Heinrich C. Mayr, Martin Pinzger (Hrsg.): INFORMATIK 2016,
Lecture Notes in Informatics (LNI), Gesellschaft für Informatik, Bonn 2016 869

Elektronische Langzeitspeicherung als SOA-Dienst – Kernelement eines vertrauenswürdigen Informationsmanagements

Tomasz Kusber[1], Steffen Schwalm[2]

Abstract: Es besteht eine hohe Notwendigkeit, nicht nur in der öffentlichen Verwaltung, sondern auch in Unternehmen, Geschäftsprozesse zu digitalisieren und für die elektronischen Dokumente und Daten (Unterlagen) auch in ferner Zukunft die Lesbarkeit, Verfügbarkeit sowie die Integrität, Authentizität und Verkehrsfähigkeit gewährleisten zu müssen. Diese Anforderungen bestehen aufgrund geltender regulatorischer Vorgaben einschließlich der Verpflichtung zum Nachweis gegenüber Prüfbehörde, Gerichte, Dritten – bei gleichzeitigen Aufbewahrungsfristen zwischen 2 und 110 Jahren oder dauernd, die teilweise auch erst nach Jahrzehnten beginnen. Mit Blick auf die sinkenden Lebenszyklen der IT bestehen insofern besondere Herausforderungen an die Erhaltung des Beweiswerts der Unterlagen sowie deren Verfügbarkeit. Ein elektronischer Langzeitspeicherdienst ermöglicht den Aufbau der notwendigen technischen Komponenten, Module und Funktionen für alle relevanten IT-Verfahren und kann als eine Grundlage für ein vertrauenswürdiges Informationsmanagement bezeichnet werden. Der Beitrag stellt anhand geltender Standards und Normen sowie der langjährigen Erfahrungen der Autoren mögliche Lösungswege sowie eine beispielhafte Architektur eines Langzeitspeicherdienstes vor.

Keywords: Elektronische Langzeitspeicherung, SOA, vertrauenswürdiges Informationsmanagement, Beweiswerterhaltung, Vertrauensdienste, eIDAS, Records Management, Informationserhaltung, Information Governance

1 Einleitung

Die Nutzung der Informationstechnologie für Abwicklungen von Geschäftsprozessen ist allgemein etabliert. Geschäftsrelevante Unterlagen liegen zunehmend ausschließlich elektronisch vor. Elektronische Dokumente können jedoch aus sich heraus weder wahrgenommen noch gelesen werden. Sie liefern aus sich heraus auch keine Hinweise für ihre Integrität und Authentizität sowie die Ordnungsmäßigkeit im elektronischen Rechts- und Geschäftsverkehr. Gleichzeitig bestehen jedoch umfassende Dokumentations- und Aufbewahrungspflichten, deren Dauer zwischen zwei und 110 Jahre oder dauernd umfasst, die einen langfristigen Nachweis von Authentizität, Integrität und Nachvollziehbarkeit elektronischer Unterlagen erfordern. Während dieser Fristen muss es zudem möglich sein, die Dokumente Prüfbehörden oder Gerichten

[1] BearingPoint GmbH, Team Secure Information Management, Kurfürstendamm 207-208, 10719, Berlin, tomasz.kusber@bearingpoint.com
[2] BearingPoint GmbH, Team Secure Information Management, Kurfürstendamm 207-208, 10719, Berlin, steffen.schwalm@bearingpoint.com

vorzulegen und anhand der Daten die genannten Nachweise zu führen (Verkehrsfähigkeit). Diese Anforderungen gelten unabhängig vom konkret eingesetzten IT-Verfahren. Insofern kann eine elektronische Langzeitspeicherung als Querschnittsaufgabe bezeichnet werden, deren Umsetzung in einem verfahrensübergreifenden IT-Dienst im Sinne einer SOA-Architektur, die Nutzung von Synergieeffekten ermöglicht und Doppelaufwände vermeidet. Ein solcher Dienst muss entsprechend der geltenden Anforderungen die Erhaltung der Daten selbst, deren Lesbarkeit/Interpretierbarkeit (Informationserhaltung) sowie des Beweiswerts der Daten (Beweiswerterhaltung) ermöglichen [Ko13], [Ro07].

Der vorliegende Beitrag stellt, auf Basis der langjährigen Praxiserfahrungen der Autoren, eine Beispielarchitektur für einen elektronischen Langzeitspeicher (LZSP) als verfahrensübergreifenden IT-Dienst sowie dessen fachliche Integration in eine SOA-Architektur vor und ist folgendermaßen gegliedert: Abschnitt 2 erläutert die grundsätzlichen Anforderungen an die Aufbewahrung elektronischer Unterlagen. Der Abschnitt 3 beschreibt die wesentlichen Funktionen und beispielhafte Architektur eines Langzeitspeicherdienstes, Abschnitt 4 fasst die Rolle eines Langzeitspeicherdienstes in einem vertrauenswürdigen Informationsmanagement zusammen, ergänzt um einen Ausblick auf zukünftige Entwicklungen.

2 Grundsätzliche Anforderungen an die Aufbewahrung elektronischer Unterlagen

2.1 Grundsatz

Wie in der Einleitung dargelegt, muss entsprechend geltenden regulatorischen Vorgaben, bis zum Ablauf der geltenden Aufbewahrungsfristen der Nachweis von Authentizität, Integrität, Verkehrsfähigkeit und Nachvollziehbarkeit elektronischer Unterlagen gegenüber Gerichten, Prüfbehörden, Dritten jederzeit verlustfrei möglich sein. Besonders in hochregulierten Branchen wie Luft- und Raumfahrt, Gesundheitswesen, LifeScience/Pharma, Forschung, Transportation oder Energiewirtschaft bedeutet dies eine umfassende Herausforderung, insbesondere angesichts Aufbewahrungsfristen von 30 Jahren oder mehr, wobei die Fristen häufig erst nach Jahrzehnten beginnen, z.B. wenn das Produkt außer Produktion geht oder das Bauteil nicht mehr genutzt wird. [Ko13].

Eine wesentliche Grundlage für eine ordnungsgemäße elektronische Langzeitspeicherung bildet ein sachgerechtes Records Management innerhalb eines vertrauenswürdigen Informationsmanagement einer Behörde oder eines Unternehmens. Praktisch gewährleistet ein sachgerechtes Records Management insbesondere

- Sicherstellung der Verfügbarkeit, Sicherheit, Compliance geschäftsrelevanter Unterlagen solange diese in der Organisation benötigt werden
- Definition der notwendigen Rollen, Verantwortlichkeiten und Regularien (Policies)
- Nachvollziehbarkeit der Geschäftsprozesse auf Basis organisatorischer und technischer Maßnahmen
- Daten- und Beweiswerterhaltung mindestens bis zum Ablauf der geltenden Aufbewahrungsfristen

und erzeugt so Unterlagen, die als eindeutiger Nachweis von Geschäftsprozessen und geschäftlichen Entscheidungen gegenüber Dritten (Gerichte, Prüfbehörden etc.) dienen können [Wi15], [To07], [To10], [ISO-30301]. Es sichert so die Vertrauenswürdigkeit der Unterlagen und damit des Informationsmanagements [ISO-30301], [Lu12], [Ko14].

Die Nutzung kryptographischer Mittel, wie fortgeschrittene oder qualifizierte elektronischer Signaturen und qualifizierte Zeitstempel sowie künftig elektronischer Siegel, ermöglicht nach geltendem Recht die Erhaltung des für die Nachweisführung notwendigen Beweiswerts[3], ohne die Verkehrsfähigkeit einzuschränken (siehe [F06], [Ro07], [BMWi07], [eIDAS]). Diese kryptographischen Mittel werden direkt am Dokument/Daten angebracht, so dass er Beweiswert, ebenso wie das Dateiformat oder die Metadaten zur inhaltlichen Beschreibung eines Dokuments, eine inhärente Eigenschaft der jeweiligen elektronischen Unterlagen bildet. Dementsprechend müssen Maßnahmen zur beweissicheren Langzeitspeicherung auch direkt an den elektronischen Unterlagen ansetzen.

Die Beweiswerterhaltung erfolgt durch eine Nachsignatur bzw. Neuverhashung (vgl. u.a. § 17 SigV, [eIDAS]), also der Anbringung einer neuen qualifizierten elektronischen Signatur oder eines qualifizierten Zeitstempels, sowie ggf. dem Neuverhashen der eigentlichen Daten, sobald die Sicherheitseignung der Signatur-/Hashalgorithmen nicht mehr gegeben ist. Durch die Verwendung von Merkle-Hashbäumen gemäß [RFC 4998] bzw. [RFC 6283] kann eine wirtschaftliche Nachsignatur einer Vielzahl von Daten gewährleistet werden. Die Nachsignatur muss dabei jeweils alle vorhergehenden Signaturen und Zeitstempel einschließen. Die nachstehende Grafik zeigt eine solche Hashbaum:

[3] Der Beweiswert ist terminologisch mit dem juristischen Begriff der „Beweiskraft“ gleichzusetzen.

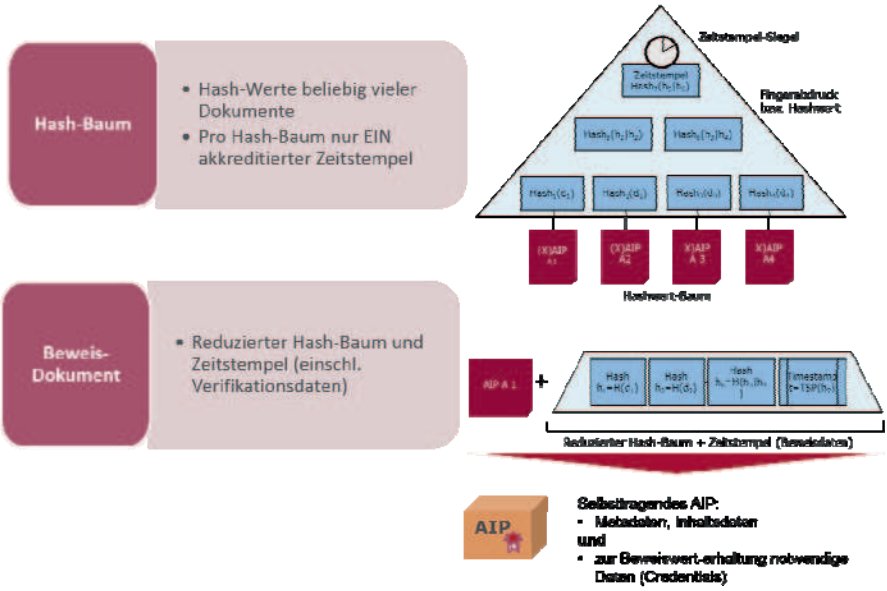

Abbildung 1: Hashbaum und Evidence Record

Daneben gilt es zum einen den Entscheidungsprozess, also die Nachvollziehbarkeit, der Unterlagen nachzuweisen[4], zum anderen, um den Nachweis zu führen, technische Daten (Gewährleistung der langfristigen Verfügbarkeit) der aufzubewahrenden Unterlagen zu erheben und langzeitzuspeichern [Lu12]. Dies bedingt schlussendlich die Langzeitspeicherung der Unterlagen in Form sog. selbsttragender Archivpakete im Sinne geltender Standards und Normen (vgl. Kap. 2.2) auchmit Blick auf die neue [eIDAS], die in EU und EFTA einheitliche, verbindliche Maßgaben für qualifizierte elektronische Signaturen, Siegel und Zeitstempel definiert und ebenso die Erhaltung von deren Vertrauenswürdigkeit und damit die Beweiswerterhaltung fordert [eIDAS], [Ku,Vo,Do,Sc16]. Verbindliche ETSI-/CEN-Normen bestimmen zudem den technischen Rahmen in der Umsetzung der [eIDAS] z.B. durch einheitliche Formate. Aufgrund der künftigen Zulässigkeit von Server-/Fern- und mobilen Signaturen ist zudem eine weitere Verbreitung signierter Dokumente, wie dies außerhalb Deutschlands z.B. in Österreich oder Großbritannien bereits der Fall ist, absehbar. Gleichzeitig gewährleistet eine beweissichere elektronische Langzeitspeicherung eine langfristige Erhaltung der aufzubewahrenden, geschäftsrelevanten Unterlagen und somit deren Verfügbarkeit (siehe [Ko13], [ISO-14721]], To07]. Als Grundlage dienen anerkannte nationale wie internationale Standards (vgl. Kap. 2.2).

Darüber hinaus stellt sich die Aufgabe der Erhaltung der aufzubewahrenden Unterlagen unter Wahrung geltender Aufbewahrungsvorgaben wie z.B. maschinelle Auswertbarkeit,

[4] z.B. bedingt durch das Prinzip der Aktenmäßigkeit gem. Art. 20 Abs. 3 Grundgesetz in öffentlichen Stellen.

originäre Darstellbarkeit der Daten. Es gilt also Dateiformate, Strukturen etc. teilweise jahrzehntelang so zu erhalten, dass die originäre Darstellung der Daten gewährleistet wird. Dabei ist der Grundsatz zu beachten, dass nicht das IT-Verfahren, sondern die Information den Aufbewahrungspflichten unterliegt. Insofern müssen auch Maßnahmen zur Informationserhaltung an den Daten selbst ansetzen [Borghoff03], [Ro07], [Giaretta11].

2.2 Relevante Standards und Normen

Die nachstehende Grafik zeigt die wesentliche Standards und Normen zur beweissicheren Langzeitspeicherung im Überblick:

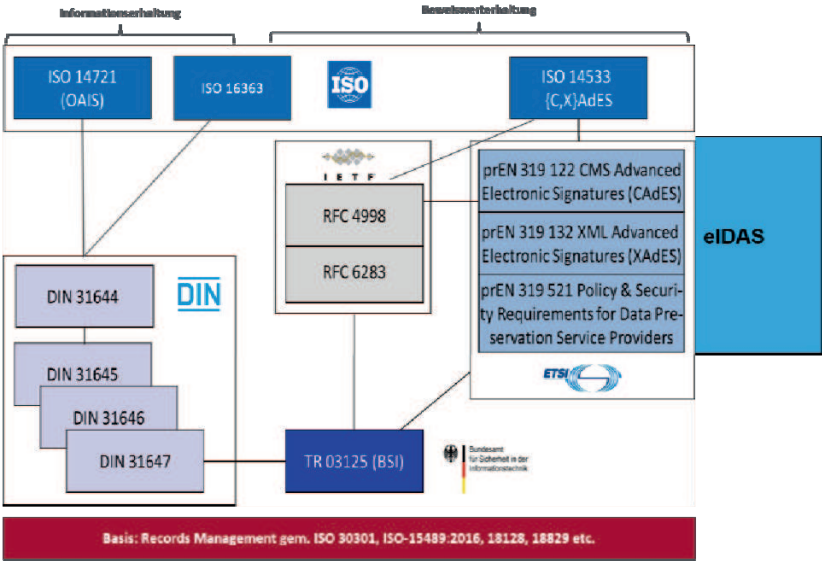

Abbildung 2: Standards und Normen zur Langzeitspeicherung

Wesentliche Basis bildet ein ordnungsgemäßes Records Management, welches anhand klarer Richtlinien, Verantwortlichkeiten und Prozesse die Identifikation und strukturierte wie anforderungsgerechte Ablage geschäftsrelevanter Unterlagen gewährleistet (vgl. [ISO30301], [ISO15489], [ISO18128], [ISO18829]). Darüber hinaus das OAIS-Modell [ISO14721] und die [ISO16363], [DIN31644], [DIN31645] die Prozesse und Informationspakete zur Informationserhaltung innerhalb eines vertrauenswürdigen digitalen Langzeitarchivs (dLZA) während die [DIN31647] die notwendigen Funktionen und Informationen zur Beweiswerterhaltung in einem OAIS-konformen dLZA beschreibt und damit die Verbindung zu den technischen Normen zur Beweiswerterhaltung bildet (vgl. [ISO14533], [EN319122], [EN319132], [EN319142], [EN319162], [RFC4998], [RFC6283]). Die [TR03125] wiederum beschreibt eine

mögliche Referenzarchitektur eines Systems zur Beweiswerterhaltung elektronischer Unterlagen mit daraus abgeleiteten Anforderungen. Sie integriert die Anforderungen aus ETSI[5] und IETF ([RFC 4998/6293]). Im praktischen Fall des betrachteten Unternehmens war diese Referenzarchitektur ein integraler Bestandteil Langzeitspeichers – als eigenständiges Modul zur Beweiswerterhaltung gem. OAIS [Ko16]. Sowohl bei [TR-03125] als auch [ISO16363] und [DIN31644] bestehen anerkannte Zertifizierungsverfahren, um die Standardkonformität konkreter Marktlösungen zu prüfen und nachzuweisen [Ko14], [DIN31644]. Daneben floss die [TR03125] in das E-Government-Gesetz des Bundes [EGovG] ein und gilt für öffentliche Stellen als sog. Stand der Technik zur Langzeitspeicherung.

3 Aufbau einer Beispielarchitektur für einen elektronischen Langzeitspeicherdienst

3.1 Notwendige Funktionscluster gem. OAIS

Wie in Kap. 2 dargestellt benötigt ein elektronischer LZSP sowohl Funktionen zur Informations- als auch zur Beweiswerterhaltung. Ziel sollte es dabei sein, so viele wie möglich vorhandene Dienste innerhalb der IT-Infrastruktur nachzunutzen. Erfahrungsgemäß sind zahlreiche Funktionen nicht langzeitspeicherspezifisch. So wird eine Signaturerzeugung einerseits im Geschäftsprozess, andererseits zur Beweiswerterhaltung (Nachsignatur) benötigt. Gleiches gilt für Konvertierungsfunktionen z.B. von Word nach PDF/A, was beim elektronischen Versand sowie zur Informationserhaltung erforderlich ist. Um eine effiziente Umsetzung zu ermöglichen und Synergien zu nutzen, bietet sich zur Clusterung der einzelnen Funktionen erfahrungsgemäß die Orientierung an den Prozessen des OAIS-Modells sowie der [TR03125] an. Diese stellen faktisch bereits konkrete Funktionsgruppen dar.

Ingest

Das erste Funktionscluster wären also die Funktionen zur Übernahme elektronischer Unterlagen in einen elektronischen LZSP bilden. Aus Gründen der IT-Sicherheit, so insbesondere dem Schutz der im LZSP abgelegten Unterlagen kann es sinnvoll sein, die Übernahmefunktionen in Funktionen zur Anbindung von Geschäftsanwendungen bzw. sendenden Systemen im sog. Pre-Ingest und die eigentlichen Kernfunktionen zur Datenübernahme im Kern-Ingest zu trennen.

[5] Empfehlung für Verwendung von {C,X,P}AdES als Signaturformat zu verwenden.

Um den LZSP als Dienst nutzen zu können ist es erforderlich, verschiedene Standardschnittstellen (z.B. WebService-Stack Spezifikationen entspr. OASIS und W3C sowie ArchiveLink bei SAP-Anbindung) gekapselt in einem sog. Konnektormodul im Pre-Ingest nach außen anzubieten. Hierüber werden in der Folge die Geschäftsanwendungen an den LZSP angebunden. Die Ablage von Daten kann dabei sowohl bei Eingang eines Dokuments in der Geschäftsanwendung z.B. E-Mails, Scan etc. als auch nach Abschluss eines Geschäftsvorfalls erfolgen. Das Konnektormodul prüft auf Basis einer sicheren Authentisierung die Zugriffsberechtigung der Geschäftsanwendung und leitet den eigentlich Request an die Kern-Ingest-Komponenten weiter. Grundsätzlich ist der Befehlsvorrat der Konnektoren zwecks standardisierter und damit effizienter Anbindung von Geschäftsanwendungen die notwendigen Kernprozesse zu beschränken. Diese sind i.d.R.: [TR03125]

- Übernahme von Daten und Erzeugung Archivinformationspakete (AIP)
- Erweiterung bereits im LZSP aufbewahrter Archivinformationspakete (z.B. durch eine weitere Mail, weiteren Dokumentenstand)
- Abruf von Datenpaketen (DIP) und einzelner Datenelemente aus Archivinformationspaketen
- Abruf technischer Beweisdaten aus AIP
- Löschen von AIP.

Mit diesem Vorgehen lässt sich faktisch jedes aktuelle IT-Verfahren an einen elektronischen LZSP anbinden. Dies wurde auch bereits für SAP realisiert [Ko15]. Für die Aufnahme von Daten aus IT-Verfahren, die nicht über die notwendigen Schnittstellen verfügt resp. der Aufwand zu deren Anpassung zu hoch ist oder die aufzubewahrenden Daten in einem Filesystem ohne Geschäftsanwendung vorliegen (z.B. Windows-Fileshare) kann eine einfache Uploadfunktion umgesetzt werden.

Die Kern-Ingestkomponente basiert verfahrensbezogen auf sog. Policies, also Regeln, wie, in welcher Form, in welchem Format, Struktur etc. die Unterlagen der verschiedenen IT-Verfahren in den elektronischen LZSP zu übernehmen sind. Diese technischen Regeln (z.B. umgesetzt als Workflows) sind anhand der regulatorischen und sonstige Anforderungen an die Aufbewahrung der Unterlagen, durch die fachlich verantwortlichen Organisationseinheiten, gemeinsam mit der IT zu definieren. Anhand dieser Policies werden die vom Pre-Ingest übergebenen SIP[6] geprüft und nur bei erfolgreicher Validierung weiterverarbeitet. Die Prüfung erfordert die Nutzung von Formatvalidierern sowohl für Metadaten (i.d.R. XML), Inhaltsdaten als auch vorhandener Signaturen und Zeitstempel. Ganz im Sinne einer diensteorientierten Architektur kann das dem LZSP immanente Krypto-Modul zur Signaturprüfung separat

[6] SIP = Submission Information Package (vgl. [ISO14721])

angesteuert werden, ohne alle übrigen Funktionen der Middleware zu nutzen oder selbige dabei zu kompromittieren [TR03125].

Neben der Form des SIP definieren die o.g. Policies Form und Inhalt der Archivinformationspakete (AIP), die aus den SIP erzeugt werden. Hierzu gehören Module mit Funktionen zur Informationserhaltung wie z.B.:

- Konvertierung von Inhaltsdaten und Validierung der Konvertierung
- Erhebung technischer Metadaten zur Beschreibung, Validierung inhaltlicher und technischer Metadaten und Volltextindizierung
- Mapping von IDs (z.B. bei SAP siehe [Ko15])
- Erzeugung und Validierung von AIP-Container

Beweiswerterhaltung

Im Ergebnis der Erzeugung eines AIP entsprechend den Vorgaben zur Informationserhaltung in der Kern-Ingestkomponente wird dieses an die Komponente zur Beweiswerterhaltung übergeben. Hierbei empfiehlt sich, eine Anlehnung an die Referenzarchitektur der [TR-03125] und deren standardisierte Komponenten, um eine wirtschaftliche Umsetzung zu ermöglichen.

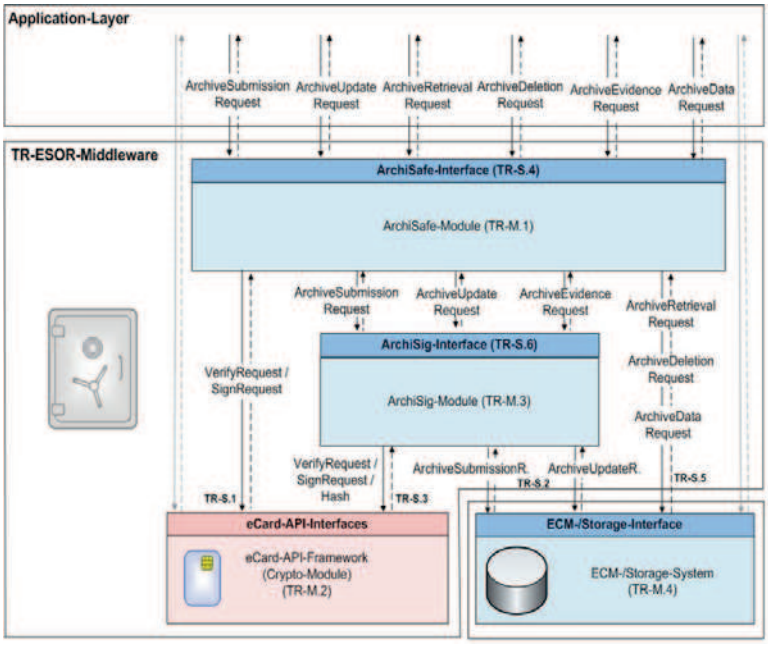

Abbildung 3: Referenzarchitektur BSI TR-03125 v1.2

Da die Middleware die Kernfunktionen zur Beweiswerterhaltung umfasst und die unmittelbar Schnittstelle zum eigentlichen Storage bildet, sind beide Cluster besonders abzusichern, z.B. durch Betrieb in einer eigenen Sicherheitszone. Um bei großen Datenmengen[7] das Performanceproblem sowohl bei XML-Datenpaketen aufgrund der Base64-Codierung (binäre Daten) als auch ZIP- oder PDF/A-3-Containern zu vermeiden, wäre folgender Weg eine Lösungsoption. Aus der Kern-Ingestkomponente können die Inhaltsdaten in einem sicheren Zwischenspeicher, der Teil des Archivspeichers ist, abgelegt und das Link hierauf sowie ein Hashwert der Inhaltsdaten als eindeutige Repräsentation m XAIP-basierten AIP abgelegt werden. Das AIP selbst wird nun einschl. Metadaten, Credentials (beweisrelevante Daten), dem Hashwert der Inhaltsdaten und dem Link als XAIP an die Middleware übergeben. Diese führt die ersten Funktionen zur Beweiswerterhaltung durch also z.B. Signaturprüfung, Einholung der Zertifikats- und Sperrinformationen. In das Hashen der für die Beweiswerterhaltung relevanten Teile des AIP werden durch Zugriff über einen gesicherten Kanal (z.B. VPN) die Inhaltsdaten mit einbezogen, jedoch nicht ohne zuvor deren Hashwert zu prüfen, um sicherzustellen, dass die Daten im Zwischenspeicherung nicht verändert wurden. Nach Aufbau des Hashbaums kann dieser sofort reduziert und damit die Evidence Records erzeugt und diese in den nichtgehashten Teilen des AIP abgelegt werden [TR03125-F]. Aufgrund des sicheren Links auf die eigentlichen Inhaltsdaten könnte, nach Abschluss der Funktionen zur Beweiswerterhaltung, vor der eigentlichen Speicher und im Archivspeicher die Unterlagen selbst, ebenso im AIP abgelegt werden. Damit wird ein vollständig selbsttragendes AIP erzeugt, welches grundsätzlich mit marktüblicher Standardsoftware lesbar und prüfbar ist. Die eindeutige AOID je AIP wird im ArchiSig-Modul erzeugt, auf Basis der [TR03125] und damit in non-proprietärer Form. Diese wird sowohl an das Cluster Datenmanagement als auch die Geschäftsanwendung (soweit vorhanden) für einen späteren Zugriff auf die AIP gegeben.

Datenmanagement (Repository)

Beim Datenmanagement handelt es sich üblicherweise um ein Standardarchivsystem, welches Funktionen zur Datenverwaltung, Zugriffskontrolle und Prozessverbindung zwischen der Kern-Ingestkomponente, der Beweiswerterhaltung sowie dem Access organisiert. Daneben realisiert es i.d.R. in der praktischen Umsetzung bzw. Produktausprägung die Funktionen zur Recherche, Workflow Zugriff, Bestandserhaltung und Systemadministration. Im Repository werden zudem, neben den Volltextindizes die inhaltlichen Metadaten der Unterlagen sowie deren eindeutige AOID für einen späteren Zugriff z.B. für Daten aus Fileshares verwaltet. Alle Zugriffe auf das Cluster Beweiswerterhaltung und Archivspeicher nach Ablage der Daten sollten aus Gründen der Komplexitätsreduktion über das Cluster Datenmanagement erfolgen.

Archivspeicher

Die AIP werden anschließend im Archivspeicher abgelegt und die erzeugte eindeutige AOID der sendenden Geschäftsanwendung sowie dem Repository des LZSP übergeben.

[7] z.B. Geodaten

Im Sinne einer serviceorientierten Architektur bietet sich die Nutzung von Standardspeicher auch für die Langzeitspeicherung auf Basis eines Sicherheitskonzepts nach ISO 27k an, um ein flexibles Daten- und Speichermanagement zu ermöglichen und den Betrieb einer teuren, separaten Infrastruktur, wie dies z.B. für WORM notwendig wäre, zu vermeiden. Die Nutzung von WORM ist aus Sicht der Langzeitspeicherung wenig empfehlenswert, da aufgrund der hochproprietären Speicherung der Daten im WORM, eine immense Abhängigkeit vom jeweiligen Hersteller besteht, was bei teilweise jahrzehntelangen Aufbewahrungsfristen ein unabsehbares Risiko für die Verfügbarkeit der Daten impliziert. Hinzu kommt, die absehbare Datenexplosion bei der Erweiterung von AIP oder der Informations- und Beweiswerterhaltung. [Spi11], [Ko15].

Access (Recherche und Zugriff)

Der Access-Cluster fasst die Module und Funktionen zur Recherche, Zugriff und Darstellung der Daten (sofern dies nicht vollumfänglich durch die Geschäftsanwendung erfolgt) zusammen. In der Praxis handelt es sich meist um Teile des für das Repository eingesetzten Archivsystems. Das Rechtekonzept des Langzeitspeichers beruht auf systembasierten Benutzerrechten. Im Klartext heißt das, dass jedes zugreifende IT-Verfahren nur als Systemnutzer behandelt wird, d.h. es wird die Systemberechtigung geprüft, nicht die Berechtigung des einzelnen personellen Nutzers in der Geschäftsanwendung.

Preservation Planning und Systemadministration

Das Cluster Preservation Planning umfasst i.d.R. Funktionen zur Überwachung der technischen Entwicklung von Formaten, Datenstrukturen, Softwarefunktionen im Sinne der Informations- und Beweiswerterhaltung, so z.B. die Kategorisierung und Pflege von Spezifikationen, das Risikomanagement, die Bewertung eingesetzter Softwaretools oder die Überwachung von Algorithmen. Hinzu kommt die Planung und Steuerung konkreter Maßnahmen wie z.B. Migration von Formaten und Strukturen, die Nachsignatur oder Hasherneuerung.

Das Cluster Systemadministration hingegen umfasst die Fach- und technische Administration des Langzeitspeichers. Beide Cluster werden in der Praxis häufig durch Funktionen des Archivsystems (Repository) abgebildet.

3.2 Mögliche Gesamtarchitektur eines IT-Dienstes zur elektronischen Langzeitspeicherung

Die in Kap. 3.1 beschriebenen Cluster, Module und Funktionen lassen sich zu folgender Gesamtarchitektur eines Langzeitspeicherdienstes zusammenfassen. Es handelt sich um eine Überblicksdarstellung in der Struktur des OAIS-Modells und enthält aus Gründen der Übersichtlichkeit nicht alle Module im Detail.

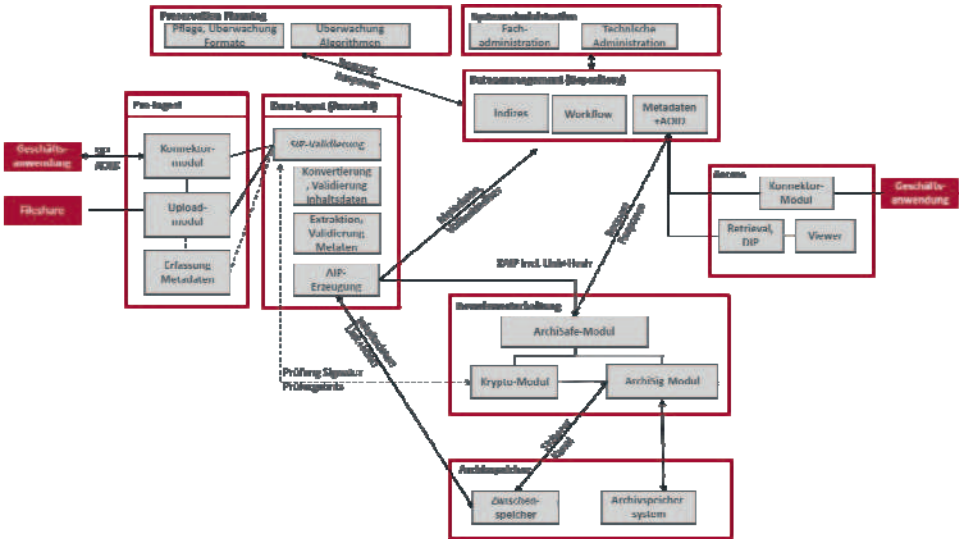

Abbildung 4: Überblick Gesamtarchitektur

Diese Architektur ist ein Beispiel, auf Basis der Projekterfahrungen der Autoren in Behörden, IT-Dienstleistern oder Unternehmen umgesetzt wurde.

4 Rolle eines elektronischen Langzeitspeicherdienstes in einem vertrauenswürdigen Informationsmanagement – Zusammenfassung und Ausblick

Vertrauenswürdigkeit eines Systems oder Unterlagen bedeutet, dass sie das sind, was sie zu sein vorgeben [DIN31644] und sind elementare Grundlage, um bestehenden Dokumentations- und Nachweispflichten erfolgreich nachzukommen [DIN31644 Kommentar]. Ein ordnungsgemäßes Records Management schafft hierfür die fachliche wie technische Basis, eine elektronische Langzeitspeicherung sichert die Authentizität, Integrität, Verkehrsfähigkeit und Nachvollziehbarkeit geschäftsrelevanter Unterlagen und damit deren Vertrauenswürdigkeit bis zum Ablauf auch jahrzehntelanger Aufbewahrungsfristen [ISO-30301], [ISO-15489], [To07], [Ro07]. Das Informationsmanagement einer Behörde oder eines Unternehmens muss sich an der Vertrauenswürdigkeit der Unterlagen messen lassen. Nur wenn diese authentisch und integer sind, können sie als valides Fundament für die Geschäftsprozesse und Entscheidungen dienen. Ein elektronischer Langzeitspeicherdienst ermöglicht den Aufbau der notwendigen technischen Komponenten, Module und Funktionen für alle

relevanten IT-Verfahren. Langzeitspeicherung ist eine Querschnittsaufgabe, die zudem nicht erst bei Abschluss eines Geschäftsvorfalls, sondern wie z.B. bei signierten Dokumenten, Mails oder gescannten Daten bei Beginn des Geschäftsprozesses (sog. frühe beweissichere Speicherung) stattfindet. Der LZSP kann als IT-Dienst insofern für den gesamten Prozess und Lebenszyklus geschäftsrelevanter Unterlagen als vertrauenswürdiger Datenraum dienen – abrufbar für alle angebundenen Geschäftsanwendungen. So kann darüber hinaus z.B. durch die Nutzung der Module des Langzeitspeichers der Eingang von Dokumenten langfristig eindeutig nachgewiesen werden (Eingangszeitstempel via Krypto-Modul und frühe Aufbewahrung), wie dies z.B. bei Versicherungen oder in Behörden realisiert wird. Die Aufbewahrung der Unterlagen in selbsttragenden AIP gewährleistet dabei die Unabhängigkeit von einer bestimmten technischen Plattform und damit Investitionssicherheit (z.B. leichter umsetzbare Migration). Die nachstehende Grafik verdeutlicht dies.

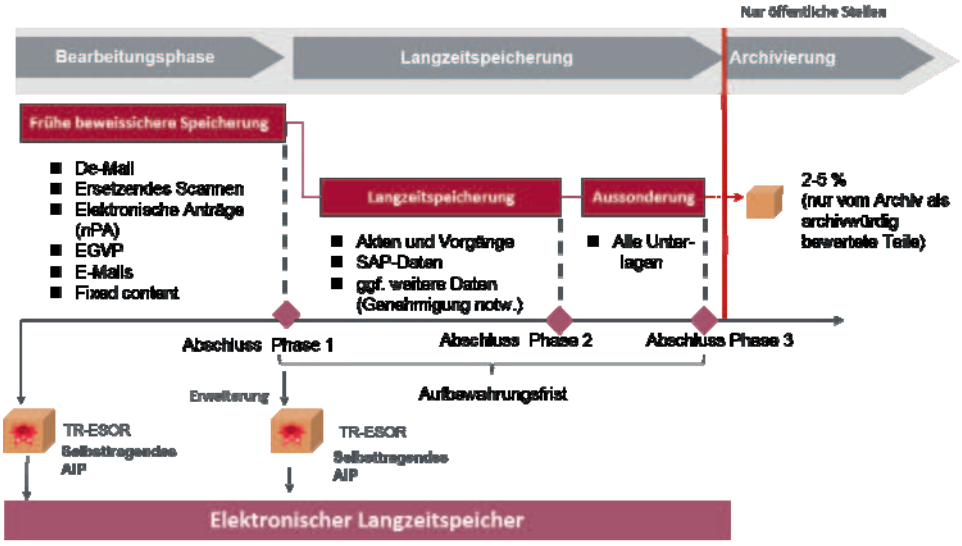

Abbildung 5: Anwendungsbereich des Langzeitspeichers

Im Hinblick auf das absehbar höhere Aufkommen signierter Dokumente im Kontext der neuen [eIDAS]-Verordnung sowie der steigenden Anforderungen an die Sicherheit geschäftsrelevanter Dokumente so z.B. in kritischen Infrastrukturen oder aufgrund der EU-Datenschutzgrundverordnung (vgl. [EU-DSGV]) oder dem IT-Sicherheitsgesetz [ITSG] etc. gewinnt ein elektronischer Langzeitspeicherdienst als sicher Datenraum eines vertrauenswürdigen Informationsmanagement erfolgskritische Bedeutung.

Literaturverzeichnis

[BMWi07] Bundesministerium für Wirtschaft und Technologie (Hrsg.): Handlungsleitfaden zur Aufbewahrung elektronischer und elektronisch signierter Dokumente, Berlin 2007.

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

[DIN31645] DIN 31645:2011 Information und Dokumentation – Leitfaden zur Informationsübernahme in digitale Langzeitarchive. 2011

[DIN31646] DIN 31646:2013 Information und Dokumentation – Anforderungen an die langfristige Handhabung persistenter Identifikatoren (Persistent Identifier). 2013

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

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

[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

[EU-DSGV] 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 (Datenschutz-Grundverordnung)

[EN319122] ETSI EN 319 122 – {1,2}, Electronic Signatures and Infrastructers (ESI); CAdES digital signatures, ETSI Draft (V1.1.0 (2016-02)

[EN319132] ETSI EN 319 132 – {1,2}, Electronic Signatures and Infrastructures (ESI); XAdES digital signatures, ETSI Draft (V1.1.0 (2016-02)

[EN319142] ETSI EN 319 142 – {1,2}, Electronic Signatures and Infrastructeres (ESI); PAdES digital Signatures, ETSI Draft (V1.1.0 (2016-02)

[EN319162] ETSI EN 319 162 – {1,2}, Electronic Signatures and Infrastrucutres (ESI); Associated Signature Containers (ASiC), ETSI Draft (V1.1.0 (2016-02)

[Fisc06] S. Fischer-Dieskau: Das elektronisch signierte Dokument als Mittel zur Beweissicherung, Baden-Baden, 2006.

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

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

[ISO14533] ISO 14533: Processes, data elements and documents in commerce, industry and administration – Long-term signature profiles. 2014

[ISO16363] ISO 16363:2012. Space data and information transfer systems - Audit and certification of trustworthy digital repositories. 2012

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

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

[ITSG] Gesetz zur Erhöhung der Sicherheit informationstechnischer Systeme (IT-Sicherheitsgesetz) vom 17. Juli 2015.

[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

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

[Ko15] U. Korte, S. Schwalm, D. Hühnlein, T. Kusber: Ersetzendes Scannen und Beweiswerterhaltung mit SAP. DACH-Security 2015. S. 72-85. Frechen 2015

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

[Lu12] Schriftgutverwaltung nach DIN ISO 15489-1. Ein Leitfaden zur qualitätssicheren Aktenführung, Hrsg. von Alexandra Lutz c/o Arbeitskreis Schriftgutverwaltung im DIN NABD 15. Berlin 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

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

[Spi11] Stephan Spitz et.al.: Kryptographie und IT-Sicherheit. Grundlagen und Anwendungen. Wiesbaden 2011

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

[To10] Peter M. Toebak: Records Management. Gestaltung und Umsetzung. Baden 2010

[TR-03125] BSI: Beweiswerterhaltung kryptographisch signierter Dokumente (TR-ESOR), TR 03125, V1.2., 2015.

[TR-03125-F] BSI: Anlage F zu TR-03125, Formate und Protokolle, TR-03125, V1.2, 2015.

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