VERTRAUENSWÜRDIGES E-GOVERNMENT – ANFORDERUNGEN UND LÖSUNGEN ZUR BEWEISWERTERHALTENDEN LANGZEITSPEICHERUNG

Referent: Steffen Schwalm, Fraunhofer Institut für Offene Kommunikationssystem FOKUS

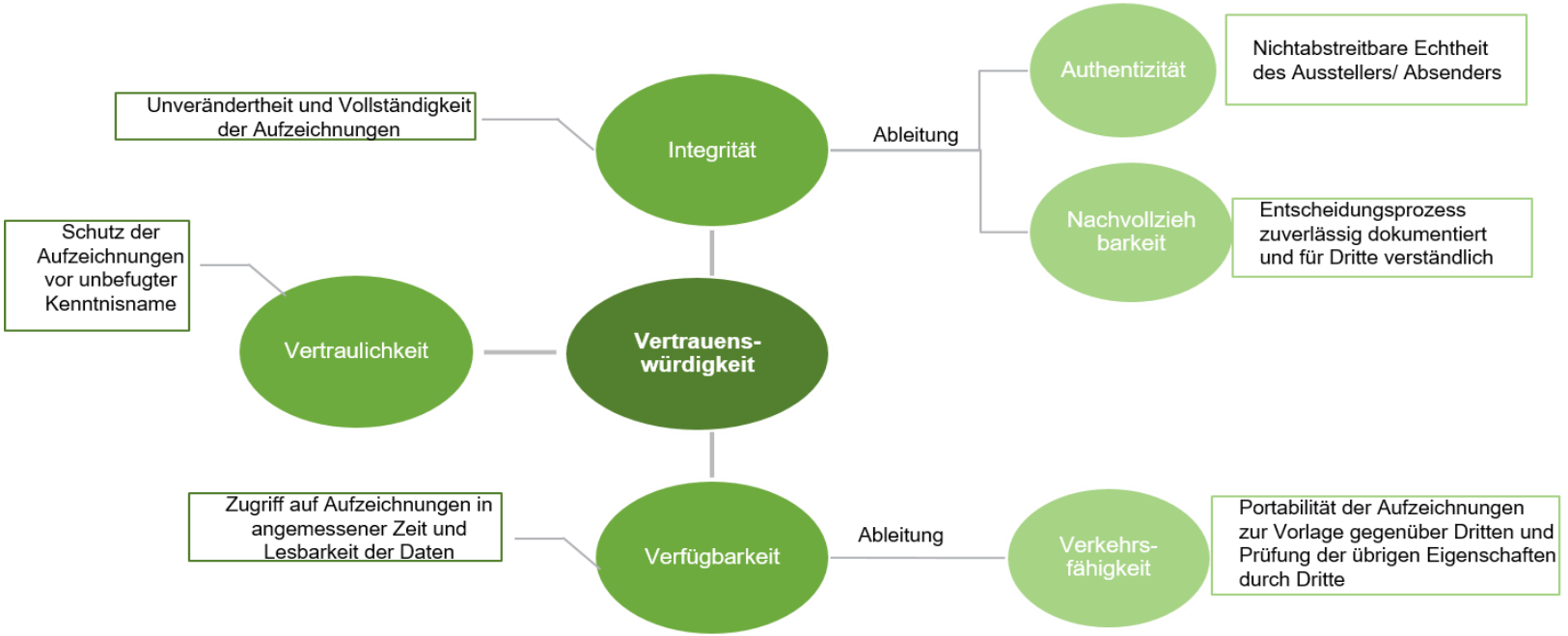
Marburg, den 05. Juni 2018

Fraunhofer FOKUS

AGENDA

1. Vertrauenswürdigkeit im E-Goverment (und E-Business)
2. Regulatorische Rahmenbedingungen
3. Fachlich-technische Rahmenbedingungen (Stand der Technik)
4. Architektur und Datenpakete
5. Fazit und Ausblick

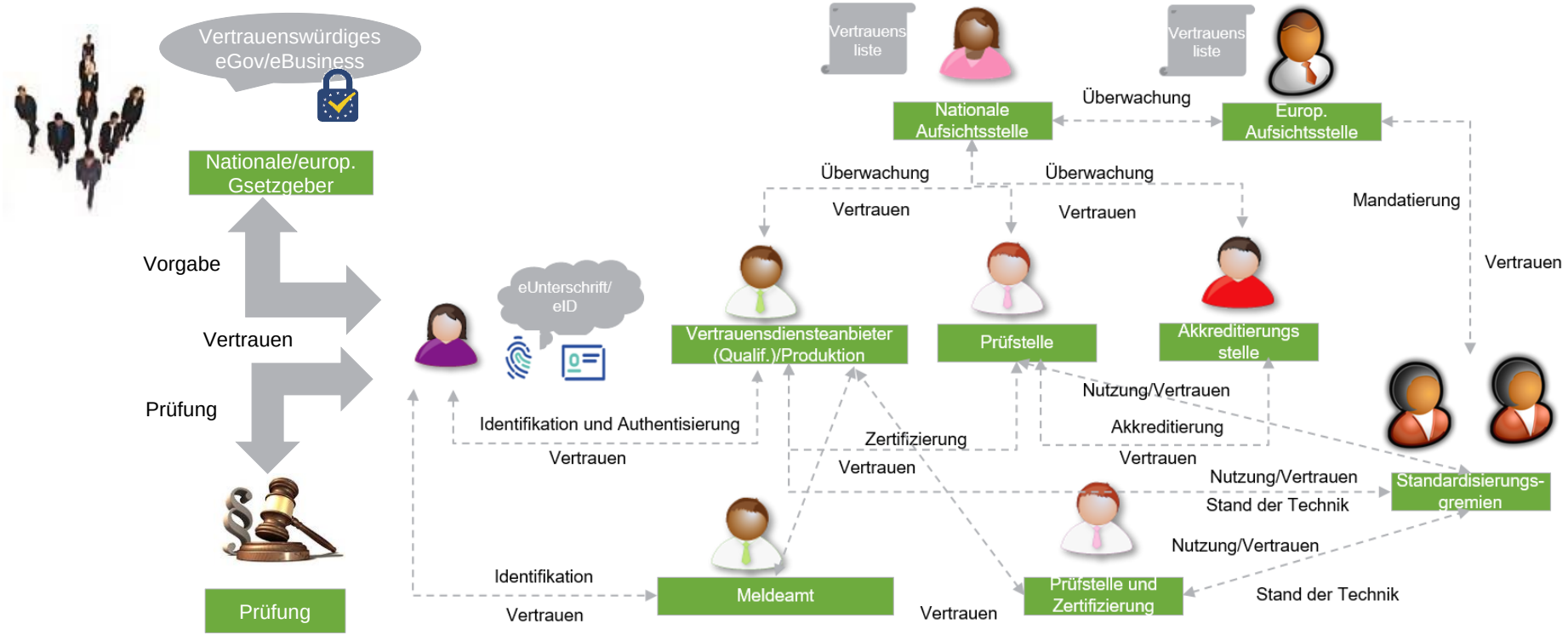
VERTRAUENSWÜRDIGES E-GOVERNMENT GEWÄHRLEISTET SCHUTZ UND NACHWEIS DER SIGNIFIKANTEN EIGENSCHAFTEN GESCHÄFTSRELEVANTER AUFZEICHNUNGEN



Gewährleistung durch definierte Prozesse, Organisation, Governance, IT (Records Management)

Fraunhofer FOKUS

VERTRAUENSWÜRDIGKEIT IM KONTEXT GESCHÄFTSRELEVANTER AUFZEICHNUNGEN ERFORDERT GRUNDSÄTZLICH VERTRAUENSWÜRDIGE, UNABHÄNGIGE DRITTE (VERTRAUENSKETTE AM BEISPIEL EIDAS)



Fraunhofer FOKUS

BEISPIEL LANGZEITSPEICHERUNG

eGovG/ Aufbewahrungs-pflichten

Nationale/europ. Gsetzgeber

Vorgabe

Vertrauen

Prüfung

Prüfung

LZSP

Auftrag

Vertrauen

IT-Dienstleister

Standardisierungs-Zertifizierungs-gremium

Nationale Aufsichtsstelle

Über-wachung

Vertrauen

Nationale Normung

Internationale Normung

Setzung Standards

Vertrauen

Normung

Vertrauen

Normung

Vertrauen

Über-wachung

Vertrauen

Prüfstelle

*

Produkt-/Lösungsanbieter

Prüfung

Vertrauen

(qualif.) Vertrauensdiensteanbieter

QZS

Vertrauen

KONZEPTIONELLE AUSNAHMEN: BLOCKCHAIN UND IUS ARCHIVI

Institutionalles Modell
(quasi nur Endarchiv)

Community-Modell
(nur Public Blockchain)

Herausforderungen

- Rechtlich nicht verankert (eGovG, eJusticeG, ZPO etc.)
- Umsetzbarkeit bei Trennung Raum und Daten in der IT (Cloud, Auftrags-DV)
- Anwendung derzeit wenn unmittelbare Rechtswirkung abgelaufen ist (Endarchiv)

→ für Records Management in E-Government/ E-Business out of scope

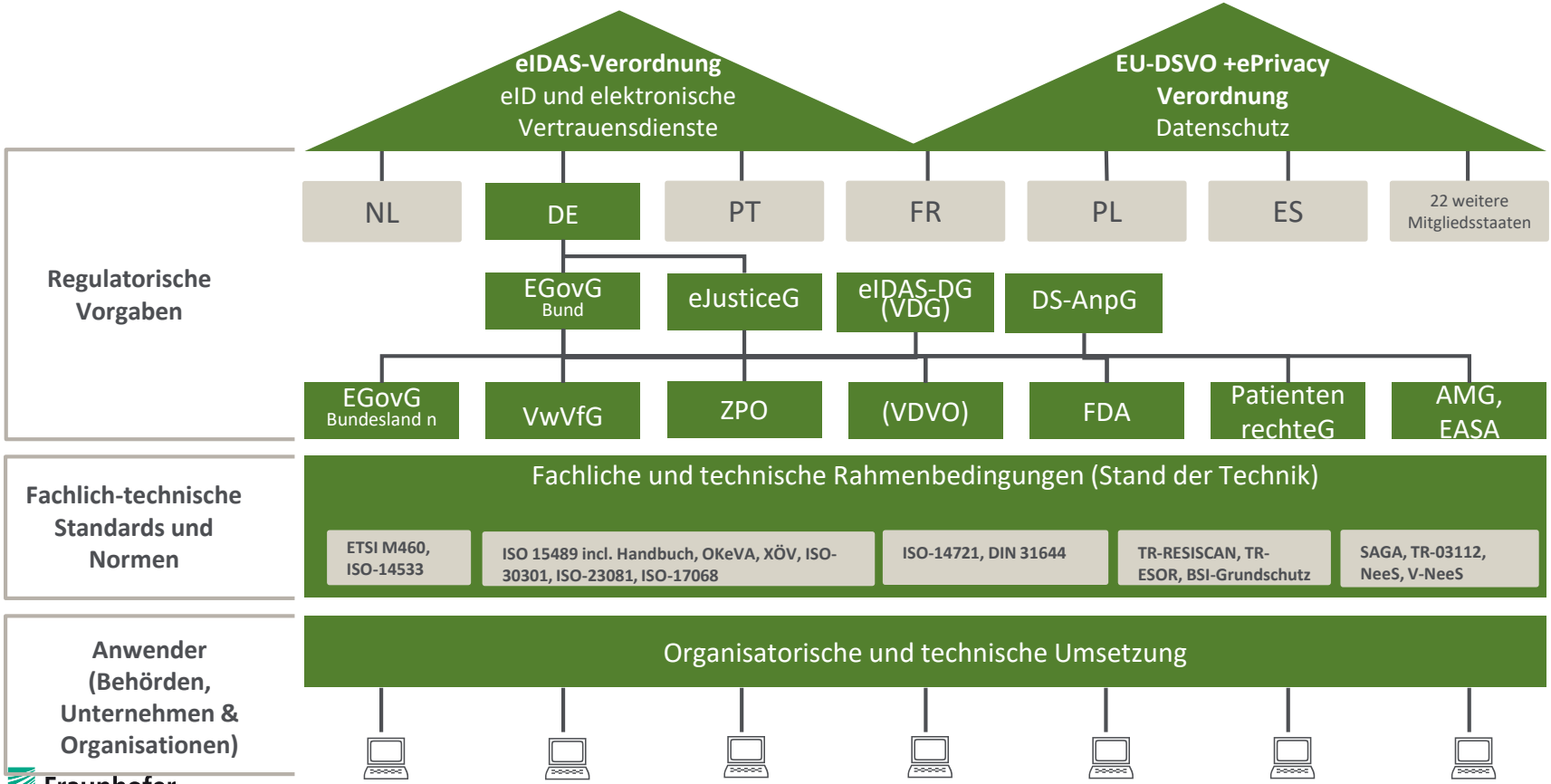
- Rechtlich nicht verankert (eGovG, ZPO etc.)
- Grundlage Vertrauenswürdigkeit der Community vs. Private Blockchain vs. Mischmodelle
- Vorrang Technik vs. Organisation?
- Datenschutz (Identitätsdaten, Content, Meta-/Transaktionsdaten)
  - Rechte des Betroffenen derzeit faktisch nicht erfüllbar bei Daten in Blockchain Hohe Komplexität bei Daten außerhalb Blockchain
    (Aufwand vs. Nutzen)
- Derzeit keine Strategien zur Archivierung (Daten und Beweiswert)

Neue Vertrauensmodelle notwendig?
(disruptive Technologien vs. bestehende Lösungen)

AGENDA

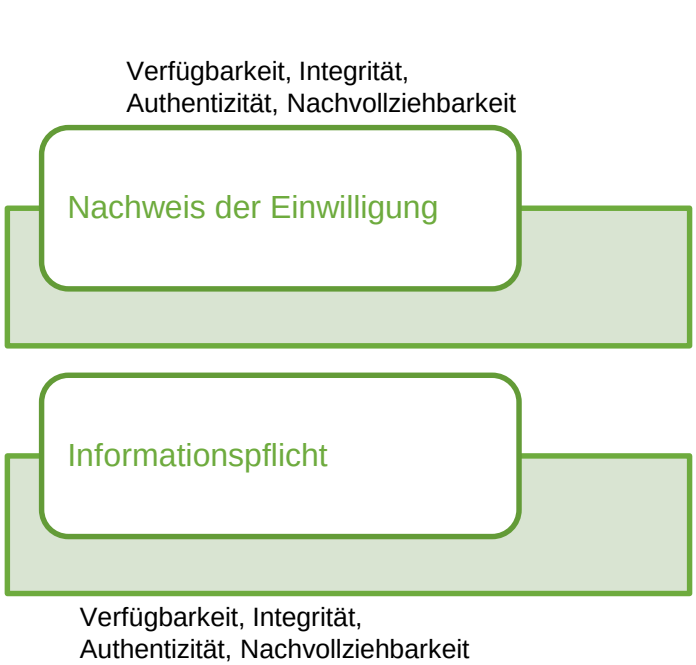
1. Vertrauenswürdigkeit im E-Goverment (und E-Business)
2. Regulatorische Rahmenbedingungen
3. Fachlich-technische Rahmenbedingungen (Stand der Technik)
4. Architektur und Datenpakete
5. Fazit und Ausblick

REGULATORISCHE UND FACHLICHE RAHMENBEDINGUNGEN



Fraunhofer FOKUS

DATENSCHUTZ UND (VERTRAUENSWÜRDIGE) LANGZEITSPEICHERUNG



Fraunhofer FOKUS

ELEKTRONISCHE PROZESSE SIND NUR SO VERTRAUENSWÜRDIG WIE DIES NACHWEISBAR IST – DER BEWEISWERT DIGITALER 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 (nur öffentliches Recht)	Öffentliche elektronische Dokumente (von Behörde) ohne qualifizierte elektronische Signatur	öffentliche elektronische Dokumente (von Behörde) mit qualifizierter elektronischer Signatur bzw. De-Mail mit qualifiziert signierter Absende-betätigung (nur im öffentlichen Recht)
Freie Beweiswürdigung des Richters	Anschein für Echtheit	Freie Beweiswürdigung des Richters	Vermutung für Echtheit

Beweiswert des Siegel → Art. 35 eIDAS (Authentizität und Integrität)
ZPO gilt auch im Verwaltungs-/Sozialrecht etc.
Ersetzendes Scannen gem. Stand der Technik gilt Beweis öffentlicher Urkunden (vgl. § 371b ZPO)

Die Verwaltung führt den Beweis durch Akten, einzelne Dokumente sind also regelmäßig nicht ausreichend, ebenso ist (nicht nur bei ersetzendem Scannen) die Beachtung des Stands der Technik nachzuweisen.
(§ 99 VwGO, OVG Greifswald, Urteile VG Wiesbaden)

AGENDA

1. Vertrauenswürdigkeit im E-Goverment (und E-Business)
2. Regulatorische Rahmenbedingungen
3. Fachlich-technische Rahmenbedingungen (Stand der Technik)
4. Architektur und Datenpakete
5. Fazit und Ausblick

SCHUTZ UND NACHWEIS GESCHÄFTSRELEVANTER AUFZEICHNUNGEN LÄSST SICH NUR DURCH ERHALTUNG DER INFORMATIONEN UND DEREN BEWEISWERTERHALTUNG ERREICHEN

Herausforderungen

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

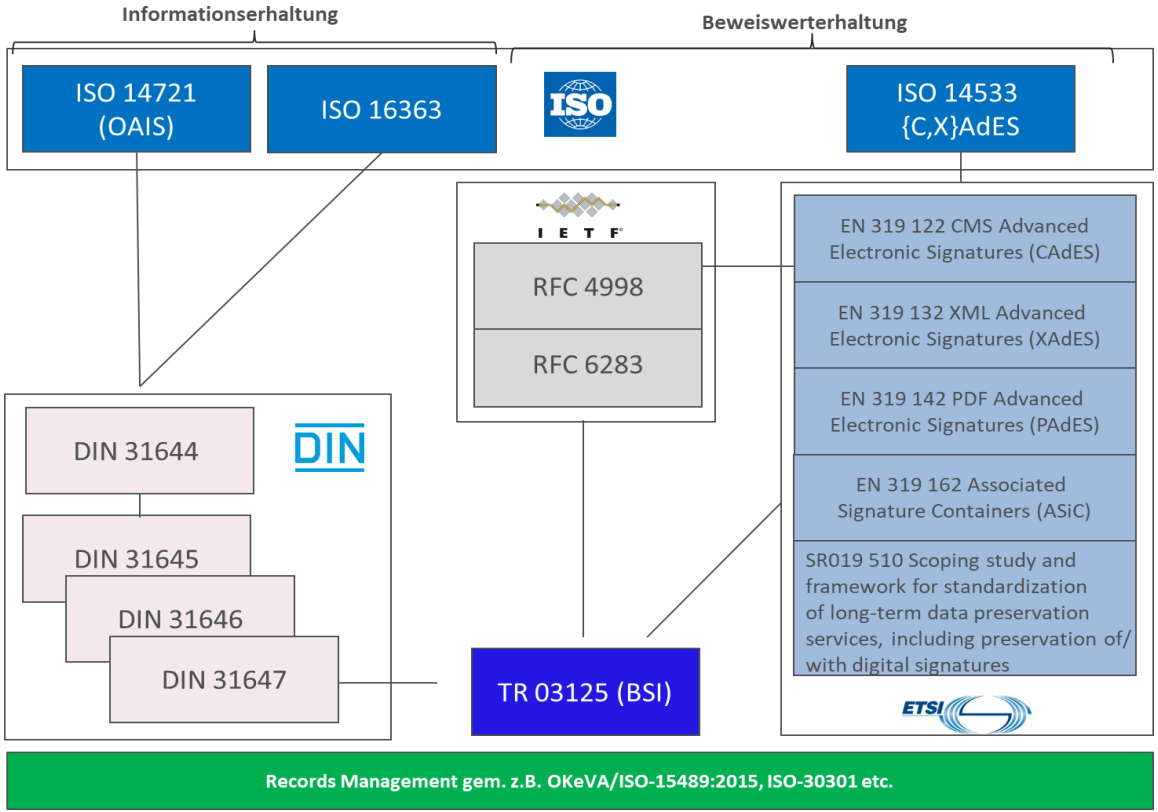
Sicherstellung

- Authentizität
- Integrität
- Nachvollziehbarkeit
- Verkehrsfähigkeit
- Verfügbarkeit
- Vertraulichkeit

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

STAND DER TECHNIK ZUR VERTRAUENSWÜRDIGEN (BEWEISSICHEREN) LANGZEITSPEICHERUNG



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

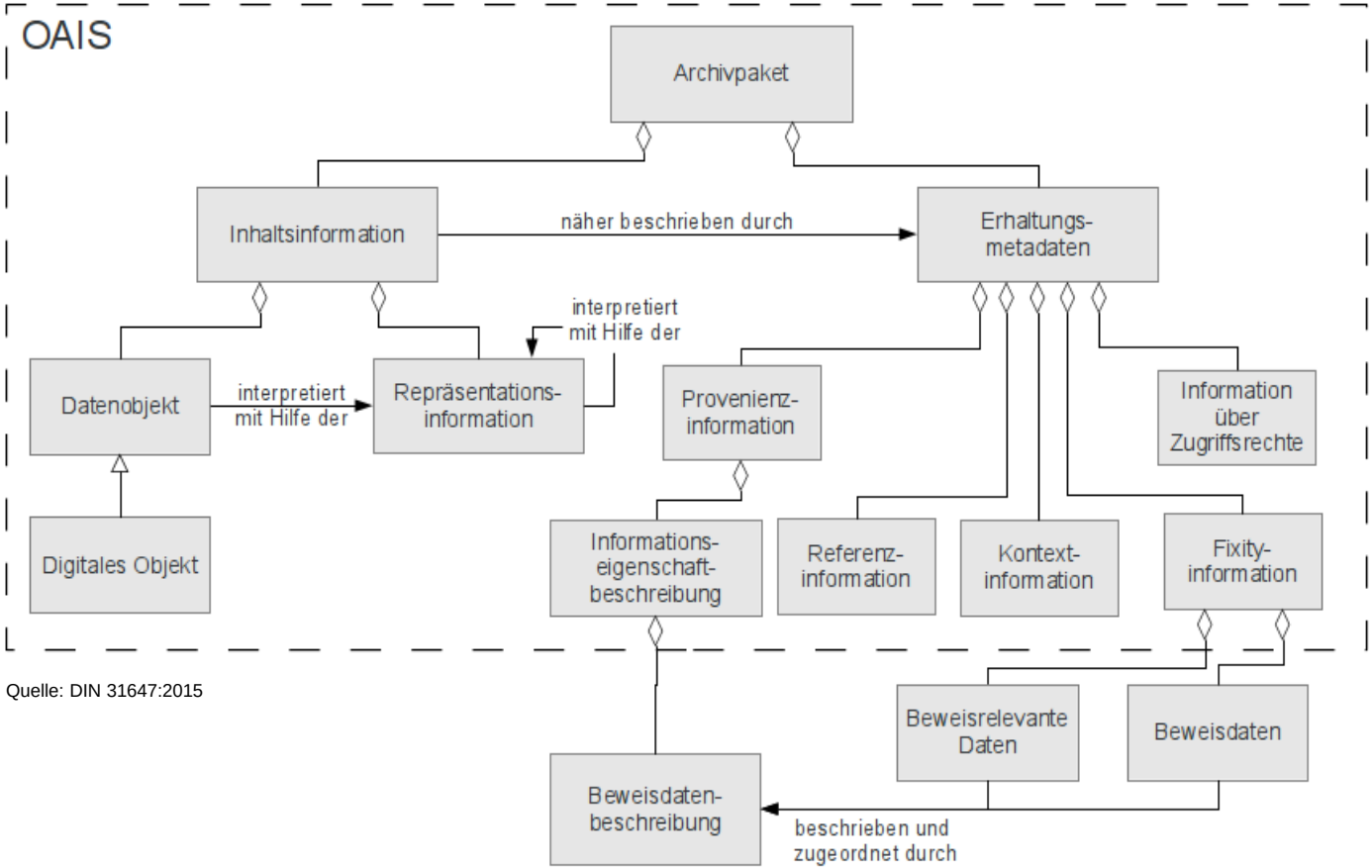
- Nutzung standardisierter Formate für Content, Metadaten
- i.d.R. physische, selbsttragende Informationspakete
- Migration zur Informationserhaltung im Preservation Planning

Beweiswerterhaltung

objektbezogen

- Beweisrelevante Daten
- Evidence Record
- Signatur- und Hasherneuerung

DATEN ZUR BEWEISWERTERHALTUNG IM AIP



Quelle: DIN 31647:2015

BEWEISWERTERHALTUNG IM KONTEXT EIDAS: ENTWICKLUNG DER PRESERVATION SERVICES UND LTA-PROFILES

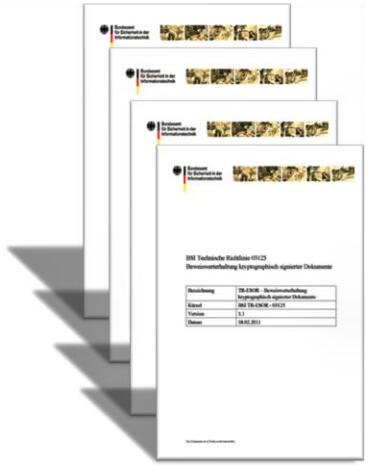
Quelle: U. Korte et al.: Beweiswerterhaltung im Kontext eIDAS - eine Case Study. DACH-Security 2016, Frechen 2016 S. 379-392

Fraunhofer FOKUS

AGENDA

1. Vertrauenswürdigkeit im E-Goverment (und E-Business)
2. Regulatorische Rahmenbedingungen
3. Fachlich-technische Rahmenbedingungen (Stand der Technik)
4. Architektur und Datenpakete
5. Fazit und Ausblick

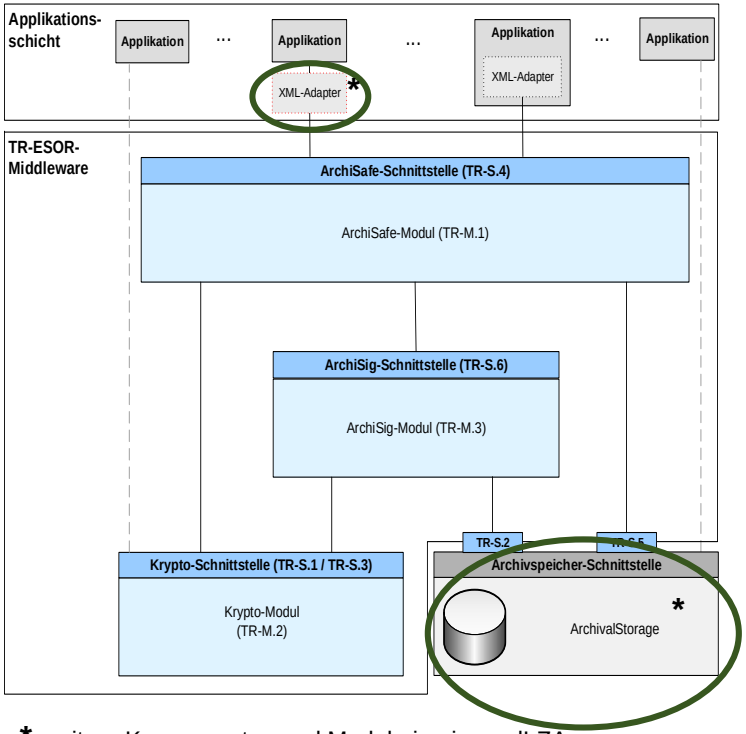
STAND DER TECHNIK ZUR BEWEISWERTERHALTUNG: BSI TR-ESOR (AKTUELL: V1.2.1, V1.3 IST IN ENTWICKLUNG)



Aktuelle Version: 1.2.1 (v1.3 in Entwicklung)

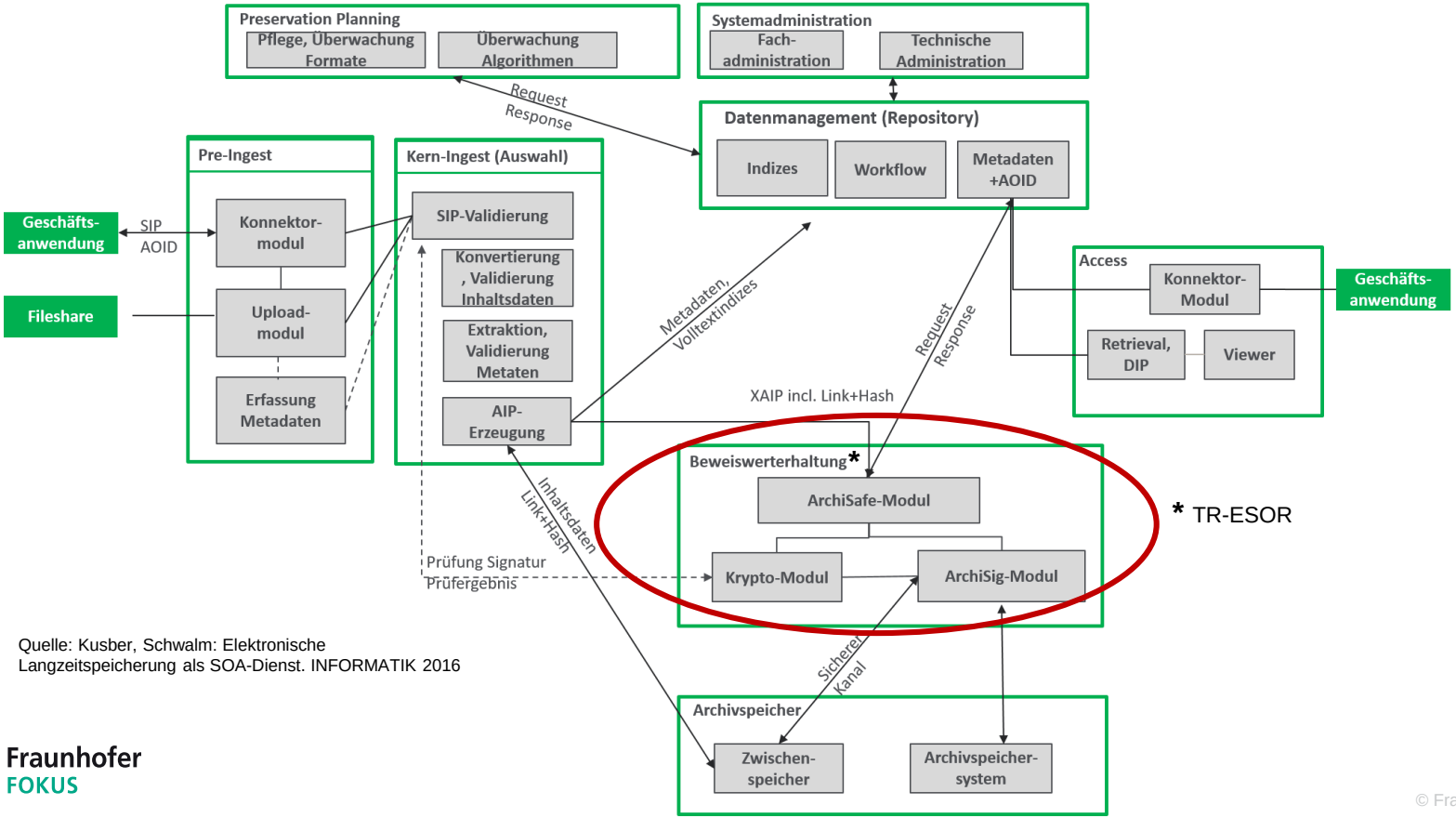
TR-ESOR Hauptdokument

- 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“



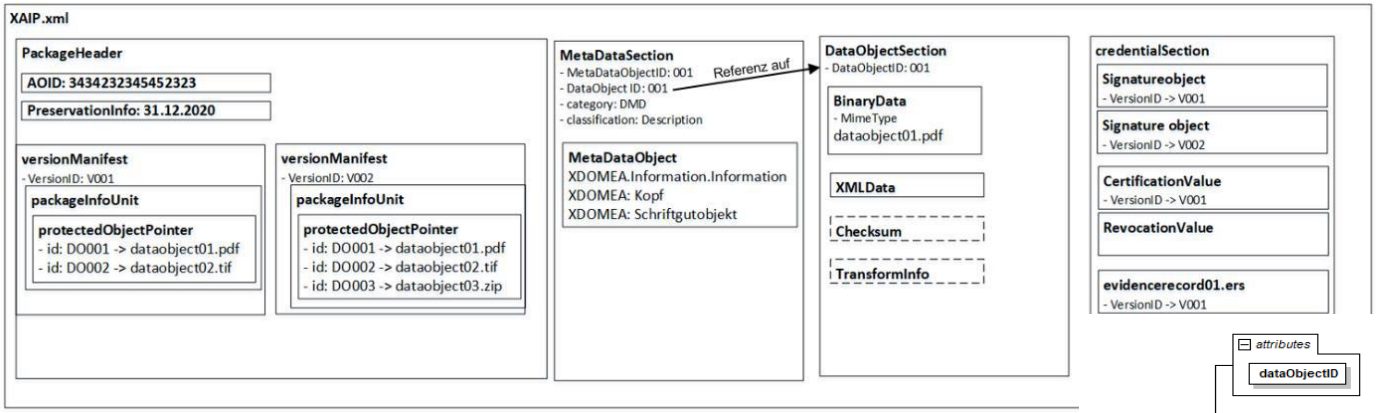
* weitere Komponenten und Module in einem dLZA

BEISPIELARCHITEKTUR EINES VERTRAUENSWÜRDIGEN DLZA ZUR INFORMATIONS- UND BEWEISWERTERHALTUNG



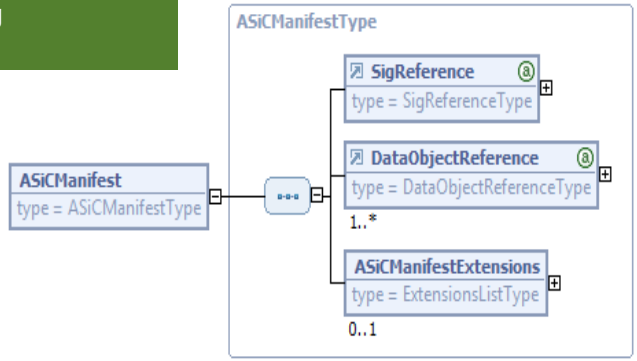
Quelle: Kusber, Schwalm: Elektronische Langzeitspeicherung als SOA-Dienst. INFORMATIK 2016

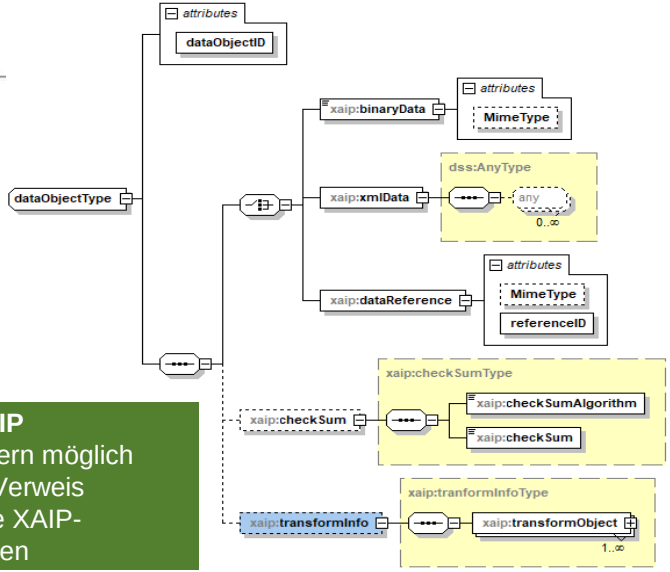
SELBSTTRAGENDE AIP-CONTAINER-FORMATE FÜR TR-ESOR V1.3 – WEITERE FORSCHUNGSABREIT: PDF/A-3



XML-formatted AIP
- ✓ Basierend auf XFDU
- ✓ Vollständig selbsttragend
- ✓ Incl. Versionierung, ERO/NERO

ASiC-E
- ✓ EN-319162
- ✓ Aufnahme n-Dateien
- ✓ Versionierung
- ✓ ERO, NERO





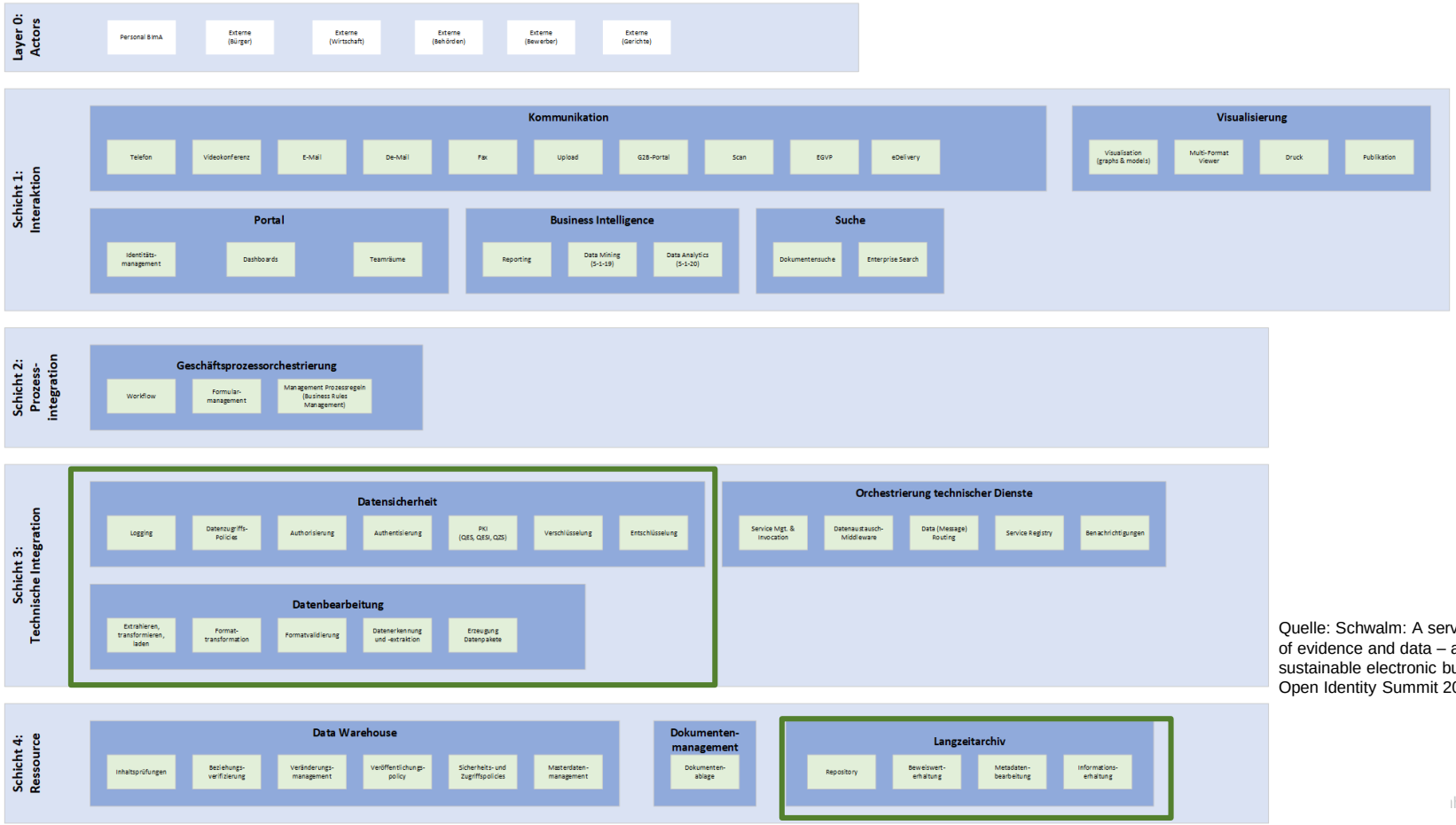
Logisches XAIP
- ✓ Content extern möglich
- ✓ Definierter Verweis
- ✓ Vollständige XAIP-Eigenschaften

Fraunhofer FOKUS

AGENDA

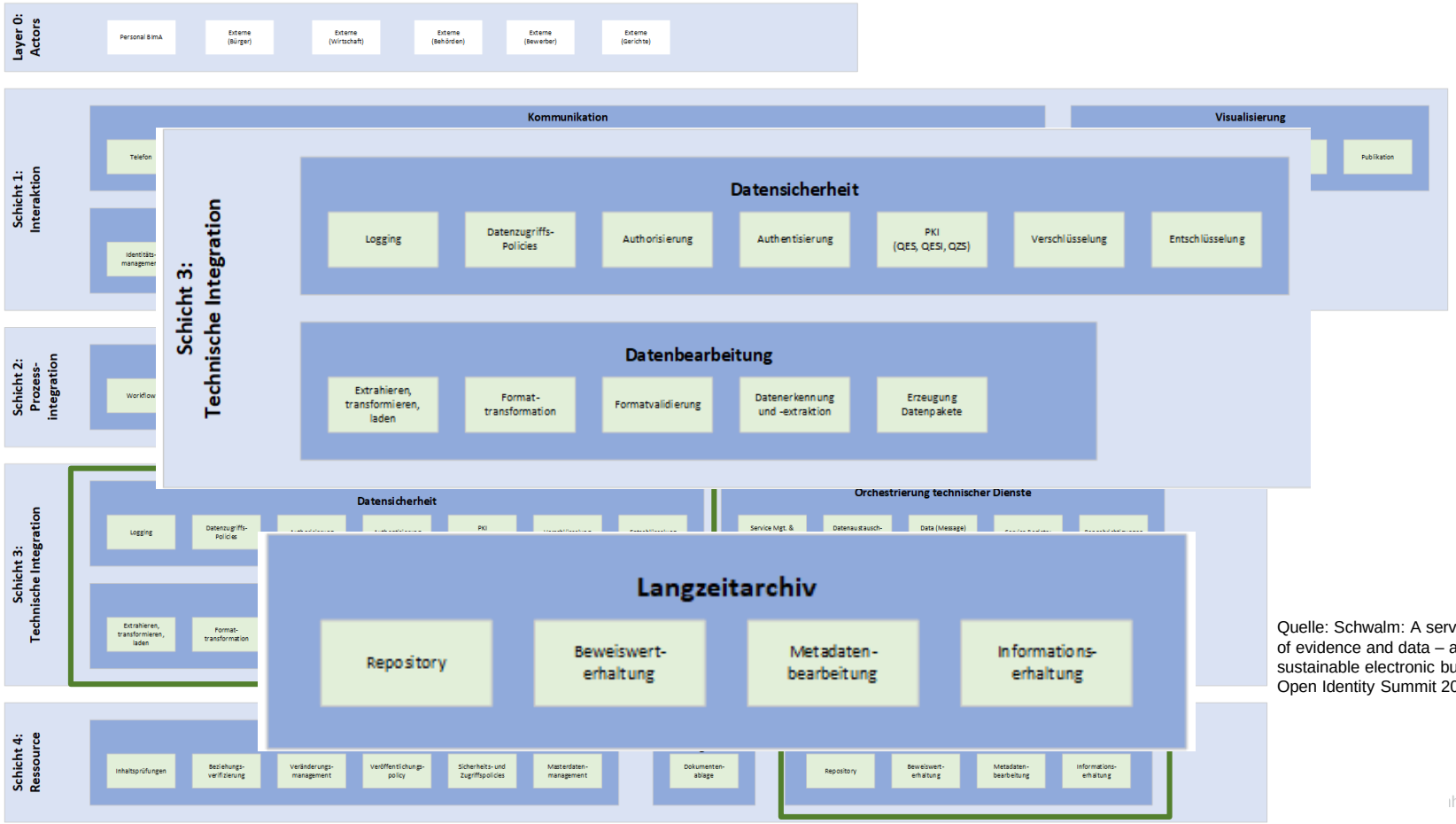
1. Vertrauenswürdigkeit im E-Goverment (und E-Business)
2. Regulatorische Rahmenbedingungen
3. Fachlich-technische Rahmenbedingungen (Stand der Technik)
4. Architektur und Datenpakete
5. Fazit und Ausblick

GESAMTARCHITEKTUR FÜR EIN VERTRAUENSWÜRDIGES E-GOVERNMENT (PRAXISBEISPIEL AUF BASIS TOGAF ®)



Quelle: Schwalm: A service for the preservation of evidence and data – a key for a trustworthy & sustainable electronic business. Open Identity Summit 2017

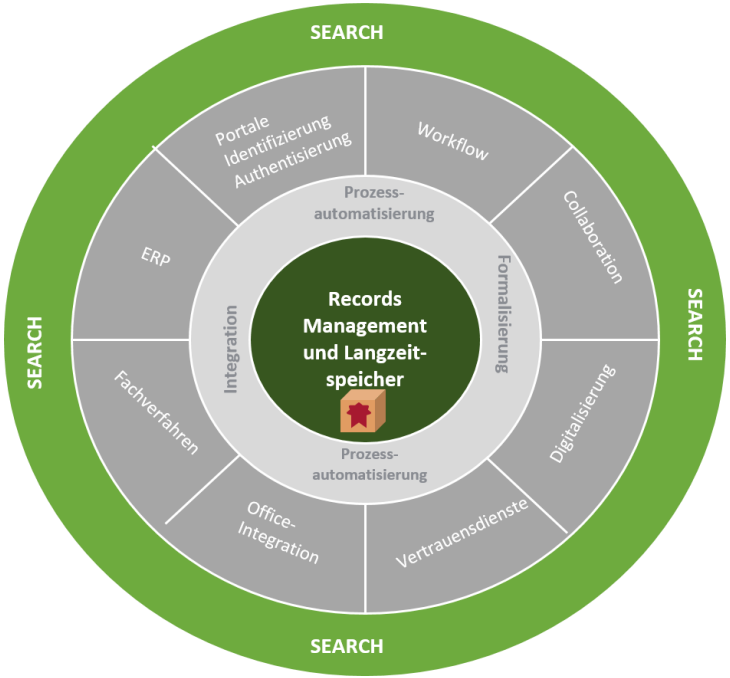
GESAMTARCHITEKTUR FÜR EIN VERTRAUENSWÜRDIGES E-GOVERNMENT (PRAXISBEISPIEL AUF BASIS TOGAF ®)



Quelle: Schwalm: A service for the preservation of evidence and data – a key for a trustworthy & sustainable electronic business.
Open Identity Summit 2017

EIN DLZA-SERVICE, DER DIE BEWEISWERT- UND INFORMATIONSERHALTUNG AUF BASIS EINES VALIDEN RECORDS MANAGEMENT GEWÄHRLEISTET, IST KERNSTÜCK EINES VERTRAUENSWÜRDIGEN E-GOVERNMENTS

Elektronische Signatur/Siegel/ Zeitstempel	• Annahme und Prüfung jeder europ. QES/QESIQ/QZS • Nutzung Siegel sofern keine Unterschrift • Nutzung Fernsignaturen ggf. Fortgeschritten
sichere Kommunikation	• Nutzung eDelivery • Annahme jeder europ. eID • Verschlüsselung, sichere Identifizierung/Authentisierung
Durchgängig elektronische Prozesse	• Verbindung der notwendigen Vertrauensdienste z.B. Websitezertifikate • Umfassende Nutzung eIDAS für hohe Sicherheit, Interoperabilität • Priorisierung entspr. Dringlichkeit • Org. Basis (Records Management)
Digitalisierung	• Nutzung eSiegel für Integritäts-sicherung gem. RESISCAN • Aufbau als Dienst
Langzeitspeicherung	• Informations- und Beweiswerterhaltung • TR-ESOR, OAIS, SR 019510



FÜR FRAGEN UND ANTWORTEN:

Fraunhofer FOKUS

Steffen Schwalm
Researcher/wiss. Mitarbeiter
Digital Public Services (DPS)

Kaiserin-Augusta-Allee 31
10589 Berlin

M + 491622806472

www.fokus.fraunhofer.de

steffen.schwalm@fokus.fraunhofer.de


Fraunhofer
FOKUS