Bundesamt
für Sicherheit in der
Informationstechnik

eIDAS, ETSI Long-Term Preservation (LTP) und BSI TR-03125 (TR-ESOR)

25. April 2019, Berlin

Dr. Ulrike Korte (BSI)

Agenda

1. Ausgangslage eIDAS
   - … die „EU-Verordnung zur Digitalisierung“

2. ETSI Long-Term Preservation (LTP)
   - TS 119 511
   - TS 119 512

3. BSI-TR 03125 Beweiswerterhaltung kryptographisch signierter Dokumente
   - Einführung
   - Neuigkeiten und aktuelle Entwicklungen

4. Zusammenspiel eARK in (L)XAIP und ASiC-AIP gemäß LTP/TR-ESOR

5. Ausblick

1. Ausgangslage eIDAS

EU-Verordnung elektronische Vertrauensdienste (eIDAS-VO)

Verbindliche Rechtsgrundlage EU-weit in Kraft seit September 2014, in den Mitgliedstaaten anwendbar seit : Juli 2016

- Einheitliche Maßgaben für sichere elektronische Geschäftsprozesse **in Europa**
- Vorgaben zur rechtlichen Bedeutung und technischen Umsetzung
- Rechtl. Detaillierung in Durchführungsakten
- Technisch: ETSI/CEN- Normen, auf die die Durchführungsakte referenzieren

- QES = Ersatz manuelle Unterschrift // QES = höchster Beweiswert

- Aufsicht und Prüfung qualifizierter Vertrauensdienste (VD) durch **europäische Aufsichtsbehörden** und **Konformitätsbewertungs-stellen (je EU-Land)** und Eintragung der Vertrauensdiensteanbieter (VDA) in **Vertrauensliste (TL)**

- Behörden müssen Signaturen und Siegel in bestimmten Formaten (siehe DRA 2015/1506/EU) akzeptieren und verarbeiten können.
- Abweichung von vorgeschriebenen ETSI-Formaten möglich bei kostenfreier Bereitstellung eines Prüftools

Kernthemen eIDAS

Neue VDs bzgl. (Q)ES, (Q)ZS, (Q) Siegel

- **Erstellen, Validieren von (Q)ES, (Q)ZS, (Q) Siegel**
- **Siegel und Organisationszertifikate möglich**
- **Kein zwingender Bezug zur natürlichen Person**
- **Produkte qual. VDA europaweit anzuerkennen**

Bewahrungsdienste

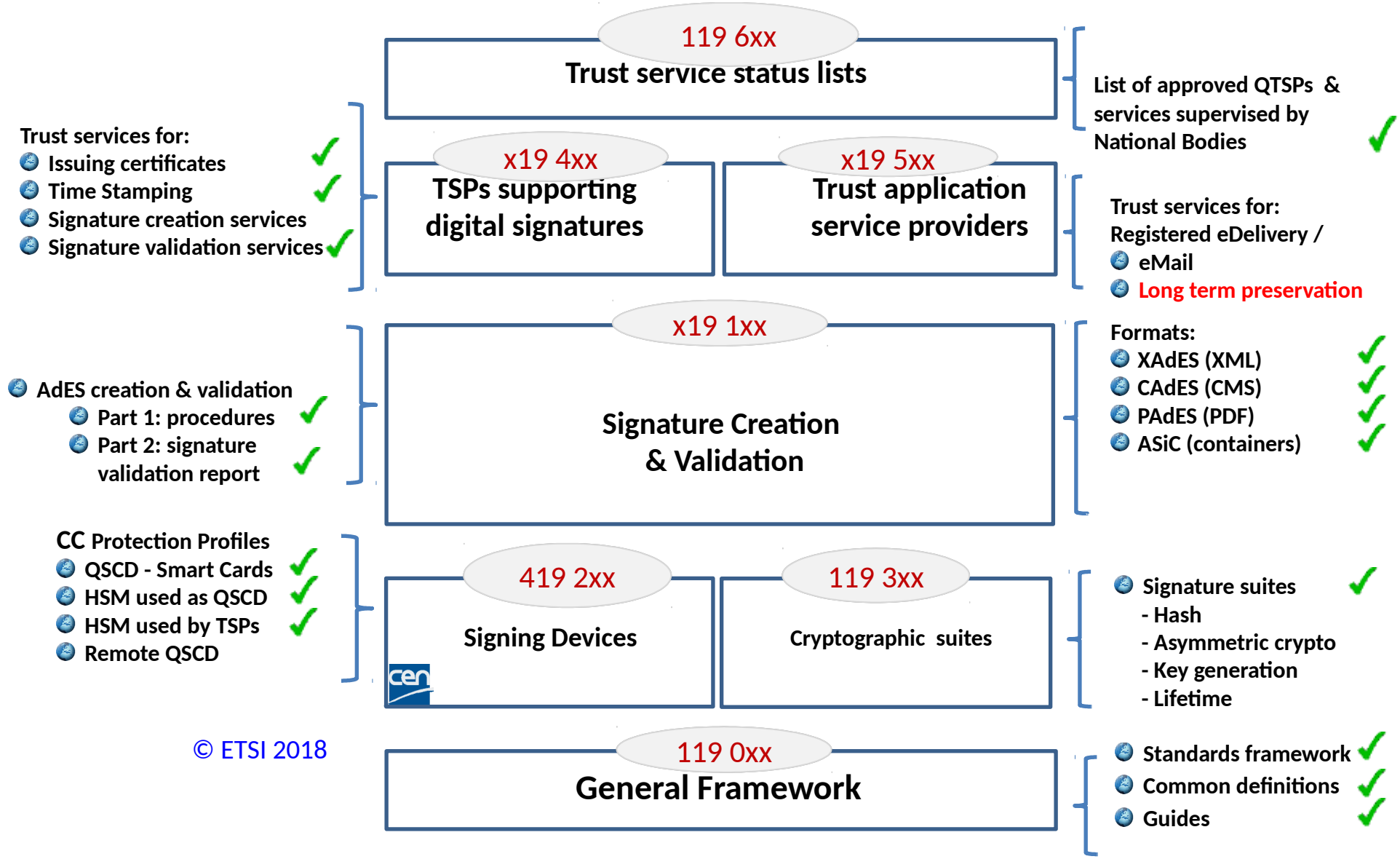
- **Beweiswerterhalt der QES, QSiegel,**
- **gem. ETSI aber auch Bewahrung allg. Daten mittels Signaturtechniken (z.B. mit Evidence Records gemäß RFC4998)**

Zustelldienste

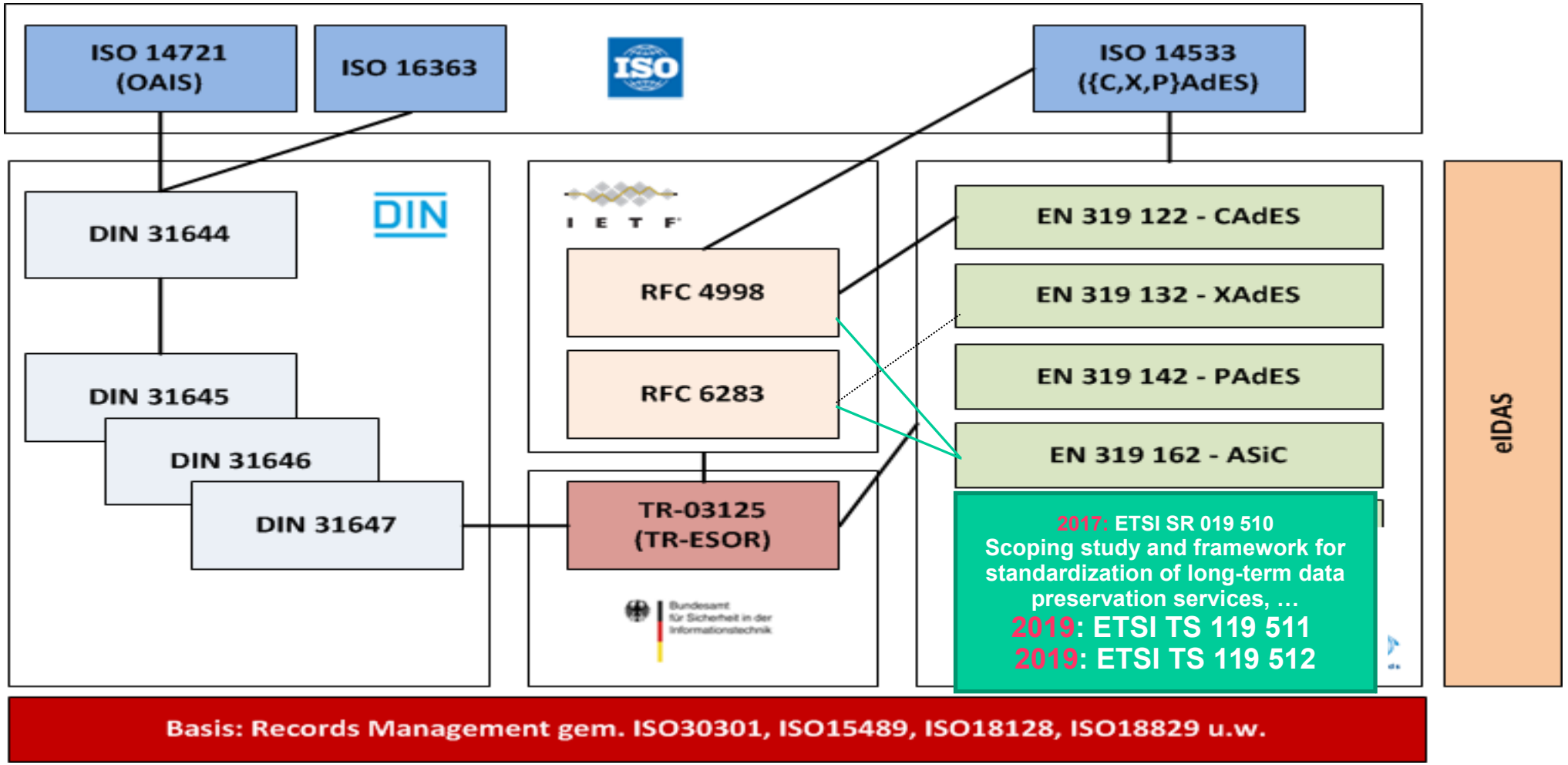
- **Nachweisbare Zustellung elektronischer Einschreiben europaweit**

Authentisierung

eIDAS Standards Framework: Published Standards



Relevant Standards for Preservation of Information and Evidence
NEW 2017-05: ETSI SR 019 510 V1.1.1
NEW 2019-04/05: ETSI TS 119 511 V1.1.1 and ETSI TS 119 512 V1.1.1

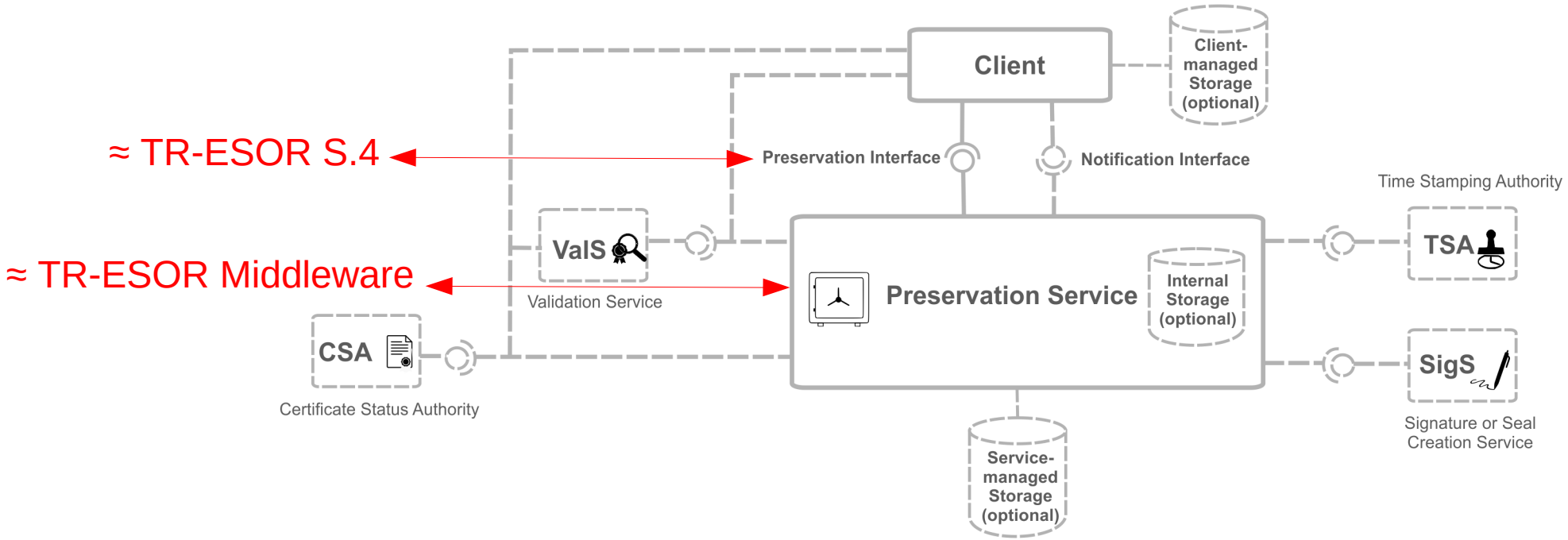


2. ETSI Long-Term Preservation (LTP)

ETSI TS 119 511

- Basis:
  - EN 319 401 "Electronic Signatures and Infrastructures (ESI); General Policy Requirements for Trust Service Providers"
- Ziel: “preservation over long periods of time .. the ability
  - to validate a digital signature, to maintain its **validity status and**
  - **to get a proof of existence** of the associated signed data”, und/oder **PDS**
  - “provision of proofs of existence over long periods of time of general data whether this data is signed or not” **PGD**
- Speichermodelle
  - Bewahrungsdienst mit Speicher **WST**
  - Bewahrungsdienst mit temporärem Speicher **WTS**
  - Bewahrungsdienst ohne Speicher **WOS**

ETSI TS 119 512: Systemarchitektur für Bewahrungsdienste



ETSI TS 119 511 – Policy and Security Requirements

- General Concept
- Extension of:
  - ETSI EN 319 401 "Electronic Signatures and Infrastructures (ESI); General Policy Requirements for Trust Service Providers"
- Further Requirements concerning
  - Operational and Notification Protocols
  - Preservation Evidences
  - Preservation of Digital Signatures
- Annex A (normative): Qualified preservation service for QES as defined by article 34 the Regulation (EU) No 910/2014
- Link: https://portal.etsi.org/TBSiteMap/ESI/ESIActivities.aspx

ETSI TS 119 512 – Preservation Protocol

- General Concept (Architecture, Goals, Storage Models, ..)
- Technical Specification of Protocol
  - First in a generic fashion and then
  - specifying the concrete syntax of the conveyed data elements for XML/SOAP and JSON/REST
- Technical Specification of Components for Operations
- Annexes, e.g.:
  - Preservation Object Formats
    - Preservation Evidence Formats (Signature-/Seal-Formate, ASiC-E, XAIP), ≈ TR-ESOR
    - Preservation Object Container (POC) Formats (ASiC-E withEvicence Record, XAIP) ≈ TR-ESOR
  - XML Schema Document and JSON Schema Document
  - Attributes to be inserted in preservation evidences
  - ...
- Link: https://portal.etsi.org/TBSiteMap/ESI/ESIActivities.aspx

ETSI TS 119 512 / TR-ESOR: Transformierbare Schnittstellen

ETSI TS 119 512				TR-ESOR V1.2 ff	Verbindlich-keitsgrad
			mit Speicher		
PreservePO	m=mandatory		X	ArchiveSubmissionRequest	m=mandatory
DeletePO	m		X	ArchiveDeletionRequest	m
RetrievePO	m		X	ArchiveEvidenceRequest	m
RetrievePO	m		X	ArchiveRetrievalRequest	m
UpdatePOC	(optional)		X	ArchiveUpdateRequest	optional
Validate Evidence	(optional)		X	VerifyRequest	optional
RetrieveInfo			X		
RetrieveTrace	(optional)		X		
Search	(optional)		X	ArchiveDataRequest	optional

2. BSI-TR 03125 Beweiswerterhaltung kryptographisch signierter Dokumente (TR-ESOR)

Die Technische Richtlinie TR 03125 TR-ESOR

Gegenstand und Ziel dieser technischen Richtlinie ist die
Beweiswerterhaltung
von kryptographisch signierten
Dokumenten
Im Kontext ihrer Aufbewahrung

Mit dem Begriff der „**kryptographisch signierten Dokumente**“ sind in dieser TR neben den **qualifiziert signierten/gesiegelten Dokumenten** (im Sinne eIDAS /VDG) auch Dokumente mit einer **fortgeschrittenen Signatur bzw. Siegel** erfasst, wie sie oft in der internen Kommunikation von Organisationen entstehen.
Nicht gemeint sind hier Dokumente mit einfachen Signaturen, basierend auf anderen (nicht-kryptographischen) Verfahren

Es können auch **nicht-signierte Dokumente** in einem TR-ESOR-System gespeichert werden.

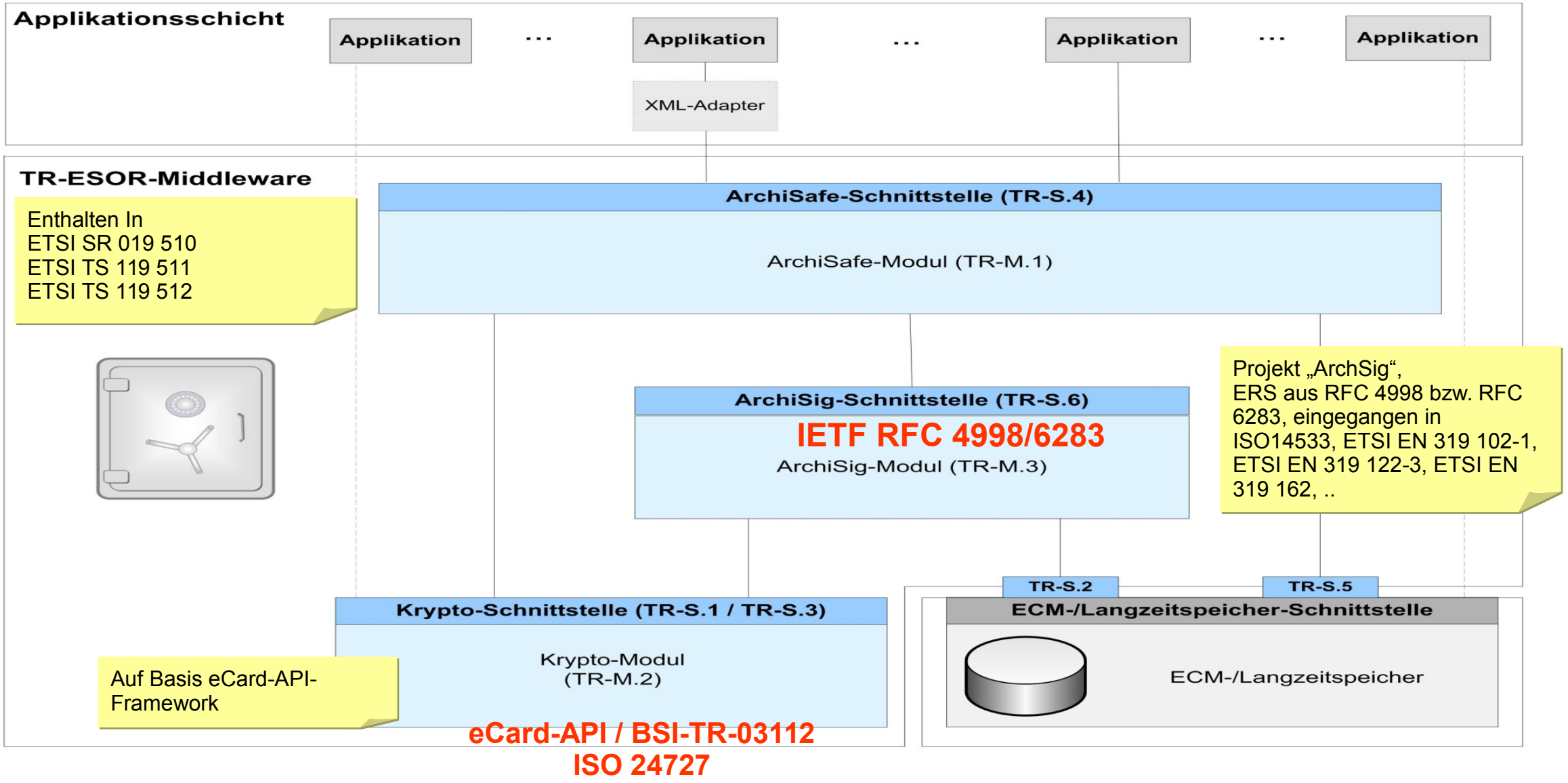
Elektronische Aktenführung/Digitalisierung

§§ 6 und 7 EGovG fordern die elektronische Aktenführung inkl. Scannen und Langzeitaufbewahrung nach dem „Stand der Technik“, mit Verweis auf TR-ESOR und TR RESISCAN, Länder u.a. NRW, Berlin, M-V

Beweisregelungen zugunsten nach Stand der Technik eingescannter Dokumente, z.B. §§ 371 b, 298a ZPO
Orientierungshilfen des BSI durch Technische Richtlinien

Umsetzung: modular-skalierbare Architektur der TR-ESOR-Middleware

Die Richtlinie beruht auf nationalen und internationalen Standards



Aktueller Stand

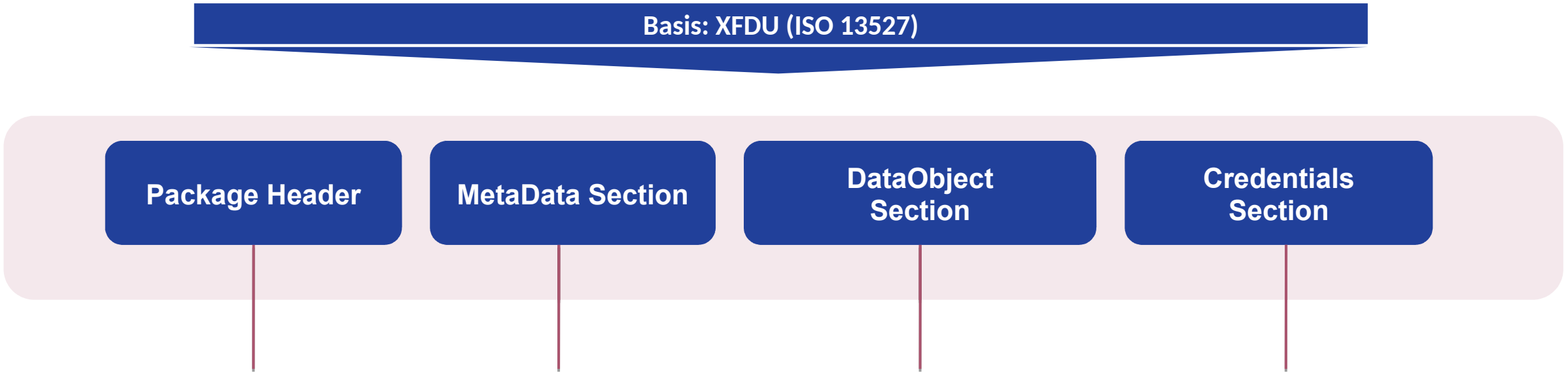
Fragen	Stand	
Mehr als 10 Produkthersteller	Produkthersteller: 13 Sekundäranbieter 8	✓
Durchgeführte Fachkunde-Schulungen und Prüfungen für angehende Prüfstellen	3	✓
Zugelassene Prüfstellen für TR 03125 TR-ESOR	datenschutzCert	✓
Zertifizierte Produkte gemäß TR 03125	5	✓
Anwender, soweit uns bekannt	Öffentliche Hand: 32 Industrie: 14 (national, international)	✓

Weiterentwicklung BSI TR 03125 TR-ESOR

- **2018-2019: Entwicklung TR-ESOR V1.2.2**
  - **Archivdatencontainer**:
    - Spezifizierung eines **logischen Archivdatencontainers** für “große Daten”/hohen Datendurchsatz
    - Profilierung des **ETSI-ASiC-Containers gemäß EN 319 162** als zusätzlicher TR-ESOR-Archivdatenobjekt-Container
  - **„Obere“ Interoperabilitäts-Schnittstelle zu TR-ESOR neben S.4:**
    - Spezifizierung einer „oberen“ technischen TR-ESOR-Schnittstelle auf Basis von **ETSI TS 119 512** „Protocols for trust service providers …“ nach Veröffentlichung von ETSI TS 119 512
- **2019-2020: Entwicklung TR-ESOR V1.3**
  - **Überarbeitets Zertifizierungskonzept**
    - für **Vertrauensdienste** ((qualifizierte) Trust Service Providers gemäß eIDAS) auf Basis von ETSI EN 319 401 und ETSI TS 119 511
    - für ein **TR-ESOR-Produkt** auf Basis von TR-ESOR V1.3 und ETSI TS 119 512
  - **Weitere Aufbau einer Beweisdaten-Interoperabilitäts-Testumgebung** auf Basis von
    - RFC4998, ISO14533, ETSI 319 122-3, ETSI 319 162-1, ETSI TS 119 512

XAIP als selbsttragendes AIP-Format zur Informations- und Beweiswerterhaltung

XAIP ist ein standardisiertes Format für selbsttragende Archiv Informations Paket (AIP), beruhend auf XFDU (ISO 13527), z.B. einsetzbar als eAkte-Format



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

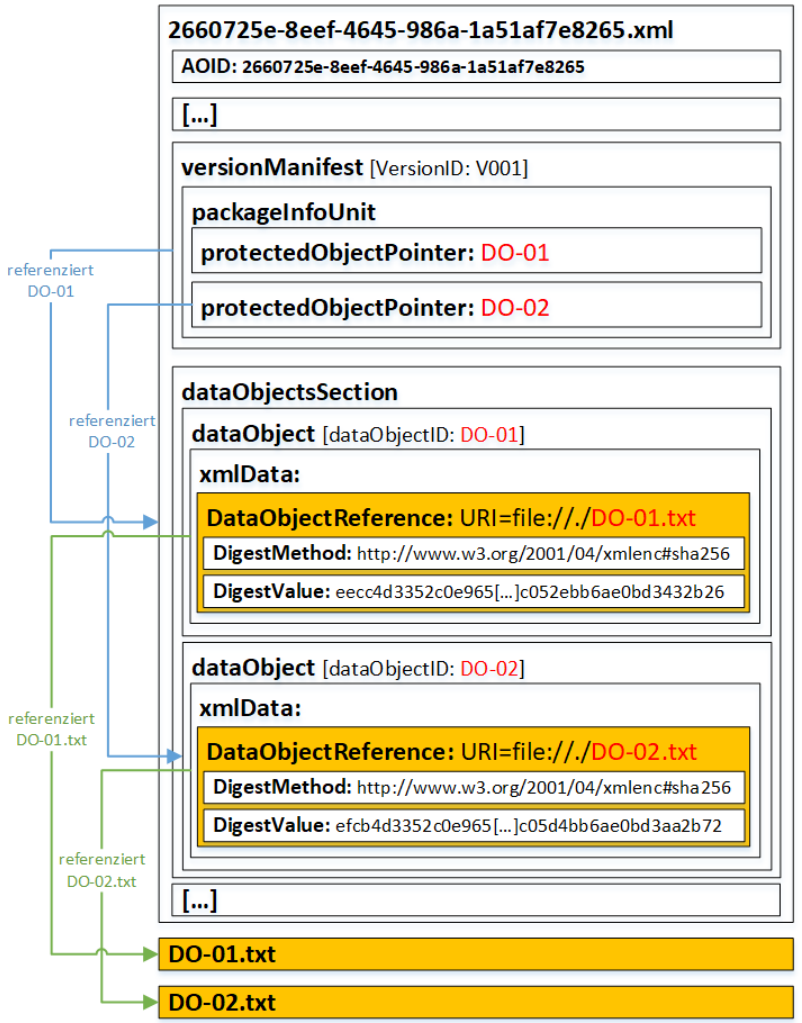
Informationen über den Geschäfts- und Archivierungskontext der Nutzdaten
z.b. Einbindung XBARCH, XDOMEA, PREMIS, eARK...

Enthält die eigentlichen Nutzdatenobjekte (XML oder Base64 kodiert)

Beweisrelevante Daten (z.B. Signaturen, Siegel, Zertifikate) und technische Beweisdaten (Evidence Record)

TR-ESOR V1.2.2: Logisches XAIP

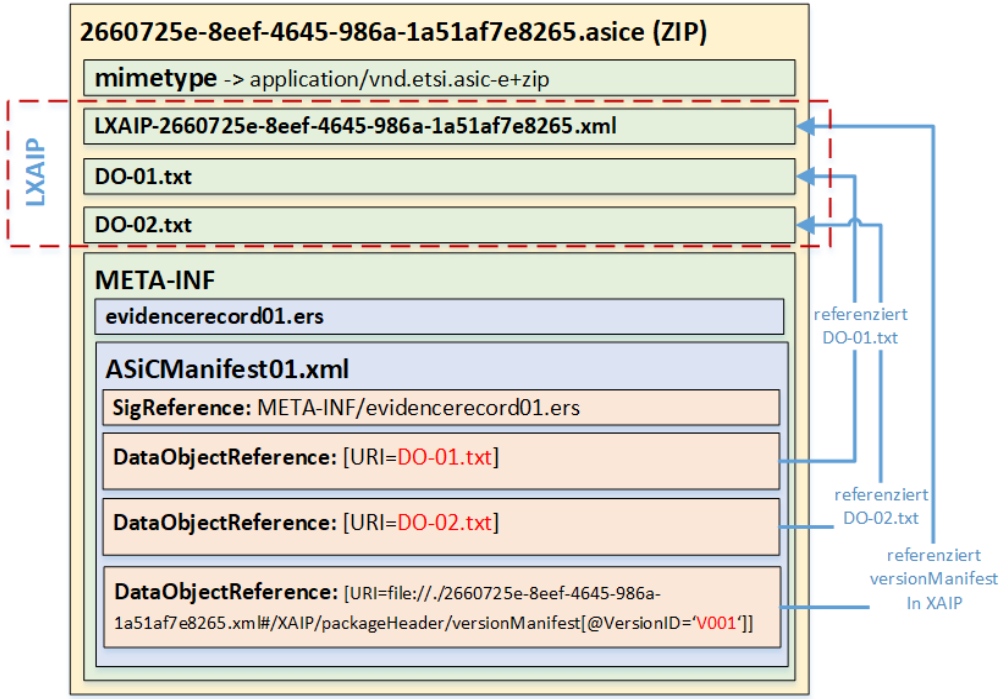
- **Logische Trennung der Inhaltsdaten und XAIP**
  - Erweiterung der vorhandenen XAIP-Definition → Rückwärtskompatibilität gesichert
  - Eindeutige Referenzierung der Inhaltsdaten aus dem Container durch eine URI
  - Element `asic:DataObjectReference` aus EN-319162 (ASiC), als Inhalt von `xaip:xmlData` → Anwendung einer EU Norm
  - Integritätsschutz der referenzierten Daten:
    - Obligatorische Prüfsumme
    - Optional: Zeitstempel, Signatur etc. (Credential section)
  - Vorteil: Besser Umgang mit großen Datenmengen
  - Nachteil: kein selbsttragender Container



"Aufwärtskompatibliät" von (L)XAIP zu ASiC-(I)XAIP

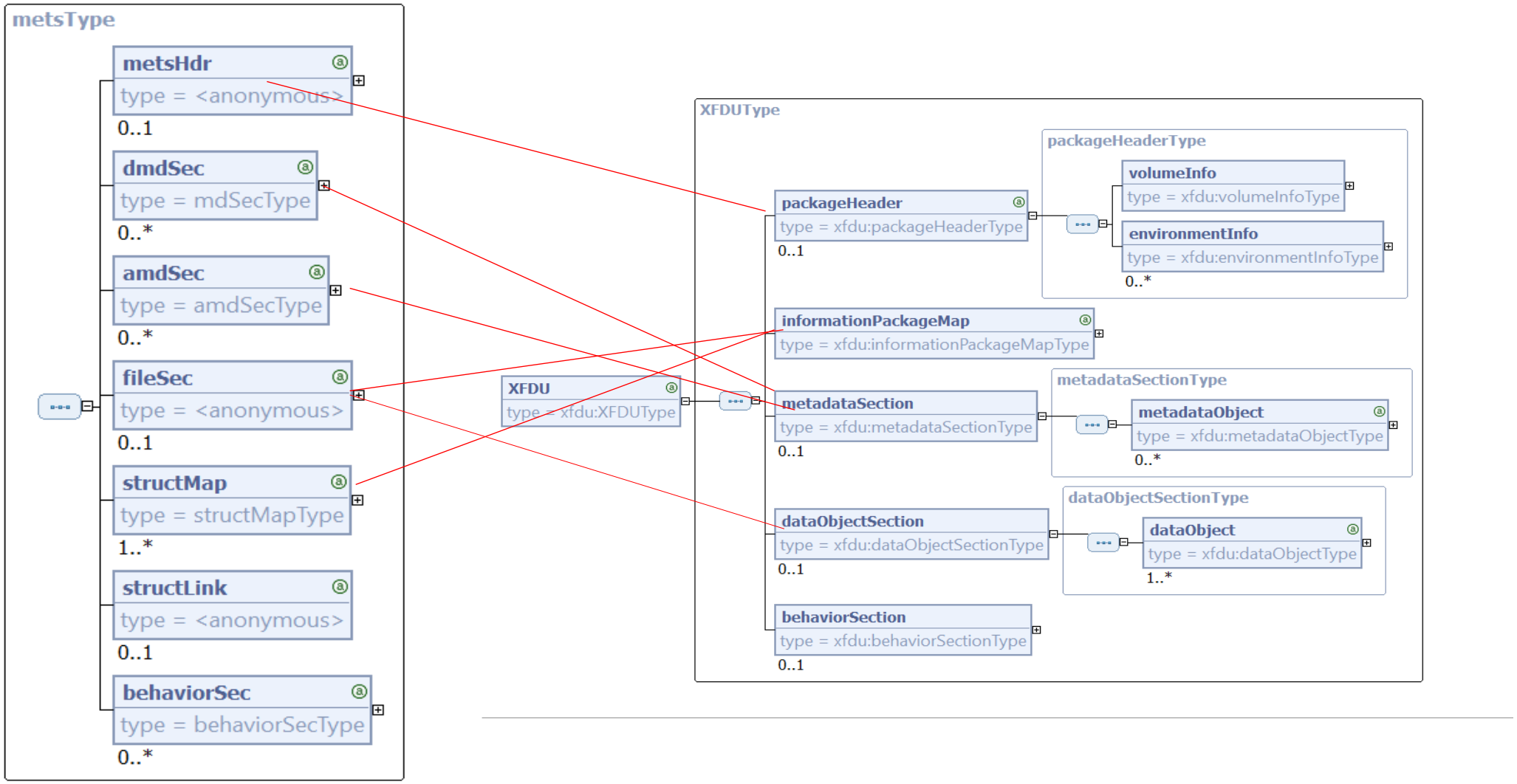
Vorzüge von LXAIP und ZIP

- Basiert auf einem LXAIP → Wiederverwendung etablierten Mechanismen (Synergie)
  - z.B. Gewinnung und Ablage von Metadaten sowie Versionierung, was in ASiC nativ nicht möglich ist
- Nahtloser Übergang zwischen LXAIP und ASiC-E-AIP ohne Weiteres möglich
  - Es handelt sich dabei um eine 1:1-Abbildung
- Die abgelegten Daten werden mit Hilfe des ZIP-Algorithmus komprimiert
- Es entsteht ein zusammenhängender Container, trotz der Verwendung eines logischen XAIP
  - Nutzung eines selbsttragenden Containerformats, im Gegenatz zum LXAIP
- Basierend auf einem europäischen Standard
  - EN 319162 (ASiC)
  - EU-weit standardisiertes Austauschformat
  - Erweiterung des ASiC um die Aspekte der Informationserhaltung (LXAIP)

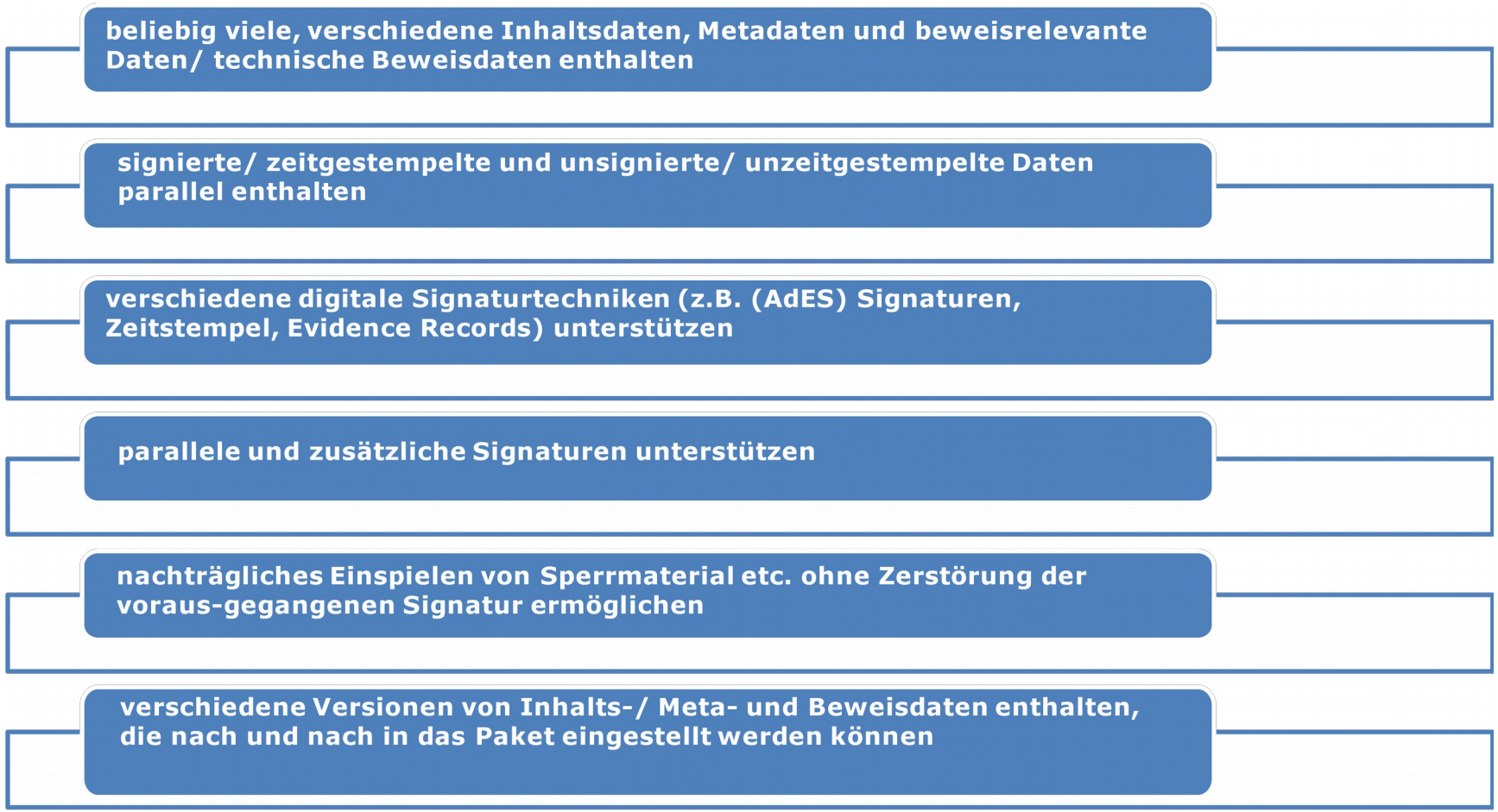


Zusammenspiel eARK in (L)XAIP und ASiC-AIP gemäß LTP/TR-ESOR

Vergleich mets-Type mit XFDU-Type



Anforderungen an Container zur Informations- und Beweiswerterhaltung

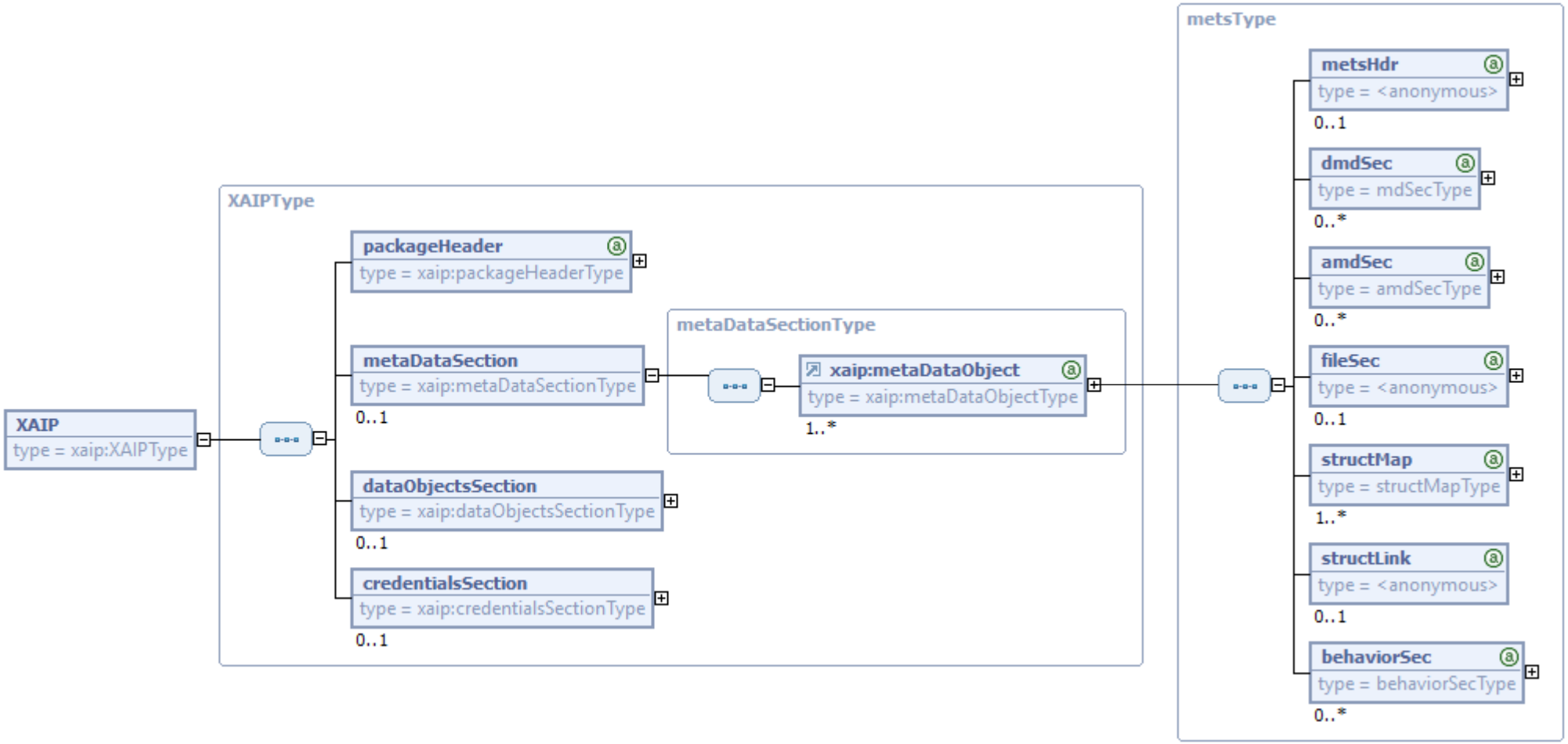


Quelle: T. Kusber, U. Korte, D. Hühnlein, M. Prechtl und B. Wild: Datenpakete zur Informations- und Beweiswerterhaltung. Ein Vergleich. DACH-Security 2017. Frechen 2017 S. 291-303

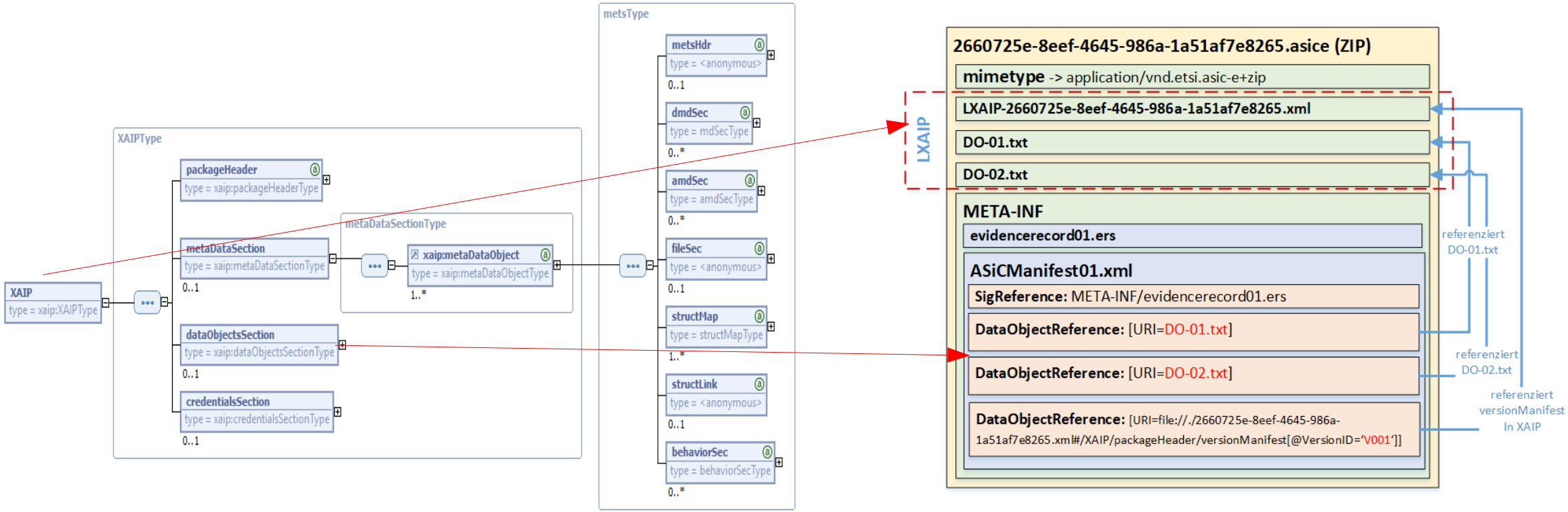
• Anforderungen an Container zur Informations- und Beweiswerterhaltung

- 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
- auf weit verbreiteten, offenen Standards weithin anerkannter, unabhängiger Standardisierungsgremien beruhen

Vorschlag 1: Normiertes Einbetten von eARK in (L-)XAIP

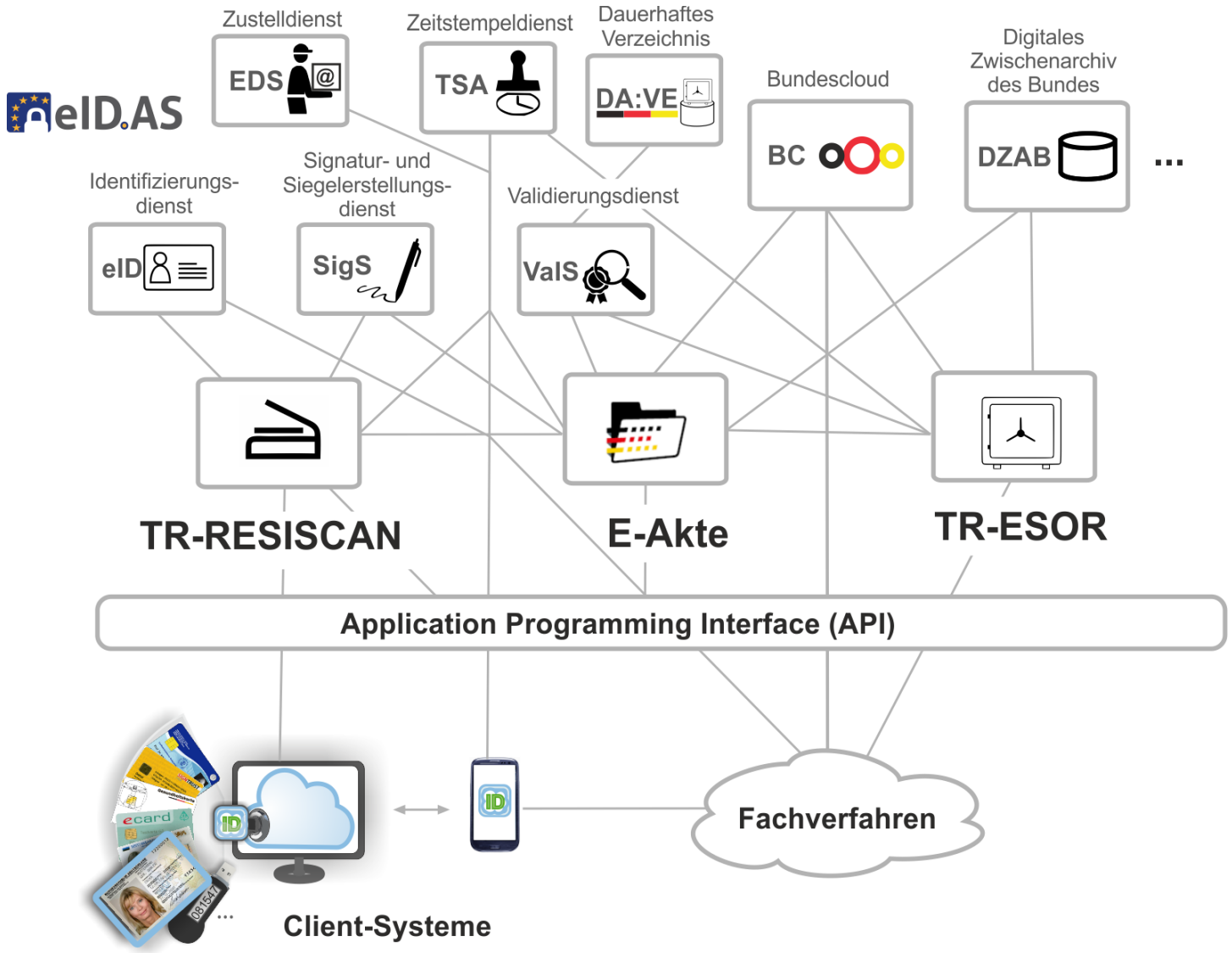


Vorschlag 2: Normiertes Einbetten von eARK in ASiC-AIP



5. Ausblick

Integriertes System zur vertrauenswürdigen Digitalisierung der deutschen Verwaltung



Vielen Dank
für Ihre Aufmerksamkeit!

Kontakt

Dr. rer. nat. Ulrike Korte
Bundesamt für Sicherheit in der Informationstechnik
Godesberger Allee 185-189
53175 Bonn
E-Mail: Ulrike.Korte@bsi.bund.de
www.bsi.bund.de

Neue ETSI - Preservation – Standards (Publikation in Kürze)

- **ETSI TS 119 511:** "Policy & Security Requirements for trust service providers providing long-term preservation of digital signatures or unsigned data using signature techniques"
  - PL: Dr. Andrea Röck, Frankreich

- **ETSI TS 119 512**: "Protocols for trust service providers providing long-term preservation of digital signatures or unsigned data using signature techniques"
  - PL: Dr. Detlef Hühnlein, Deutschland