



ArchiSafe Spezifikation

ARS Spezifikation 1.0

Funktionale Anforderungen an eine dauerhafte und rechtssichere elektronische

Ablage

VERSION 1.0

Dokumententitel: ARS Funktionale Anforderungen
Dateiname: 2007-02-12_Std_ARS_1_0_V10.doc
Version: 1.0
Anzahl Seiten: 33
Status: Freigegeben

erstellt am:	02.07.2006	von:	Dr. W. Zimmer
geprüft am:	27.09.2006	von:	T. Schäfer
Geändert am:	27.09.2006	von:	T. Schäfer
Freigegeben am:	12.02.2007	von:	T. Schäfer

Standort: PTB
Verteiler:

Inhalt

0	Versionshistorie	3
0.1	Dokumentverantwortlicher	3
0.2	Verteilerliste.....	3
1	Zielsetzung des Dokumentes.....	4
2	Einführung	7
3	Grundsätzliche Anforderungen an die langfristige Aufbewahrung elektronischer Dokumente.....	8
4	Allgemeine technisch-funktionale Anforderungen	13
5	Allgemeine systemtechnische Anforderungen	21
6	Empfehlungen für die Systemarchitektur	24
6.1	Komponenten und Module.....	24
6.2	Schnittstellen des elektronischen Archiv-Service	27
7	Referenzen	32

0 Versionshistorie

Version	Editor	Datum	Kommentar
0.2	Dr. W. Zimmer	26.06.2006	Entwurf
		02.07.2006	Entwurf
0.22	T. Schäfer	21.07.2006	Überarbeitung
0.23	Dr. W. Zimmer	01.08.2006	Überarbeitung
0.5	Dr. W. Zimmer	03.08.2006	Überarbeitung
1.0	T. Schäfer	12.02.2007	Freigabe

0.1 Dokumentverantwortlicher

Rolle	Name / OE	Bemerkung
Dokumentverantwortlicher	Tobias Schäfer	

0.2 Verteilerliste

Rolle	Name / OE	Bemerkung
Projektleiter PTB	Hr. Tobias Schäfer	
CC DS	Hr. Jobst Biester	
CC VBPO	Fr. Jutta Lautenschlager	
Extern	Hr. Dr. Wolf Zimmer	

1 Zielsetzung des Dokumentes

Dieses Dokument ist eine Spezifikation zur Unterstützung des ArchiSafe Konzepts für die rechtssichere elektronische Langzeitspeicherung von elektronischem Schriftgut. Die Beziehungen zwischen dem ArchiSafe Konzept (**ArchiSafe Recordkeeping Strategy**), den Spezifikationen, die dieses Konzept unterstützen und den ArchiSafe Empfehlungen für die Umsetzung zeigt die folgende Abbildung.

Rechtssichere Schriftgutverwaltung Anforderungen Schlussfolgerungen aus dem DOMEA Organisationskonzept Einführung in ARS	
ARS 1.0 Spezifikation 1: Funktionale Anforderungen an eine dauerhafte & rechtssichere elektronische Ablage	ARS DOMEA Empfehlungen 1: Funktionale Anforderungen an eine dauerhafte, rechtssichere elektronische Ablage
ARS 2.0 Spezifikation 2: ARS XML Datenpakete & Metadatenschema	ARS DOMEA Empfehlungen 2: XML Datenschemata
ARS 3.0 Spezifikation 3: ARS Langzeitdokumentenformate	ARS DOMEA Empfehlung 3: Langzeitdokumentenformate
ARS 4.0 Spezifikation 4: ARS Signaturdaten- & Signaturverifikationsdatenformate	ARS DOMEA Empfehlung 4: Elektronische Signaturen
ARS 5.0 Spezifikation 5: ARS Import- & Exportschnittstellen	ARS DOMEA Empfehlung 5: Import & Export
ARS: ArchiSafe Recordkeeping Strategy	

Abb. 1: ArchiSafe Spezifikationen

Im Einzelnen beschreiben die Spezifikationen und Empfehlungen die folgenden Inhalte:

Einführung in ARS (ArchiSafe Recordkeeping Strategy): Dieses Dokument erläutert das ArchiSafe Konzept aus verwaltungsrechtlicher Sicht und die sich hieraus ergebenden grundsätzlichen Anforderungen und Ziele von ArchiSafe. Die detaillierten funktionalen und technischen Anforderungen und Definitionen werden in fünf Spezifikationen beschrieben.

Spezifikationen: Diese fünf Dokumente spezifizieren die funktionalen und technischen Anforderungen, die den ARS Standard unterstützen. Nutzer und Anwender des ARS Konzeptes sind gehalten, die obligatorischen Anforderungen des vorgeschlagenen Standards einzuhalten und den optionalen Empfehlungen weitestgehend zu folgen.

Die fünf Spezifikationen im Einzelnen sind:

- **Spezifikation 1:** Funktionale Anforderungen an eine dauerhafte und rechtssichere elektronische Ablage. Dieses Dokument beschreibt die allgemeinen und grundsätzlichen Anforderungen und Funktionen, die ein elektronisches, ARS konformes Ablagesystem erfüllen muss, um elektronisches Schriftgut rechtssicher und dauerhaft elektronisch aufbewahren zu können.
- **Spezifikation 2:** ARS Metadaten und ARS XML-Schema. Dieses Dokument spezifiziert und beschreibt die für eine rechtssichere und dauerhafte elektronische Ablage von elektronischem Schriftgut erforderlichen Metadaten (2a) und eine technische Definition des ARS Langzeitspeicherformats (2b).
- **Spezifikation 3:** Dieses Dokument spezifiziert die aus Sicht von ARS zulässigen Dokumentformate, die für eine rechtssichere, dauerhafte elektronische Ablage geeignet sind und von allen ARS konformen Systemen unterstützt werden sollten.
- **Spezifikation 4:** Dieses Dokument spezifiziert die Syntax und Semantik der durch ARS unterstützten elektronischen Signaturen und Signaturverifikationsdaten.
- **Spezifikation 5:** Dieses Dokument beschreibt die Import- und Export-Schnittstellen von ARS konformen Langzeitspeichersystemen.

Empfehlungen: Die ARS Empfehlungen liefern Hintergrundinformationen, erläuterndes Material und Beispiele zur Unterstützung der Standards und zugehörigen Spezifikationen abgeleitet aus dem Fachkonzept und den praktischen Erfahrungen aus der Umsetzungsrealisierung in der Physikalisch-Technischen Bundesanstalt.

Beziehung zwischen den Spezifikationen: Die Zusammenhänge zwischen den einzelnen Spezifikationen verdeutlicht die folgende Abbildung.

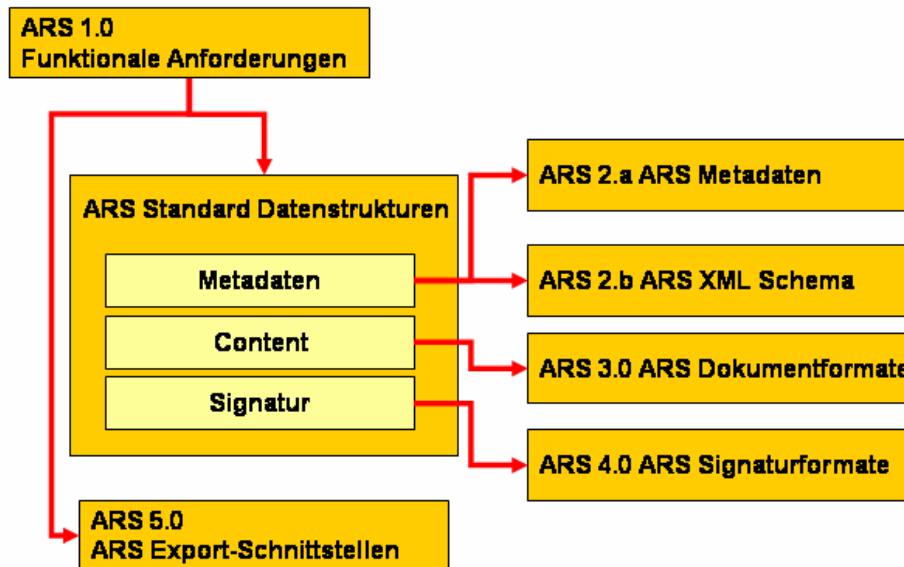


Abb. 2: Beziehungen zwischen den ArchiSafe Spezifikationen

Die Spezifikation 1 (Funktionale Anforderungen) definiert die allgemeinen Anforderungen an einen elektronischen Datenspeicher zur rechtssicheren und dauerhaften Ablage von elektronischem Schriftgut. Insbesondere muss das System in der Lage sein, die abgelegten Dokumente und Daten im Bedarfsfall in einem standardisierten Format zu exportieren.

Die allgemeinen und obligatorischen Merkmale dieses Standarddatenformats (Syntax und Semantik des gesamten Archivpakets und der Metadaten zur Beschreibung des Dokumentkontextes) definiert die Spezifikation 2 (ARS Standard Datenstrukturen), die Spezifikationsdetails der Signaturdaten und Signaturverifikationsdaten beschreibt die Spezifikation 4 (ARS Signaturformate). Die Spezifikation 3 (ARS Langzeitdokumentformate) definiert Dokumentformate die für eine dauerhafte Speicherung von Daten und Informationen in Übereinstimmung mit anerkannten Verwaltungsstandards (DOMEA, SAGA) geeignet sind.

Die Spezifikation 5 (ARS Import- und Export-Schnittstellen) schließlich beschreibt die funktionalen Schnittstellen und Mechanismen für den Datenaustausch.

2 Einführung

Für eine dauerhafte und rechtssichere Aufbewahrung von elektronisch gespeichertem Schriftgut muss sichergestellt sein, dass die Vollständigkeit, Integrität, Authentizität und Verkehrsfähigkeit des elektronischen Schriftguts mindestens für die Dauer gesetzlich vorgeschriebener Aufbewahrungsfristen durch geeignete Maßnahmen gewährleistet werden kann. Der Zweck dieser Spezifikation ist, funktionale Anforderungen an IT-Systeme zu definieren und zu beschreiben, die aus Sicht der verwaltungsrechtlichen Anforderungen für eine dauerhafte und rechtssichere Aufbewahrung von elektronischem Schriftgut durch die Systeme erfüllt werden müssen¹.

Diese Spezifikation gilt im Zusammenhang mit folgenden weiteren Spezifikationen:

- ARS 2.0 : ARS XML Datenpakete und Metadatenschema
- ARS 3.0 : ARS Langzeitdokumentenformate,
- ARS 4.0 : ARS Signaturdaten – und Signaturverifikationsdatenformate und
- ARS 5.0 : ARS Import- und Exportschnittstellen

¹ Eine ausführliche Darstellung der verwaltungsrechtlichen Anforderungen und Rahmenbedingungen ist unter www.archisafe.de zu finden.

3 Grundsätzliche Anforderungen an die langfristige Aufbewahrung elektronischer Dokumente

Für dieses Dokument wird „elektronische Archivierung“ definiert als langfristige, revisions- und rechtssichere Aufbewahrung (Ablage) von elektronischem Schriftgut (Dokumente, Bestands- und Leistungsdaten) nebst den zugehörigen Verwaltungsdaten und Prozessinformationen (Metadaten). Ein „elektronisches Archivsystem“ bezeichnet ein IT-System, das für die dauerhafte, rechts- und revisionssichere Aufbewahrung von elektronischem Schriftgut eingerichtet und verwendet wird.

Recht- und Ordnungsmäßigkeit des Verwaltungshandelns

Die Ablage elektronischer, insbesondere elektronisch signierter Dokumente ist grundsätzlich so auszugestalten, dass die aus rechtlicher Sicht geforderten und vom Betreiber eines elektronischen Langzeit-Speichersystems zu erbringenden Nachweise für die Recht- und Ordnungsmäßigkeit des Verwaltungshandelns noch nach langer Zeit, mindestens aber für die Dauer der gesetzlich festgelegten Aufbewahrungsfrist der jeweiligen Dokumente geführt werden können.

Vollständigkeit und Verkehrsfähigkeit

Die dauerhafte Ablage elektronischer Dokumente muss vollständig und verkehrsfähig erfolgen, so dass der Stand, der Hergang und die Bearbeitung eines elektronisch dokumentierten Verwaltungsvorgangs auch für Dritte aus den abgelegten Unterlagen nachvollziehbar bleiben.

Verkehrsfähige elektronische Aufbewahrung von (digitalen) Daten und Dokumenten bedeutet, dass die zur Aufbewahrung bestimmten Daten und Dokumente für die Dauer gesetzlicher Aufbewahrungsfristen in Form und Inhalt authentisch und vollständig technisch verfügbar und wiedergabefähig, auf zum Zeitpunkt der Wiedergabe dem Stand der Technik entsprechenden elektronischen Geräten, aufbewahrt werden.

Insbesondere elektronisch signierte Dokumente müssen über den gesamten Aufbewahrungszeitraum mit einem vertretbaren zeitlichen und technischen Aufwand zugänglich, darstellbar und vollständig überprüfbar sein. Das bedeutet, sie müssen zusammen mit allen notwendigen Verifikationsdaten und erneuten elektronischen Signaturen in einer beweiskräftigen Form aufbewahrt werden.

tigen Form mindestens für die Dauer der gesetzlich vorgeschriebenen Aufbewahrungsfristen verkehrsfähig gehalten werden.

Da sich Aufbewahrungsfristen aufgrund gesetzlicher Vorgaben ändern können, muss das elektronische Archivsystem grundsätzlich unterschiedliche Verfügbarkeiten gemäß fachspezifischen Informationslebenszyklen gewährleisten können.

Langfristig stabile und standardisierte Nutzdatenformate

Für die rechtssichere und dauerhafte Ablage elektronischer Dokumente müssen langfristig stabile und eindeutig interpretierbare Nutzdatenformate verwendet werden, für die eine nachhaltige Verkehrsfähigkeit über die Dauer der gesetzlichen Aufbewahrungsfristen nach heutigem Wissensstand zumindest vermutet werden kann und deren Spezifikation standardisiert oder mindestens öffentlich zugänglich ist².

Den Empfehlungen von SAGA³ und DOMEA 2.1⁴ folgend kommen dafür heute vor allem ASCII (7-bit), XML, TIFF und PDF (PDF-A) in Frage.

Dort, wo in vorhandenen Fachsystemen eine Umstellung auf langzeitspeicherungstaugliche Formate (noch) nicht möglich ist, ist daher vorzusehen, die Daten unmittelbar vor dem Signieren und / oder der Übergabe in den Langzeitspeicher in die empfohlenen Formate zu konvertieren.

Metadaten und Datenschnittstellen zu Drittsystemen sind, den Empfehlungen von SAGA und DOMEA folgend, grundsätzlich über XML und entsprechende Schemadefinitionen zu beschreiben und zu realisieren.⁵

² Das gilt sowohl für die tatsächlichen Inhaltsdaten als auch für die in aller Regel als Metadaten kodierten Vorgangsdaten und ist eine wichtige Voraussetzung für eine hohe Beweiskraft hinsichtlich des Inhalts elektronischer Dokumente. Ein solches Vorgehen erhält zudem die Aussicht, dass technische Komponenten zur Visualisierung der Dokumente über den Aufbewahrungszeitraum hinaus verfügbar sind und dass eine Formattransformation elektronisch signierter Dokumente vermieden werden kann..

³ SAGA 2.1 – Standards und Architekturen für E-Government Anwendungen, Schriftenreihe KBSt, Bd. 82, Sep. 2005.

⁴ DOMEA Organisationskonzept 2.1, Dokumentenmanagement und elektronische Archivierung im IT-gestützten Geschäftsgang, Schriftenreihe KBSt, Bd. 61, Nov. 2005.

⁵ Ausführlichere Informationen hierzu in den ArchiSafe Spezifikation 2b und 3: XML Schema und Langzeitdokumentformate

Revisionssicherheit

Als „revisionssicher“ wird eine Aufbewahrung elektronischer Daten und Dokumente gemäß dem Konzept papierarmes Büro der KBSt (DOMEA-Konzept) bezeichnet, wenn diese entsprechend den Vorgaben aus §§ 239, 257 HGB, §§ 146, 147 AO und der Grundsätze ordnungsgemäßer IT-gestützter Buchführungssysteme (GoBS) sicher, unverändert, vollständig, ordnungsgemäß, verlustfrei reproduzierbar und datenbankgestützt recherchierbar sind.

Die Definition der Revisionssicherheit geht über eine rein technische Implementierung hinaus und betrifft vielmehr das Gesamtverfahren im Umgang mit den archivierten Dokumenten. Dies umfasst insbesondere alle Verfahren zur Verarbeitung, Speicherung, Ausgabe bis hin zur Vernichtung der verwalteten Dokumente. Für eine revisionssichere elektronische Archivierung wird daher gefordert, dass beliebige digitalisierte Dokumente, sowie die zugehörigen Metadaten

- sicher
- unveränderbar
- vollständig
- ordnungsgemäß
- verlustfrei reproduzierbar und
- eindeutig recherchierbar

verwaltet werden.

Behördliche Unterlagen müssen bei allen verwendeten Verfahren den Kriterien der Vollständigkeit, der Integrität, der Authentizität sowie der Nachvollziehbarkeit und der Rechtmäßigkeit des Verwaltungshandelns genügen. Hierbei ist insbesondere zu beachten, dass aufgrund der Anforderungen an die revisionssichere Verwaltung von Dokumenten diverse Aspekte bei der Implementierung zu berücksichtigen sind. Neben der Erfüllung der allgemeinen, gesetzlichen Anforderungen, in der Hauptsache festgeschrieben durch die Abgabenordnung (AO), das Handelsgesetzbuch (HGB), die Grundsätze ordnungsgemäßer IT-gestützter Buchführungssysteme (GoBS), die Grundsätze zum Datenzugriff und zur Prüfbarkeit digitaler Unterlagen (GDPdU) sowie dem Signaturgesetz (SigG), müssen unter anderem auch die Einhaltung der verschiedenen Vorschriften, Verordnungen und Dienstanweisungen der jeweiligen Behörde oder Verwaltungseinheit gewährleistet sein und entsprechend realisiert werden. Darüber hinaus ist es erforderlich, Gesetzesgrundlagen wie das Bundesdaten-

schutzgesetz (BDSG) in den angewandten Verfahren zur elektronischen Archivierung anzuwenden (Löschen von nicht mehr benötigten Daten).

Nachweis der Revisionsicherheit

Für den Betrieb eines revisionsssicheren elektronischen Archivsystems ist die Prüfung und Bescheinigung der Ordnungsmäßigkeit des Verfahrens zur elektronischen Archivierung (Revisionsicherheit) zum dauerhaften Nachweis der Vollständigkeit, der Echtheit, der Unverfälschtheit und Verfügbarkeit der elektronisch abgelegten Dokumente auf der Grundlage einer ausführlichen System- und Verfahrensdokumentation durch einen unabhängigen Gutachter erforderlich. Die System- und Verfahrensdokumentation muss einem sachverständigen Dritten (Gutachter) in angemessener Zeit einen Überblick über sämtliche Aspekte des Verfahrens ermöglichen.

Erhalt des Rechtszustandes

Elektronische Daten sind grundsätzlich geeignet, im Rechtsverkehr Beweiskraft für das Verwaltungshandeln zu erbringen. Die Beweiskraft elektronischer Daten wird maßgeblich davon bestimmt, wie der Nachweis gelingt, dass die Dokumente seit ihrer Erstellung oder Aufbewahrung nicht mehr verändert worden sind (Integrität) und in Form und Inhalt vom bezeichneten Aussteller herrühren (Authentizität).

In der elektronischen Kommunikation werden Integrität und Authentizität vor allem über qualifizierte elektronische Signaturen gewährleistet. Das System muss daher in der Lage sein, neben den eigentlichen Nutzdaten gegebenenfalls auch Signatur- und Signaturverifikationsdaten langfristig aufzubewahren und rechtskräftig zu erhalten. Hierzu gehört die Verwendung eindeutig interpretierbarer, langfristig stabiler und standardisierter Signaturdatenformate ebenso wie die rechtzeitige und beweiskräftige Signaturerneuerung.

Signaturgesetzkonformität

Die Erzeugung, Prüfung und Speicherung von elektronischen Signaturen, respektive elektronisch signierter Dokumente muss gesetzeskonform erfolgen. Das betrifft insbesondere:

- Den Einsatz qualifizierter und akkreditierter Signaturen
- Die gesetzeskonforme Signaturerneuerung
- Die gesetzeskonforme Verifikation elektronischer Signaturen

Signaturerneuerung

Elektronische Signaturen müssen rechtzeitig vor Ablauf der Sicherheitseignung der verwendeten kryptographischen Algorithmen gemäß den Vorgaben des Signaturgesetzes erneuert werden. Die Signaturerneuerung sollte weitgehend automatisch und wirtschaftlich erfolgen. Für die Signaturerneuerung wird daher empfohlen, ein effizientes und performantes Verfahren auf der Basis des ArchiSig-Prinzips, www.archisig.de, bereit zu stellen. Dabei ist nachweislich sicher zu stellen, dass durch das Verfahren die notwendigen gesetzlichen Vorschriften und Auflagen, insbesondere des SigG bzw. der SigV (speziell §17 SigV) erfüllt werden.

Daten- und Geheimnisschutz

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

Spezielle, den Daten- und Geheimnisschutz betreffende Anforderungen an elektronische Langzeitspeicher müssen mit einem wirtschaftlich vertretbaren Aufwand erfüllbar sein. Die Dokumente müssen auf Anforderung auch verschlüsselt abgelegt werden können.

Soweit für bestimmte Zwecke, wie z.B. die Einstellung in einen elektronischen Langzeitspeicher oder die Transformation von Daten, Signaturen des (technischen) Archivars benötigt werden, sollten diese ggf. auch unter einem Pseudonym möglich sein.⁶

⁶ Pseudonym-Zertifikat i.S. des SigG

4 Allgemeine technisch-funktionale Anforderungen

Eine rechtssichere Ablage muss zu jedem Zeitpunkt aus dem Fachverfahren und /oder vorgelagerten Prozessen heraus möglich sein

Um ein flexibles und skalierbares System bereit zu stellen, soll es dem Bearbeiter vor Ort möglich sein, geschäftsrelevante Dokumente zu jedem Zeitpunkt im elektronischen Langzeitspeicher abzulegen. Dies gilt insbesondere für elektronisch signierte Dokumente, die rechtssicher abgelegt werden müssen.

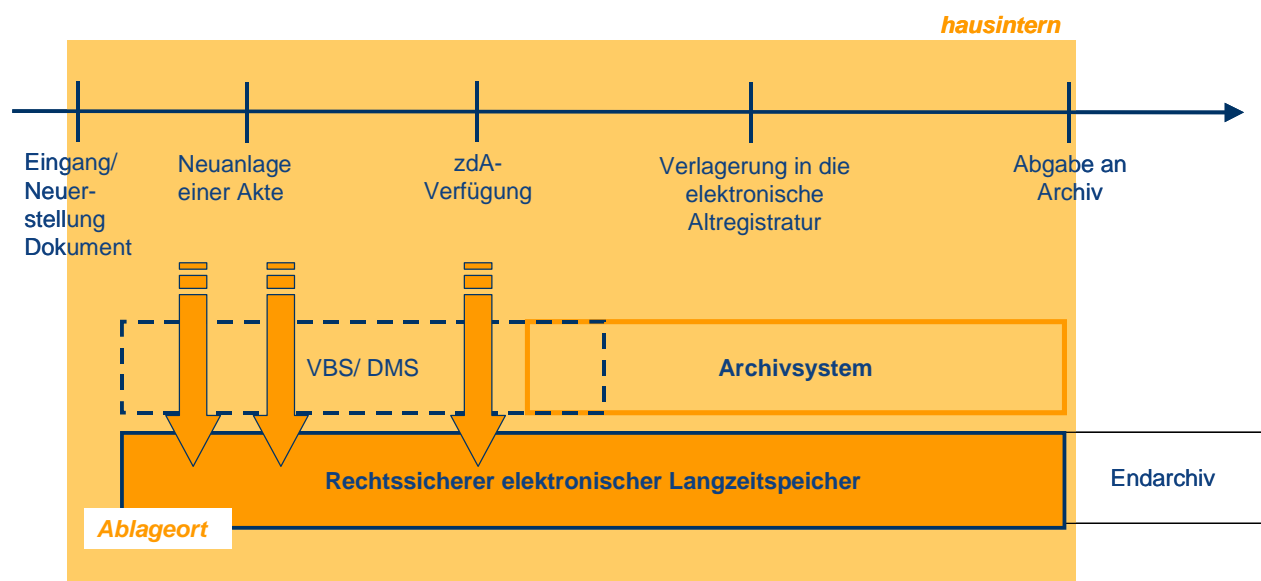


Abb. 3: Parallelität von Vorgangsbearbeitungssystem (VBS) und elektronischem Langzeitspeicher

Vor dem Hintergrund, dass die Ablage elektronisch signierter Dokumente in einem Fachverfahren in der Regel nicht den Anforderungen an die Erhaltung der Beweiskraft genügen kann, muss die beweiskräftige Ablage kritischer Dokumente noch während der Bearbeitung eines Vorgangs gewährleistet werden können. Dies kann manuell oder automatisch (Batch-Verfahren) erfolgen.

Zugriff auf den elektronischen Langzeitspeicher

Der Zugang und Zugriff auf den elektronischen Langzeitspeicher zu Zwecken der Ablage, der Recherche oder des Aufrufs abgelegter Dokumente sollte in jedem Falle nachweisbar über definierte Schnittstellen und ausschließlich aus dem Fachsystem erfolgen. Unberechtigte Zugriffe sind durch das System zuverlässig und nachweislich zu verhindern.

Vorgangs- oder prozessbezogene Metadaten, die für einen permanenten operativen Zugriff benötigt werden, werden grundsätzlich im Fachverfahren angelegt und verwaltet. Unabhängig davon sollte das elektronische Archivsystem (auf Anforderung) in der Lage sein, aus archivierten Metadaten eine Indexdatenbank zur Unterstützung von Recherchefunktionen aus dem Fachverfahren zur Verfügung zu stellen.

Dokumentkennung

Für im Langzeitspeicher abgelegte Dokumente muss das elektronische Archivsystem eine systemweit eindeutige Dokumentkennung (Dokument-ID) zur Verfügung stellen können, die im Fachverfahren als Referenz auf die archivierten Daten verwaltet wird. Damit ist auch das Fachverfahren grundsätzlich das führende System, aus dem heraus die Ablage, respektive der Aufruf abgelegter Dokumente, per Request und Übergabe der Dokumentkennung möglich sind.

Das elektronische Archivsystem quittiert dem Fachverfahren die ordnungsgemäße Ablage des Dokuments.

Einsatz sicherer Signaturanwendungen und Verwendung elektronischer Signaturen mit ausreichend hohem Sicherheitsniveau

Hierunter sind folgende bereits in ArchiSig formulierte Anforderungen zu subsumieren⁷:

Einsatz sicherer Signaturanwendungskomponenten

Bei der Langzeitspeicherung elektronisch signierter Dokumente kann nur der Beweiswert erhalten werden, der von Anfang an besteht. Maßgeblich für den Beweiswert elektronisch signierter Dokumente ist die Qualität der eingesetzten Signaturen und Signaturanwendungskomponenten. Daraus folgt:

⁷ ArchiSig – Beweiskräftige und sichere Langzeitarchivierung digital signierter Dokumente. Anforderungskatalog Version 2.0, Dezember 2002.

- Für die Signaturerstellung und Signaturprüfung sollten möglichst geprüfte und bestätigte Signaturanwendungskomponenten eingesetzt werden.
- Für die Visualisierung der eingesetzten Datenformate sollten standardisierte, besser noch, geprüfte und bestätigte Präsentationskomponenten zur Verfügung stehen.
- Die IT-Fachanwendungen, respektive die IT-Laufzeitumgebungen sollten über nachweislich wirksame Zugangs- und Zugriffskontrollen verfügen.

Verwendung langfristig stabiler Signaturdatenformate

Um die Prüfbarkeit und die Interoperabilität elektronisch signierter Dokumente über die verwaltungsrechtlichen Aufbewahrungsfristen hin zu gewährleisten, sollten bei der Signaturerstellung standardisierte Signaturdatenformate verwendet werden. Dies betrifft neben den eigentlichen Signaturdatenformaten auch die Formate von Zertifikaten, Sperrlisten und Zertifikatsstatusabfragen. Dabei sollte die Kompatibilität mit den Normen und Empfehlungen von ISIS-MTT und des Signaturlbndnisses sichergestellt sein.⁸

Verwendung akkreditierter Signaturen

§ 126a BGB verlangt zur Erfllung der gesetzlichen Schriftform, sofern diese elektronisch abgebildet werden soll, die Verwendung von qualifizierten Signaturen nach dem Signaturgesetz. Die Beweiseignung kann durch den Einsatz akkreditierter Signaturen noch gesteigert werden, da in diesem Fall auf die fr die Nachweisfhrung erforderliche Dokumentation bei den akkreditierten Zertifizierungsdiensteanbietern langfristig zugegriffen und zudem die Vermutung ihrer technisch-organisatorischen Sicherheit geltend gemacht werden kann (§ 15 Abs. 1 Satz 4 SigG).

Nachweis eines mglichst authentischen Signierzeitpunktes durch Zeitstempel

Ffr den Nachweis, dass die einer elektronischen Signatur zugrunde liegenden bzw. beigefgten Zertifikate zum Signaturzeitpunkt gltig und nicht gesperrt und die eingesetzten kryptographischen Algorithmen und Parameter zum Signaturzeitpunkt sicher-

⁸ ISIS-MTT Specification, Optional Profile, SigG-Profile, Version 1.1, Mgrz 2004.

heitsgeeignet waren, sollte möglichst zeitgleich zur Signaturerstellung und / oder Signaturprüfung ein elektronischer Zeitstempel eingeholt und mitgespeichert werden. Die Qualität des Zeitstempels muss dabei mindestens der Qualität der Signatur entsprechen.

Bereitstellung und Integration notwendiger Verifikationsdaten

Die für eine spätere Signaturverifikation erforderlichen Verifikationsdaten sollten unmittelbar nach der Signaturerstellung und / oder -prüfung beschafft und in das Dokument, respektive das „Archivobjekt“ in langfristig verkehrsfähiger Form reproduzierbar integriert werden. Die Gültigkeitsprüfung muss umfassend und vollständig sein. Sie muss sich auf die gesamten Zertifikatsketten (Signaturzertifikate des Users, der Zertifizierungsstelle und der Wurzelzertifizierungsinstanz) sowie alle Verifikationsdaten und Zeitstempel beziehen. Sämtliche Prüfschritte sollten in übersichtlicher Weise und nachvollziehbar protokolliert werden können.

Wahl des Signaturzeitpunktes

Bei der Verifikation elektronischer Signaturen sollte der Signaturzeitpunkt grundsätzlich aus einem vertrauenswürdigen Zeitstempel der Signatur entnommen werden können. Ist dieser nicht vorhanden, können auch andere authentische Zeitangaben verwendet werden.

Sicherung signierter und unsignter Dokumente

Neben elektronisch signierten Dokumenten sollten auch die Authentizität und Integrität nicht signierter Daten ab dem Zeitpunkt der Überführung in einen elektronischen Langzeitspeicher automatisch durch elektronische Signaturen und qualifizierte Zeitstempel gesichert werden können.

Löschen nicht benötigter Daten

Mit Blick auf zu erfüllende datenschutzrechtliche Bestimmungen oder Aufbewahrungsfristen muss eine vollständige und explizite Löschung (i. S. einer unwiederbringlichen Vernichtung) einzelner elektronisch signierter Dokumente und / oder Daten einschließlich der zugehörigen Signaturen und Verifikationsdaten vor Ablauf gesetzlich vorgeschriebener Aufbewahrungs-

fristen mit einem wirtschaftlich vertretbaren Aufwand möglich sein. Die Beweiskraft der im Langzeitspeicher verbleibenden Dokumente muss dabei erhalten bleiben.

Um die Nachvollziehbarkeit des Handelns zu gewährleisten, muss der Löschvorgang von Dokumenten, Signaturen oder Verifikationsdaten protokolliert werden können.

Integrationsfähigkeit und Interoperabilität

Die Integrierbarkeit des elektronischen Langzeitspeichers in bestehende Informationssysteme (Fachanwendungen) sowie die Interoperabilität der verwendeten Nutzdaten- und Signaturdatenformate muss mindestens für die Dauer der gesetzlich vorgeschriebenen Aufbewahrungsfristen sichergestellt werden können.

Das elektronische Archivsystem sollte daher die lose Kopplung von Archivsystem und Fachanwendungen auf der Basis transparenter und standardisierter Schnittstellen (Services) realisieren, um auf diese Weise von Anfang an die Anbindung weiterer Fachverfahren auf der Basis einer service-orientierten Architektur konzeptionell und softwaretechnisch zu unterstützen.

Durch die vorgeschlagenen technischen Lösungen der Langzeitspeicherung dürfen insbesondere keine Behinderungen entstehen für

- den Wechsel von Datenformaten in Fachverfahren und
- den Austausch von Anwendungssystemen oder -komponenten.

Datenschnittstellen

Die von der KBSt veröffentlichten „Standards und Architekturen für E-Government-Anwendungen (Vers. 2.1, Schriftenreihe der KBSt, Bd. 82, vom Sept. 2005) empfehlen Metadaten und Datenschnittstellen zu Drittsystemen grundsätzlich über XML und entsprechende Schemadefinitionen zu beschreiben und zu realisieren.

ArchiSafe empfiehlt daher für die Kommunikation zwischen den Fachverfahren und dem Archiv die Verwendung von XML als Beschreibungssprache für in sich abgeschlossene Archivobjekte, die sich über ein vereinbartes XML-Schema selbst beschreiben und so alle wichtigen und hinreichenden Informationen enthalten, die man für einen späteren Zugriff benötigt.

Die Beschreibung und Kapselung der zu archivierenden Nutz- und Metadaten durch ein gültiges XML-Schema verspricht folgende Vorteile:

- Das Archivobjekt kann vor der Übergabe an den elektronischen Langzeitspeicher auf syntaktische Richtigkeit evaluiert werden.
- Fachverfahrensspezifische Erweiterungen der Metadaten sind mit wenig Aufwand durch Erweiterung und / oder Einschluss zusätzlicher XML-Schemata möglich.

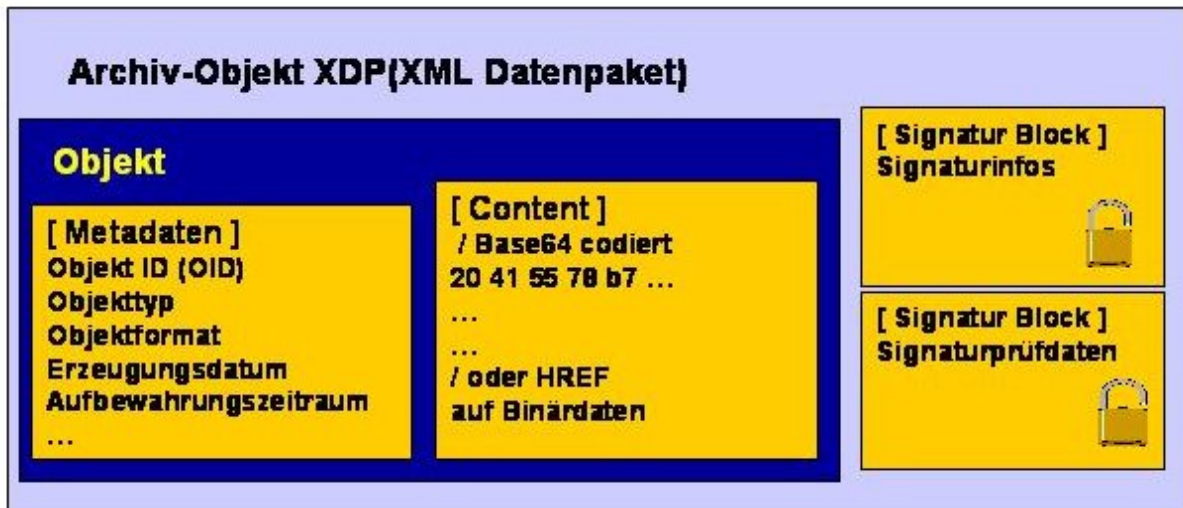


Abb. 4 : Schematische Darstellung eines XML Archivobjektes

Im einfachsten Fall besteht ein solches Archivobjekt (Abb. 4) neben einer Versionsangabe und der Angabe der zugeordneten XML-Schemadatei, aus einem Block, der die Inhaltsdaten enthält (Objektblock) und gegebenenfalls aus einem oder mehreren Signaturblöcken. Der Objektblock kann selbst wieder ein oder mehrere in XML eingebettete Dokumente enthalten. Jeder Block enthält als Einleitung Metadaten, in denen beispielsweise eine Dokumentkennung (Dokument-ID), eine Beschreibung des Dokumentes und seiner Herkunft abgelegt werden können.

Für das Dokument selbst ist als Standard PDF-A (ISO 19005) vorgesehen, das um in XML eingebettet werden zu können, zunächst in ein Textformat (Base64) konvertiert wird.

Falls das Dokument aus Performancegründen nicht in die XML-Datei eingebettet werden soll, muss der Objektblock eine systemweit eindeutige Referenz auf die zusätzlich archivierte Binär-Datei erhalten. Darüber hinaus können die eigentlichen Inhaltsdaten (Dokumentinhalte) auch in mehreren unterschiedlichen Formaten abgelegt werden.

Zugriffsmethoden (Servicekontrakte)

Folgende Zugriffsmethoden müssen durch ein elektronisches Archivsystem grundsätzlich unterstützt werden:

- Ablegen von Archivobjekten im Archiv, inklusive
- Übergabe und Verwaltung einer Aufbewahrungsfrist
- Übergabe und Verwaltung einer eindeutigen ArchivObjekt-ID (archive unique identifier, AUID) für das archivierte Objekt.
- Rückgabe eines Archivobjektes (nach Übergabe einer AUID).
- Löschen von Objekten (Dokumenten und Metadaten) aus dem Archiv (nach Übergabe einer AUID) und Rückgabe des Status der Löschung. Der Löschvorgang wird grundsätzlich vom Fachverfahren initiiert.
- Übergabe und Prüfung einer AUID

Eine vollständige und explizite Löschung (i. S. einer unwiederbringlichen Vernichtung) von archivierten Objekten muss auch vor Ablauf der bei der Archivierung übergebenen Aufbewahrungsfrist möglich sein. Um die Nachvollziehbarkeit des Handelns zu gewährleisten, muss der Löschvorgang protokolliert werden können.

Skalierbarkeit

Das elektronische Archivsystem muss skalierbar und dem Bedarf der Behörden entsprechend ausbaufähig sein.

Grundsätzlich müssen die vorgeschlagenen technischen Konzepte und Lösungen

- den Betrieb mandanten- und instanzenfähiger Lösungen und
- den Einsatz kryptographischer Sicherheitstechniken, wie qualifizierte elektronische Signaturen, qualifizierte elektronische Zeitstempel und Verschlüsselung

unterstützen. Hierzu gehört:

- in Abhängigkeit vom Dokumenttyp und dem jeweiligen Aufbewahrungszweck müssen für die Archivobjekte spezifische Parametrisierungen (wie Aufbewahrungsdauer, Zugriffsberechtigungen, zugeordnetes Fachverfahren, sowie die Ablage von Verifikations- und / oder Prozessdaten etc.) möglich sein,
- spezielle Anforderungen, wie etwa die Integritätssicherung logisch zusammengehöriger Dokumente (z.B. Vollständigkeit von Akten), müssen auf Anforderung berücksichtigt werden können.

Mandantenfähigkeit

Das elektronische Archivsystem muss „mandantenfähig“ sein, d. h. verschiedene Teilarchive/Subarchive verwalten können, um auf diese Weise die Aufbewahrung elektronischer Dokumente und Daten logisch und physikalisch voneinander trennen zu können.

Migrationsfähigkeit

Die Archivlösung muss für den Fall der Ablösung oder Erneuerung von Hard- bzw. Softwarekomponenten geeignete Migrationsszenarien unterstützen, so dass die rechts- und revisions-sichere Langzeitverfügbarkeit der archivierten Daten durch das Archivsystem jederzeit zuverlässig gewährleistet werden kann.

5 Allgemeine systemtechnische Anforderungen

Für den Betrieb eines rechts- und revisionssicheren elektronischen Archivdienstes muss das System folgende grundsätzlichen nicht-funktionalen Anforderungen erfüllen:

- hohe Skalierbarkeit und Flexibilität
- gute Wartbarkeit, Änderbarkeit und Erweiterbarkeit
- gute Analysierbarkeit und Testbarkeit,
- hohe Fehlertoleranz und Stabilität,
- hohe Sicherheit und Zuverlässigkeit,
- modularer Aufbau des Systems
- einfacher Betrieb und Administration
- anerkannte Standards in den Komponenten, Diensten und Schnittstellen
- möglichst vollständig automatisierte Installation
- Plattformunabhängigkeit.

Allgemeine Sicherheits- und Betriebsanforderungen

Die Sicherheit und Verfügbarkeit der elektronischen Archivierung wird nicht allein durch die Speichermedien und die kryptographischen Maßnahmen bestimmt. Das gesamte Archivierungsverfahren muss abgesichert und in einer Verfahrensdokumentation ausführlich beschrieben sein. Hierzu gehört auch die detaillierte Beschreibung der für den sicheren und stabilen Betrieb einzuhaltenden Betriebsbedingungen. Darüber hinaus müssen alle Prozesse in dem Archivsystem gegen Unbefugte besonders gesichert sein. Durch Betriebsstörungen dürfen keine Inkonsistenzen oder Datenverluste auftreten.

Zugriffschutz und Benutzerverwaltung

Der Zugriff auf das Archivsystem sollte ausschließlich aus den Fachanwendungen auf der Basis der hier hinterlegten Zugriffsrechte erfolgen. Die Benutzerverwaltung für die Administration des Speichersystems muss eine missbräuchliche und unautorisierte Benutzung des Systems ausschließen. Sämtliche Zugriffe sind aussagekräftig zu protokollieren.

Betriebsbedingungen

Für das elektronische Archivsystem ist eine ausführliche Dokumentation der einzuhaltenden Betriebsbedingungen sowie der Wartungsaufgaben und Wartungsintervalle zu erstellen. Die Inhalte dieser Dokumentation sind in der Regel Bestandteil der anzufertigenden Betriebs- handbücher und eines Schulungskonzeptes.

Datensicherung

Die Speicherung der Archiv-Daten sollte auf mindestens zwei hochperformanten Plattensub- systemen an zwei unterschiedlichen Standorten erfolgen.

In Abhängigkeit von den Anforderungen an die Verfügbarkeit der Daten und Systeme emp- fiehlt es sich, das elektronische Archivsystem auch bei laufender Datensicherung verfügbar zu halten. Für eine zusätzliche Sicherung der Archiv-Daten sind ggf. zwei Tape-Libraries an jeweils unterschiedlichen Standorten (auch remote) vorzuhalten.

Restart

Unter „Restart“ wird der konsistente Wiederanlauf nach einer Betriebsstörung verstanden. Bei einer Betriebsstörung darf maximal das letzte, noch nicht archivierte Dokument verloren gehen. Batch-Aufträge müssen konsistent und ohne doppelte Speicherung von Dokumenten erneut aufsetzbar sein. Für den Wiederanlauf des elektronischen Archiv-Systems nach ei- nem eventuell eingetretenen Backup-Fall (Datenbank) bzw. einem Disaster-Recovery der Objekt-Daten sind geeignete Mittel zur Verfügung zu stellen, die die Integrität des Systems gewährleisten und eine Rückkehr in den Normalbetrieb in einem wirtschaftlich vertretbaren Zeitraum erlauben.

Recovery

Zur Gewährleistung der Revisionssicherheit muss das angebotene System über eine Reco- veryfunktion zur Wiederherstellung des Archivsystems einschließlich einer ggf. vorhandenen Indexdatenbank von den Speichermedien verfügen. Dabei muss ein Teilrecovery für die Konsistenzsicherung und Wiederherstellung eingegrenzter Daten- bzw. Speicherbereiche und der Indexdatenbank und ein Vollrecovery als Absicherung für einen Katastrophenfall möglich sein.

Performante und Speicherplatz sparende Archivierung und Kompression

Das elektronische Archivsystem sollte von Anfang an eine performante und Speicherplatz / Kosten sparende Archivierung unterstützen.

Um den Speicherplatz wirtschaftlich nutzen zu können, sollte das System über die Möglichkeit der Datenkomprimierung verfügen. Aus Gründen der Rechts- und Revisionsicherheit, insbesondere für elektronisch signierte Dokumente, dürfen jedoch ausschließlich verlustfreie Kompressionsverfahren zum Einsatz kommen.

Leistungseigenschaften des eArchiv-Service

Die Leistungsfähigkeit des elektronischen Archivsystems sollte durch folgende Parameter (Key Performance Indikatoren) qualifiziert werden:

- Maximale Schreibgeschwindigkeit für Objekte mit einer durchschnittlichen Größe von 50 kB, 100 kB und 300 kB für je ein Objekt bzw. 1000 Objekte im Block;
- Anzahl gleichzeitiger Lesezugriffe pro Zeiteinheit für Archivobjekte mit einer mittleren Datengröße von 50 kB, 100 kB, 300 kB und jeweils 1 Mio, 10 Mio, 20 Mio und 50 Mio Objekten im Archiv;
- Anzahl gleichzeitiger Schreibzugriffe pro Zeiteinheit für Archivobjekte mit einer mittleren Datengröße von 50 kB, 100 kB, 300 kB und jeweils 1 Mio, 10 Mio, 20 Mio und 50 Mio Objekten im Archiv;
- Dauer eines Lesezugriff im Mittel für Archivobjekte mit einer mittleren Datengröße von 50 kB, 100 kB, 300 kB und jeweils 1 Mio, 10 Mio, 20 Mio und 50 Mio Objekten im Archiv;
- Größe des Speicherplatzbedarfs für Nettodatenvolumina von 20 TB, 50 TB oder 100 TB;

6 Empfehlungen für die Systemarchitektur

In Anbetracht der vielfältigen, denkbaren Einsatzszenarien und Anforderungen empfiehlt ArchiSafe ein elektronisches Archivsystem auf der Basis einer stringenten service-orientierten Architektur zu implementieren, die sich vor allem durch lose Kopplung der Systemkomponenten und die Verwendung offener und standardisierter Schnittstellen auszeichnet.

6.1 Komponenten und Module

Ein solcher elektronischer Archiv-Dienst sollte insbesondere folgende Komponenten und Dienste bereitstellen respektive miteinander verbinden:

Diverse Fachverfahren, resp. VBS / DMS als Plattform und führende Systeme zur Dokumentenverwaltung und Vorgangsbildung

Die Fachverfahren initiieren den Request für die Ablage im elektronischen Langzeitspeicher und verwalten die vom Langzeitspeichersystem erzeugten Dokumentkennungen für die im Langzeitspeicher abgelegten Dokumente, respektive Akten oder Vorgänge. Hierzu gehört, die Dokumentkennungen gespeicherter Dokumente mit den für die operative Vorgangsbearbeitung vorgehaltenen Dokumentinstanzen zu verknüpfen.

Die Fachanwendungen erzeugen auch mittels XML-Schnittstelle die im Langzeitspeicher abzulegenden XML-Archivobjekte auf der Basis spezifizierter und vereinbarter XML-Schemas.

Eine einheitliche Archivschnittstelle

Die Fachverfahren kommunizieren mit dem elektronischen Langzeitspeicher über eine einheitliche Archiv-Schnittstelle (Archiv-Service) zur Übergabe der zu archivierenden Objekte (Dokumente, Akten, Vorgänge) an die Langzeitspeicherung.

Die Archivschnittstelle (der Archiv-Service, i. S. eines „Archiv-Hubs“) zur Übergabe von elektronischem Schriftgut aus den Fachanwendungen an das Langzeitspeichersystem wird in einer systemunabhängigen Middleware abgebildet. Der Archiv-Service evaluiert und prozessiert auf der Grundlage standardisierter Zeichensätze und Datenformate, sowie syntaktischer und semantischer Vereinbarungen für die Strukturen der im Langzeitspeicher abzulegenden Datenobjekte. Der Archiv-Service fordert darüber hinaus gegebenenfalls kryptographische

Funktionen wie Signaturen, Zertifikatsprüfungen und Zeitstempel an und sollte zumindest XML-Formate auf der Basis definierter XML-Schemata verarbeiten können.

Die Kommunikationseröffnung mit dem Archiv-Service aus den Fachanwendungen erfolgt in fachspezifischen Serviceeintrittspunkten (Service-Adaptoren). Die Service-Adapter eröffnen und steuern die Kommunikation mit dem Archiv-Service auf der Grundlage vereinbarter Protokoll- und / oder Nachrichtenstandards.

Im Kern besteht der Archiv-Service aus einem XML Prozessor mit definierten Schnittstellen (Kommunikationskanälen) zu den Fachverfahren und zum elektronischen Langzeitspeicher. Darüber hinaus sollte der Archiv-Service die Anbindung zusätzlicher Services, wie beispielsweise einem Signaturdienst (zur Erzeugung und / oder Prüfung elektronischer Signaturen) und einem Zeitstempeldienst ermöglichen.

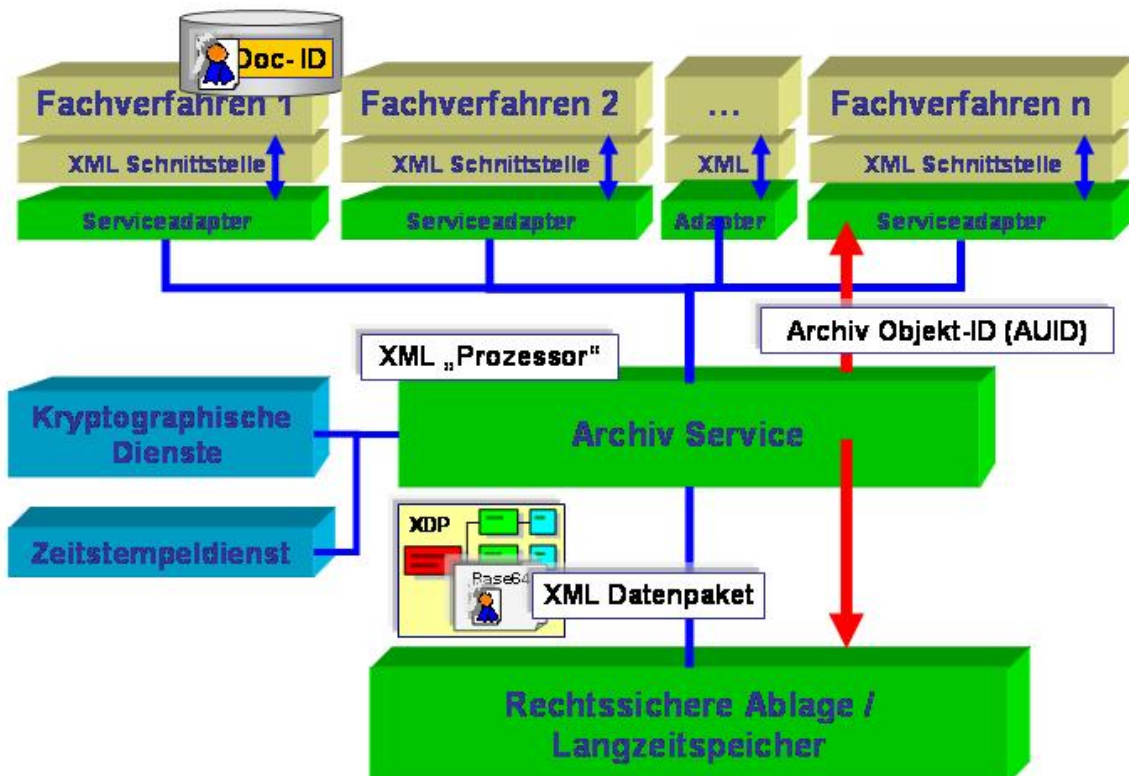


Abb. 5: Service-Orientierte Architektur des elektronischen Archivs (Übersicht)

Kryptographische Dienste zur Erstellung und Verifikation von elektronischen Signaturen

Kryptographische Dienste signieren auf Anforderung durch die Fachverfahren die in den elektronischen Langzeitspeicher einzustellenden Dokumente oder versehen sie mit einem Zeitstempel. Die kryptographischen Dienste verifizieren zudem auf Anforderung durch das Fachverfahren die Signaturen und Zertifikate signierter Dokumente und stellen der Speicherschnittstelle die Verifikationsdaten zur Verfügung.

Für den Fall, dass die Signaturprüfung abschlägig beschieden wird, soll die Ablage im Langzeitspeicher nicht möglich sein.

Ein Zeitstempeldienst

Die Übergabe an den elektronischen Langzeitspeicher kann optional mit einem Zeitstempel für die zu speichernden Dokumente kombiniert werden. Darüber hinaus wird ein qualifizierter Zeitstempeldienst für die Signaturerneuerung elektronisch qualifiziert signierter Dokumente nach § 17 SigV benötigt.

Für den Einsatz kryptographischer Komponenten (resp. Signaturanwendungskomponenten) ist in der Regel eine Bestätigung nach SigG für diese Komponenten Voraussetzung.

Ein rechts- und revisionssicheres Langzeitspeichersystem

Im Backend liegt schließlich das elektronische Langzeitspeichersystem, in das grundsätzlich nur „Original“-Dokumente nebst den zugehörigen Vorgangsmetadaten abgelegt werden sollen. Parallel hierzu werden gegebenenfalls Kopien der Dokumente und Metadaten zum Zwecke der Vorgangsbildung und Vorgangsbearbeitung weiterhin im Fachverfahren vorgehalten. Über die Verwaltung eindeutiger Dokumentkennungen (AUID) stellt das Langzeitspeichersystem sicher, dass zu jedem Zeitpunkt aus dem Fachverfahren heraus in wirtschaftlich vertretbaren Zeiträumen auf die abgelegten „Originale“ zugegriffen werden kann.

Dieses Vorgehen garantiert die rechtssichere Ablage von „Original“-Dokumenten, ohne das Langzeitspeichersystem mit vorgangsspezifischen Logiken zu überfrachten.

Ein Such- und Darstellungsdienst (Viewer, optional)

Um einen vom Fachverfahren unabhängigen Zugriff auf den Langzeitspeicher zu ermöglichen, kann – auf Anforderung - ergänzend ein Such- und Darstellungsdienst sinnvoll sein. Über diesen Dienst, der die im Langzeitspeicher vorhandenen Metadaten datenbankgestützt redundant vorhält, kann im Fall des Ausfalls des führenden Systems eine Rekonstruktion der Vorgänge oder Akten erfolgen. Bei Bedarf sollten darüber hinaus die archivierten Daten und Dokumente in einer weiterverwendbaren Form präsentiert (Viewer) oder exportiert werden können.

6.2 Schnittstellen des elektronischen Archiv-Service

Der Austausch von Daten sollte grundsätzlich über eine XML-Schnittstelle und auf der Basis standardisierter Kommunikations- und Transportprotokolle erfolgen. Die XML-Schnittstelle ist durch ein erweiterbares XML-Schema (wie in der ArchiSafe Spezifikation 2b beschrieben) zu spezifizieren und zu implementieren.

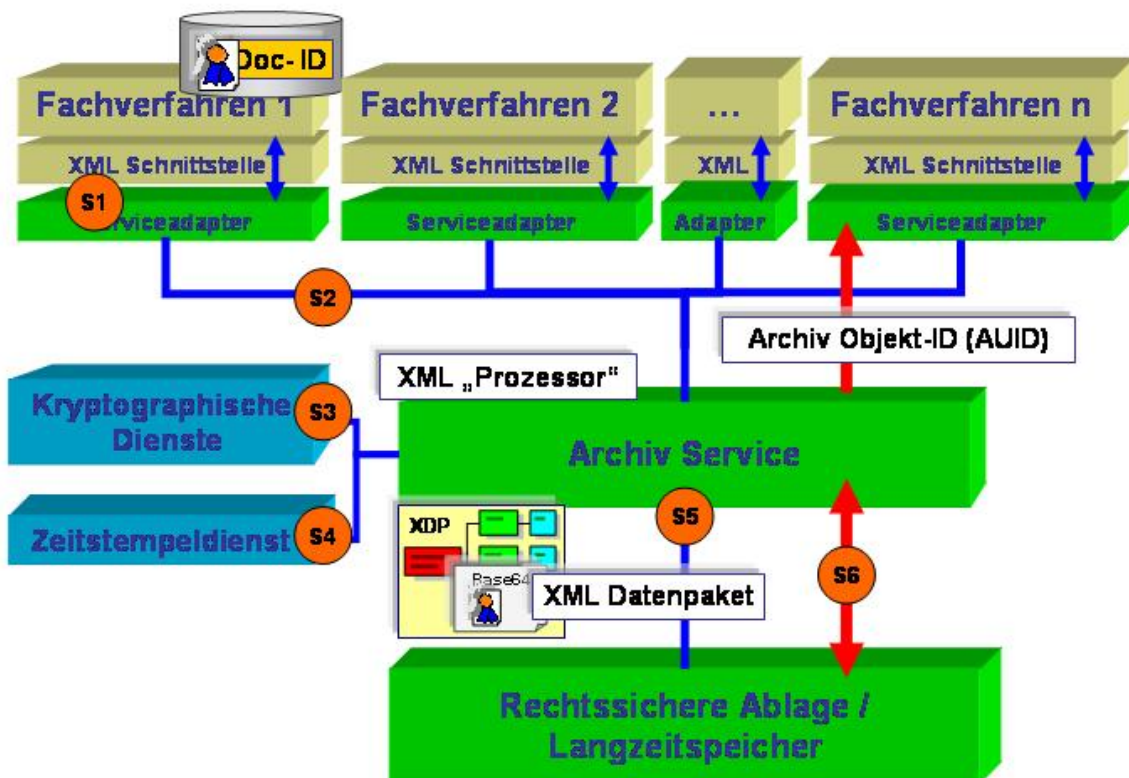


Abb. 6: Archiv Schnittstellen

Zur Umsetzung eines service-orientierten Kommunikationskonzeptes muss die Systemlösung zumindest die folgenden funktionalen Schnittstellen unterstützen:

S1: Schnittstelle zwischen Fachverfahren und Archiv-Service (Service-Adapter)

In dieser Schnittstelle wird die Kommunikation mit dem Archiv-Service über einen ArchiveRequest bzw. ein ArchiveRetrieval eröffnet und verwaltet. Nach erfolgreicher Anmeldung am Archiv-Service übergibt der Serviceadapter die zur Archivierung vorgesehenen Objekte (ArchiveRequest) oder eine ArchivObjekt-ID für eine Rückgabe archivierter Objekte (ArchiveRetrieval).

Der ArchiveRequest sollte synchron und asynchron erfolgen können. Im Falle eines synchronen ArchiveRequest zur Speicherung erwartet die Fachanwendung, im Gegensatz zum asynchronen ArchiveRequest, unmittelbar eine Bestätigung (ArchiveAckn) über die erfolgreiche Ablage des übergebenen Objekts im Langzeitspeicher. Die Bestätigung sollte im Erfolgsfall die ArchivObjekt-ID und im Fehlerfall zusätzlich eine verständliche und eindeutige Fehlermeldung zurückgeben. Die Archivierung wird abgebrochen, wenn

- die Kommunikation mit dem Archivsystem unterbrochen ist,
- das Archivobjekt nicht dem vereinbarten XML-Schema entspricht,
- eine (außerhalb des Archivs erzeugte) ArchivObjekt-ID im System bereits vorhanden ist,
- die Signaturprüfung fehlschlägt.

Der ArchiveRetrieval übergibt eine im Fachverfahren verwaltete ArchivObjekt-ID für den Rückruf eines Archivobjektes aus dem Langzeitspeicher. Das Fachverfahren erwartet in diesem Falle die Rückgabe des gesamten im Langzeitspeicher abgelegten Archivobjekts.

Der ArchiveRetrieval ist mit einer verständlichen Fehlermeldung abzubrechen, wenn

- im Langzeitspeicher kein dieser ID zugeordnetes Objekt gefunden werden kann,
- die Verbindung mit dem Archivsystem unterbrochen ist oder
- keine Zugriffsberechtigung für die ArchivObjekt-ID besteht.

Der Archivadapter sollte darüber hinaus in der Lage sein, die Archivsitzung für einen konfigurierbaren Zeitraum oder eine konfigurierbare Anzahl von Archivobjekten offen zu halten, um mögliche Batcharchivierungsprozesse zu unterstützen.

Über einen ArchiveRequest wird auch eine synchrone oder asynchrone Löschung archivierter Objekte (DeleteArchiveObject) initiiert und gleichfalls der Erfolg oder Misserfolg der Ope-

ration synchron, bzw. asynchron durch das System bestätigt. Dabei sollte zumindest die ArchivObjekt-ID als Parameter übergeben werden.

Erst nach erfolgreicher Löschung kann auch die Verknüpfung der ArchivObjekt-ID im Fachverfahren aufgelöst werden.

S2: Schnittstelle zwischen Service-Adapter und Archiv-Service

An der Schnittstelle zwischen Service-Adapter und der Archivmiddleware (Archiv-Service) wird das Archivobjekt übergeben (entweder als ArchiveRequest oder ArchiveRetrieval).

Im Fall eines ArchiveRequest prüft die Archivmiddleware die Syntax des Archivobjekts und die (im XML-Container eingebettete) ArchivObjekt-ID und weist die Archivierung im Fehlerfall ab. Falls für den ArchiveRequest keine ArchivObjekt-ID eingetragen ist, sollte diese in der Archivmiddleware⁹ generiert und dem Objekt hinzugefügt werden können.

Nach erfolgreicher Syntaxprüfung führt der Archiv-Service auf Anforderung zusätzliche Operationen wie Signaturerstellung, Signaturprüfung oder Einholung eines Zeitstempels, aus, schreibt die Ergebnisse der zusätzlichen Operationen in das Archivobjekt und übergibt dann das so komplettierte Paket an den elektronischen Langzeitspeicher.

Nach erfolgreicher Ablage des Archivobjekts im Langzeitspeicher quittiert die Middleware den Erfolg der Aktion mit einem ArchiveAckn dem Fachverfahren unter Rückgabe der ArchivObjekt-ID.

Im Falle eines ArchiveRetrieval wird der Request bei fehlender ArchivObjekt-ID abgelehnt.

S3: Schnittstelle zwischen Archiv-Service und Signaturdiensten

Auf Anforderung führt der Archiv-Service (die Archivmiddleware) zusätzliche kryptographische Operationen, wie Signaturerstellung, Signatur- und Zertifikatsprüfung aus.

Im Fall der Signaturerstellung übergibt die Middleware das zu signierende Objekt an eine nach SigG sichere Signaturanwendungskomponente. Diese erzeugt einen gültigen Hashwert und signiert diesen. Das Signaturergebnis (ein CMS- oder PKCS#7-Container) wird durch den Archiv-Service in das Archivobjekt geschrieben.

Im Falle der Signaturprüfung übergibt die Middleware die Signaturdaten (ein CMS- oder PKCS#7-Container) an eine Signaturanwendungskomponente mit dem Ziel zunächst einer

⁹ oder als Anfrage an den elektronischen Langzeitspeicher

mathematischen Signaturprüfung. Schlägt die mathematische Signaturprüfung fehl, sollte die Archivierung abgelehnt werden.

Im Falle der Zertifikatsprüfung übergibt die Middleware den Signaturcontainer an eine Signaturanwendungskomponente oder ein OCSP-Relay mit dem Ziel einer OCSP-Anfrage bei einem oder mehreren Trustcentern zur Prüfung der Gültigkeit der für den Signaturinhaber ausgestellten Zertifikate. Die Ergebnisse der OCSP-Anfrage werden durch den Archiv-Service in das Archivobjekt eingetragen.

Im Falle der Rückgabe archivierter Objekte (ArchiveRetrieval), gewährleistet die (mathematische) Signaturprüfung die Feststellung der Integrität der Archivobjekte.

S4: Schnittstelle zwischen Archiv-Service und Zeitstempeldienst

Auf Anforderung holt der Archiv-Service einen Zeitstempel ein. Zu diesem Zweck übergibt der Archiv-Service dem Zeitstempeldienst einen aus dem Objekt erzeugten Hashwert und lässt diesen durch den Zeitstempeldienst mit einer signierten Zeitangabe versehen.

Das Ergebnis wird durch den Archiv-Service in das Archivobjekt eingetragen.

S5 / S6 : Schnittstelle zwischen Archiv-Service und elektronischem Langzeitspeicher

Die Schnittstelle zwischen Archiv-Service und elektronischem Langzeitspeicher ist für den Anwender völlig transparent. Der Langzeitspeicher speichert, verwaltet und löscht die übergebenen Archivobjekte.

Der Langzeitspeicher bestätigt dem Archiv-Service die ausgeführten Operationen durch eine Statusmeldung und die Rückgabe der für das System eindeutigen ArchivObjekt-ID. Die ArchivObjekt-ID wird im Fachverfahren, in der Archivmiddleware oder im Langzeitspeicher erzeugt und dauerhaft mit dem Archivobjekt (XML-Datei) verknüpft.

Der Langzeitspeicher sichert, dass die ArchivObjekt-ID systemweit eindeutig ist. Falls ein Fachverfahren versucht ein Objekt unter einer bereits vorhandenen ID abzuspeichern, ist die Archivierung mit einer aussagekräftigen Fehlermeldung abzulehnen.

Im Falle eines ArchiveRetrieval prüft die Langzeitspeichersoftware die Gültigkeit der ArchivObjekt-ID und die Zulässigkeit des Zugriffs anhand des in der ArchivObjekt-ID eingebetteten Mandantenkennzeichens für das Fachverfahren.

Schnittstellenspezifikation und Beschreibung



ArchiSafe Spezifikation ARS Funktionale Anforderungen



Die Schnittstellenspezifikation und Beschreibung sollte, den Empfehlungen des V-Modells des Bundes folgend, auf der Basis von Anwendungsfällen (use cases) und Aktivitätsdiagrammen erfolgen.

7 Referenzen

- ANSI X3.4** ANSI X3.4 Information Systems – Coded Character Sets – 7-Bit American National Standard Code for Information Interchange (7-Bit ASCII)
- ARS 2.a** ArchiSafe Spezifikation 2.a – ARS Metadatenstruktur, Braunschweig, 2005
<<http://www.archisafe.de>>
- ARS 2.b** ArchiSafe Spezifikation 2.b – ARS XML-Schema, Braunschweig, 2005
<<http://www.archisafe.de>>
- DOMEA21** DOMEA Organisationskonzept 2.1: Dokumentenmanagement und elektronische Archivierung im IT-gestützten Geschäftsgang, Schriftenreihe der KBSt, Bd. 61, November 2005.
- DOMEA20TA** DOMEA Erweiterungsmodul zum Organisationskonzept 2.0: Technische Aspekte der Archivierung elektronischer Akten, Schriftenreihe der KBSt, Bd. 67, Oktober 2004.
- ISO 646** ISO/IEC 646, Information technology – ISO 7-bit coded character set for information interchange;
Note: the character encoding defined in ISO/IEC 646 is equivalent to ANSI X3.4 (ASCII) and ECMA-6
- ISO 19005-1** ISO 19005-1 „Document management – Electronic document file format for long-term preservation – Part 1: Use of PDF 1.4 (PDF/A-1)“, ISO 2005
- ISO-Latin-1** ISO-Latin-1: <<http://anubis.dkuug.dk/JTC1/SC2/WG3/docs/n411.pdf>>
beziehungsweise als kostenpflichtiger ISO-Standard:
"ISO/IEC 8859-1:1998 — Information technology — 8-bit single-byte coded graphic character sets — Part 1: Latin alphabet No. 1" <<http://www.iso.org/>>
- PDF14** PDF Reference 1.4, Adobe Portable Document Format, Version 1.4, Adobe Systems Incorporated, 3rd ed. (ISBN 0-201-75839-3)
<<http://partners.adobe.com/public/developer/en/pdf/PDFReference.pdf>>

UNICODE	Unicode Standard, Unicode Consortium (ISBN 0-201-61633-5), < http://unicode.org/versions/Unicode4.1.0/ > This is functionally equivalent to ISO/IEC 10646:2003 – Information technology – Universal Multiple-Octet Coded Character Set (UCS). < http://www.iso.org/ >
SAGA21	SAGA Standards und Architekturen für E-Government-Anwendungen, Schriftenreihe der KBSt, Bd. 82, September 2005.
TIFF6	TIFF Revision 6.0, Final – June 3, 1992 < http://partners.adobe.com/public/developer/en/tiff/TIFF6.pdf >
XML	Extensible Markup Language (XML) 1.0, second edition, W3C Recommendation, 6.October 2000, < http://www.w3.org/TR/2000/REC-xml-20001006 >
XMP	XMP Adobe eXtensible Metadata Platform; < http://www.adobe.com/products/xmp >
XML Schema	XML Schema, W3C Recommendation, May 2001 < http://www.w3.org/TR/xmlschema-0/ >(Primer) < http://www.w3.org/TR/xmlschema-1/ >(Structures) < http://www.w3.org/TR/xmlschema-2/ >(Datatypes)