

ARCHISAFE

Rechts- und revisionssichere Langzeitarchivierung elektronischer Dokumente



Elektronische Dokumente sind aus dem öffentlichen Verwaltungshandeln nicht mehr wegzudenken. Die papiergebundene Aktenführung und das Büro als organisatorische Grundeinheit klassischer Verwaltung verlieren angesichts der flächendeckenden Einführung IT-gestützter Vorgangsbearbeitung zunehmend an Bedeutung. Wer aber die elektronische Akte als eine wesentliche Voraussetzung für weitere Fortschritte im E-Government will, der muss sich heute schon Gedanken machen, wie er die **Authentizität und Integrität, die Vertraulichkeit und Vollständigkeit digitaler Unterlagen nachhaltig**, und das bedeutet mindestens für den Zeitraum gesetzlich vorgeschriebener Aufbewahrungsfristen, **gewährleistet**. Elektronische Akten haben, wie ihre Vorgänger in Papierformat, im Rahmen des vom Gesetzgeber vorgeschriebenen ordnungsgemäßen Verwaltungshandelns über die unmittelbare Bearbeitung auch eine Nachweisfunktion zu erfüllen. Der Wechsel zu einer elektronischen Dokumenteninfrastruktur, mit zunehmend auch elektronisch signierten Dokumenten bleibt unvollständig, ohne ein adäquates elektronisches Archiv, das die langfristige und rechtssichere Aufbewahrung und Verfügbarkeit elektronischer Informationen gewährleistet. In der Praxis stehen Behörden dabei vor folgenden **Herausforderungen**:

- *Signaturalgorithmen veralten – §17 SigV sieht deswegen eine Übersignatur vor, die man allerdings auch mit einem Zeitstempel vornehmen kann, der mindestens die gleiche Qualität wie die Signaturen hat ('qualifizierte Zeitstempel').*
- *An die Nachweisbarkeit des Zeitpunktes der Erstellung eines Dokumentes werden mitunter höhere Anforderungen gestellt, als sie die Signatur erfüllen kann. Die Signatur alleine bezieht nämlich nur die (ggf. unsichere) Systemzeit am Arbeitsplatz ein.*
- *Die Mechanismen zur Sicherung der Beweiskraft sollen die Handhabbarkeit von archivierten elektronischen Dokumenten im normalen Arbeitsablauf in keiner Weise einschränken.*
- *Das Dokument soll auch in vielen Jahren prüfbar sein.*

Da hier eine rechts- und revisionssichere Archivierung besonders wichtig ist, hat die Physikalisch-Technische Bundesanstalt (**PTB**) ein Konzept erarbeitet, das Anwender dabei unterstützt, eine adäquate Archivierungsinfrastruktur zu erstellen und dabei den Gedanken einer Service Orientierten Architektur (SOA) zu verfolgen.

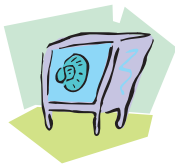


Das im Rahmen der E-Government-Initiative BundOnline 2005 begonnene Projekt ArchiSafe unterstützt und fördert die **Einführung bundeseinheitlicher Standards für die rechts- und revisionssichere Langzeitspeicherung (Archivierung) elektronischer Dokumente.**

Mit der Begründung eines standardisierten Datenaustauschformats für die Nutzdaten (Inhaltsdaten, Beschreibungs- und Signaturdaten) im XML-Format und der Implementierung einer Software-Referenzarchitektur schafft

ArchiSafe wesentliche Grundlagen für die Einführung und Nutzung zentraler als auch dezentraler elektronischer Archive bis hin zum Bundesarchiv.

Im Rahmen dieses Projektes sind, gemeinsam mit dem Bundesamt für Sicherheit in der Informationstechnik, der Bundesnetzagentur, der KBSt, dem Bundesarchiv und Mitarbeitern aus mehr als 20 verschiedenen Bundes- und Landesbehörden, Anforderungen und technische Lösungsmöglichkeiten für eine dauerhafte rechts- und revisionssichere elektronische Ablage rechtsverbindlicher und rechnungsbegründender elektronischer Unterlagen erörtert, bewertet und veröffentlicht worden (www.archisafe.de), die neben der sicheren und langfristig verkehrsfähigen Aufbewahrung der Unterlagen auch die Anforderungen des Signaturgesetzes erfüllen.



Zu den bestimmenden **Ergebnissen und Empfehlungen** des Projektes ArchiSafe gehören:

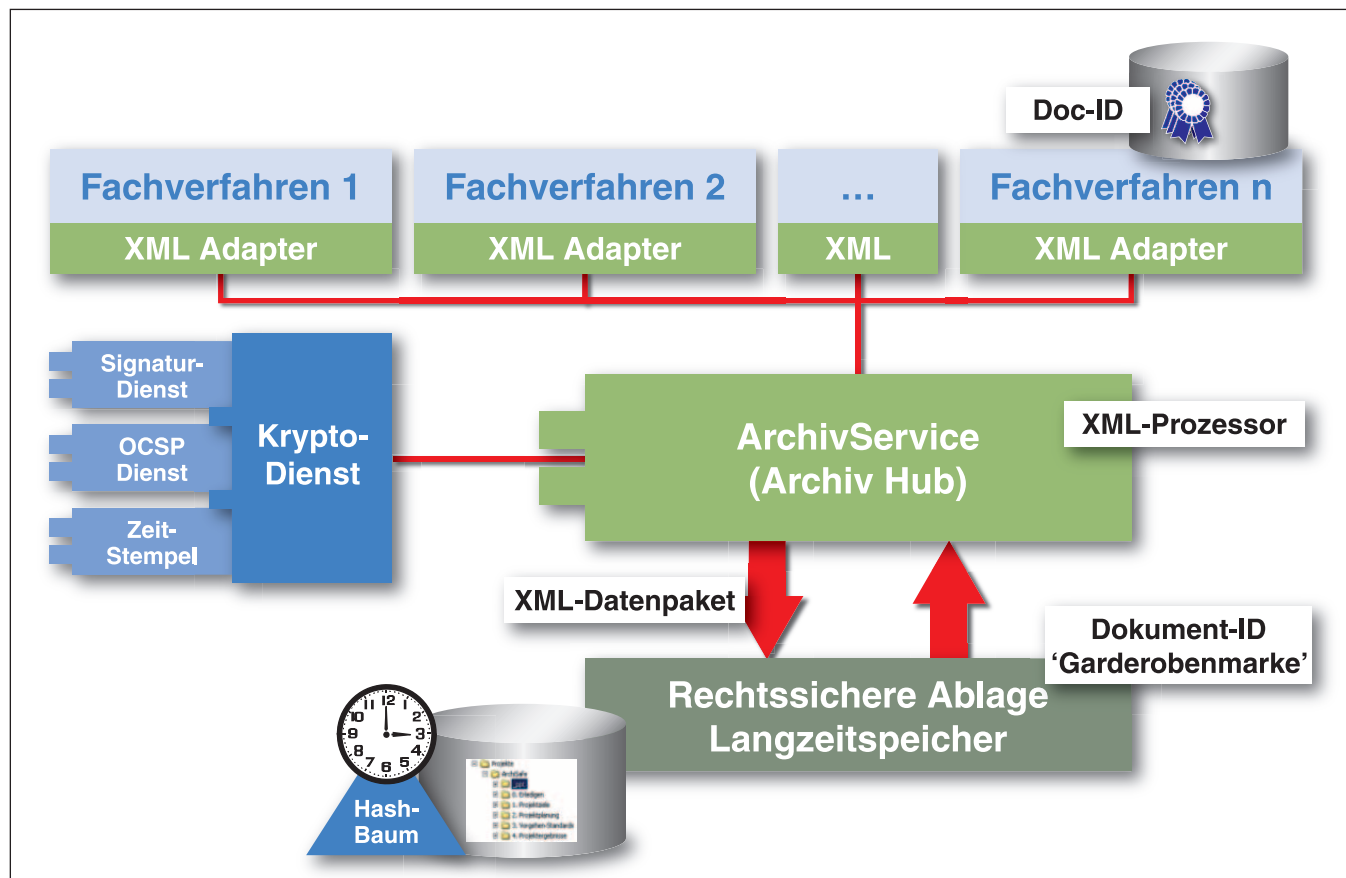
- die Verwendung eindeutig interpretierbarer, langfristig stabiler und veröffentlichter Nutzdatenformate
- die Verwendung eindeutig interpretierbarer, langfristig stabiler und standardisierter Signaturdatenformate
- die Berücksichtigung der Sicherheitseignung kryptografischer Algorithmen und Verwendung elektronischer Signaturen mit ausreichend hohem Sicherheitsniveau (qualifizierte elektronische Signatur)
- die Archivierung erforderlicher Verifikationsdaten in verkehrsfähiger Form
- die rechtzeitige und beweiskräftige Signaturerneuerung
- die stabile Verfügbarkeit technischer Komponenten
- die sichere Transformation elektronisch signierter Dokumente
- die Gewährleistung des Daten- und Geheimnisschutzes
- eine erhöhte Sicherheit durch Redundanz bei der Speicherung und Erneuerung elektronisch signierter Dokumente
- die Kosteneffizienz durch Nachnutzbarkeit, Skalierbarkeit und den Einsatz standardisierter und wirtschaftlicher Techniken und Technologien

Die ArchiSafe-Referenz-Architektur

Technisch gesehen basiert das ArchiSafe-Konzept auf einer serviceorientierten, geschichteten und mandantenfähigen Softwarearchitektur.

Ein **Fachverfahren (Dokumentenmanagement- oder Vorgangsbearbeitungssystem)** dient als Plattform und führendes System zur Dokumentenverwaltung und Vorgangsbildung sowie als Schnittstelle zur Langzeitspeicherung. Das Fachverfahren initiiert den Request für die Ablage elektronischer Dokumente im elektronischen Archiv und verwaltet die vom Archivsystem erzeugten Dokumentkennungen für die im Langzeitspeicher abgelegten Dokumente. Hierzu gehört die Verknüpfung der Dokumentkennungen gespeicherter Dokumente mit den für die operative Vorgangsbearbeitung vorgehaltenen Dokumentinstanzen und Prozessdaten.

Abbildung 1: ArchiSafe Architekturschema



Das Fachverfahren kommuniziert mit dem Langzeitspeicher über eine einheitliche Archiv-Schnittstelle (Archivservice) zur Übergabe der zu archivierenden Objekte (Dokumente, Vorgänge, Akten) an die Langzeitspeicherung.

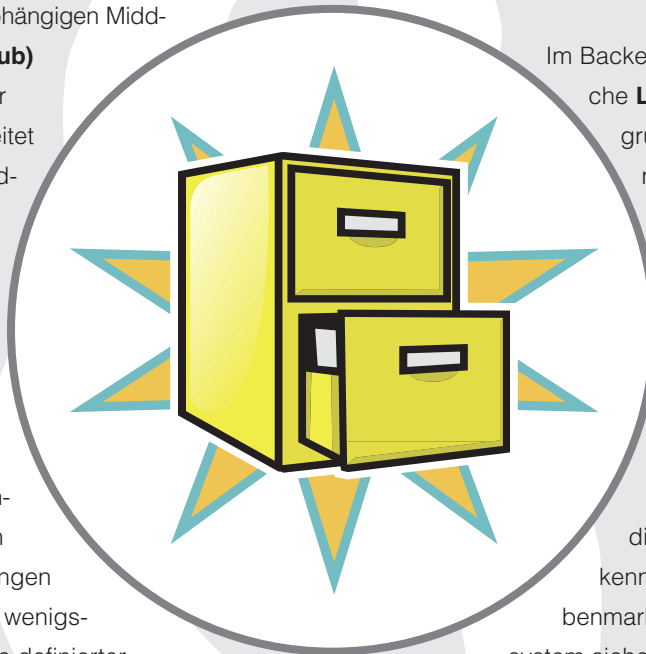
Der Archivservice für die Übergabe von elektronischem Schriftgut aus den Fachanwendungen an das Langzeitspeichersystem wird in einer systemunabhängigen Middleware-Komponente (**Archive Hub**) abgebildet (s. Abbildung 1). Der Archivservice prüft und verarbeitet die Archivobjekte auf der Grundlage standardisierter Zeichensätze und Datenformate sowie syntaktischer und semantischer Vereinbarungen für die Strukturen der im Langzeitspeicher abzulegenden Datenobjekte. Der Archivservice fordert darüber hinaus gegebenenfalls kryptografische Funktionen wie Signaturen, Zertifikatsprüfungen und Zeitstempel an und sollten wenigstens XML-Formate auf der Basis definierter XML-Schemata verarbeiten können.

Die Erzeugung der standardisierten Archivobjekte und die Kommunikationseröffnung mit dem Archivservice erfolgt in fachspezifischen Serviceschnittstellen (Service-Adaptern).

Im Kern besteht der Archivservice aus einem **XML-Prozessor** mit definierten Schnittstellen (Kommunikationskanälen) zu den Fachverfahren und zum elektronischen Langzeitspeicher. Darüber hinaus soll der Archivservice die Anbindung zusätzlicher Dienste, wie beispielsweise den Signaturdienst und den Zeitstempeldienst ermöglichen. Die **kryptografischen Dienste** signieren auf Anforderung durch das Fachverfahren die in den elektronischen Langzeitspeicher einzustellenden Dokumente oder versehen sie mit einem Zeitstempel. Sie verifizieren zudem auf Anforderung durch das Fachverfahren die Signaturen und Zertifikate signierter Dokumente und stellen dem Archivservice die Verifikationsdaten zur Verfügung, der diese wiederum für eine spätere Nachweisfunktion in einem standardisierten Format in die Archivobjekte einbettet.

Im Projekt ArchiSafe werden die kryptografischen Dienste über das Kernsystem der **virtuellen Poststelle** des Bundes abgebildet.

Die Übergabe an den elektronischen Langzeitspeicher kann optional mit einem Zeitstempel für die zu speichernden Dokumente kombiniert werden. Darüber hinaus wird ein Zeitstempeldienst für die Signaturerneuerung elektronisch signierter Dokumente nach § 17 SigV benötigt. Das Projekt ArchiSafe setzt hierbei auf das als rechtssicher eingestufte und bewährte ArchiSig-Verfahren auf (<http://www.archisig.de>).



Im Backend liegt schließlich das eigentliche **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 Vergabe eindeutiger Dokumentenkennungen (**Dokument-ID**, 'Gardero-benmarken') 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 Originaldokumenten, ohne das Langzeitspeichersystem mit vorgangsspezifischen Logiken zu überfrachten. Für die Realisierung einer mandantenfähigen Lösung kann die Dokument-ID zusätzlich mit einer eindeutigen Kennung für das zuständige Fachverfahren verknüpft werden. Auf diese Weise lässt sich über ein Berechtigungskonzept im Fachverfahren sicherstellen, dass unzulässige Zugriffe auf die archivierten Daten verhindert werden.

Um einen vom Fachverfahren unabhängigen Zugriff auf den Langzeitspeicher zu ermöglichen, kann – auf Anforderung – ergänzend ein **Such- und Darstellungsdienst** sinnvoll sein. Insbesondere dann, wenn eine mandantenfähige Lösung angestrebt wird. Über diesen Dienst, der die im Langzeitspeicher vorhandenen Metadaten datenbankgestützt redundant vorhält, kann bei einem Ausfall des führenden Systems eine Rekonstruktion der Vorgänge oder Akten erfolgen. Bei Bedarf können die Daten und Dokumente in einer weiterverwendbaren Form präsentiert (Viewer) oder exportiert werden. Die Implementierung eines solchen Dienstes darf jedoch auf keinen Fall die Möglichkeit einräumen, die gesetzlich vorgeschriebenen Datenschutzbestimmungen zu unterlaufen.

IBM Aktivitäten im Bereich ArchiSig und ArchiSafe

Seit 2004 nutzen Kunden der IBM ein funktionales **Erweiterungsmodul für IBM Archivsysteme**, um signierte Dokumente langfristig rechtssicher zu archivieren. Diese setzt die Vorgaben des Bundesprojektes ArchiSig vollständig um.

Das IBM Archivsystem – z. B. **IBM Content Manager oder FileNet P8** – übernimmt dabei die Speicherung der Dokumente. Zusätzlich werden hier Signaturen, falls sie in Form von weiteren Dateien zum Dokument vorliegen, als Dokument-Zusatzobjekt (Part) gespeichert.

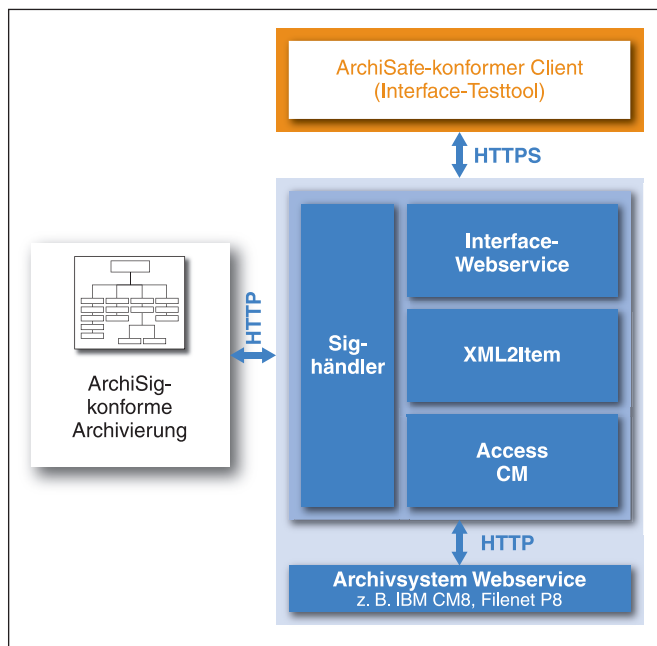


Abbildung 2 Integration eines IBM Archivsystems in ArchiSafe

Parallel zur Archivierung eines Dokumentes im IBM Archivsystem werden die zur Beweissicherung notwendigen Informationen (z. B. Hashwerte über Dokument und Signatur, sowie OSCP Prüfergebnisse) an das Erweiterungsmodul übertragen.

Die Erweiterung organisiert die Speicherung dieser Informationen in einer relationalen Datenbank in Form von **Hashbäumen** nach ArchiSig.

Durch einen täglichen Abschluss dieser Hashbäume mit einem Zeitstempel kann später tagesgenau bewiesen werden, wann das Dokument archiviert wurde. Wenn die im Laufe der Zeit eine **Übersignatur** erforderlich wird, werden die bestehenden Zeitstempel wieder zeitgestempelt. Dadurch wird die Beweiskraft der Dokumente und Signaturen langfristig gesichert.

Bei einer vollständigen **Prüfung** wird ein Dokument zunächst aus dem IBM Archivsystem exportiert. Über eine Revisionsanwendung wird dann zu diesem Dokument das Beweisdokument nach dem LTANS Standard/ietf.org exportiert. Dann erfolgt die Prüfung aller Signaturen und Zeitstempel.

Wenn Dokumente im IBM Archivsystem gelöscht werden, bleiben die zugehörigen Informationen zur Beweissicherung erhalten. Da diese keine Informationen über den Inhalt des Dokumentes enthalten, ist dies datenschutzrechtlich unbedenklich.

Die Lösung kann zur Durchführung der kryptographischen Operationen optional die BundOnline Basiskomponente „Virtuelle Poststelle“ einbinden.

Diese Erweiterung wurde auch genutzt, um das Archivsystem als Langzeitspeicher in die ArchiSafe-Referenzarchitektur zu integrieren. Durch eine lose Kopplung der Komponenten über **Webservices** wurde eine flexible Schnittstelle geschaffen, die es ermöglicht, durch geringe Anpassungen jegliche Archivierungsszenarien abzubilden. Dabei wurde besonderen Wert auf die von der PTB im Rahmen des ArchiSafe-Projekts gegebenen Empfehlungen gelegt.

Die Erweiterung des IBM Archivsystems für ArchiSafe ermöglicht es also, mit geringem Aufwand die Beweiskraft archivierter Dokumente – gleich ob signiert oder unsigniert – wesentlich zu erhöhen, und damit elektronischen Dokumenten einen mit Papierdokumenten vergleichbaren Beweiswert zu geben.



Ansprechpartner für das Projekt ArchiSafe

IBM kooperiert mit der CSC Deutschland Solutions GmbH und der Physikalisch-Technischen Bundesanstalt (PTB) bei dem Projekt ArchiSafe (Langzeitarchivierung). CSC und IBM beraten bei der Planung und Realisierung ArchiSafe-konformer Archivierungssysteme.



Physikalisch-Technische Bundesanstalt Braunschweig:

Herr Dir. u. Prof. Dr. Siegfried Hackel,

Behördenansprechpartner im Rahmen der Initiative

BundOnline 2005

Tel.: +49 531 592-8400

Fax.: +49 531 592-8406

E-Mail: siegfried.hackel@ptb.de



CSC Deutschland Solutions GmbH

Susanne Körner

Hohenzollerndamm 183

10713 Berlin

Tel.: +49 30 61653-201

E-Mail: skorner@csc.com

IBM Deutschland GmbH

Hanno Wiechmann

Frankfurter Str. 3c

38122 Braunschweig

Tel.: +49 531 2872536

E-Mail: hanno.wiechmann@de.ibm.com

Weitere Informationen sind auf folgenden Websites verfügbar:

<http://www.archisafe.de>

<http://de.country.csc.com/de/index.shtml>

ibm.com/software/de/db2/cm.html

ibm.com/gold/portal/servlet/gold/public-germany/Welcome



IBM Deutschland GmbH

70548 Stuttgart

ibm.com/de

IBM Österreich

Obere Donaustraße 95

1020 Wien

ibm.com/at

IBM Schweiz

Vulkanstrasse 106

8010 Zürich

ibm.com/ch

Die IBM Homepage finden Sie unter:

ibm.com

IBM, das IBM Logo, das e-Logo und ibm.com sind eingetragene Marken der IBM Corporation.

Weitere Unternehmens-, Produkt- oder Servicenamen können Marken anderer Hersteller sein.

Gedruckt in Deutschland.

© Copyright IBM Corporation 2007

Alle Rechte vorbehalten.