

ArchSafe

ArchSafe Spezifikation

ARS Spezifikation 5.0

ARS Schnittstellen

VERSION 1.0

Dokumententitel: ARS Schnittstellen
Dateiname: 2007-05-07_Std_ARS_5_0_V10.doc
Version: 1.0
Anzahl Seiten:
Status: Abgeschlossen

erstellt am:	07.01.2007	von:	Dr. W. Zimmer
geprüft am:	22.01.2007	von:	T. Schäfer
Geändert am:	30.01.2007	von:	T. Schäfer
Freigegeben am:	07.05.2007	von:	T. Schäfer

Standort: PTB
Verteiler: Nutzerbeirat

Inhalt

0	Versionshistorie	4
0.1	Dokumentverantwortlicher	4
0.2	Verteilerliste.....	4
1	Zielsetzung des Dokumentes	5
2	Einführung	8
3	Schnittstellen.....	9
3.1	Grundsätzliche Anforderungen an die Schnittstellen.....	9
3.1.1	<i>Geringer Integrationsaufwand</i>	<i>9</i>
3.1.2	<i>Verfügbare Plattformen.....</i>	<i>9</i>
3.1.3	<i>Schnittstellenübersicht.....</i>	<i>9</i>
3.2	Weitere verfügbare Funktionalitäten und Anforderungen.....	14
3.2.1	<i>Erstellung und Verifikation elektronischer Signaturen.....</i>	<i>14</i>
3.2.1.1	Einsatz bestätigter Signaturkomponenten.....	14
3.2.1.2	Unterstützung unterschiedlicher Einsatzszenarien	14
3.2.1.3	Unterstützung verschiedener Signaturformate	15
3.2.1.4	Anforderung und Verifikation von Zeitstempeln	15
3.2.1.5	Signaturerneuerung nach dem ArchiSig Prinzip.....	15
3.2.1.6	Weitere kryptographische Operationen	16
3.3	(Sprachunabhängige) Spezifikation der Schnittstellen (API).....	16
3.3.1	<i>ArchiveSubmit.....</i>	<i>16</i>
3.3.2	<i>ArchiveRetrieval.....</i>	<i>18</i>
3.3.3	<i>ArchiveDelete.....</i>	<i>18</i>
3.3.4	<i>ArchiveRetentionInfo</i>	<i>19</i>
3.3.5	<i>ArchiveCreateEvidenceRecord.....</i>	<i>20</i>
3.3.6	<i>ArchiveRenewEvidenceRecord</i>	<i>20</i>
3.3.7	<i>ArchiveVerifyEvidenceRecord:ForArchiveObject</i>	<i>21</i>
3.3.8	<i>ArchiveVerifyEvidenceRecord</i>	<i>21</i>
4	Kommunikationsmechanismen	22
4.1	Asynchrone Kommunikation	22



ArchiSafe Spezifikation ARS Schnittstellen



4.2 Sichere Netzwerkkommunikation.....	22
4.3 Autorisierung und Zugriffskontrolle	23
5 Referenzen	24

0 Versionshistorie

Version	Editor	Datum	Kommentar
0.5	Dr. W. Zimmer	07.01.2007	Entwurf
0.53	Tobias Schäfer	22.01.2007	QS
0.54	Tobias Schäfer	30.01.2007	Versendung an Nutzerbeirat
1.0	Tobias Schäfer	07.05.2007	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 Spezifikation 1.0: Funktionale Anforderungen	ARS DOMEA Empfehlungen 1: Funktionale Anforderungen
ARS Spezifikation 2.0: ARS XML Datenschema	ARS DOMEA Empfehlungen 2: XML Datenschema
ARS Spezifikation 3.0: ARS Langzeitdokumentenformate	ARS DOMEA Empfehlung 3: Langzeitdokumentenformate
ARS Spezifikation 4.0: ARS Signaturformate	ARS DOMEA Empfehlung 4: Elektronische Signaturen
ARS Spezifikation 5.0: ARS Schnittstellen	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 geeigneten Dokumentformate, die für eine rechtssichere, dauerhafte elektronische Ablage von ARS konformen Systemen jedenfalls unterstützt werden müssen.
- **Spezifikation 4:** Dieses Dokument spezifiziert die von ARS konformen Systemen unterstützten elektronischen Signaturformate.
- **Spezifikation 5:** Dieses Dokument beschreibt die 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 Realisierung in der Physikalisch-Technischen Bundesanstalt.

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

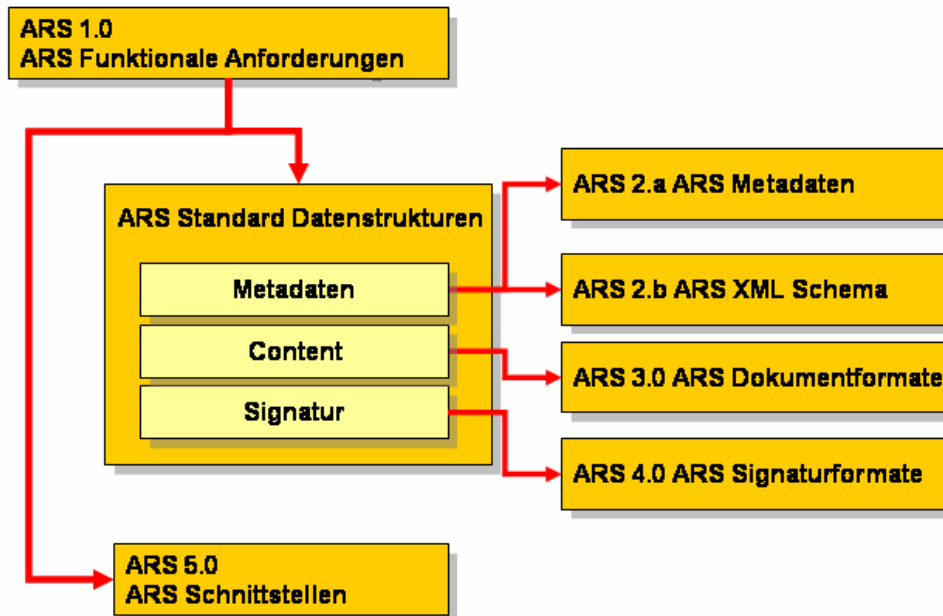


Abb. 2: Beziehungen zwischen den ArchiSafe Spezifikationen

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 unterstützten Signaturformate 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 Schnittstellen)** schließlich beschreibt die funktionalen Schnittstellen und Mechanismen für den Datenaustausch.

2 Einführung

Die plattform- und herstellerunabhängige Integration eines zukunftsfähigen Archivdienstes (Service) für die dauerhafte und rechtssichere Aufbewahrung von elektronischem Schriftgut in vorhandene IT-Landschaften, basiert nach dem ArchiSafe Konzept auf der losen Kopplung zwischen dem für den Benutzer transparent agierenden elektronischen Langzeitspeicher und den angeschlossenen IT-Verfahren (Fachanwendungen, ERP-Systeme, Dokumentenmanagementsysteme), die den Archivdienst für die dauerhafte Aufbewahrung des von ihnen erzeugten und verwalteten elektronischen Schriftgutes nutzen.

Eine wichtige Grundlage hierfür sind transparente und standardisierte Schnittstellen und Protokolle für den Import und Export der zur dauerhaften Ablage bestimmten Dokumente und Daten.

Der Zweck dieser Spezifikation ist, herstellerunabhängige Schnittstellen für die dauerhafte elektronische Ablage digitaler Dokumente und Daten zu beschreiben, die von einem ArchiSafe konformen elektronischen Archivsystem jedenfalls unterstützt werden müssen.

Diese Spezifikation gilt im Zusammenhang mit folgenden weiteren Spezifikationen:

- ARS 1.0 : ARS Funktionale Anforderungen an eine dauerhafte und rechtssichere elektronische Ablage [ARS 1]
- ARS 2.0 : ARS XML Datenpakete und Metadatenschema [ARS 2]
- ARS 3.0 : ARS Langzeitdokumentenformate [ARS 3],
- ARS 4.0 : ARS Signaturformate [ARS 4]

3 Schnittstellen

In diesem Abschnitt werden die Anforderungen und Funktionen einer ArchiSafe konformen elektronischen Archivschnittstelle beschrieben und sprachunabhängig spezifiziert. Grundlage hierfür sind die in der ARS Spezifikation 1 [ARS 1] definierten und beschriebenen funktionalen Anforderungen an die rechts- und revisionssichere Ablage von elektronischem Schriftgut.

3.1 Grundsätzliche Anforderungen an die Schnittstellen

In diesem Abschnitt werden grundsätzliche Anforderungen an ArchiSafe konforme Schnittstellen für den Import und Export beschrieben.

3.1.1 Geringer Integrationsaufwand

Die Integration eines ArchiSafe konformen elektronischen Archivdienstes soll möglichst geringen (einmaligen und kontextspezifischen) Integrationsaufwand verursachen. Hieraus folgt, dass es sich um eine so genannte „High-Level“-API handeln muss, die von technischen Details abstrahiert.

3.1.2 Verfügbare Plattformen

Die Schnittstellen müssen für mindestens eine international verfügbare und stabile Entwicklungsumgebung (C, C++, C#, Java) und Betriebssystemplattform (MS Windows, Linux, Unix) zur Verfügung stehen.

3.1.3 Schnittstellenübersicht

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.

Nach den in [ARS 1] spezifizierten und beschriebenen funktionalen Anforderungen an eine dauerhafte rechts- und revisionssichere Ablage elektronischer Dokumente muss ein ArchiSafe konformes System jedenfalls folgende funktionale Schnittstellen und Funktionalitäten bereitstellen (s. Abb. 3):

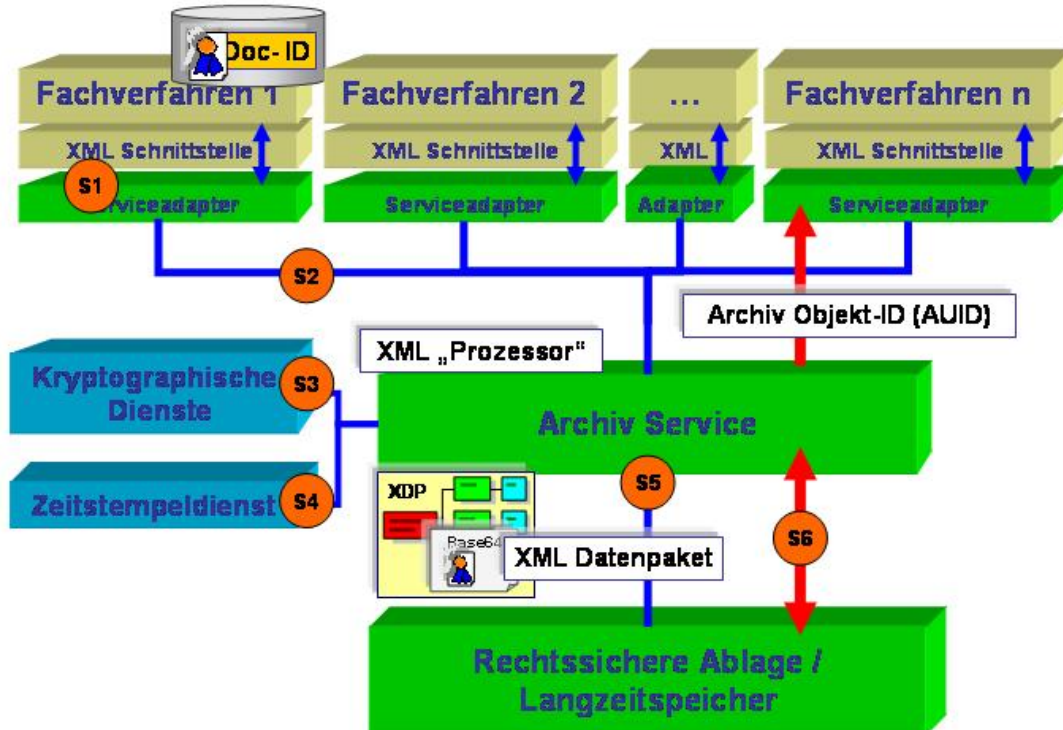


Abb. 3: Archiv Schnittstellen

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

In dieser Schnittstelle wird die Kommunikation mit dem Archiv-Service über einen ArchiveSubmit bzw. einen ArchiveRetrieval eröffnet und verwaltet. Nach erfolgreicher Anmeldung am Archiv-Service übergibt der Serviceadapter die zur Archivierung vorgesehenen Objekte (ArchiveSubmit) oder eine ArchivObjekt-ID für eine Rückgabe archivierter Objekte (ArchiveRetrieval).¹

Im Falle eines ArchiveSubmit zur Speicherung erwartet die Fachanwendung eine Bestätigung (ArchiveAckn) über die erfolgreiche Ablage des übergebenen Objekts im Langzeitspeicher. Die Bestätigung sollte im Erfolgsfall die in der Archiv-Middleware oder im Langzeit-

¹ Die Struktur, Syntax und Semantik der Archivobjekte ist in [ARS 2] spezifiziert und beschrieben.

speicher erzeugte 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,
- eine 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.²

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 ArchiveRetrieval wird auch die Löschung archivierter Objekte (DeleteArchiveObject) initiiert und gleichfalls der Erfolg oder Misserfolg der Operation 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 ArchiveSubmit oder ArchiveRetrieval).

Im Fall eines ArchiveSubmit prüft die Archivmiddleware die Syntax des Archivobjekts und die ggf. im XML-Container eingebettete ArchivObjekt-ID und weist die Archivierung im Fehlerfall

² Nach der ARS Spezifikation [ARS 2] handelt es sich dabei um ein wohlgeformtes XML Dokument.

ab. Falls für den ArchiveSubmit keine ArchivObjekt-ID eingetragen ist, sollte diese in der Archivmiddleware oder per Anfrage an den elektronischen Langzeitspeicher 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 (eine PKCS#7- oder XML-Signatur) wird durch den Archiv-Service in das Archivobjekt geschrieben.

Im Falle der Signaturprüfung übergibt die Middleware die Signaturdaten (eine PKCS#7- oder XML Signatur) an eine Signaturanwendungskomponente mit dem Ziel zunächst einer mathematischen Signaturprüfung. Schlägt die mathematische Signaturprüfung fehl, sollte die Archivierung abgelehnt werden.

Im Falle der Zertifikatsprüfung übergibt die Middleware den Signaturcontainer oder das Zertifikat 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 und zusätzlich erhaltene Zertifikate werden durch den Archiv-Service in das Archivobjekt eingetragen.

Anm.: In der Regel erfolgt die Signaturprüfung mit der Zertifikatsprüfung gemeinsam in einer Signaturanwendungskomponente. Die dabei erhaltenen zusätzlichen Daten (OCSP-Response, Zertifikate bis zur obersten Wurzel) und ein erstellter Prüfbericht werden dem Archivobjekt beigefügt. Die Verifikationsdaten können dabei je nach Datenformaten entweder in den signierten Daten selbst hinzugefügt werden (z.B. bei CMS oder PKCS#7) oder dem ArchivObjekt in seiner XML-Struktur beigefügt werden. Der Prüfbericht sollte ebenfalls in das ArchivObjekt eingefügt werden.

Im Falle der Rückgabe archivierter Objekte (ArchiveRetrieval), gewährleistet eine (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 ggf. 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 (in der optimalen Konfiguration weltweit) eindeutig ist. Falls ein Fachverfahren versucht ein Objekt unter einer bereits vorhandenen ID abzuspeichern, ist die Archivierung mit einer aussagekräftigen Fehlermeldung abzulehnen (Um derartige Fehler zu vermeiden kann ein Fachverfahren eine ArchivObjekt-ID kurzzeitig reservieren und dadurch sicherstellen dass sie für den Request dann zur Verfügung steht und noch nicht anderweitig vergeben wurde).

Im Falle eines ArchiveRetrieval prüft die Langzeitspeichersoftware die Gültigkeit der ArchivObjekt-ID und die Zulässigkeit des Zugriffs beispielsweise anhand einer Signatur des Retrie-

val-Requests, die mit dem jeweiligen Teil des Mandanten des Langzeitspeichers logisch assoziiert und nur diesem den Zugriff auf die darin enthaltenen Dokumente sichert.

3.2 Weitere verfügbare Funktionalitäten und Anforderungen

Über die beschriebenen Schnittstellen hinaus muss ein ArchiSafe konformes elektronisches Archivsystem die im Folgenden näher beschriebenen Anforderungen und Funktionalitäten erfüllen:

3.2.1 Erstellung und Verifikation elektronischer Signaturen

Bei der Erzeugung und Verifikation elektronischer Signaturen müssen unterschiedliche Einsatzszenarien und jedenfalls die in [ARS 4] spezifizierten Signaturformate unterstützt werden.

3.2.1.1 Einsatz bestätigter Signaturkomponenten

Für die Erzeugung qualifizierter elektronischer Signaturen und Zeitstempel dürfen nur von der Bundesnetzagentur als sicher bestätigte Signaturerstellungseinheiten eingesetzt werden. Für Signaturanwendungskomponenten (Anwenderprogramme, Funktionsbibliotheken, Chipkartenleser) ist eine Bestätigung von Produkten für qualifizierte elektronische Signaturen gemäß §§ 15 Abs. 7 S. 1, 17 Abs. 4 SigG und §§ 11 Abs. 3 und 15 SigV durch das Bundesamt für Sicherheit in der Informationstechnik oder andere durch den Gesetzgeber zugelassene Zertifizierungsstellen erforderlich.

Für technische Komponenten eingesetzter oder genutzter Zertifizierungsdienste (Verzeichnisdienstkomponenten, Zeitstempeldienstkomponenten, Schlüsselgeneratoren) ist eine Bestätigung für technische Komponenten gemäß § 14 (4) SigG und §§ 16 und 17 SigV durch das Bundesamt für Sicherheit in der Informationstechnik oder andere durch den Gesetzgeber zugelassene Zertifizierungsstellen erforderlich.

3.2.1.2 Unterstützung unterschiedlicher Einsatzszenarien

Die in einer ArchiSafe konformen Umgebung eingesetzten Signaturkomponenten (Signaturanwendungskomponenten und Signaturerstellungseinheiten) sollten die Erstellung und die Verifikation elektronischer Signaturen in verschiedenen Einsatzszenarien unterstützen. Hierzu gehören:

- die Erstellung und Verifikation von Einzel-, Mehrfach- und Massensignaturen,

- die Erstellung und Verifikation elektronischer Signaturen unterschiedlicher Qualitätsstufen, mindestens aber qualifizierter elektronischer Signaturen und qualifizierter elektronischer Signaturen mit Anbieterakkreditierung

Bei einer serverbasierten Signaturerzeugung und -verifikation sollten verschiedene Einsatzszenarien (Stapelverarbeitung, Request-Response-Mechanismus etc.) unterstützt werden.

3.2.1.3 Unterstützung verschiedener Signaturformate

Eine ArchiSafe konforme Umgebung muss jedenfalls die in [ARS 4] spezifizierten Signaturformate unterstützen.

3.2.1.4 Anforderung und Verifikation von Zeitstempeln

Grundlage für eine sichere Verknüpfung von Zeitattributen mit Dokumenten im Archiv-Umfeld sind vertrauenswürdige elektronische Zeitstempel. Insbesondere muss bei der Prüfung einer qualifizierten elektronischen Signatur die Gültigkeit des Zertifikates zum Erstellungszeitpunkt der Signatur herangezogen werden.

Für das Ausstellen von Zeitstempeln muss ein ArchiSafe konformes System jedenfalls das in [ARS 4] nach [RFC 3161] spezifizierte Time Stamp Protocol (TSP) und Zeitstempelformat unterstützen.³

3.2.1.5 Signaturerneuerung nach dem ArchiSig Prinzip

Für die langfristige und effiziente Sicherung des Beweiswertes qualifizierter elektronischer Signaturen gemäß § 17 SigV muss eine ArchiSafe konforme Umgebung die Signaturerneuerung nach dem ArchiSig Konzept [ArchiSig] auf der Basis der in [ARS 4] spezifizierten Archive-Time-Stamp Syntax (ATS), bzw. der darauf aufbauenden (internationalen) Evidence Record Syntax (ERS) unterstützen [LTANS:ERS].

Dabei müssen folgende Funktionalitäten bereitgestellt werden:

- Erstellung und Prüfung von Evidence Records
- Erstellung und Prüfung von Archive Time Stamps (als untergeordnete Operation zur Erstellung und Prüfung des Evidence Records)
- Funktionen zur Realisierung der

³ Siehe dazu auch ISIS-MTT Spezifikation [ISIS-MTT] (Part 4 – Operational Protocols)

- Erneuerung des Zeitstempels (Übersignatur nur über Zeitstempel und Hashbäume)
- Erneuerung des Hashbaums (komplette Konstruktion eines neuen Hashbaumes basierend auf neuen Algorithmen)

3.2.1.6 Weitere kryptographische Operationen

Über die Erstellung und Verifikation elektronischer Signaturen und Zeitstempel hinaus sollten die in einer ArchiSafe konformen Umgebung eingesetzten Technologien (Komponenten/Module) auch für weitere kryptographische Operationen genutzt werden können. Insbesondere wird empfohlen, die Verschlüsselung von Daten in den Formaten CMS und S/MIME zu unterstützen.

3.3 (Sprachunabhängige) Spezifikation der Schnittstellen (API)

Dieser Abschnitt gibt eine sprachunabhängige Spezifikation der Funktionen, die von einer ArchiSafe konformen Umgebung mindestens zur Verfügung gestellt werden sollten.

3.3.1 ArchiveSubmit

Mit der **ArchiveSubmit** Funktion wird die Archivierung eines in [ARS 2] spezifizierten XML Archivobjektes initiiert. Standardmäßig wird bei der Übergabe des Archivobjektes (XML Dokument) an die ArchiSafe Middleware die Konformität mit einem vereinbarten XML Schema geprüft. Im Fehlerfall wird die Archivierung abgewiesen.

Die Funktion sollte mindestens folgende Aufrufparameter und Optionen vorsehen:

- das zu speichernde XML Dokument (XML-Datei), optional: ersatzweise eine URI zur gespeicherten XML-Datei
- **optional:** einen Link (URI) auf eine XML-Schemadatei, gegen die die Prüfung vorgenommen werden soll,
- **optional:** eine Archivobjekt-ID falls diese durch die Fachanwendung erzeugt und nicht bereits in den XML-Container eingetragen ist,
- **optional:** Angabe einer Aufbewahrungsfrist;
Anm.: es wird jedoch empfohlen, Aufbewahrungsfristen standardmäßig in den Metadaten des XML Containers einzutragen und durch die Middleware oder die produktspezifische Speicher- software auszulesen.
- **optional:** Signaturen (Bezeichner) für zusätzlich auszuführende Operationen wie:

- Signatur erstellen,
- Signatur prüfen,
- Zeitstempel erstellen,
- Verschlüsselung;
- **optional:** zusätzliche Fachschlüssel (-signaturen) mit denen eine Überprüfung der Zugriffsberechtigung unterstützt wird,

Anm.:

- (1) Es wird empfohlen, die Prüfung der Signatur elektronisch signierter Dokumente standardmäßig vorzunehmen. Die Middleware sollte dafür in der Lage sein, die hierfür notwendigen Informationen aus den XML-Metadaten zu extrahieren (auszulesen).
- (2) Es wird empfohlen, zu speichernde Archivobjekte standardmäßig mit einem Zeitstempel zu versehen und so zumindest die Integrität auch unsigned Dokumente zu schützen.
- (3) Falls das Archivobjekt bei der Ablage zusätzlich verschlüsselt werden soll, müssen die Schlüsselinformationen (Verschlüsselungsalgorithmus und Schlüsselparameter wie z.B. die Länge) zusätzlich angegeben werden. Das ArchiSafe Konzept sieht für die Ablage keinerlei archivspezifische PKI-Funktionalität vor.
- (4) Desweiteren sollte das ArchivObject um die entsprechenden zur Verifikation notwendigen (und bei der initialen Prüfung bereits eingeholten) Verifikationsdaten (OCSP-Response und Zertifikatskette bis zur Wurzel) angereichert werden. ([ERDOC])

Die Ausführung zusätzlicher Operationen soll nach dem ArchiSafe Konzept in der Middleware erfolgen. Rechtlich relevante Funktionsergebnisse, wie Signaturen, Signaturprüfergebnisse oder Zeitstempel müssen in die dafür vorgesehen Metadaten eingetragen oder in anderer Weise dem XML Container maschinenlesbar hinzugefügt werden.

Der Rückgabewert der Funktion ArchiveSubmit ist im Erfolgsfall die ArchivObjekt-ID.

Die Funktion muss mit einer verständlichen Fehlermeldung abgebrochen werden, wenn:

- die Verbindung zum Archiv unterbrochen ist,
- die Syntax des XML Archivobjekts nicht dem vereinbarten oder angezeigten Schema entspricht,
- eine der zusätzlichen Operationen fehlschlägt,
- eine übergebene oder erzeugte Archivobjekt-ID im System schon vorhanden ist,
- keine Aufbewahrungsfrist angegeben oder eingetragen ist.

3.3.2 ArchiveRetrieval

Mit der Funktion **ArchiveRetrieval** wird eine Kopie des Archivobjektes an das aufrufende System zurückgegeben. Je nach Systemkonfiguration sind dabei folgende Schritte sinnvoll:

- Verifikation des Evidence Records für das ArchivObject
- Prüfung der Integrität des bzw. der Objekte durch Neubildung eines gespeicherten Hashwertes, der Prüfung der Signatur (mathematische Signaturprüfung) und der Verifikationsdaten oder der Zeitstempelsignatur und Übergabe des Prüfergebnisses an die aufrufende Anwendung.
- Übergabe des bei der Archivierung erstellten Prüfberichts (ggf. als Alternative zur Prüfung der Signaturen im Objekt)

Die Funktion sollte mindestens folgende Aufrufparameter und Optionen vorsehen:

- die Archivobjekt-ID des angeforderten Archivobjektes, Wildcards sind unzulässig,
- **optional:** zusätzliche Fachschlüssel (-signaturen) mit denen eine Überprüfung der Zugriffsberechtigung unterstützt wird,

Der Rückgabewert der Funktion ist das Archivobjekt, d.h. ein XML Dokument und das Ergebnis der Integritätsprüfung.

Anm.: Die Darstellung (Ansicht) des zurückgegebenen Archivobjektes obliegt der aufrufenden Anwendung.

Die Funktion muss mit einer verständlichen Fehlermeldung abgebrochen werden, wenn

- die Verbindung mit dem Archiv unterbrochen ist,
- die angegebene Archivobjekt-ID im System nicht existiert.

Sollte die Integritätsprüfung fehlschlagen, muss die Rückgabe des Objektes mit einem deutlichen Warnhinweis abgeschlossen werden.

3.3.3 ArchiveDelete

Mit der **ArchiveDelete** Funktion wird eine unwiederbringliche Löschung von Archivobjekten veranlasst.

Hinweis: Das ArchiSafe-Konzept empfiehlt keine automatisierte Löschung von Archivobjekten nach Ablauf von Aufbewahrungsfristen durch das Langzeitspeichersystem. Vielmehr sollte die Löschung archivierter Objekte in jedem Fall durch die zuständige Fachanwendung oder einer eigens autorisierten Administrationskonsole angestoßen werden.

Die Funktion sollte mindestens folgende Aufrufparameter und Optionen vorsehen:

- die Archivobjekt-ID des zu löschenden Archivobjektes oder
- eine Liste von Archivobjekt-IDs der zu löschenden Archivobjekte
- **optional:** Fachschlüssel (-signatur) zur Unterstützung der Erkennung der Zugriffs- und Löschberechtigung.

Der Rückgabewert der Funktion ist die Archivobjekt-ID des gelöschten Archivobjektes.

Die Funktion wird mit einer verständlichen Fehlermeldung abgebrochen, wenn

- die Verbindung mit dem Archiv unterbrochen ist,
- die angegebene Archivobjekt-ID im System nicht existiert,
- die Löschung aus technischen Gründen nicht durchgeführt werden kann.

3.3.4 ArchiveRetentionInfo

Mit der Funktion **ArchiveRetentionInfo** wird eine Auskunft über die im angefragten Auskunftszeitraum zur Aussonderung (Löschung) anstehenden Archivobjekte nachgefragt.

Die Funktion sollte mindestens folgende Aufrufparameter und Optionen vorsehen:

- den Auskunftszeitraum
- **optional:** einen Fachschlüssel (-signatur) zur Unterstützung der Erkennung der Zugriffsberechtigung.

Der Rückgabewert der Funktion **ArchiveRetentionInfo** ist eine, gegebenenfalls auch leere, Liste von Archivobjekt-IDs, der Archivobjekte, deren Aufbewahrungsfrist in dem angegebenen Zeitraum abläuft.

Die Funktion wird mit einer verständlichen Fehlermeldung abgebrochen, wenn:

- die Verbindung mit dem Archiv unterbrochen ist,
- der angegebene Auskunftszeitraum ungültig ist.

Die Administration eines ArchiSafe-konformen elektronischen Langzeitspeichers sollte darüber hinaus mindestens durch die folgenden Funktionen unterstützt werden:

3.3.5 ArchiveCreateEvidenceRecord

Mit der Funktion **ArchiveCreateEvidenceRecord** wird ein nach [LTANS:ERS] spezifizierter EvidenceRecord für den Nachweis erzeugt, dass ein Archivobjekt oder eine Gruppe von Archivobjekten zu einem bestimmten Zeitpunkt im Langzeitspeicher tatsächlich vorhanden ist und nicht verändert wurde.

Hierzu müssen zumindest die Daten übergeben werden oder worden sein, für die der EvidenceRecord erzeugt werden soll, also beispielsweise die Dokumente und ggf. bestehende EvidenceRecords die aus Fremdsystemen importiert wurden. [ArchiSig]

Im Normalfall werden sich alle diese Daten zum Zeitpunkt des Aufrufs bereits im Langzeitspeicher befinden.

Der EvidenceRecord kann separat oder auch im Archivobjekt selbst abgespeichert werden. Zusätzlich sollten für diese Funktion folgende Optionen für die Übergabe vorgesehen werden:

- Verschlüsselte Daten
- Verweis auf (verschlüsselte oder unverschlüsselte) Daten oder Hashwerte

Das System generiert dann basierend auf den gesammelten Daten entsprechend dem ArchiSig-Konzept [ArchiSig] die Hashbäume und Archivzeitstempel und den daraus sich ergebenden EvidenceRecord.

Der Rückgabewert der Funktion ist eine URI oder eine ID auf einen nach [LTANS:ERS] spezifizierten EvidenceRecord.

3.3.6 ArchiveRenewEvidenceRecord

Mit der Funktion **ArchiveRenewEvidenceRecord** soll ein bereits existierender EvidenceRecord erneuert werden. Dabei müssen zumindest folgende Übergabeparameter und Optionen vorgesehen werden:

- ID oder URI zum zu erneuernden EvidenceRecord,
- Information, ob lediglich ein Time Stamp Renewal (Übersignatur nur über Hashwerte) oder ein Hash Tree Renewal (Rekonstruktion des Hash-Baumes) durchgeführt werden soll,
- Daten oder Verweis auf Daten wie bei *ArchiveCreateEvidenceRecord* (für Hash Tree Renewal).

Der Rückgabewert der Funktion ist die ID oder URI auf den erneuerten EvidenceRecord.

3.3.7 **ArchiveVerifyEvidenceRecord:ForArchiveObject**

Mit der Funktion ***ArchiveVerifyEvidenceRecord:ForArchiveObject*** soll ein EvidenceRecord eines ArchivObjekts auf seine Gültigkeit hin überprüft werden. Hierzu müssen zumindest folgende Übergabeparameter vorgesehen werden:

- Das zu prüfende Dokument (mit seiner URI oder ID)
- Daten oder Verweise auf Daten wie bei *ArchiveCreateEvidenceRecord*
- Signaturen für Prüftiefen: keine, lokale oder Online-Prüfung der Zertifikate
- Eine Prüf-Policy (oder deren ID im System) die festlegt, welche Algorithmen und Parameter in welchem Zeitfenster vom Betreiber als sicher angesehen werden.

Alle Daten außer der Dokument-ID können ebenfalls vom System mit gültigen Standardwerten vorbelegt sein und werden in diesem Falle nur dann benötigt, wenn sie von den Standardsystemwerten abweichen sollen.

Der Rückgabewert der Funktion *ArchiveVerifyEvidenceRecord:ForArchiveObject* ist das Prüfergebnis.

3.3.8 **ArchiveVerifyEvidenceRecord**

Neben der Standardfunktion *ArchiveVerifyEvidenceRecord:ForArchiveObject* kann (optional) auch die Funktion ***ArchiveVerifyEvidenceRecord*** angeboten werden. Mit ihr wird ein EvidenceRecord auf seine Gültigkeit hin überprüft. Hierzu müssen zumindest folgende Übergabeparameter vorgesehen werden:

- Der zu prüfende EvidenceRecord
- Daten oder Verweise auf Daten wie bei *ArchiveCreateEvidenceRecord*
- Signaturen für Prüftiefen: keine, lokale oder Online-Prüfung der Zertifikate
- Eine Prüf-Policy (oder deren ID im System) die festlegt welche Algorithmen und Parameter in welchem Zeitfenster vom Betreiber als sicher angesehen werden.

Der Rückgabewert der Funktion *ArchiveVerifyEvidenceRecord* ist das Prüfergebnis.

4 Kommunikationsmechanismen

In diesem Abschnitt werden die Anforderungen einer ArchiSafe konformen Kommunikationsinfrastruktur beschrieben. Grundlage hierfür sind die in der ARS Spezifikation 1 [ARS 1] definierten und beschriebenen funktionalen Anforderungen an die rechts- und revisionssichere Ablage von elektronischem Schriftgut.

4.1 Asynchrone Kommunikation

Das für ArchiSafe bestimmende Konzept der losen Kopplung zwischen dem für den Benutzer transparent agierenden elektronischen Langzeitspeicher und den angeschlossenen IT-Verfahren (Fachanwendungen, ERP-Systeme, Dokumentenmanagementsysteme) lässt sich am wirksamsten auf der Basis asynchroner, nachrichtenorientierter Kommunikation erreichen.

Anm.: Asynchrone Kommunikation erhöht die Unabhängigkeit der Komponenten und ist insbesondere die geeignete Wahl für die Kommunikation von Systemen über nicht-deterministische Verbindungen oder den massenhaften (Batch-) Import von Archivobjekten. Asynchrone Kommunikationsmodelle lassen sich sowohl auf Basis von Webservice-Architekturen als auch des CORBA Komponentenmodells (CCM) verwirklichen.

4.2 Sichere Netzwerkkommunikation

Für die rechts- und revisionssichere elektronische Langzeitspeicherung von elektronischem Schriftgut sind Authentizität, Integrität und Vertraulichkeit elektronischer Informationen auch beim elektronischen Transport zwischen den möglicherweise verteilten Komponenten zu gewährleisten.

ArchiSafe konforme Lösungen müssen daher den Schutz der transportierten Daten und Informationen entweder durch Maßnahmen der Transportsicherheit (TLS/SSL) für eine Punkt-zu-Punkt-Kommunikation oder der Nachrichtensicherheit (bspw. SOAP mit XML Verschlüsselung und XMLDSIG oder OSC1) für eine Ende-zu-Ende-Kommunikation oder durch eine Kombination sicherheitsgeeigneter Maßnahmen auf beiden Ebenen garantieren (Abb.4).

Hinweis: TLS/SSL schützt nur den Transport und ist überall dort wo Zwischenstationen (Intermediäre) existieren, die Daten auf Anwendungsebene nutzen oder verarbeiten nicht ausreichend. In diesem Fall erfordert die Gewährleistung von Sicherheit, dass Teile einer Sendung verschieden behandelt werden und individuell geschützt werden können.

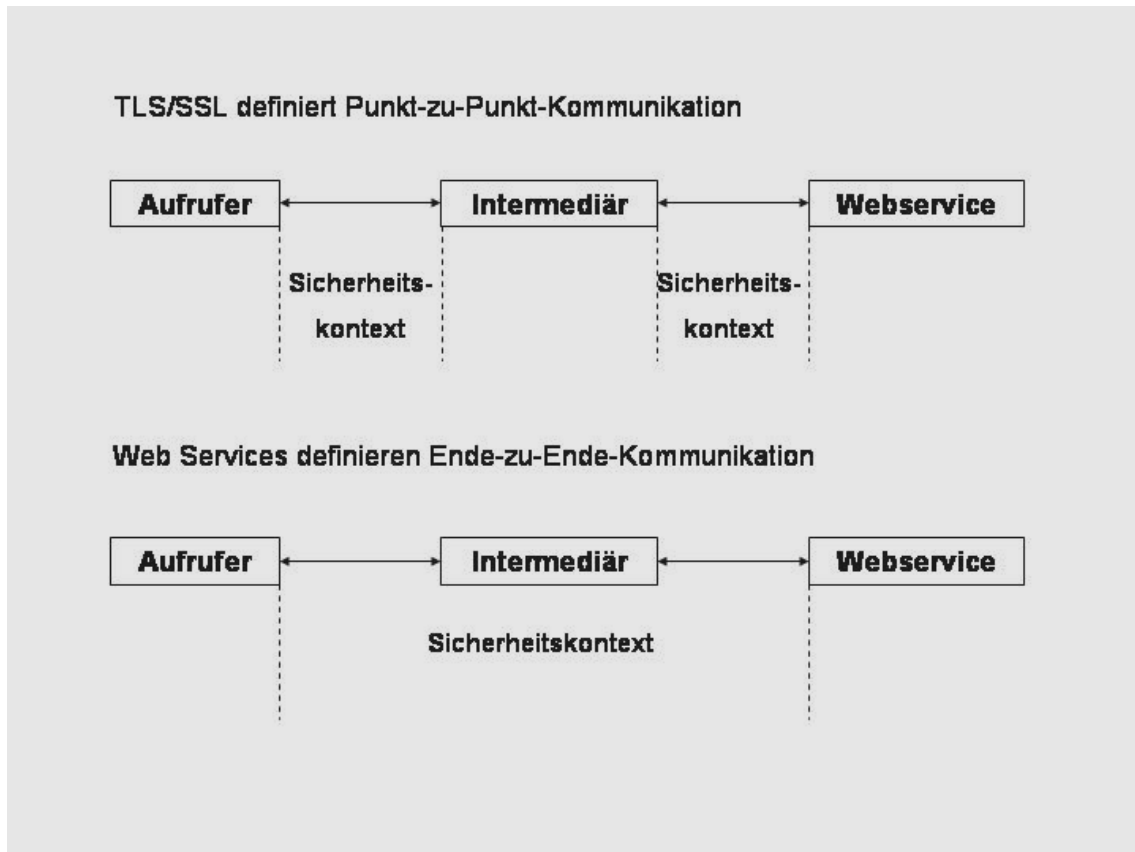


Abb. 4: Security-Kontext am Beispiel Webservice-Kommunikation

4.3 Autorisierung und Zugriffskontrolle

Der dauerhafte Schutz der in einem ArchiSafe konformen Langzeitspeicher abgelegten Informationen und Daten erfordert besondere Vorkehrungen für die Zugriffsberechtigung durch IT-Systeme und Personen. ArchiSafe konforme elektronische Archivsysteme sollten daher zumindest die Autorisierung (die Zugriffsrechte) von Benutzern und Komponenten auf der Grundlage einer für die Dauer der Kommunikation gesicherten und überprüfbaren Authentifizierung gewährleisten.

Anm.: Es dürfen lediglich autorisierte Instanzen Zugriff auf die im Langzeitspeicher abgelegten Daten und Informationen erhalten. Dabei können zusätzlich bestimmte Zugriffsarten (lesen, schreiben, löschen) je nach Zugriffsprofil eingeschränkt werden. Wichtig ist, dass die Bindung an die Identität (einer Person oder Komponente) auch nach erfolgreicher Authentifizierung überprüfbar bleibt.

5 Referenzen

- ArchiSig** Roßnagel, A., Schmücker, P. (Hrsg.): Beweiskräftige elektronische Archivierung, Economica-Verlag, ISBN 3-87081-427-6
- ARS1** ARS Spezifikation 1.0: Funktionale Anforderungen an eine dauerhafte und rechtssichere elektronische Ablage
<<http://www.archisafe.de>>
- ARS2** ARS Spezifikation 2.a: ARS-Metadatenstruktur;
ARS Spezifikation 2.b: ARS-XML Schema
<<http://www.archisafe.de>>
- ARS3** ARS Spezifikation 3.0: ARS Langzeitdokumentenformate
<<http://www.archisafe.de>>
- ARS4** ARS Spezifikation 4.0: ARS Signaturformate
<<http://www.archisafe.de>>
- CORBA** Common Object Request Broker Architecture
<<http://www.omg.org/corba-corner>>
- ETSI-TS** ETSI-TS 101 861 V 1.2.1 Time stamping profile, März 2002, unter :
<<http://www.etsi.org>>
- ERDOC** Stefanie Fischer-Dieskau: Der Elektronische Rechtsverkehr: Das elektronisch signierte Dokument als Mittel zur Beweissicherung (Anforderungen an seine langfristige Aufbewahrung), Nomos Verlag, Baden-Baden, 2006
- ISO/IEC 10118-3** ISO/IEC 10118-3, Information technology – Security techniques – Hash functions – Part 3: Dedicated hash functions, 1998
- LTANS:ERS** Brandner, R., Gondrom, T., Pordesch, U., Evidence Record Syntax (draft-

ietf-Itans-ers-09), October, 2006, unter
<<http://www.ietf.org/internet-drafts/draft-ietf-Itans-ers-09.txt>>

- MER 1980** Merkle, R., "Protocols for Public Key Cryptosystems, Proceedings of the 1980 IEEE Symposium on Security and Privacy (Oakland, CA, USA)", pages 122-134, April 1980.
- OSCI** Online Service Computer Interface (OSCI) – Transport v1.2
<<http://www.osci.de>>
- SOAP** Simple Object Access Protocol, Gudgin, M., Hadley, M., Mendelsohn, N., Moreau, J-J., Nielsen, H. F., SOAP Version 1.2 Part 1: Messaging Framework. REC-soap12-part1-20030524, W3C, Juni 2003,
<<http://www.w3.org/TR/soap12-part1>>
- TSP 2001** Adams, C., Cain, P., Pinkas, D., Zuccherato, R.: RFC 4161 – Internet X.509 Public Key Infrastructure Time Stamp Protocol (TSP), August 2001, unter:
<<http://www.ietf.org/rfc/rfc3161>>
- TLS / SSL** Transport Layer Security Protocol / Secure Socket Layer Protocol
Dierks, T., Allen, C., - The TLS Protocol version 1.0, RFC 2246 (Proposed Standard) IETF, Januar 1999, aktualisiert durch RFC 3546
<<http://www.ietf.org/rfc/rfc2246>>
- XMLDSIG** Eastlake, D., Reagle, J., Solo, D.: (Extensible Markup Language) XML-Signature Syntax and Processing. IETF Request For Comment 3275, März 2002, unter: <<http://www.ietf.org/rfc/rfc3275.txt>>