# INFORMATIONS- UND BEWEISWERTERHALTUNG IN A NUTSHELL – ÜBERSICHT ÜBER LÖSUNGSOPTIONEN FÜR ARCHIVINFORMATIONSPAKETE.

Dr, Ulrike Korte, Bundesamt für Sicherheit in der Informationstechnik
Tomasz Kusber und Steffen Schwalm, Fraunhofer Institut für Offene Kommunikationssystem FOKUS

Marburg, den 07. März 2018

Fraunhofer FOKUS

Bundesamt für Sicherheit in der Informationstechnik

# AGENDA

1. Ausgangssituation und Zielsetzung
2. Informations- und Beweiswerterhaltung im Überblick
3. Lösungsoptionen für AIP zur Informations- und Beweiswerterhaltung
4. Bewertung der verschiedenen Optionen
5. Fazit und Ausblick


© Fraunhofer FOKUS

# DIE EIDAS-VERORDNUNG SCHAFFT EINEN EINHEITLICHEN RAHMEN FÜR VERTRAUENSWÜRDIGE DIGITALE TRANSAKTIONEN IN BEHÖRDEN UND UNTERNEHMEN

## 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

## eID und Vertrauensdienste

- Elektronische Identifizierung
  - Elektronische Identifizierungssysteme
    - Elektronische Identifizierungsmittel
- Vertrauensdienste
  - Elektronische Signaturen
  - Elektronische Siegel
  - Elektronische Zeitstempel
  - Website-Authentifizierung
  - Elektronischer Zustelldienst
  - Bewahrungsdienst

## 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 |

# SICHERHEIT UND NACHWEISFÄHIGKEIT LÄSST SICH NUR DURCH ERHALTUNG DER INFROMATIONEN UND DEREN BEWEISWERT ERREICHEN

## Herausforderungen

- Lange Aufbewahrungs-fristen
- 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

## Informations- und Beweiswerterhaltung

- verfahrens-/herstellerneutral
- Formalisierte Daten (Struktur, Metadaten, Content, beweisrelevante Daten, technische Beweisdaten)
- Objektbezogen
- Nutzung etablierter Standards
- Definierte einheitliche Prozesse
- Diensteorientiert (SOA)
- Verbindliche Rollen, Verantwortlichkeiten, Regelungen, SLA
- Vertrauenswürdig

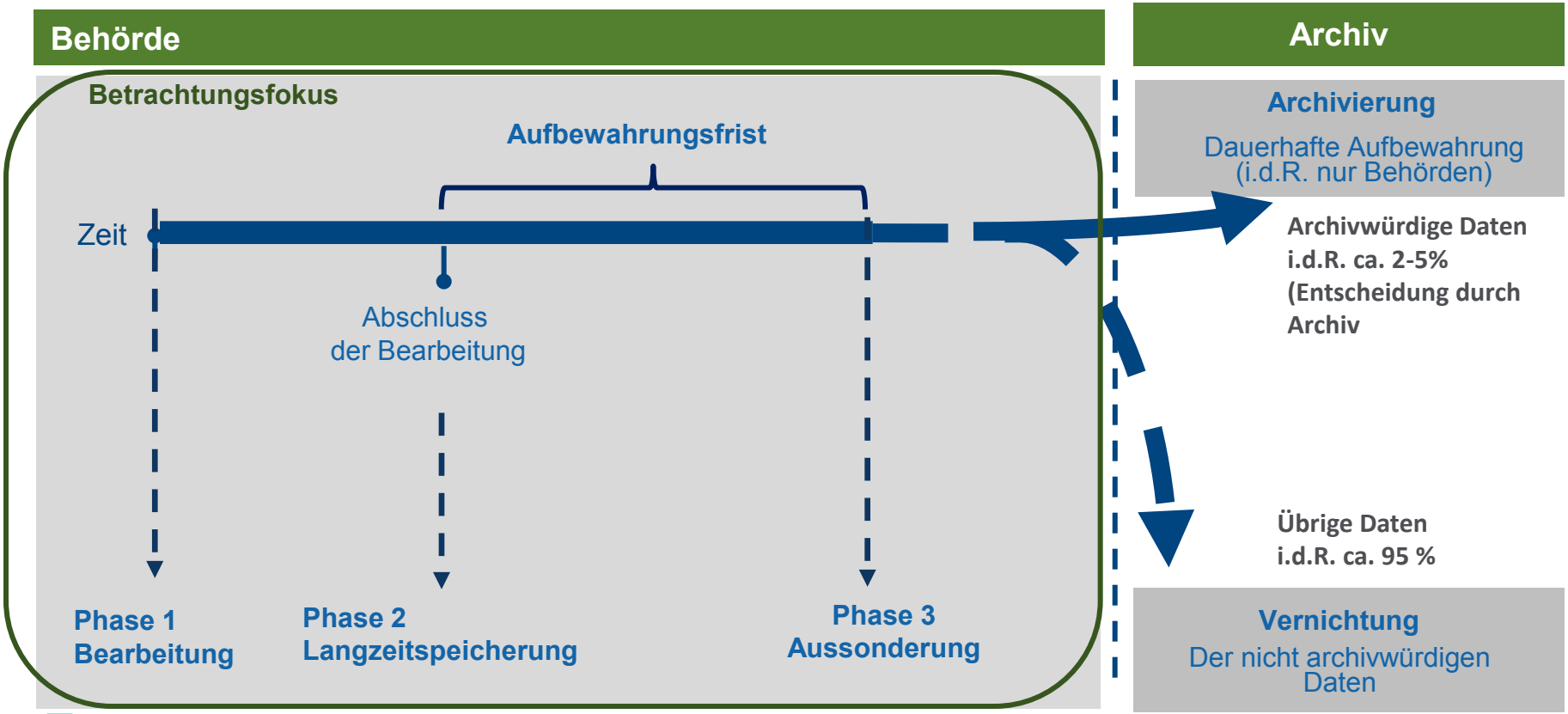
Fraunhofer FOKUS

Bundesamt für Sicherheit in der Informationstechnik



© Fraunhofer FOKUS

# LEBENSZYKLUS ELEKTRONISCHER UNTERLAGEN- BETRACHTUNGSFOKUS



# 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

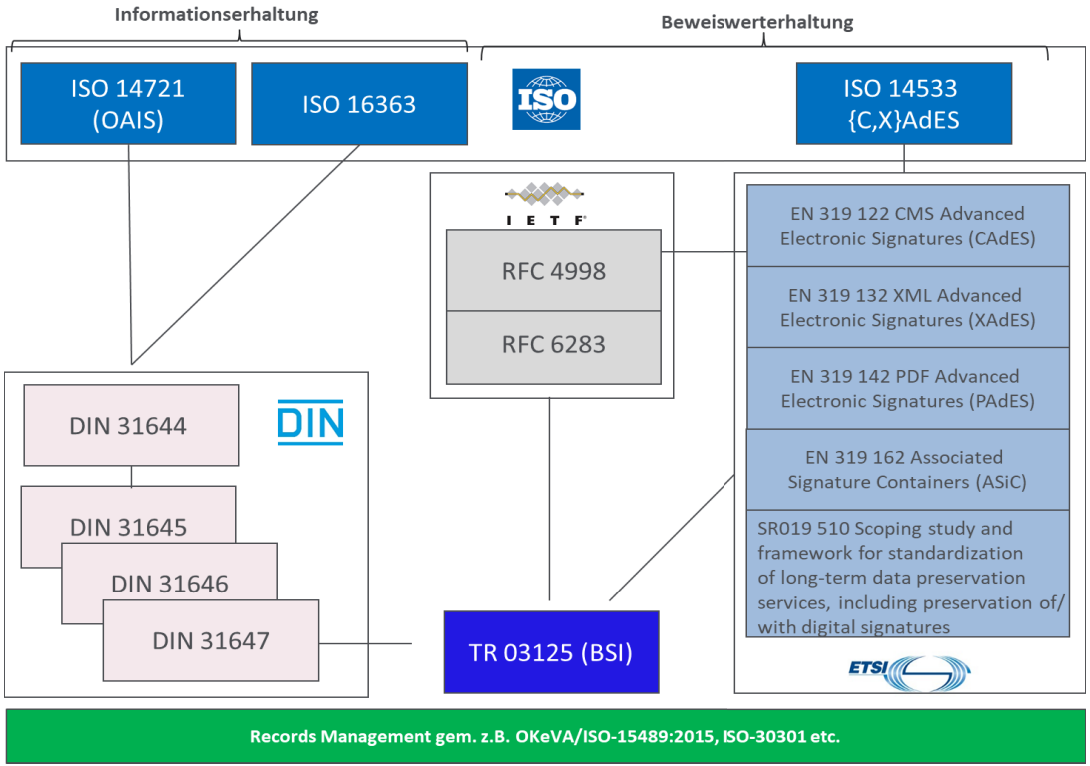
© Fraunhofer FOKUS

# AGENDA

1. Ausgangssituation und Zielsetzung
2. Informations- und Beweiswerterhaltung im Überblick
3. Lösungsoptionen für AIP zur Informations- und Beweiswerterhaltung
4. Bewertung der verschiedenen Optionen
5. Fazit und Ausblick


© Fraunhofer FOKUS

# NORMATIVER RAHMEN ZUR BEWEISSICHEREN LANGZEITSPEICHERUNG





© Fraunhofer FOKUS

# ANFORDERUNGEN AN AIP-FORMATE ZUR INFORMATIONS- UND BEWEISWERTERHALTUNG (1/2)

- beliebig viele, verschiedene Inhaltsdaten, Metadaten und beweisrelevante Daten/ technische Beweisdaten enthalten
- signierte/ zeitgestempelte und unsignierte/ unzeitgestempelte Daten parallel enthalten
- verschiedene digitale Signaturtechniken (z.B. (AdES) Signaturen, Zeitstempel, Evidence Records) unterstützen
- parallele und zusätzliche Signaturen unterstützen
- nachträgliches Einspielen von Sperrmaterial etc. ohne Zerstörung der vorausgegangenen Signatur ermöglichen
- verschiedene Versionen von Inhalts-/ Meta- und Beweisdaten enthalten, die nach und nach in das Paket eingestellt werden können


© Fraunhofer FOKUS

# ANFORDERUNGEN AN AIP-FORMATE ZUR INFORMATIONS- UND BEWEISWERTERHALTUNG (2/2)

- eine Referenzmöglichkeit enthalten können, dass entsprechende Nutzdaten-, Metadaten- und beweisrelevanten Daten/ Beweisdaten verknüpft, die durch ein spezielles Objekt der digitalen Signaturtechnik geschützt werden
- unterstützen, dass Versionen oder spezielle Elemente des AIP gezielt ausgelesen werden können
- performant auch bei großen Datenmengen/ Dateien (z.B. Geodaten) sein
- eine wirtschaftliche Realisierung (z.B. auf Basis von Open Source Software-komponenten, serviceorientierten Architekturen oder Softwarekomponenten mit kostengünstigen Lizenz- und Servicemodellen) ermöglichen
- selbsttragend sein, also alle zur Informations- und Beweiswerterhaltung, also dem Aufbewahrungszweck, notwendigen Daten in standardisierter Form enthalten
- auf weit verbreiteten, offenen Standards weithin anerkannter, unabhängiger Standardisierungsgremien beruhen (insbesondere Compliance zu ETSI (eIDAS)


© Fraunhofer FOKUS

# AGENDA

1. Ausgangssituation und Zielsetzung
2. Informations- und Beweiswerterhaltung im Überblick
3. Lösungsoptionen für AIP zur Informations- und Beweiswerterhaltung
4. Bewertung der verschiedenen Optionen
5. Fazit und Ausblick


© Fraunhofer FOKUS

# XAIP IST EIN STANDARDISIERTES FORMAT ZUR INFORMATIONS- UND BEWEISWERTERHALTUNG – EINE INTEGRATION IN ANDERE PAKETFORMATE (ZIP, PDF/A-3) IST MÖGLICH. (BEDARF: BEHÖRDEN UND UNTERNEHMEN)

**Basis: 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.
- ERO: Beweisrelevante Daten (Zertifikatsinfos, Sperrlisten etc.); NERO: ERS

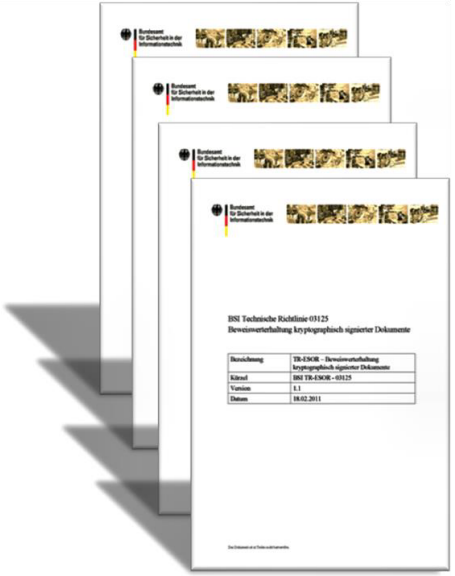
Fraunhofer FOKUS

Bundesamt für Sicherheit in der Informationstechnik



© Fraunhofer FOKUS

# DIE TR-ESOR BILDET DEN STAND DER TECHNIK ZUR BEWEISWERTERHALTENDEN LANGZEITSPEICHERUNG UND BEINHALTET MIT XAIP EIN FLEXIBLES FORMAT FÜR SELBSTTRAGENDE AIP GEM. OAIS UND DIN 31647.




**Aktuelle Version: 1.2.1**

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“

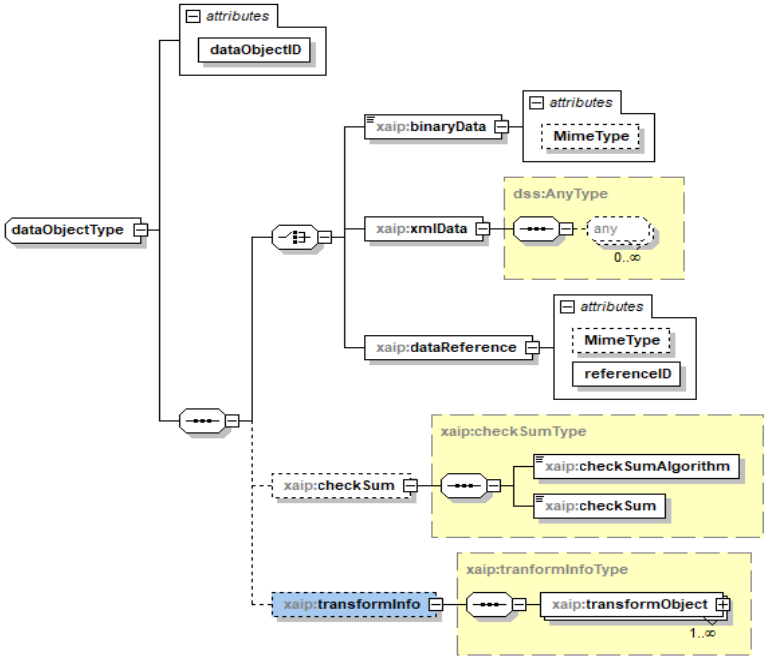
## Praxiserfahrungen

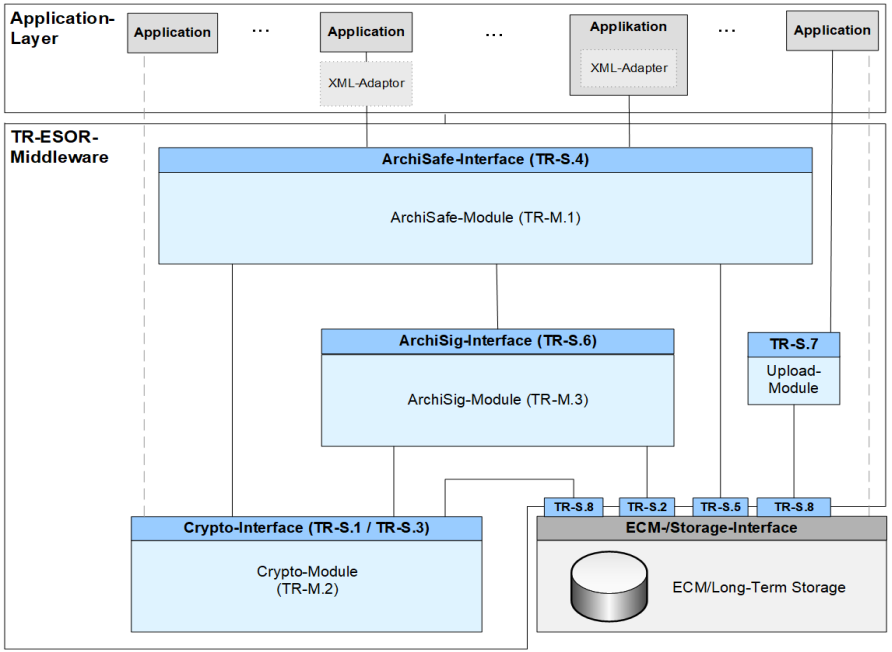
- XAIP ist hochflexibel und leicht anwendbar
- Aufnahme beliebiger 1-n Daten je Objekt möglich
- Aufnahme Metadaten, Content, beweisrelevante und technische Beweisdaten
- Aufnahme XDOMEA, PREMIS für fachliche/technische Metadaten
- Flexibler Schutz der Daten, deren Beweiswert zu erhalten ist, durch Protected Pointer gekennzeichnet
- Versionierung möglich
- Zugriff auf Einzelobjekte vermeidet Abruf des kompletten Containers
- Performanceeinschränkungen an WebServices bei BigData durch XML-immanente Base64-Codierung (z.B. Forschungseinrichtungen, Industrie, Finanzsektor, Energiewirtschaft)

Fraunhofer FOKUS

Bundesamt für Sicherheit in der Informationstechnik

# EIN LOGISCHES (X-)AIP ERMÖGLICHT EINE HOHE PERFORMANCE IM VORHANDENEN STANDARD




- Aufnahme Element Data Reference
- Beinhaltet eindeutige ID des DataObjects (ReferenceID

- Upload-Modul zur standardisierten Aufnahme
- Standardschnittstelle Upload
- Definition Basisfunktionen des Moduls
- Prüfung XAIP
- Erzeugung AOID und Weitergabe an Applikation

Fraunhofer FOKUS

Bundesamt für Sicherheit in der Informationstechnik

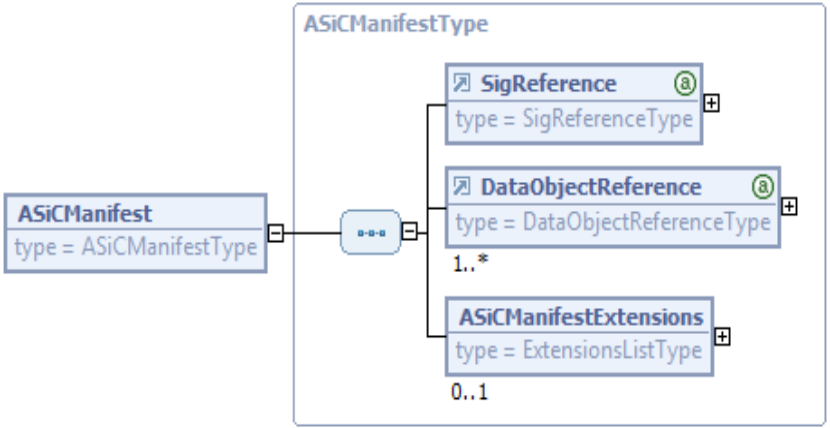


© Fraunhofer FOKUS

# ZIP/ASIC: ASIC IST IN EN 319 162 GENORMT UND KANN BELIEBIGE DATENOBJEKTE (ASIC-E) INCL. SIGNATUREN, ER UND ZEITSTEMPEL AUFNEHMEN – ES BERUHT AUF DEM ZIP-FORMAT GEM. ISO 21320-1. (BEDARF: BEHÖRDEN, NATIONALE+INTERNATIONALE UNTERNEHMEN)

**ASiC-E ist relevante Ausprägung für die Langzeitspeicherung**

- Jedes Datenobjekt kann mit 1-n CAdES-/XAdES-Signaturen, Zeitstempeln oder technischen Beweisdaten (EvidenceRecords) assoziiert sein
- Beinhaltet untergliederbares Stammverzeichnis für Datenobjekte
- Metadaten, Signaturen, ER werden im MetaINF-Verzeichnis abgelegt
- Beweiswerterhaltung auf Basis RFC4998/6283
- mehrere Manifeste möglich, aber Versionierung nicht sichtbar
- durch Nutzung ZIP, verlustfreie Komprimierung möglich



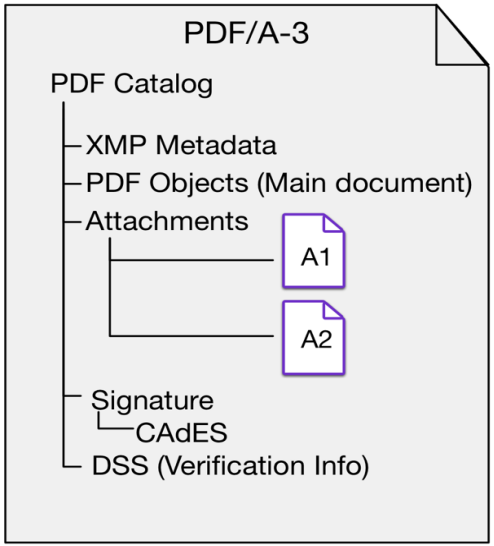

**ToDo:** Aufnahme in BaseLine-Varianten in Fortschreibung von Implementing Act 2015/1506/EU, Detailspezifikation in TR-ESOR v1.3



© Fraunhofer FOKUS

# PDF/A-3 IST IN ISO 19005-3 GENORMT UND BEINHALTET MIT XMP (ISO 16684-1) ZUDEM EINEN EBENSO STANDARDISIERTEN WEG ZUR EINBETTUNG VON METADATEN. (BEDARF INSBESONDERE IN INTERNATIONALEN KONZERNEN, DA WELTWEITER STANDARD)

- Grundlage ist das 1995 erschienene PDF/A (1)-Format
- Wesentliche Anforderung an Archivformat ist der Verzicht auf aktive Inhalte, Verschlüsselung JavaScript, externe Referenzen auf Farbräume und Zeichensätze
- ermöglicht die Einbettung jeglicher Datenobjekte – auch Fremdformate
- Einbindung erfolgt als File-Attachments, was auch in PDF-2.0 Standard übernommen wurde
- bei eingebetteten Datenobjekt ist Angabe der Beziehung zum PDF/A-3-Dokument notwendig: Alternative, Source, Data, oder Supplement
- Einbettung Metadaten via XMP, das bereits weitere Standards (u.a. Dublin Core beinhaltet, weitere Metadaten via Definition über PDF/A-Erweiterungsschema
- durch Einbettung ZIP, verlustfreie Komprimierung möglich
- PDF-Viewer visualisiert nur PDF-Hauptdokument
- Nutzung aller PAdES-Signaturen inkl. LTA-Profiles und Einbettung ER möglich, Signatur bezieht sich immer aufs komplette PDF/A-Dokument




**ToDo:** Weitere Standardisierung spez. Versionierung, Zugriff Nutzung weiterer Signaturformate sowie ERO/NERO notwendig

# AGENDA

1. Ausgangssituation und Zielsetzung
2. Informations- und Beweiswerterhaltung im Überblick
3. Lösungsoptionen für AIP zur Informations- und Beweiswerterhaltung
4. Bewertung der verschiedenen Optionen
5. Fazit und Ausblick


© Fraunhofer FOKUS

# VERGLEICH DER OPTIONEN (1/2)

| Anforderung | XFDU/XAIP | ASiC | PDF/A-3 |
|---|---|---|---|
| Beliebige viele Nutzdaten, Metadaten, beweisrelevante Daten/ Beweisdaten, | X | X | X |
| Signierte/unsignierte Daten | X | X | X<br>Aber: Nachsignierung werden alle Objekte signiert (keine protected pointer) |
| Verschiedene Signaturtechniken erzeugen und verifizieren | X<br>AdES-Signaturen, Zeitstempel, ER | X<br>AdES-Signaturen, Zeitstempel, ER | X<br>PAdES, andere nur in spezifischer Lösung |
| Parallele Signaturen | X | X | Eingeschränkt:<br>Realisierbar für CM-Signaturen, Visualisierung und Verifikation nicht standardisiert |
| nachträgliches Einspielen von Sperrmaterial ohne Verletzung Beweiswert | X | X | Eingeschränkt:<br>Nur bei Verwendung PAdES LTA-Profile, erfordert immer neuen QZS |

# VERGLEICH DER OPTIONEN (2/2)

| Anforderung | XFDU/XAIP | ASiC | PDF/A-3 |
|---|---|---|---|
| Versionierung Nutz-, Meta- und Beweisdaten | X | Eingeschränkt:<br>Keine Versionierung des ASiC-Manifest, nur Ablage verschiedene Manifeste möglich | Eingeschränkt:<br>Update-Mechanismus über Anhängen neuer bzw. geänderter Objekte ans Ende der Datei |
| Performant auch bei großen Datenmengen/ Dateien | Eingeschränkt:<br>Base64-Codierung (Lösung mit log. XAIP) | X | X |
| Wirtschaftlich | X | X | X |
| Selbsttragend möglich | X<br>(Zusammenbau nach S.2/S.5/S.8 bei log. XAIP | X | X |
| Parallele Signaturen | X | X | Eingeschränkt:<br>Realisierbar für CMS-Signaturen, Visualisierung und Verifikation nicht standardisiert |

# AGENDA

1. Ausgangssituation und Zielsetzung
2. Informations- und Beweiswerterhaltung im Überblick
3. Lösungsoptionen für AIP zur Informations- und Beweiswerterhaltung
4. Bewertung der verschiedenen Optionen
5. Fazit und Ausblick


© Fraunhofer FOKUS

# FAZIT UND AUSBLICK

**AIP-Formate zur Informations- und Beweiswerterhatlung**

**XAIP**

- etabliert
- Flexible Einbindung und Zugriff auf n-Datenobjekten
- Definition ERO/NERO möglich
- Hohes Speichervolumen durch Base64-Codierung → lösbar mit log. XAIP

**ASiC**

- Europaweit (ZIP weltweit) genormt und ZIP-Komprimierung möglich
- Einbettung von n-Datenobjekten incl., Struktur- und Metadaten, ER incl. ERO/NERO möglich
- Einbettung Zeitstempel, ER, mehrere Manifeste als Basis für effiziente Nutzung derzeit nicht im BaseLine Profile enthalten
- Umsetzung in TR-ESOR v1.3

**PDF/A-3**

- Weltweites Container- und Dokumentenformat (ISO-Norm) zur Langzeitspeicherung, aber umfassende Beschreibung notwendig
- ZIP-Komprimierung und automatisierte Dokumentverarbeitung
- Nur PAdES-Signaturen (Einbettung weiterer Signaturformate nur als anwenderspezifische Lösung)
- Keine ERO/NERO bzw. kein Zugriff auf einzelne Datenobjekte im Standard möglich

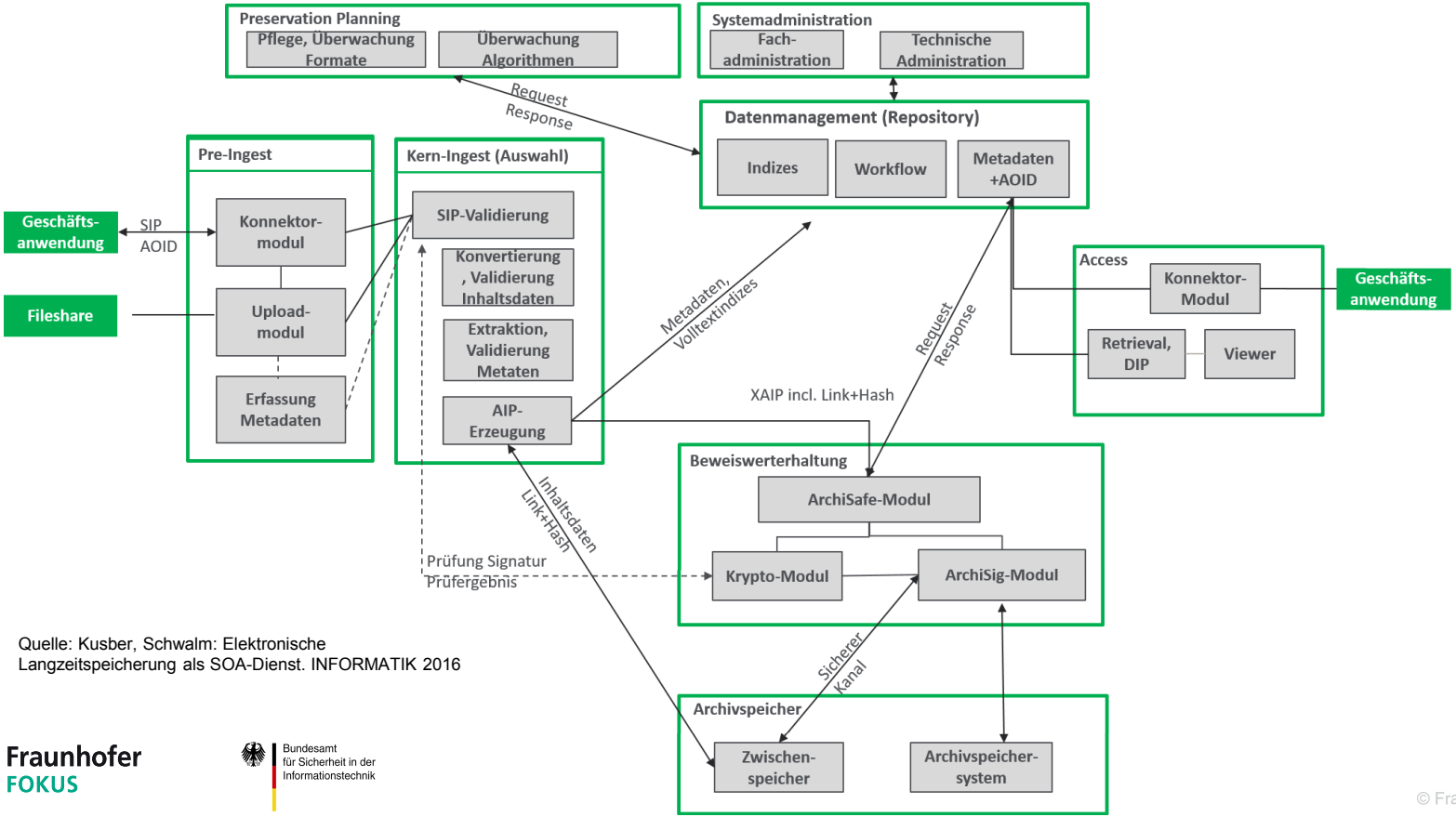
**Basis und Bedarf sind vorhanden. Die Umsetzung von ASiC erfolgt mit TR-ESOR v1.3.**
**Für PDF/A-3 sind noch umfassende Standardisierungsarbeiten auf ISO-ebene notwendig.**

Bundesamt
für Sicherheit in der
Informationstechnik

Fraunhofer
FOKUS


© Fraunhofer FOKUS

# BEISPIELARCHITEKTUR DLZA ZUR INFORMATIONS- UND BEWEISWERTERHALTUNG

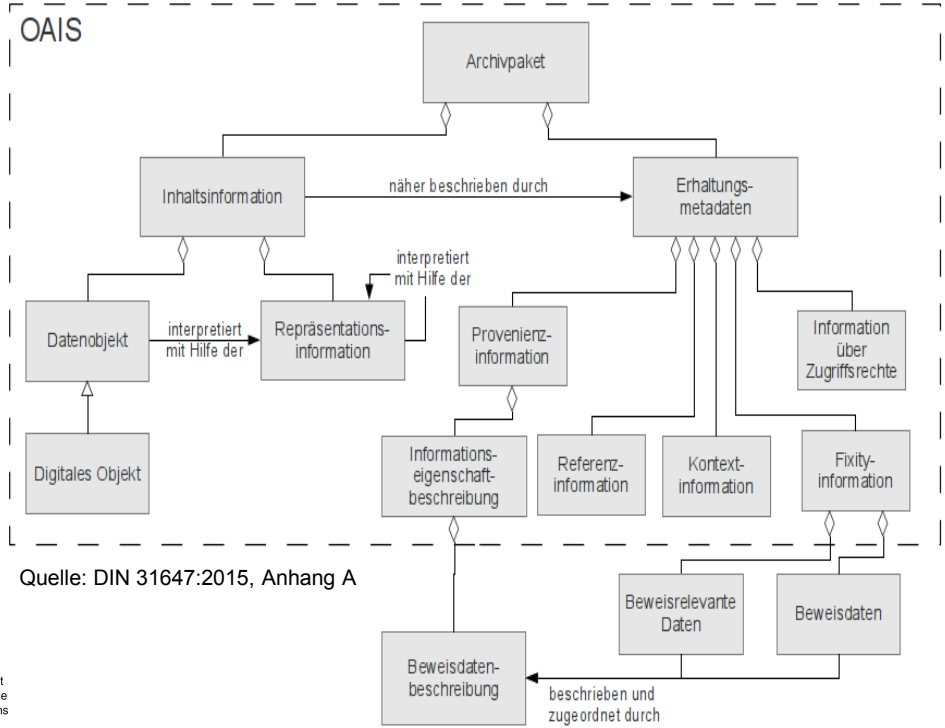



Quelle: Kusber, Schwalm: Elektronische Langzeitspeicherung als SOA-Dienst. INFORMATIK 2016


© Fraunhofer FOKUS

# NORMATIVER RAHMEN ZUR BEWEISSICHEREN LANGZEITSPEICHERUNG

**Informations- und Beweiswerterhaltung in einem AIP gem. OAIS (ISO 14721)**




Quelle: DIN 31647:2015, Anhang A


© Fraunhofer FOKUS