und genutzten Signaturtechniken mittels jeweils einem ASiC-Manifest. Unter Verwendung von mehreren ASiC-Manifesten können mehrere Zusammenhalte in einem ASiC-Container abgelegt werden, ohne dass eine Reihenfolge unter den Zusammenhalten erkennbar ist.
Performant auch bei großen Datenmengen/Dateien z.B. Geodaten	**Eingeschränkt:** Einbettung in XML erfordert Nutzung Bas64-Codierung	**Ja** Aufgrund der Einbindung großer Datenmengen durch Referenzen und mögliche Mischung von logischem und physischem XAIP	**Ja**
Wirtschaftlich	**Ja:** Keine zusätzlichen Lizenzpflichten	**Ja** Effiziente Speicherform durch Referenzen Keine zusätzlichen Lizenzpflichten	**Ja** Effiziente Speicherform durch Kompression;

Anforderung	XAIP	Logisches XAIP (LXAIP)	ASiC
			Keine zusätzlichen Lizenzpflichten
Selbsttragend	Ja	Ja Bei referenzierten Inhaltsdaten nur wenn diese nachträglich in das XAIP bzw. LXAIP inkludiert werden	Ja

5 Fazit und Ausblick

Der vorliegende Aufsatz untersucht, inwieweit, neben dem für die beweiswerterhaltende Langzeitspeicherung etablierten XAIP [TR-03125-F], weitere Lösungswege, logisches XAIP oder ASiC [EN319162] oder PDF/A-3 [ISO19005-3] geeignet sind. Bei allen Optionen wurde geprüft, ob diese, ähnlich XAIP als selbsttragende Archivinformationspakete genutzt werden können.

Das logische XAIP würde dabei auf die bestehenden Prozesse und Anforderungen von XAIP aufsetzen. Das LXAIP offeriert eine Variante, um umfangreiche Inhaltsdaten auf einem performanten Weg in den Archivspeicher zu überführen und on demand in der [TR-03125]-konformen Middleware abzurufen, um die Operationen zur Beweiswerterhaltung durchzuführen. Damit wird vermieden, die natürlich Grenzen bestehender Webservice-Schnittstellen zu überschreiten und inakzeptable hohe Ladezeiten bei der Ablage und Abruf von AIP mit großen Datenmengen zu erzeugen. Die dem Aufsatz zugrundeliegenden Betrachtungen haben ergeben, dass die Spezifikation eines LXAIP zum einen in absehbarer Zeit und in Compliance zu bestehenden Standards und Normen möglich ist. Aus diesem Grund wird das LXAIP in der neuen Fassung der TR-ESOR (Version 1.3.), deren Publikation 2019 erfolgt, enthalten sein.

Das LXAIP ist zugleich die Grundlage, um ASiC [EN319162] als AIP-Container zu verwenden. Das im Kontext [EIDAS] durch ETSI (Mandat 460 der EU-Kommission) standardisierte Format kommt dabei nur in der Ausprägung ASiC-E in Frage-. ASiC-E lässt, im Gegensatz zu ASiC-S die Ablage beliebig vieler Nutzdaten in vollständiger Compliance zur zugrundeliegenden [EN319162] zu. Der Zusammenhang zwischen den Signaturinformationen in ASiC-E sowie den Header-/Meta-/Nutzdaten wird auf Basis der Mechanismen im LXAIP hergestellt und so beide Lösungsoptionen sinnvoll verknüpft. ASiC-E wird, äquivalent dem LXAIP als weiteres Containerformat in der TR-ESOR (Version 1.3.) enthalten sein. Die finale Spezifikation

erfolgt in Übereinstimmung mit den derzeit laufenden Standardisierungs- und Forschungsarbeiten auf europäischer Ebene (ETSI) zur technischen Ausgestaltung der sog. PreservationServices zur Beweiswerterhaltung gem. [EIDAS].

Für PDF/A-3 bewegen sich, wie in Kap. 4 angegeben, die Forschungsarbeiten noch auf der Lösung grundsätzlicher Fragestellungen, Zudem sind weitere Standardisierungsaktivitäten auf ISO-Ebene notwendig, bevor das Format als Container zur Beweiswerterhaltung spezifiziert und verwendet werden kann.

Literatur

[2015/1506/EU] DURCHFÜHRUNGSBESCHLUSS (EU) 2015/1506 DER KOMMISSION zur Festlegung von Spezifikationen für Formate fortgeschrittener elektronischer Signaturen und fortgeschrittener Siegel, die von öffentlichen Stellen gemäß Artikel 27 Absatz 5 und Artikel 37 Absatz 5 der Verordnung (EU) Nr. 910/2014 des Europäischen Parlaments und des Rates über elektronische Identifizierung und Vertrauensdienste für elektronische Transaktionen im Binnenmarkt anerkannt werden, 8. September 2015

[ArchiSafe] ArchiSafe Fachkonzept v1.1. Physikalisch Technische Bundesanstalt. 2006

[BGB] Bürgerliches Gesetzbuch, Ausfertigungsdatum: 18.08.1896, zuletzt geändert durch Art. 1 G v. 22.7.2014 I 1218, [BSIGS] IT-Grundschutz-Kompendium. Bundesamt für Sicherheit in der Informationstechnik, Bonn 2017

[BSIGS] BSI-Grundschutzkompendium. Bundesamt für Sicherheit in der Informationstechnik. Bonn 2017

[DIN31644] DIN 31644:2012 Information und Dokumentation – Kriterien für vertrauenswürdige digitale Langzeitarchive. 2012

[DIN31647] DIN 31647:2015 Beweiswerterhalt kryptografisch signierter Dokumente, 2015.

[EUDSGVO] VERORDNUNG (EU) 2016/679 DES EUROPÄISCHEN PARLAMENTS UND DES RATES vom 27. April 2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten, zum freien Datenverkehr und zur Aufhebung der Richtlinie 95/46/EG (Datenschtz-Grundverordnung)

[EGOVG] Gesetz zur Förderung der elektronischen Verwaltung (E-Government-Gesetz - EGovG) vom 25.07.2013

[EASA] Easy Access Rules for Airworthiness and Environmental Certification. (Regulation (EU) No 748/2012). Part 21.A.55. published February 2018.

[EIDAS] VERORDNUNG (EU) Nr. 910/2014 DES EUROPÄISCHEN PARLAMENTS UND DES RATES über elektronische Identifizierung und Vertrauensdienste für elektronische Transaktionen im Binnenmarkt und zur Aufhebung der Richtlinie 1999/93/EG“ vom 23.07.2014

[eJusticG] Gesetz zur Förderung des elektronischen Rechtsverkehrs mit den Gerichten vom 10. Oktober 2013

[EN319122] ETSI EN 319 122 – {1,2,3}, Electronic Signatures and Infrastructers (ESI); CAdES digital signatures, ETSI V1.1.1, (2016-04)

[EN319132] ETSI EN 319 132 – {1,2}, Electronic Signatures and Infrastructures (ESI); XAdES digital signatures, ETSI V1.1.1, (2016-04)

[EN319142] ETSI EN 319 142 – {1,2}, Electronic Signatures and Infrastructeres (ESI); PAdES digital Signatures, ETSI V1.1.1 (2016-04)

[EN319162] ETSI EN 319 162 – {1,2}, Electronic Signatures and Infrastrucutres (ESI); Associated Signature Containers (ASiC), ETSI V1.1.1 (2016-04)

[EU-DLR] RICHTLINIE 2006/123/EG DES EUROPÄISCHEN PARLAMENTS UND DES RATES über Dienstleistungen im Binnenmarkt“ vom 12.12.2006 [EUDSGVO] VERORDNUNG (EU) 2016/679 DES EUROPÄISCHEN PARLAMENTS UND DES RATES vom 27. April 2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten, zum freien Datenverkehr und zur Aufhebung der Richtlinie 95/46/EG (Datenschtz-Grundverordnung)

[EuroSOX] RICHTLINIE 2006/43/EG DES EUROPÄISCHEN PARLAMENTS UND DES RATES vom 17. Mai 2006 über Abschlussprüfungen von Jahresabschlüssen und konsolidierten Abschlüssen, zur Änderung der Richtlinien 78/660/EWG und 83/349/EWG des Rates und zur Aufhebung der Richtlinie 84/253/EWG des Rates

[FDA] CFR - Code of Federal Regulations Title 21. ITLE 21--FOOD AND DRUGS CHAPTER I--FOOD AND DRUG ADMINISTRATION DEPARTMENT OF HEALTH AND HUMAN SERVICES SUBCHAPTER A—GENERAL PART 11 ELECTRONIC RECORDS; ELECTRONIC SIGNATURE

[Fi06] S. Fischer-Dieskau: Das elektronisch signierte Dokument als Mittel zur Beweissicherung, Baden-Baden, 2006.

[Gia11] D. Giaretta: Advance Digital Preservation. Berlin, Heidelberg 2011

[GXP] Sammlung von Guten Arbeitspraxis Richtlinien, z. B. GCP – Good Clinical Practice oder GLP – Good Laboratory Practice etc

[ISO13527] ISO 13527:2010, Space data and information transfer systems -- XML formatted data unit (XFDU) structure and construction rules, 2010

[ISO14533-1] ISO 14533-1:2014, Processes, data elements and documents in commerce, industry and administration -- Long term signature profiles -- Part 1: Long term signature profiles for CMS Advanced Electronic Signatures (CAdES)

[ISO14533-2] 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)

[ISO14533-3] ISO 14533-3:2017 Processes, data elements and documents in commerce, industry and administration -- Long term signature profiles -- Part 3: Long term signature profiles for PDF Advanced Electronic Signatures (PAdES)

[ISO14721] ISO 14721:2012, Space data and information transfer systems — Open archival information system — Reference model, 2nd Edition, 2012

[ISO15489] ISO 15489-1:2016: Information and documentation - Records management - Part 1: Concepts and principles. 2016

[ISO16684-1] ISO 16684-1, Graphic technology – Extensible metadata platform (XMP) specification – Part 1: Data model, serialization and core properties, 2012

[ISO19005-1] ISO19005-1, Document management — Electronic document file format for long-term preservation – Part 1: Use of PDF 1.4 (PDF/A-1), 2005

[ISO19005-3] ISO19005-3, Document management — Electronic document file format for long-term preservation – Part 3: Use of ISO 32000-1 (PDF/A-3), 2012

[ISO21320-1] ISO/IEC 21320-1:2015. Information technology -- Document Container File -- Part 1: Core. 2015

[ISO27001] ISO/IEC 27001:2013: Information technology — Security techniques — Information security management systems — Requirements. 2013

[ISO30301] ISO 30301:2011, Information and documentation - Management systems for records - Requirements. 2011

[ISO32000-1] ISO 32000-1, Document management — Portable document format – Part 1: PDF 1.7, 2008

[Ko13] U. Korte, S. Schwalm, D. Hühnlein: Vertrauenswürdige und beweiswerterhaltende Langzeitspeicherung auf Basis von DIN 31647 und BSI TR-03125, Informatik 2013, GI-LNI, P220, ISBN 978-3-88579-614-5, S. 550-566, 2013

[KoScDH14] U. Korte, S. Schwalm, D. Hühnlein: Standards for the preservation of evidence and trust. Proceedings Archiving 2014, Springfield 2014 S. 9-14

[Ko14] U. Korte, S. Schwalm, D. Hühnlein: Standards und Lösungen zur langfristigen Beweiswerterhaltung. DACH-Security 2014, S. 46-58. Frechen 2014

[Ko16] U. Korte, S. Schwalm, D. Hühnlein, T. Kusber: Beweiswerterhaltung im Kontext eIDAS - eine Case Study. DACH-Security 2016, Frechen 2016 S. 379-392

[Ko17] U. Korte, S. Schwalm, D. Hühnlein, M. Prechtl, B. Wild: Datenpakete zur Informations- und Beweiswerterhaltung. Ein Vergleich. DACH-Security 2017. Frechen 2017 S. 291-303

[KSDV15] T. Kusber, S. Schwalm, A. Dörner, T. Vogt, Die Bedeutung der eIDAS-Verordnung für Unternehmen und Behörden. Neue Chancen und Herausforderungen für vertrauenswürdige elektronische Geschäftsprozesse in Europa, Berlin, 2015

[KuSc16] T. Kusber, S. Schwalm: Elektronische Langzeitspeicherung als SOA-Dienst – Kernelement eines vertrauenswürdigen Informationsmanagements. INFORMATIK 2016 S. 869-882

[MiniKGovG] Minikommentar zum Gesetz zur Förderung der elektroni-schen Verwaltung sowie zur Änderung weiterer Vorschriften. Bundesministerium des Innern. Berlin 2013

[OASI-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

[OASIS-VR] Hühnlein, D., OASIS DSS v1.0 Profile for Comprehensive Multi-Signature Verification Reports Version 1.0, Committee Specification 01, 12 November 2010

[PREMIS] PREMIS Data Dictionary for Preservation Metadata Version 3.0, 2015

[PSD2] RICHTLINIE (EU) 2015/2366 DES EUROPÄISCHEN PARLAMENTS UND DES RATESvom 25. November 2015 über Zahlungsdienste im Binnenmarkt, zur Änderung der Richtlinien 2002/65/EG, 2009/110/EG und 2013/36/EU und der Verordnung (EU) Nr. 1093/2010 sowie zur Aufhebung der Richtlinie 2007/64/EG

[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

[Ro07] A. Rossnagel: Langfristige Aufbewahrung elektronischer Dokumente, Anforderungen und Trends, Baden-Baden, 2007

[RoSc06] A. Rossnagel, P. Schmücker

[Sc15] S. Schwalm: Langzeitspeicherung und Archivierung – zwei Seiten einer Medaille! Aktuelle Standardsund Normen zur beweiswerterhaltenden Aufbewahrung elektronischer Unterlagen in: Proceedings der 18. Tagung des AK „Archivierung von Unterlagen aus digitalen Systemen“. Wien 2015 S. 5-25

[Sc17] S. Schwalm: A service for the preservation of evidence and data – a key for a trustworthy & sustainable electronic business. Open Identity Summit 2017. Lecture Notes in Informatics (LNI). Proceedings. Bonn 2017 S. 131-144

[SR019510] ETSI SR 019 510, Electronic Signatures and Infrastructures (ESI); Scoping Study and framework for standardization of long-term data preservation services, including preservation of/with digital signatures, ETSI V1.1.1 (2017-05)

[To07] Peter M. Toebak: Records Management. Ein Handbuch. Baden 2007

[TR-03112] BSI Technical Guideline TR-03112-1eCard-API-Framework. Version 1.1.5, 2015

[TR-03125] BSI: Beweiswerterhaltung kryptographisch signierter Dokumente (TR-ESOR), TR 03125, V1.2.1, 2018.

[TR-03125-F] BSI TR 03125, Beweiswerterhaltung kryptographisch signierter Dokumente, Anlage TR-ESOR-F: Formate, Version 1.2.1, 2018

[TR-03125-E] BSI Technische Richtlinie 03125 Beweiswerterhaltung kryptographisch signierter Dokumente Anlage TR-ESOR-E: Konkretisierung der Schnittstellen auf Basis des eCard-API-Frameworks, Version 1.2.1, 2018

[TR-03125-C1] BSI Technical Guideline 03125. Preservation of Evidence of Cryptographically Signed DocumentsAnnex TR-ESOR-C.1:Conformity Test Specification (Level 1 - Functional Conformity), Version 1.2.1, 2018

[TR-03125-C2] BSI Technical Guideline 03125. Preservation of Evidence of Cryptographically Signed DocumentsAnnex TR-ESOR-C.1:Conformity Test Specification (Level 2 – Technical Conformity), Version 1.2.1, 2018

[TR-03138] BSI Technische Richtlinie 03138 Ersetzendes Scannen. Version 1.1, 2017

[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

[VDG] Vertrauensdienstegesetz vom 18. Juli 2017 (BGBl. I S. 2745), das durch Artikel 2 des Gesetzes vom 18. Juli 2017 (BGBl. I S. 2745) geändert worden ist

[VERS] Victorian Electronic Records Strategy, vgl. unter http://prov.vic.gov.au/government/vers

[VS18] T. Vogt, S. Schwalm: eIDAS-ready?. Status Quo und Roadmap zur Umsetzung elektronischer-Vertrauensdienste in Behörden und Unternehmen. Berlin 2018

[We18] M. Weber, T Vogt, W. Krogel, S. Schwalm: Records Management nach ISO 15489. Einführung und Anleitung. Berlin 2018

[Wi15] Bruno Wildhaber et.al.: Leitfaden Information Governance. Zürich 2015

[ZPO] Zivilprozessordnung in der Fassung der Bekanntmachung vom 5. Dezember 2005 (BGBl. I S. 3202; 2006 I S. 431; 2007 I S. 1781), die zuletzt durch Artikel 11 Absatz 15 des Gesetzes vom 18. Juli 2017 (BGB. I S. 2745) geändert worden ist