Langzeitspeicherung und Archivierung - zwei Seiten einer Medaille!

Aktuelle Standards und Normen zur beweiswerterhaltenden Aufbewahrung elektronischer Unterlagen

Steffen Schwalm, Business Advisor

19. Tagung des Arbeitskreises „Archivierung von Unterlagen aus digitalen Systemen“ , Wien, den 10. März 2015

Agenda

- **Einführung und rechtlich-organisatorischer Rahmen**
- Aktuelle Normen und Standards zur beweiswerterhaltenden Langzeitspeicherung
- Aktuelle Anwendungsfälle und Ausblick.

Aktuelle Herausforderung elektronischer Geschäftsprozesse

Sicherheit und Nachweisfähigkeit lässt sich nur durch Standardisierung errreichen.

Herausforderungen

- Lange Aufbewahrungsfristen
- Zurückgehende Lebens-zyklen IT-Verfahren
- Sicherstellung Daten- und Beweiswerterhalt (Dokumentationspflichten)
- Medienbruchfreie Prozesse, sichere Kommunikation
- Minimierung Kosten und Ressourceneinsatz

Sicherstellung

- Authentizität
- Integrität
- Verlässlichkeit
- Verkehrs-fähigkeit
- Lesbarkeit

Lösung: Beweissichere Aktenführung und Langzeitspeicherung

- Verfahrens-/ Herstellerunabhängig
- Objektbezogen
- Nutzung etablierter Standards
- Definierte einheitliche Prozesse
- Formalisierte Daten
- Diensteorientiert
- Verbindliche Regularien, vollständige Akten, Compliance
- Vertrauenswürdig

EU-Verordnung elektronische Vertrauensdienste (eIDAS)

Verbindliche Rechtsgrundlage seit September 2014, Implementing Acts: Juli 2016

Regelungsinhalte

- Einheitliche Maßgaben für sichere elektronische Geschäftsprozesse in Europa
- Vorgaben zur rechtlichen Bedeutung und technischen Umsetzung
- QES = Ersatz Unterschrift
- QES = höchster Beweiswert

- Notifizierung qualifizierter Vertrauens-dienste durch einheitliche Zertifizierungsstellen je EU-Land
- Eintragung der VDA in Trusted List

- Behörden müssen alle Produkt quallif. VDA annehmen und prüfen können
- Rechtliche Detaillierung in Implementing Acts
- Technisch: ETSI- Normen, auf die die Implementing Acts referenzieren
- Abweichung von ETSI möglich bei kostenfreier Bereitstellung eines Prüftools

Kernthemen eIDAS

QES, QZS, Siegel

- Organisationszertifikate möglich
- Kein zwingender Bezug zur natürlichen Person
- Produkte qualif. VDA europaweit anzuerkennen

Verwahrungsdienste

- Beweiswerterhalt der QES, QZS, Siegel etc. gem. ETSI

Zustelldienste

- Nachweisbare Zustellung europaweit

Authentisierung

- Einheitliche Identifkation
- Umsetzung: 2018

Handlungsbedarf

- **Erzeugung und Prüfung der QES/QZS/Siegel des entspr. Landes**
- **Einfachere Nutzung**

- **Beweiswerterhaltung gem. ETSI**
- **Anpassung Archivierung**

- **Nutzung Zustelldienste**
- **Durchgängig elektron. Prozesse**

- **Durchgängig elektron. Prozesse**
- **Zeit bis 2018**

Beweiswert elektronischer Unterlagen

private elektronische Dokumente (von Bürger/Unternehmen) ohne qualifizierte elektronische Signatur	private elektronische Dokumente (von Bürger/Unternehmen) mit qualifizierter elektronischer Signatur bzw. De-Mail mit qualifiziert signierter Absendebestätigung	Öffentliche elektronische Dokumente (von Behörde) ohne qualifizierte elektronische Signatur	öffentliche elektronische Dokumente (von Behörde) mit qualifizierter elektronischer Signatur bzw. De-Mail mit qualifiziert signierter Absendebetätigung
Freie Beweiswürdigung des Richters	Anschein für Echtheit	Freie Beweiswürdigung des Richters	Vermutung für Echtheit

eIDAS: höchster Beweiswert mit qualifizierter elektronischer Signatur!

Bedingung: Aufbewahrung im Aktenzusammenhang; eine unvollständige Aktenführung führt zu einer Beweislastumkehr zuungunsten der Verwaltung

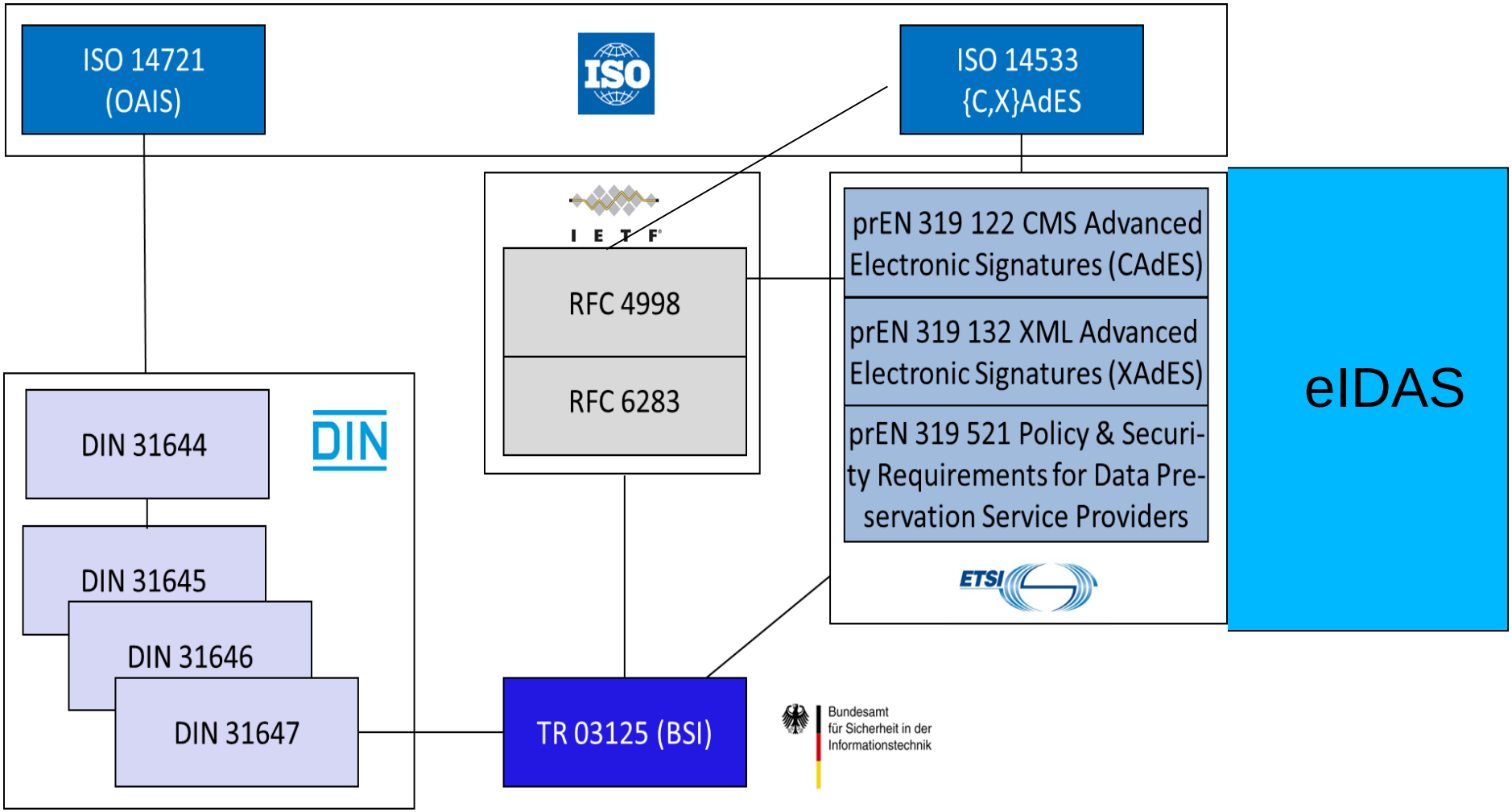
Die Verwaltung führt den Beweis durch Akten (§ 99 VwGO, OVG Greifswald)!

Agenda

- Einführung und rechtlich-organisatorischer Rahmen
- **Aktuelle Normen und Standards zur beweiswerterhaltenden Langzeitspeicherung**
- Aktuelle Anwendungsfälle und Ausblick.

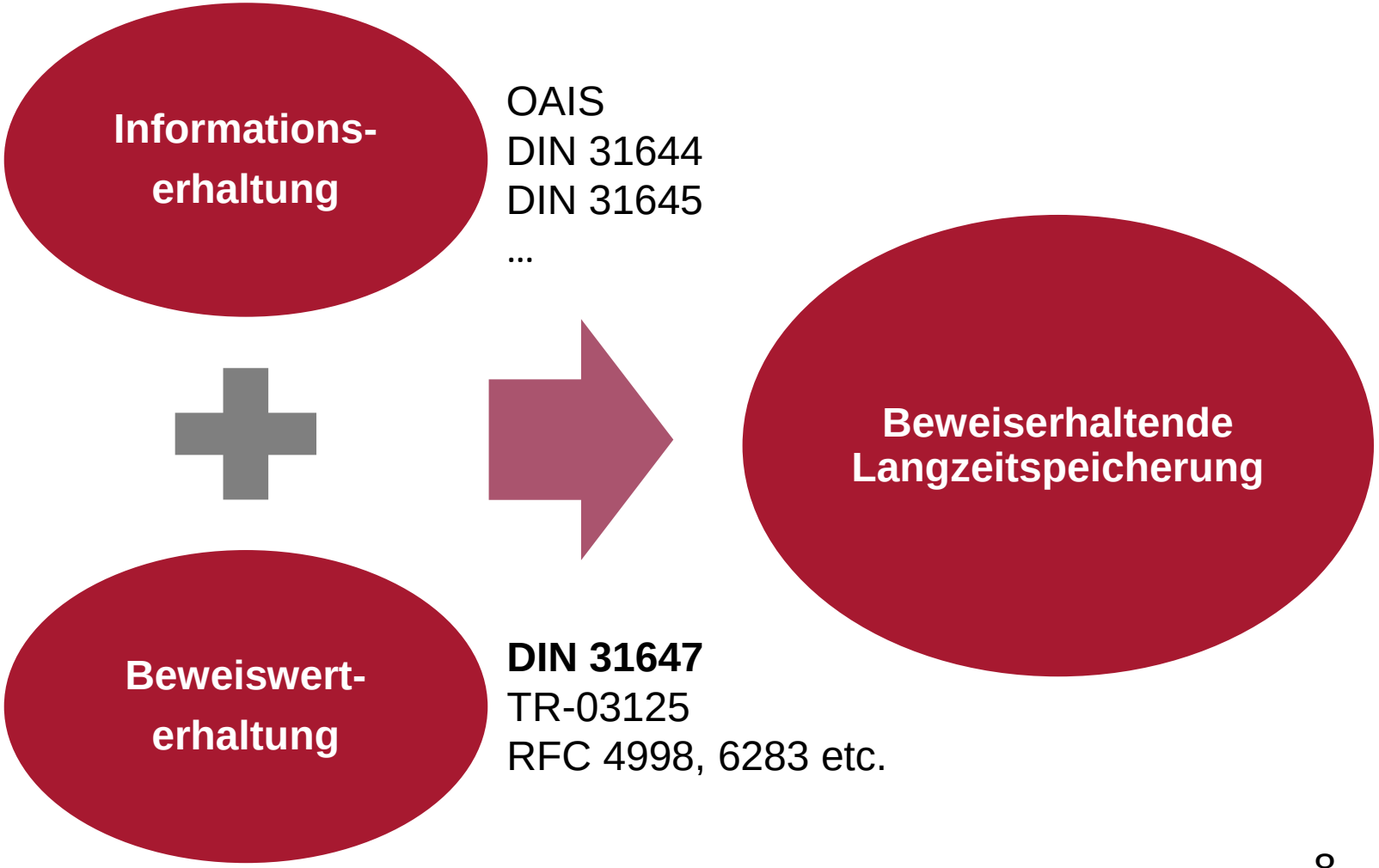
Normen und Standards zur Langzeitspeicherung und Beweiswerterhaltung

Die DIN 31647 sowie die TR-ESOR vereinigen die relevanten Standards zur Erhaltung elektronischer Unterlagen

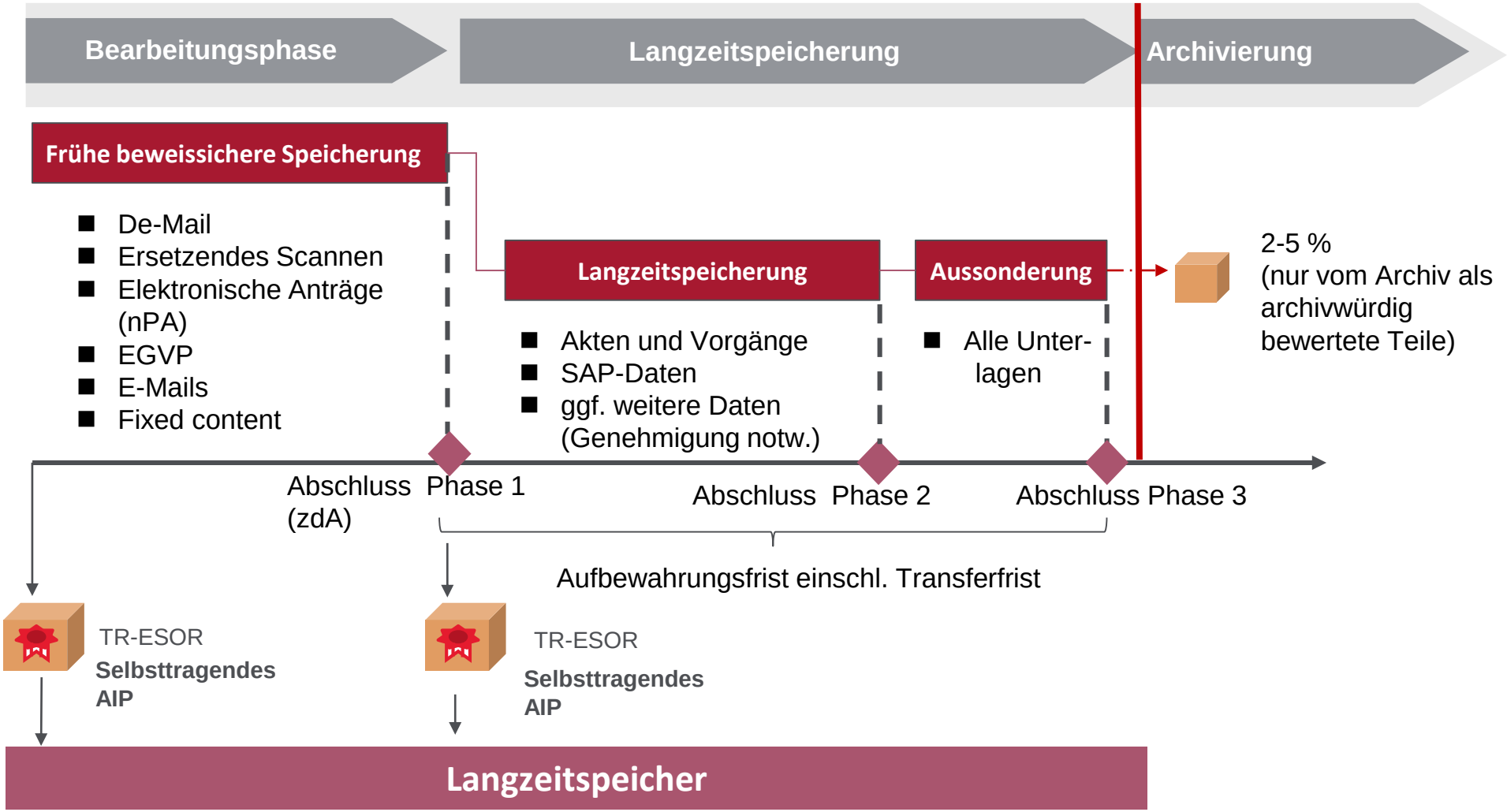


Eine beweiswerterhaltende Langzeitspeicherung sichert die Erhaltung der Daten und deren Beweiswert.

Zur Umsetzung werden geltende Standards und Normen eingesetzt.



Mögliche Anwendungsfälle einer beweissicheren Langzeitspeicherung



DIN 31647: Neben den Informationen zur Erhaltung der Daten selbst, sind diejenigen zur Erhaltung des Beweiswerts erforderlich

Die AIP sind um die notwendigen Daten zur Beweiswerterhaltung zu ergänzen

Beweisrelevante Daten

Zur Beweisführung notwendig von Metadaten und Inhaltsdaten abzugrenzen:

- Signaturen und Informationen zu Signaturprüfung
- Zeitstempel
- Sperrdaten
- Zertifikaten und Zertifikatstatusinformationen

==> Beleg, dass die ggf. außerhalb des Archives erzeugten Signaturen und Zeitstempel gültig sind bzw. zum Erstellungszeitpunkt gültig waren.

Technische Beweisdaten

Zur dauerhaften Beweissicherung notwendig:

- Evidence Record (RFC 4998, 6283)
- Archivzeitstempel ausreichender Qualität über die gespeicherten Daten zum Nachweis
- der Integrität und Authentizität
- der rechtzeitigen periodischen Übersignierung

- ==> Beleg, dass das Archivdatenobjekt ab dem Zeitpunkt der Erzeugung der Beweisdaten nicht mehr verändert wurde

Die DIN 31647 beschreibt ein generisches System zur Beweiswerterhaltung

Ein digitales Langzeitarchiv, das den Beweiswert der elektronischen Unterlage erhält, erfüllt die folgenden Anforderungen und Funktionen

Funktionale Anforderungen

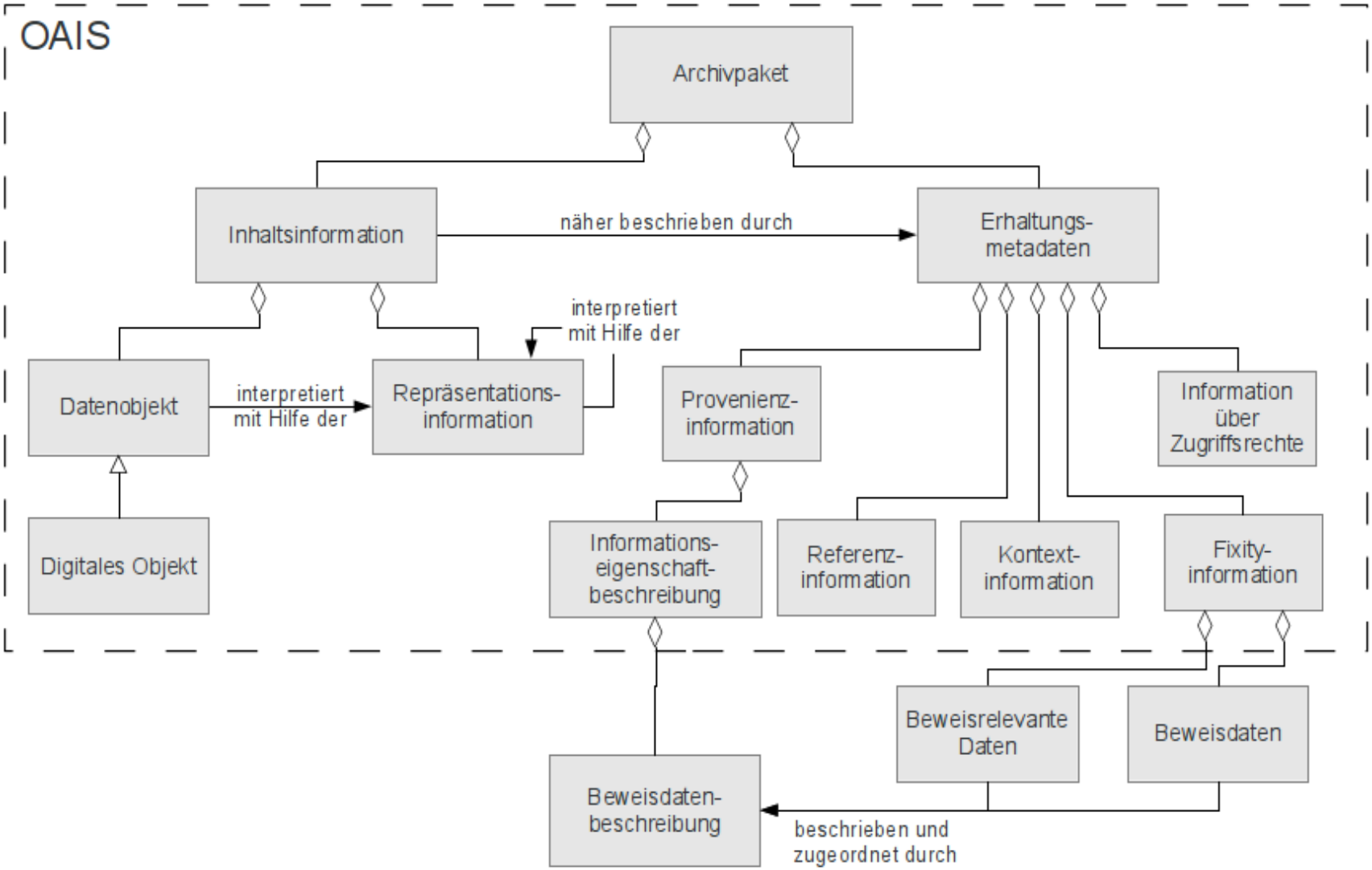
- Hashen von AIP
  - Möglichst zeitnah nach Erstellung AIP
  - Sicherheitsgeeignete Algorithmen
  - Hashalgorithmus entspricht dem des Archivzeitstempels
- Sortierung, Kanonisierung der Daten
- Nachvollziehbarkeit
- Ungehinderter Datenaustausch
  - Selbsttragende AIP
  - Keine Verletzung des Beweiswerts

Funktionen

- Einholen und Prüfen der beweisrelevaten Daten des SIP
- Erzeugung technischer Beweisdaten (Archivzeitstempel)
  - Möglichst zeitnah hashen
- Abruf des AIP mit den technischen Beweisdaten
- Prüfung technischer Beweisdaten
- Erhaltung und Erneuerung der technischen Beweisdaten des AIP
  - Neusignierung
  - Hasherneuerung

Basis:
- RFC 4998, 6283 (Evidence Records)

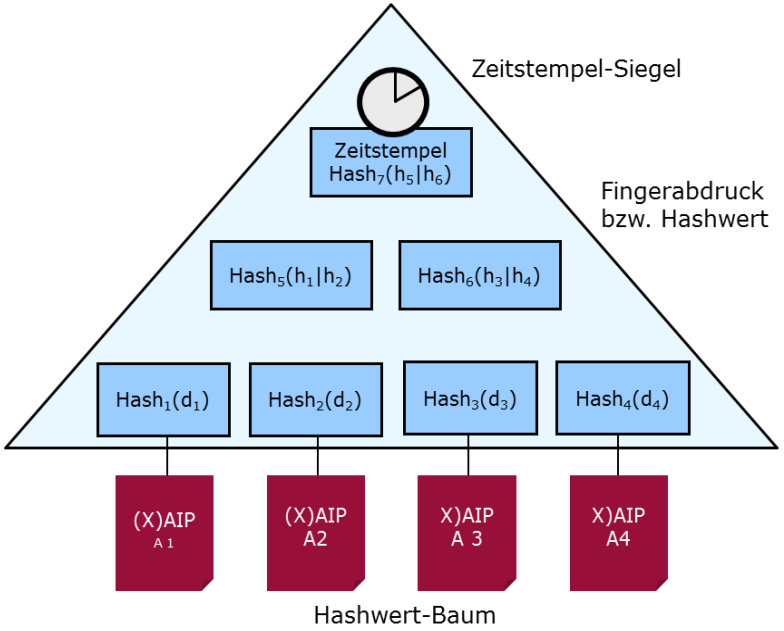
Einordung der DIN 31647 in OAIS



Beweiswerterhaltung gem. RFC 4998/6283

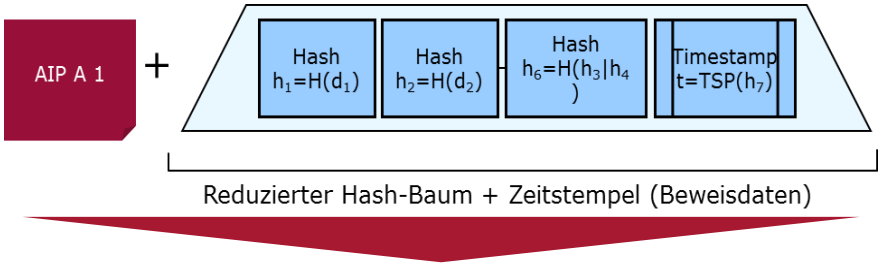
Hash-Baum

- Hash-Werte beliebig vieler Dokumente
- Pro Hash-Baum nur EIN akkreditierter Zeitstempel



Beweis-Dokument

- Reduzierter Hash-Baum und Zeitstempel (einschl. Verifikationsdaten)



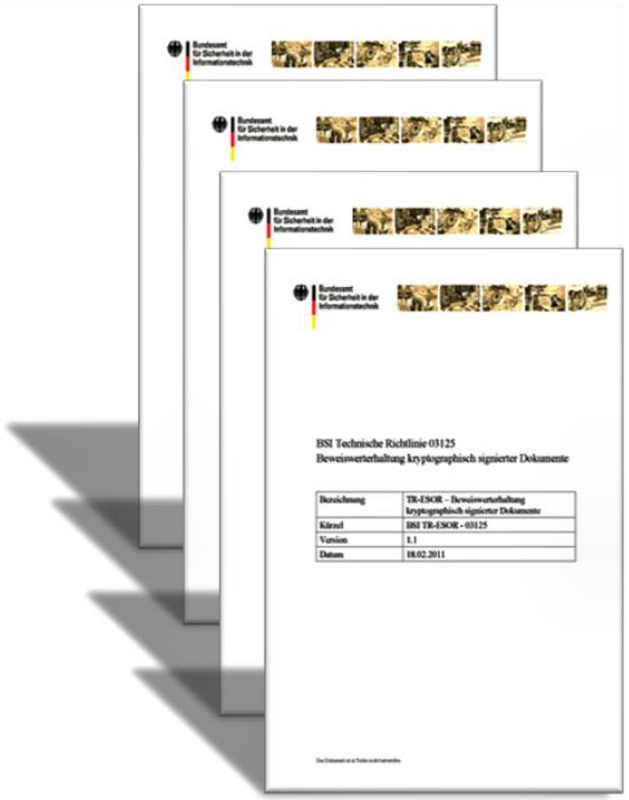
Selbsttragendes AIP:

- Metadaten, Inhaltsdaten

und

- zur Beweiswert-erhaltung notwendige Daten (Credentials)

TR-ESOR v1.2 ist eine Umsetzungsvariante der DIN 31647



TR-ESOR Hauptdokument

- TR-ESOR-M.1 ArchiSafe Modul
- TR-ESOR-M.2 Krypto Modul
- TR-ESOR-M.3 ArchiSig Modul
- TR-ESOR-S Schnittstellen
- TR-ESOR-B Bundesbehördenprofil
- TR-ESOR-F Formate
- TR-ESOR-E Konkretisierung d. Schnittstellen auf Basis des eCard-API Frameworks
- TR-ESOR-VR Verifikationsreport für ausgewählte Datenstrukturen
- TR-ESOR-ERS Profilierung der Evidence Records auf Basis von RFC 4998 und RFC 6283
- TR-ESOR-XBDP Profilierung des XAIP
  mit XBARCH, XDOMEA und PREMIS
- TR-ESOR-C.1 Testspezifikation „Funktionale Konformität“
- TR-ESOR-C.2 Testspezifikation „Technische Konformität“
- TR-ESOR-C.3 Testspezifikation „Bundesbehörden-Profil“

+ Englisch Version BSI TR-03125 Version 1.2 (in Planung)

TR-03125 v1.2 im Überblick

- Aufbau auf XFDU
- Hashen Nettoinhalt
- Klarstellungen hinsichtlich Profilierungen
- Anpassungen Prozesse (Erweiterung, Löschen etc.)
- Volle Abwärtskompatibilität
- Behördenprofil sowie Zertifizierungsanhänge C1-3

Wesentliche Inhalte Behördenprofil

Thema	Maßgaben
Format	• XAIP gem. Anhang F als MUSS-Anforderung • Validierung bei ArchiveSubmissionRequest • XAIP (B) als SOLL-Anforderung • Langfristig lesbare Formate als MUSS-Anforderung
Konformität	• Funktionale Konformität vorausgesetzt • Technische Konformität vorausgesetzt • Profilierung gem. eCARD-API-Framework voraugesetzt

Prozesse	• Löschprozess:
	  • Prüfung Bewertungsvermerk (Anbietungspflicht gem. § 2 BArchG)
	  • Prüfung Aufbewahrungsfrist

TR-ESOR-Profil-XBDP beschreibt die Ausgestaltung des XAIP für den bundesbehördlichen Umfeld

Mit Hinblick auf die Vorlagen aus den Bundes- und entsprechenden Länderarchivgesetzen wird die Rolle des sog. Bewertungsvormerks konkretisiert.

Aus den „preservation“-Informationen (Inhalt der *status*-Feldes innerhalb des *xaip:preservationInfoType* in XAIP) muss klar hervorgehen, welchen Status das Archivierungsobjekt aufweist, der vor dem Löschen des Objektes ausgewertet werden muss (Bewertungsvermerk).

Die **Status**-Information wird vom zuständigen Archiv erzeugt und nimmt einen der folgenden drei Werte an:

- **A** – (archivwürdig) – erst nach erfolgter Übergabe an das zuständige Archive und stattgefundener Löschfreigabe seitens des Archivs darf das Archivobjekt aus dem Langzeitspeicher gelöscht werden,
- **B** – (bewerten) – die Daten müssen vorweg vom zuständigen Archiv bewertet werden, danach wird gem. Status A bzw. V vorgegangen,
- **V** – (vernichten) – das Löschen des Archivobjektes ist nach dem Ablauf der Aufbewahrungsperiode direkt möglich.

Eine alternative Vorgehensweise ist zulässig, impliziert aber eine Erläuterung, dass diese gleichwertige Funktionalität anbietet

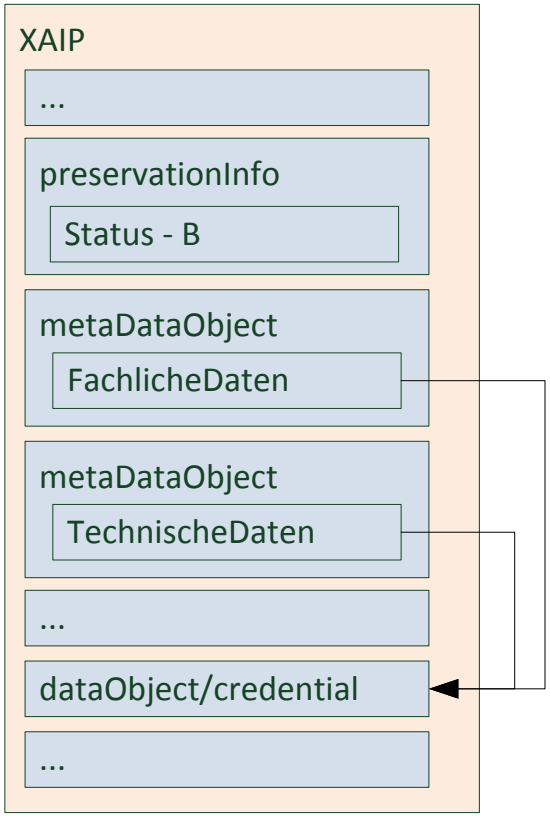
TR-ESOR-Profil-XBDP beschreibt die Ausgestaltung des XAIP für den bundesbehördlichen Umfeld

Insbesondere der Umgang mit Metadaten zur Beschreibung von Geschäfts- und Archivierungskontext ist hervorzuheben

Definition von zwei Arten der Metadaten, die sich jeweils auf ein innerhalb eines XAIP abgelegtes Datenobjekt/Credential beziehen:

- Technische Metadaten – beschreiben technische Gegebenheiten des abgelegten Objektes und bestehen im wesentlichen aus:
  - gem. dem Standard **XBARCH** des Bundesarchivs Definierten Datenstrukturen zur Ablage der technischen Metadaten (verpflichtend)
  - Optionalen Teil für die Ablage von zusätzlichen technischen Metadaten gem. dem **PREMIS**-Standard (Auswahl orientiert an XBARCH)
- Fachliche Metadaten – enthalten fachliche Inhalte zum korrespondierenden Objekt
  - Elektron. Schriftgut wird mit Hilfe des Elementen aus dem XDomea-Standard beschrieben
  - Weitere fachliche Metadaten entspr. Kategorisierung XFDU einbindbar

Die abgelegten Metadaten sind einer strengen Klassifikation unterzogen.



TR-03125 – Anhang-ERS

Die nachhaltige Erhaltung des Beweiswertes sowie der technischen Konformität und Interoperabilität

Vordergründige **Ziele**, die mit Anhang-ERS verfolgt wurden:

- langfristige und system- sowie plattformunabhängige Interpretierbarkeit der Daten,
- Interoperabilität zwischen unterschiedlichen Implementierungen von TR-ESOR
  - Hier insbesondere eine nahtlose Migration der Daten zwischen solchen Systemen, ohne die bestehende beweiswerterhaltende Aspekte zu verlieren

Der dabei ausgewählte Ansatz bestand darin, eine Definition eines Interoperabilitätsprofils für die beiden existierenden Ausprägung des Evidence Records zu erstellen, welche die Einhaltung der o.g. Ziele garantiert:

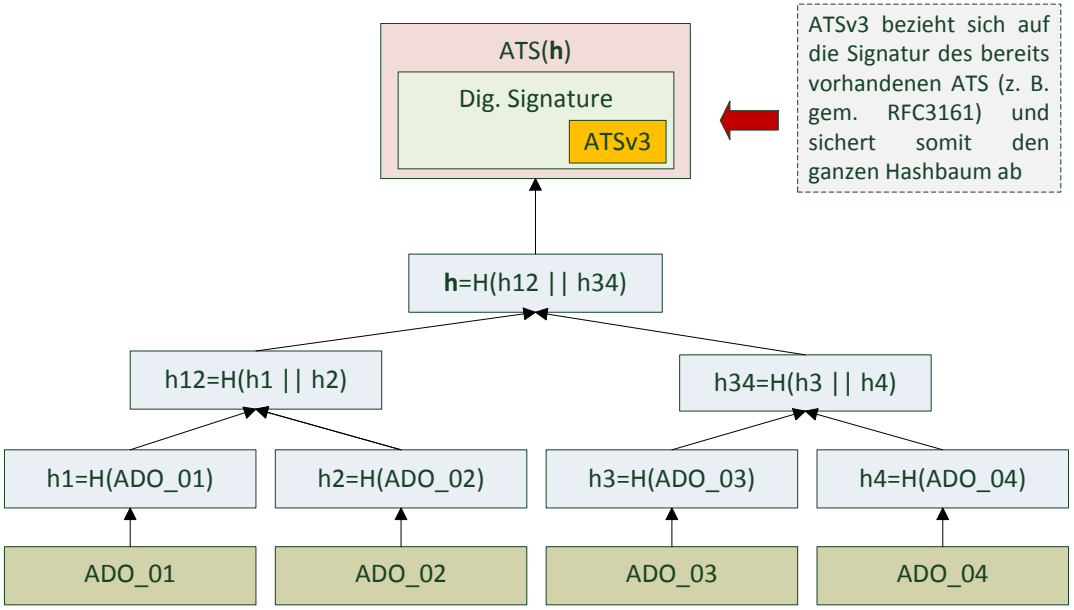
- **Basis-ERS-Profil** (verpflichtend) – ein Interoperabilitätsprofil für einen gem. [RFC4998] aufgebauten Evidence Record (ASN.1-konformer ERS), basiert auf [ISO14533-1] (CMS) und Langzeit-Basissignaturprofile (CAdES-Baseline-Profile) von ETSI
- **Basis-XERS-Profil** (optional) – ein Interoperabilitätsprofil für einen gem. [RFC6283] aufgebauten Evidence Record (XML-konformer ERS), basiert auf [ISO14533-2] (XMLDsig) sowie Langzeit-Basissignaturprofile (XAdES-Baseline Profile) von ETSI

Eine besondere Bedeutung innerhalb eines Evidence Record wird dem darin beinhaltenden **Archivzeitstempel** beigemessen:

- Definition eines Interoperabilitätsprofils für einen gem. [RFC3161] aufgebauten **Zeitstempel,**
- optionale Berücksichtigung des Einsatzes von „archive-time-stamp-v3“ (**ATSv3**) von ETSI (vgl. [ETSI TS 101 733] v. 2.2.1, Kap. 6.4.3) – Öffnung in die Richtung der kommenden europäischen Standards

Evidence Record vs. {C/X}-AdES-basierte Ansätze

Der Anhang ERS der TR-ESOR v.1.2 beschreibt die Möglichkeiten zur Interoperabilität zwischen RFC 4998/6283 und weiteren Lösungen zur beweiswerterhaltenden Aufbewahrung.



- Die Aspekten der Überschaubarkeit und Wirtschaftlichkeit bilden die Säulen des Vergleich der beiden Ansätze
  - ein qualifizierte ATS über ein gr. Merkle-Hashbaum (mit mehrerer Signaturen) – wirtschaftliche Lösung
  - ein ATSv3 über eine Signatur – kostspielig
- Ziel: Datenmigration aus einem System A in ein System B, beide System vertreten ein anderes Paradigma
  - Aufnahme des ATSv3 als zusätzliches Zeitstempelformat innerhalb von TR-03125
  - Optionale Benutzung eines Evidence Records (gem. RFC4998 oder RFC6283) als sog. „proof-of-evidence“ innerhalb der ETSI Standards

Associated Signature Container (ASIC) von ETSI

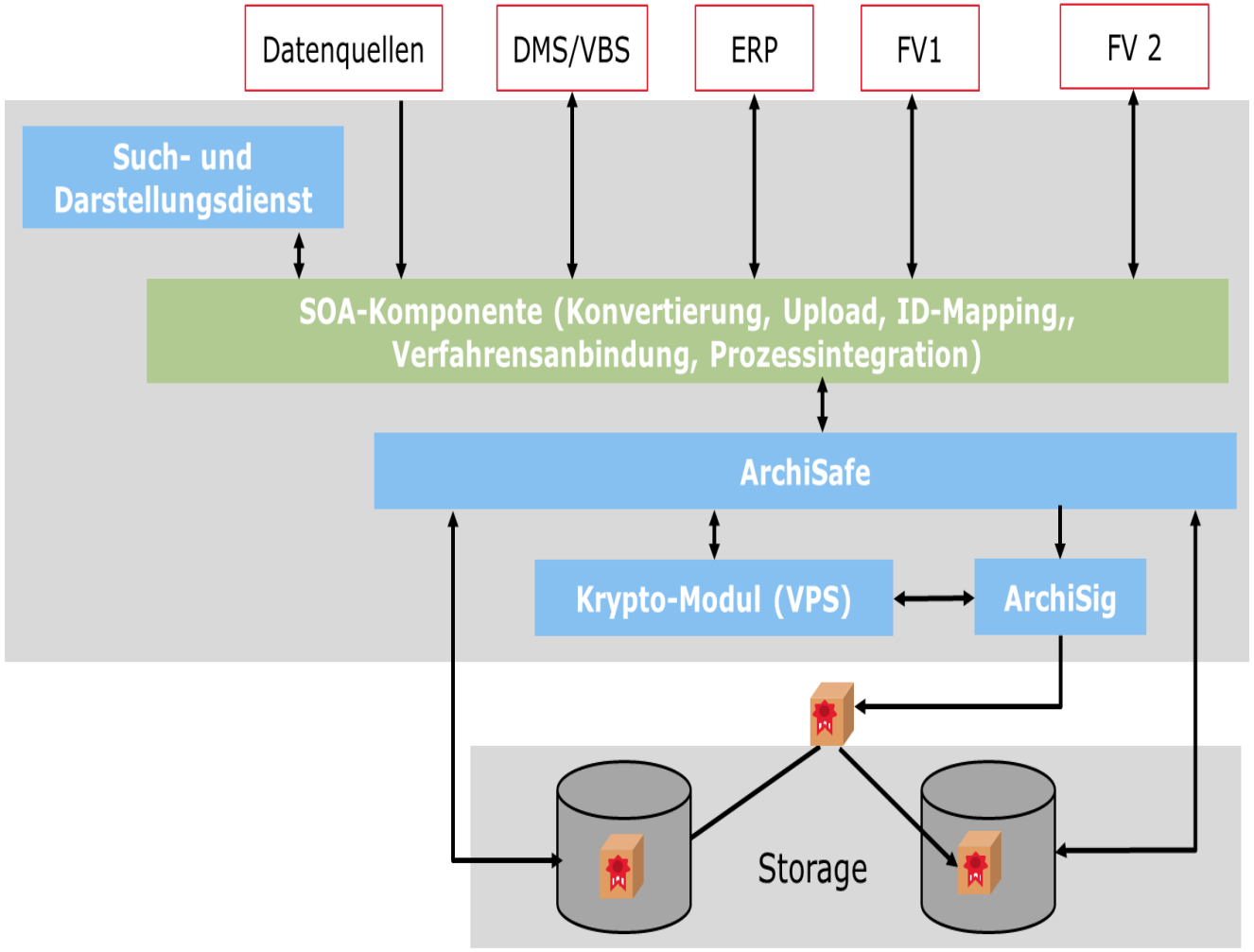
ASiC gibt einen wohldefinierten Container vor, indem die Daten zusammen mit dazugehörigen digitalen Signaturen aufbewahrt werden können.

- Gem. ETSI-EN 319162 basiert ein ASiC jeweils auf CAdES oder XAdES.
- Es werden folgende Signaturobjekte unterstützt
  - Signatur gemäß CAdES,
  - Signatur gemäß XAdES,
  - Zeitstempeltoken gem. RFC3161
- Ein ASiC basiert auf dem ZIP-Format.
- Man unterscheidet zwei Typen eines ASiCs:
  - ASiC-S - Simple Associated Signature Container, der nur ein signiertes Objekt beinhaltet
  - ASiC-E - beinhaltet ein oder mehrere signierte Objekte, jeweils mit möglichen mehrerer Signaturen und/oder Zeitstempeln.

Agenda

- Einführung und rechtlich-organisatorischer Rahmen
- Aktuelle Normen und Standards zur beweiswerterhaltenden Langzeitspeicherung
- **Aktuelle Anwendungsfälle und Ausblick**

Mögliche Lösungsarchitektur eines IT-Dienstes zur beweissicheren Langzeitspeicherung



- Offene Schnittstellen
- Webservices
- Standardisiert (Common Criteria, ISO-14533)
- Verfahrensanbindung im XML-Adapter (außerhalb der Referenzarchitektur
- Datenablage:
  - Funktionale und technische Konformität:
    - Alle digitalen Daten
    - Ausgabe nach XAIP muss möglich sein
  - Behördenprofil:
    - XAIP (SOLL)
- Datenabruf:
  - ArchiveRetrieval Request (Datenpaket)
  - ArchiveDataRequest (Einzeldatei in XAIP)

Aktuelle Anwendungsfälle/-umfang

Eine beweissichere Aufbewahrung geschäftsrelevanter Unterlagen ist branchenübergreifend ein essentieller Erfolgsfaktor nachvollziehbarer Geschäftsprozesse

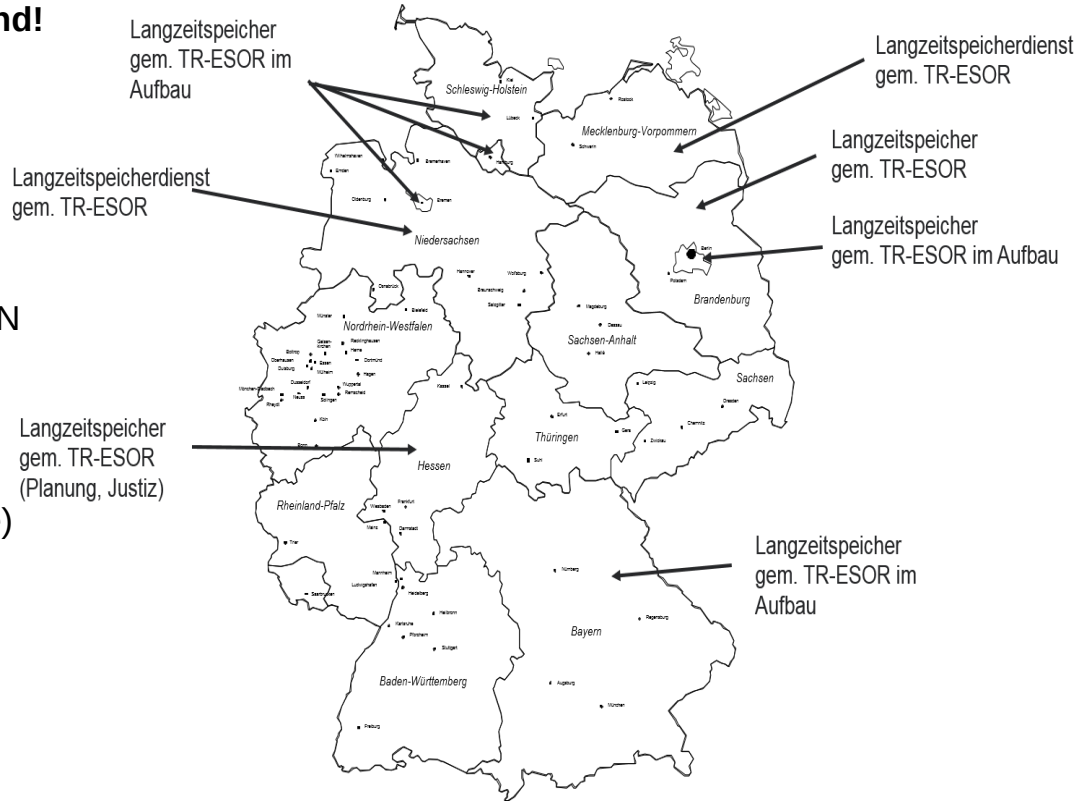
BA, Bundes-archiv
- Digitales Zwischenarchiv
- **Zentraler Dienst für Bund!**
- Fokus DMS/VBS

BMG
- Verfahrensübergreifender Dienst
- Aktuell Fachdaten

BImA
- Basis eRB und RESISCAN

BfArM
- Fachdaten
- Frühe Sicherung (Anträge)

N.N. (z.B. PTB etc.)
- Dezentrale Lösungen
- Alle Unterlagen



Unternehmen: Versicherungen, Banken, Luft- und Raumfahrt, Krankenkassen , HealthCare

Fazit & Ausblick

Ziel ist der Aufbau wirtschaftlicher Lösungen und übergreifender Standards zur Informations- und Beweiswerterhaltung

Einheitliche europäische Standards

- Verbesserung Interoperabilität und Konvergenz unterschiedlicher Ansätze
- Wirtschaftliche Form zur Beweiswerterhaltung
- Durchgängig elektronische und nachweisbare Prozesse im internationalen Rechts- und Geschäftsverkehr
- Einbeziehung der Erfahrung aus der Informationserhaltung

ASiC als universelles Austauschformat

- Standardisiertes ZIP-Format
- Speicherung großer Datenmengen ohne Nachteile der Base64-Codierung bei XML-Datenpaketen
- europäisches Austauschformat für nachweisbar authentische wie integre Daten
- Beweiswerterhaltung komplexer Daten (z.B. Einreichungen in Pharma/Industrie etc.) möglich

Europaweit Nachhaltigkeit elektronischer Geschäftsprozesse

- **Vertrauenswürdige Lösung zur Informations- und Beweiswerterhaltung**
- **Übergreifende Nutzung von Erfahrungen und Lösungen**
- **Aufbau übergreifender IT-Dienste möglich**
- **Nachhaltigkeit und Langfristigkeit elektronischer Geschäftsprozessse**

Für Fragen und Antworten:

Steffen Schwalm
Business Advisor

T +49 30 88004 9148
C + 49 162.2806472
steffen.schwalm@bearingpoint.com

BearingPoint GmbH
Kurfürstendamm 207-208
10719 Berlin, Germany

Thank you!