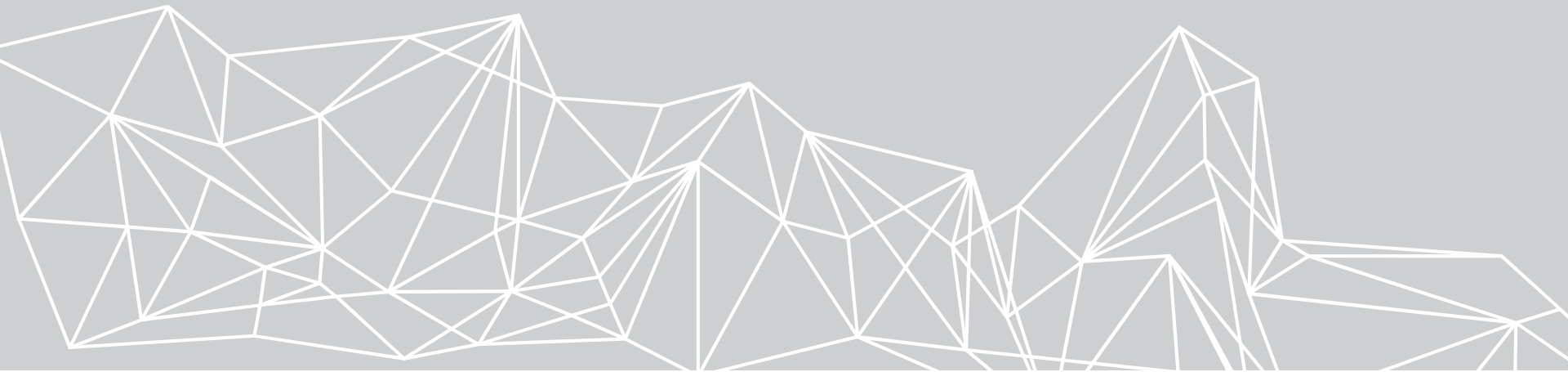


# INFORMATIONSFORUM „SICHER IST SICHER? – BEWEISWERT DIGITALER UNTERLAGEN“



Steffen Schwalm  
Projektgruppe TR-ESOR  
(Projektleitung: Fr. Dr. Ulrike Korte, Bundesamt für Sicherheit in der Informationstechnik;  
Projektmitglieder: Fraunhofer FOKUS, ecsec GmbH)

# AGENDA

1. Ausgangssituation
2. Normative Einordnung
3. Fachliche-technische Rahmenbedingungen
4. Lösungsbeispiele

# SICHERHEIT UND NACHWEISFÄHIGKEIT LÄSST SICH NUR DURCH STANDARDISIERUNG ERREICHEN – FÜR ALLE UNTERLAGEN

## Herausforderungen

Lange Aufbewahrungsfristen

Zurückgehende Lebenszyklen IT-Verfahren

Sicherstellung Daten- und Beweiswerterhalt (Dokumentationspflichten)

Medienbruchfreie Prozesse, sichere Kommunikation

Minimierung Kosten und Ressourceneinsatz

## Sicherstellung

- Authentizität
- Integrität
- Verlässlichkeit
- Verkehrsfähigkeit
- Lesbarkeit

## Lösung: Beweissichere Aktenführung und Langzeitspeicherung

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

# DIE EIDAS-VERORDNUNG SCHAFFT EINEN EINHEITLICHEN RAHMEN FÜR EIN VERTRAUENSWÜRDIGES E-GOVERNMENT

## eIDAS (seit 2014)

Verbindlich in EU und EFTA

Einheitliche, weltweit gültige, technische Standards

Fern- und Serversignaturen und Siegel

Beweiswerterhaltung notwendig

Zertifizierte qualifizierte Anbieter (TSP)

Verpflichtende Anerkennung durch öffentlichen Stellen in EU und EFTA

## Verbindliche Standards

ETSI Conformity Assessment Framework

General Policy Requirements

ETSI EN 319 401

Requirements for Conformity Assessments

ETSI EN 319 403

Website Certs

ETSI EN 319 411-1

Qualified Certs

ETSI EN 319 411-2

Public Key Certs

ETSI EN 319 411-3

Attribute Certs

ETSI EN 319 411-4

Time Stamps

ETSI EN 319 421

## eID und Vertrauensdienste

Elektronische Identifizierung

Elektronische Identifizierungssysteme

Elektronische Identifizierungsmittel

Elektronische Signaturen

Elektronische Siegel

Elektronische Zeitstempel

Website-Authentifizierung

Elektronischer Zustelldienst

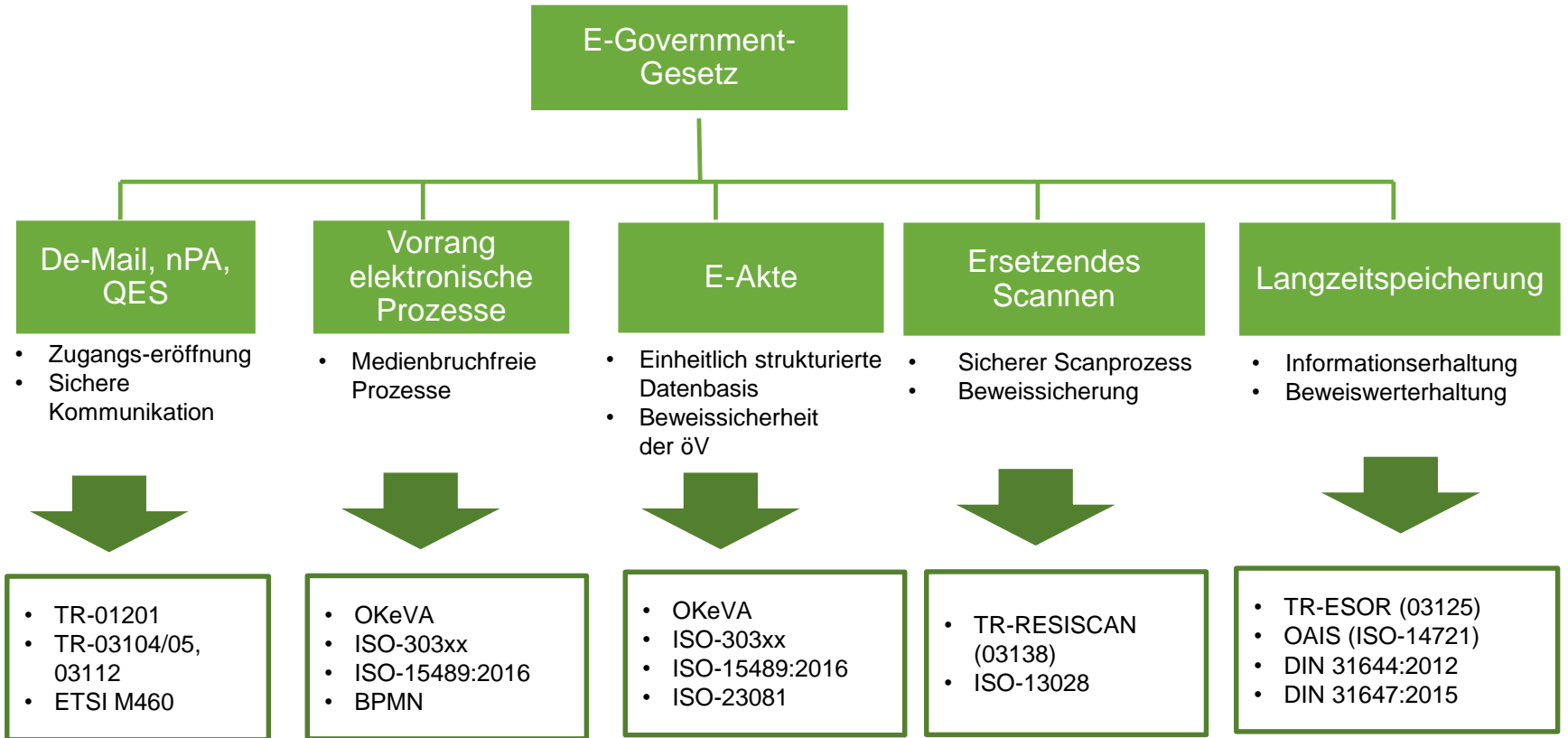
Bewahrungsdienst

Vertrauensdienste

Vertrauenswürdiges eGovernment



# GRUNDLEGENDE REGULATORISCHER RAHMEN IM BUND



# LEBENSZYKLUS ELEKTRONISCHER UNTERLAGEN

## Bundesbehörde

## Bundesarchiv

Aufbewahrungsfrist

Zeit

Abschluss  
der Bearbeitung

Phase 1  
Bearbeitung

Phase 2  
Langzeitspeicherung

Phase 3  
Aussonderung

Archivierung

Dauerhafte Aufbewahrung  
(i.d.R. nur Behörden)

Archivwürdige Daten  
i.d.R. ca. 2-5%  
(Entscheidung durch  
Barch)

Übrige Daten  
i.d.R. ca. 95 %

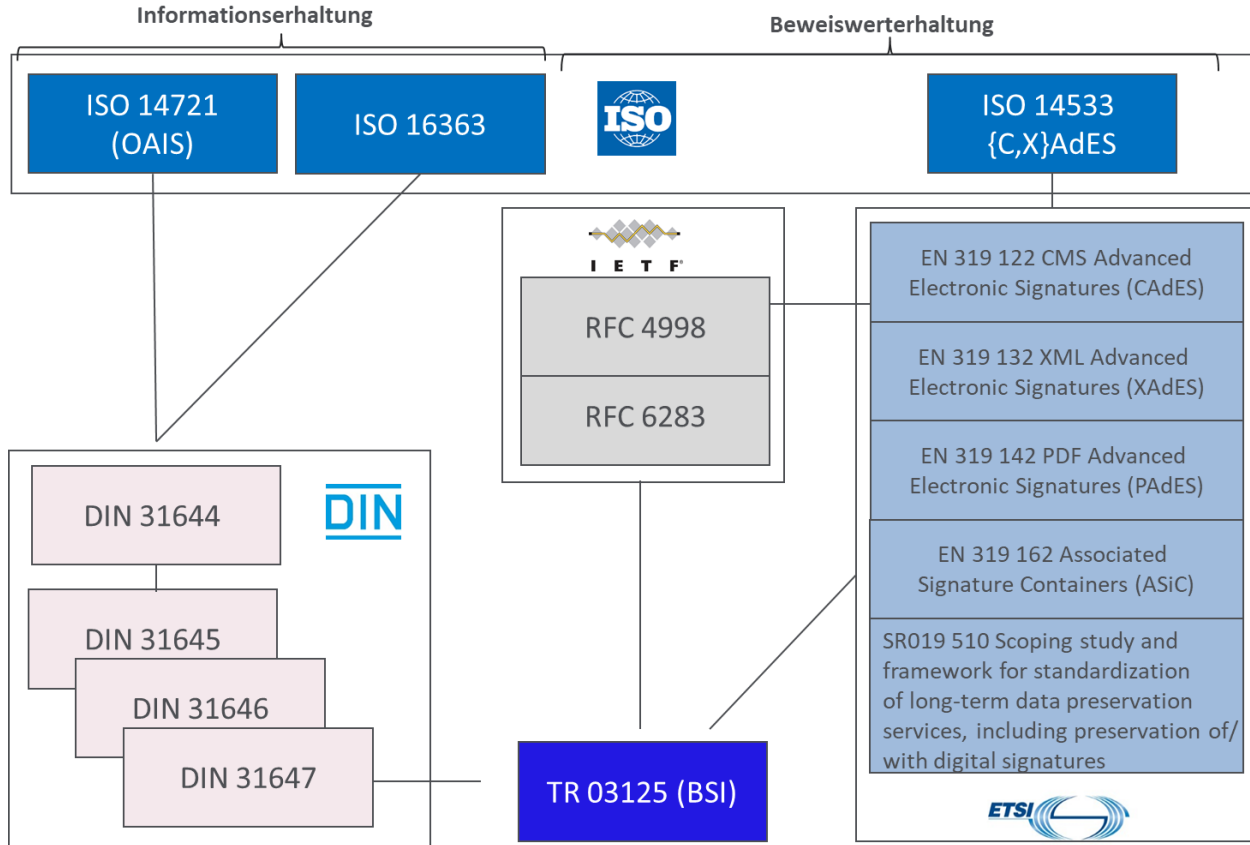
Vernichtung

Der nicht archivwürdigen  
Daten

# AGENDA

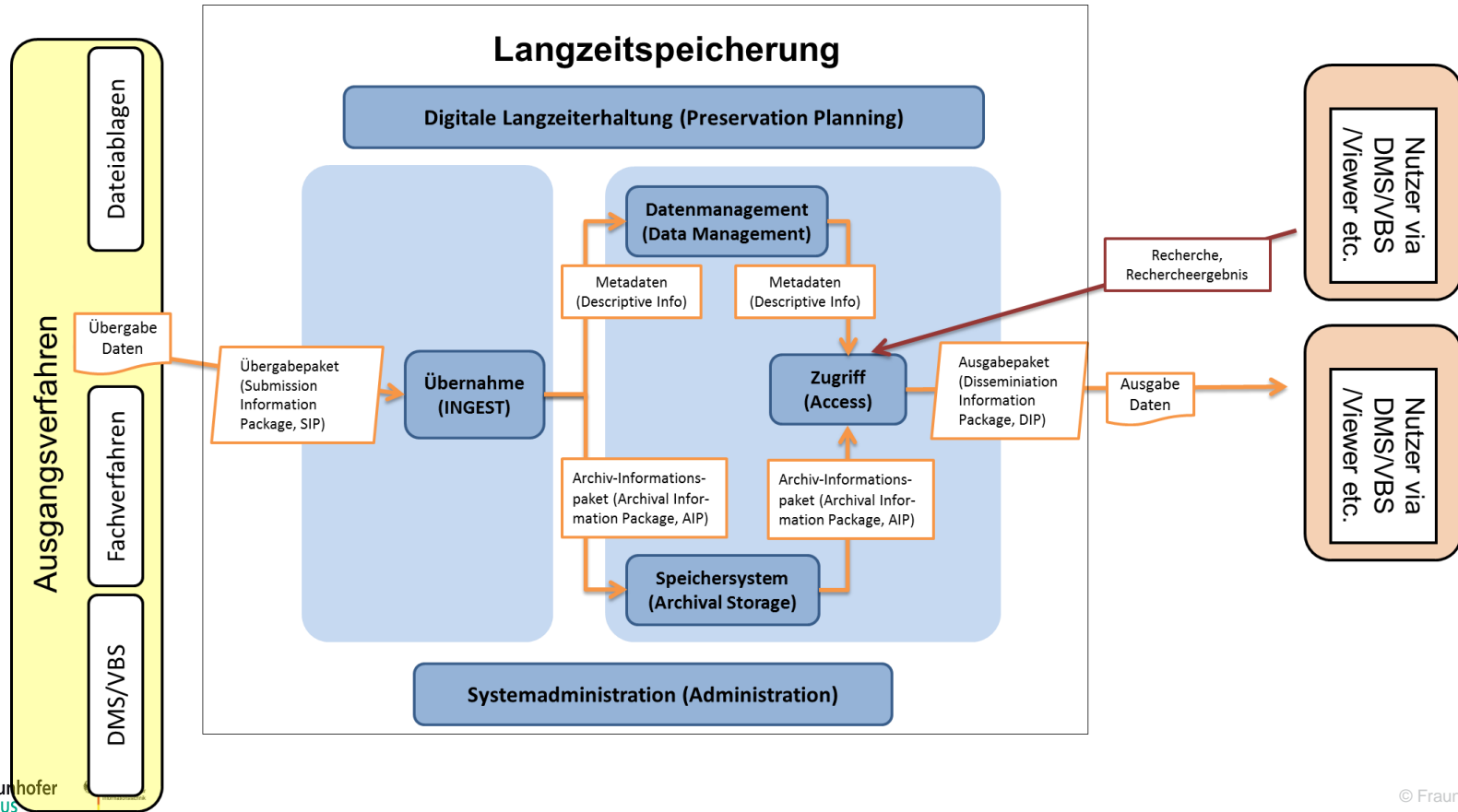
1. Ausgangssituation
2. Normative Einordnung
3. Fachliche-technische Rahmenbedingungen
4. Lösungsbeispiele

# NORMATIVER RAHMEN ZUR BEWEISSICHEREN LANGZEITSPEICHERUNG





# DAS OAIS-MODELL DEFINIERT DIE NOTWENDIGEN PROZESSE UND INFORMATIONSPAKETE



# EINE BEWEISSICHERE LANGZEITSPEICHERUNG ERHÄLT DIE UNTERLAGEN UND DEREN BEWEISWERT BIS ZUM ABLAUF DER GELTENDEN AUFBEWAHRUNGSFRIST

Wahrung der Authentizität, Integrität, Verfügbarkeit, Verkehrsfähigkeit, Nachvollziehbarkeit

## Informationserhaltung

### Wohldefinierte Prozesse

- Ingest
- Data Management
- Archival Storage
- Access
- Systemadministration
- Preservation Planning

### Wohldefinierte Informationspakete

- Submission Information Package
- Selbsttragende AIP
- Dissemination Information Package

### Objektbezogene Maßnahmen

- Nutzung standardisierter Formate für Content, Metadaten
- i.d.R. physische, selbsttragende Informationspakete
- Migration zur Informationserhaltung im Preservation Planning

## Beweiswerterhaltung

### objektbezogen

- Beweisrelevante Daten
- Evidence Record
- Signatur- und Hasherneuerung

© Fraunhofer FOKUS

# DIE TR-ESOR BILDET DEN STAND DER TECHNIK ZUR BEWEISWERTERHALTENDEN LANGZEITSPEICHERUNG GEM. EGOVG



**Aktuelle Version: 1.2  
(abwärtskompatibel)**

## 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 XBARC, XDOMEA und PREMIS

### Level für Konformitätstest

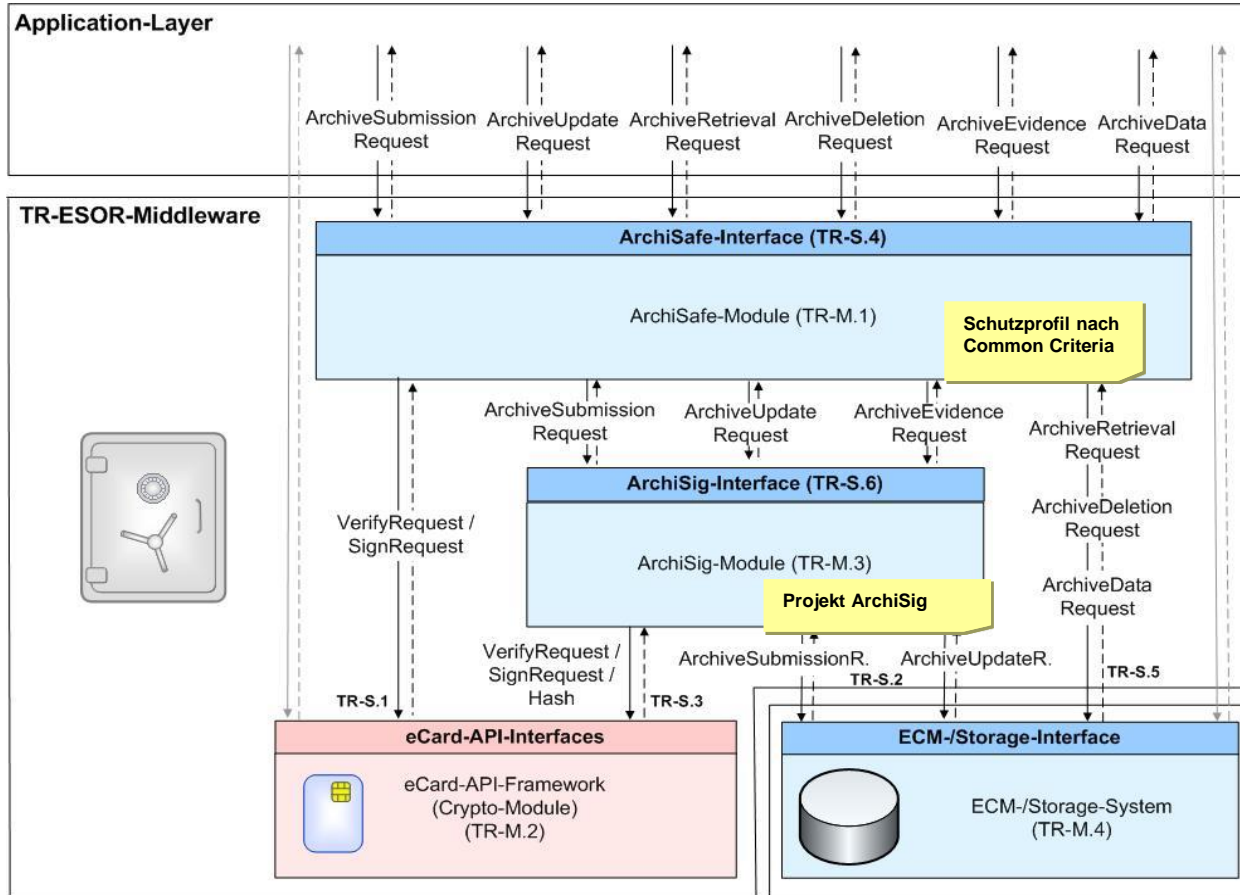
TR-ESOR-C.1 Testspezifikation „Funktionale Konformität“

TR-ESOR-C.2 Testspezifikation „Technische Konformität“

TR-ESOR-C.3 Testspezifikation „Bundesbehörden-Profil“

- Aktuelle Version: 1.2
- Version 1.2.1 wird ca. Q1/2018 veröffentlicht
  - Sprachlich-formale Anpassung auf eIDAS
  - Ergänzungen bei Signatur-/Siegelprüfung (alle Verfahren nach eIDAS)
- Version 1.3 ist in Erstellung
- Schwerpunkte:
  - Ergänzungen entspr. Rückmeldungen der Anwender und europ. Standardisierung Logisches XAIP für „Big Data“
  - Spezifikation eines profilierten ETSI-ASiC-Containers gemäß EN 319 162 als zusätzlichen Archivdatenobjekt-Container
  - Fertigstellung des Anhangs TR-ESOR-X zum Thema „Beweisdatenaustausch-Format“
  - Technische Detailanpassungen im Hinblick auf europ. Standardisierung (TRESOR VR und E)
  - Hinzunahme REST und JSON
- Parallel:
  - Aufbau Testtool für technische Beweisdaten als Onlineservice
  - Interoperabilitätsworkshops

# DIE REFERENZARCHITEKTUR DER TR-ESOR ERMÖGLICHT EINE EFFIZIENTE WIE DIENSTEORIENTIERTE UMSETZUNG



- Schnittstellen: Webservices
  - Technische Konformität C2: Umsetzung S4 entspr. TR-ESOR Anhang E
- Standardisiert (Common Criteria, ISO-14533)
- Verfahrensanbindung im XML-Adapter (außerhalb der Referenzarchitektur)
- Submission/Änderung:
  - Funktionale und technische Konformität (C1-C2)
    - Input: Alle Formate
    - Ausgabe nach XAIP muss möglich sein
  - Behördenprofil:
    - Input: XAIP [B] (SOLL)
    - Ausgabe nach XAIP muss möglich sein
- Datenabruf:
  - ArchiveRetrieval Request (Datenpaket)
  - ArchiveDataRequest (Einzeldatei in XAIP)

# EIN SELBSTTRAGENDES (X-)AIP BEINHÄLT ALLE FÜR DIE INFORMATIONEN- UND BEWEISWERTERHALTUNG NOTWENDIGEN DATEN IN EINEM INFORMATIONSPAKET – HARD- UND SOFTWARENEUTRAL.

## XFDU (ISO-13527)

Package Header

MetaData Section

DataObject Section

Credentials Section

Informationen über die logische Struktur (en) der Archivdaten, den Absender und die Aufbewahrungszeit

Informationen über den Geschäfts- und Archivierungskontext der Nutzdaten

Enthält die eigentlichen Nutzdatenobjekte (XML oder Base64 kodiert)

Beweisrelevante Daten (ERO) und technische Beweisdaten (NERO)

## Wesentliche Eigenschaften

Preservation Info: Status für Aussonderungsvermerk

Basierend auf XBARCH, XDOMEA PREMIS

Content: PDF/A, TIFF/PDF-R etc.

Signaturen/Siegel, Zeitstempel, Zertifikatsinformationen, Sperrlisten etc., ERS

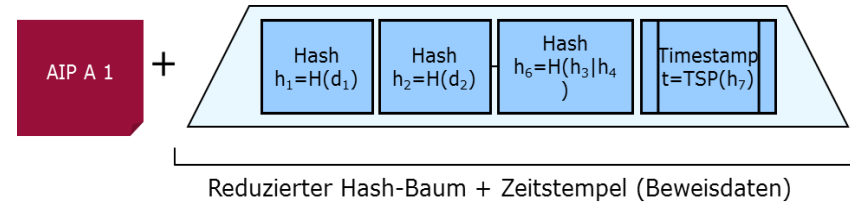
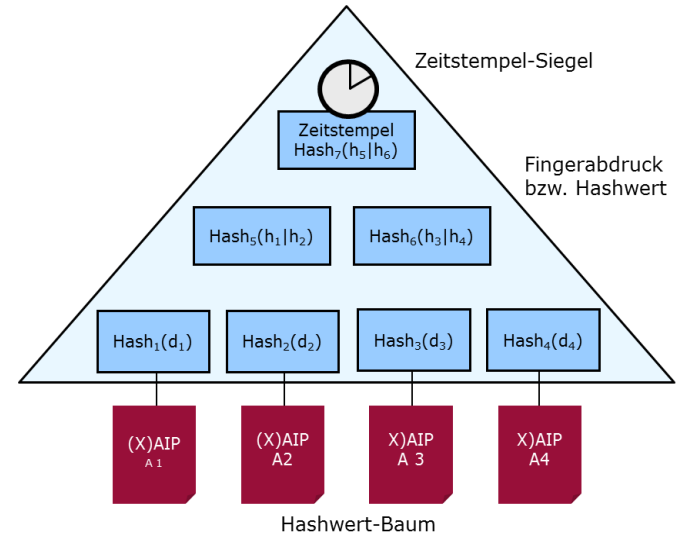
# DAS HASHBAUMVERFAHREN NACH ARCHISIG ERMÖGLICHT EINE EFFIZIENTE WIRTSCHAFTLICHE BEWEISWERTERHALTUNG ALLER UNTERLAGEN

## Hash-Baum

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

## Beweis-Dokument

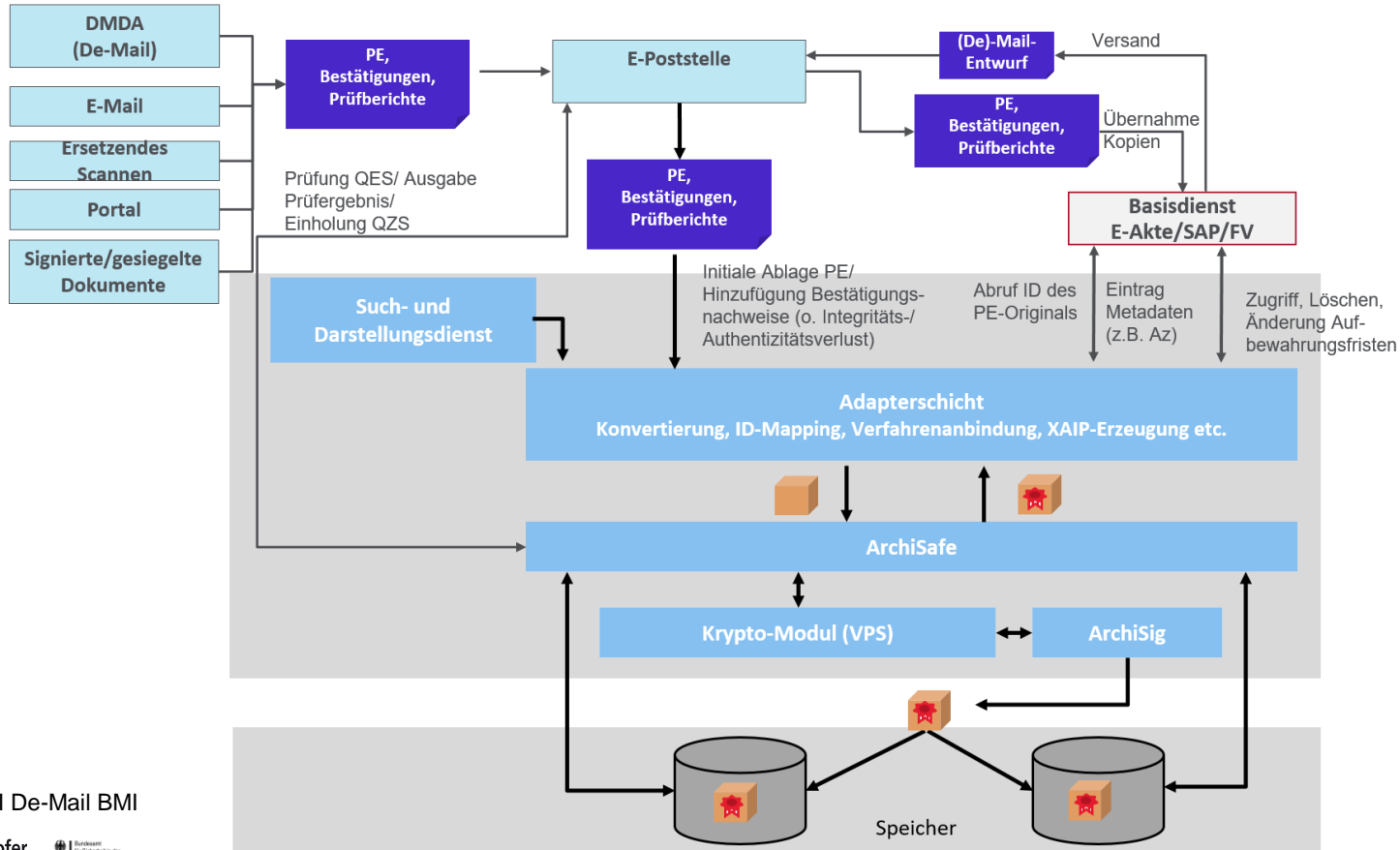
- Reduzierter Hash-Baum und Zeitstempel (einschl. Verifikationsdaten)



# AGENDA

1. Ausgangssituation
2. Normative Einordnung
3. Fachliche-technische Rahmenbedingungen
4. Lösungsbeispiele

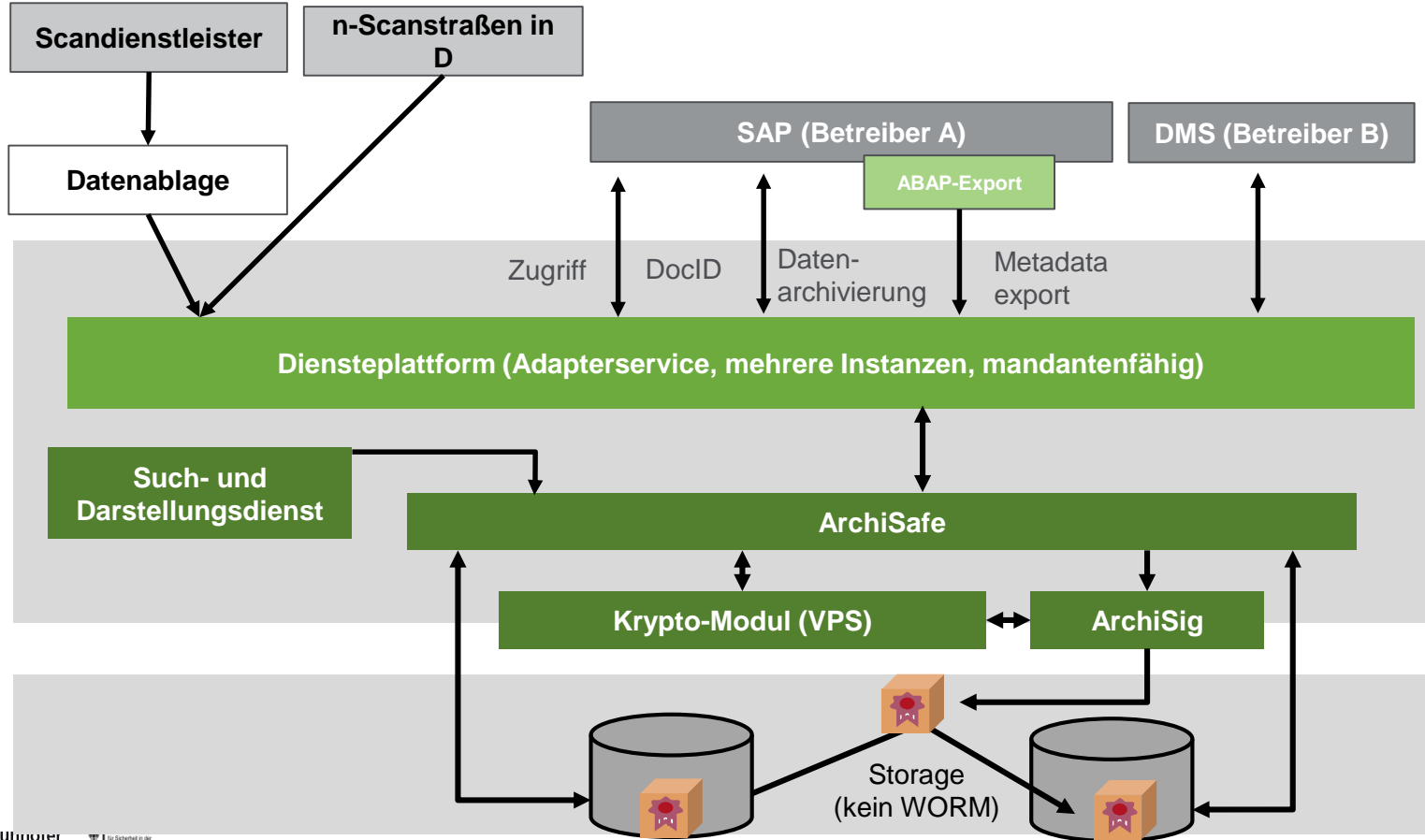
# DER LANGZEITSPEICHER IST EIN QUERSCHNITTSSERVICE FÜR ALLE UNTERLAGEN IM GESAMTEN LEBENSZYKLUS



Quelle: EGI De-Mail BMI



# BEISPIELARCHITEKTUR EINER BUNDESBEHÖRDE (AUSZUG)



# BEISPIELHAFT GROBARCHITEKTUR EINES LANGZEITSPEICHERSERVICE

Applikations-  
level

Electronic  
delivery services

WebPortal

File  
system

ECM

SAP

Share-  
point

Ersetz.  
Scannen

Register

Forschungsdaten

FV  
xyz

Integration,  
Konnektion

Konnektoren (WS, JSON, REST)

Authentisierung

Authorisierung

Protokollierung, Logging

Core Archive

## Informationserhaltung

Formatkonvertierung

Formatvalidierung

Extraktion, Erhebung  
Metadaten

Erzeugung (X-)AIP

Viewer

Recherche und Zugriff

Administration  
(Client, System)

Überwachung  
Formate

## Beweiswerterhaltung

Administration  
(Client, System)

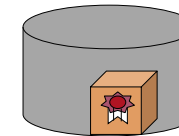
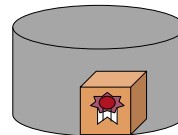
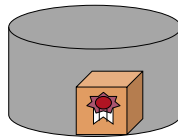
TR-ESOR

ArchiSafe-Modul

Krypto-Modul

Archisig-Modul

Speicher  
(HSM)



# LÖSUNGEN ZUR BEWEISWERTERHALTENDEN LANGZEITSPEICHERUNG WERDEN BRANCHENÜBERGREIFEND EINGESETZT (AUSWAHL)

BA, Bundesarchiv

- Digitales Zwischenarchiv
- **Zentraler Dienst für Bund!**
- Alle Unterlagen

BMG + BfArM

- Proof of Concept

BImA

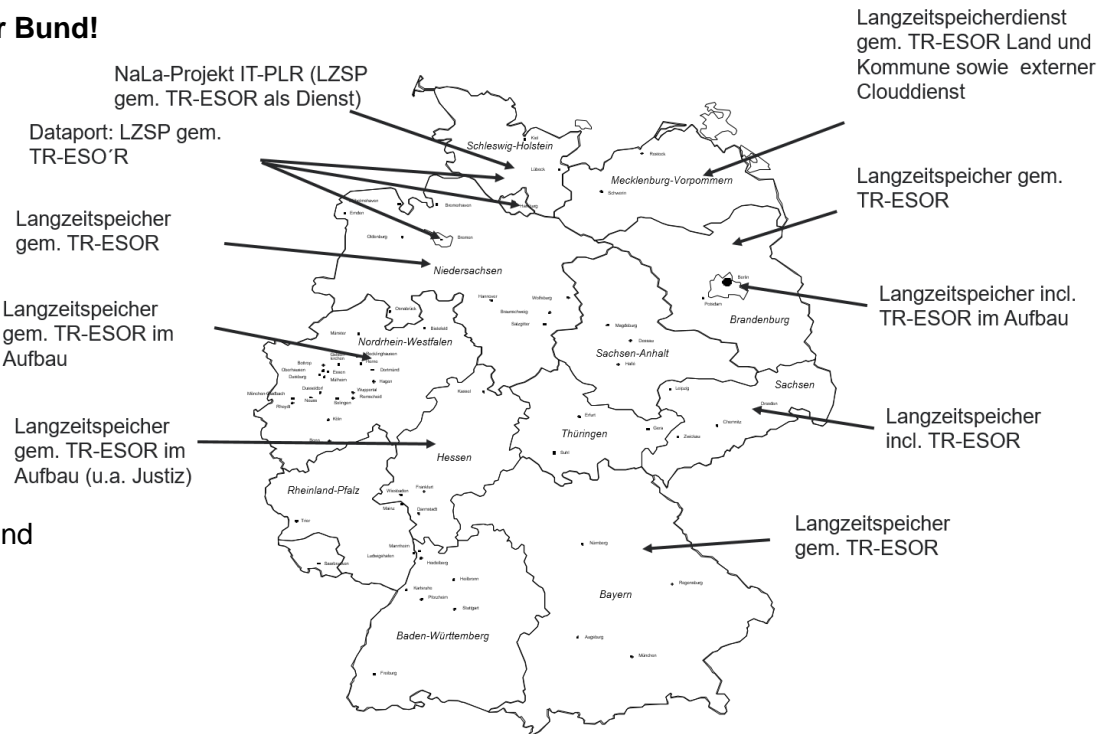
- eRechnung
- ePersonalakte

Airbus

- IT-Dienst
- Verfahrensübergreifend

Deutsche Rente

- Beweiserhaltung



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

# KONTAKT

Fraunhofer FOKUS  
Kaiserin-Augusta-Allee 31  
10589 Berlin, Germany  
[www.fokus.fraunhofer.de](http://www.fokus.fraunhofer.de)

Steffen Schwalm  
Wissenschaftlicher Mitarbeiter  
[steffen.schwalm@fokus.fraunhofer.de](mailto:steffen.schwalm@fokus.fraunhofer.de)  
Tel. +49 162 280 64 72