Nutzungsmöglichkeiten des E-ARK-SIPs

Anforderungen AIP-Formate zur Informations- und Beweiswerterhaltung

- 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 voraus-gegangenen Signatur ermöglichen
- verschiedene Versionen von Inhalts-/ Meta- und Beweisdaten enthalten, die nach und nach in das Paket eingestellt werden können

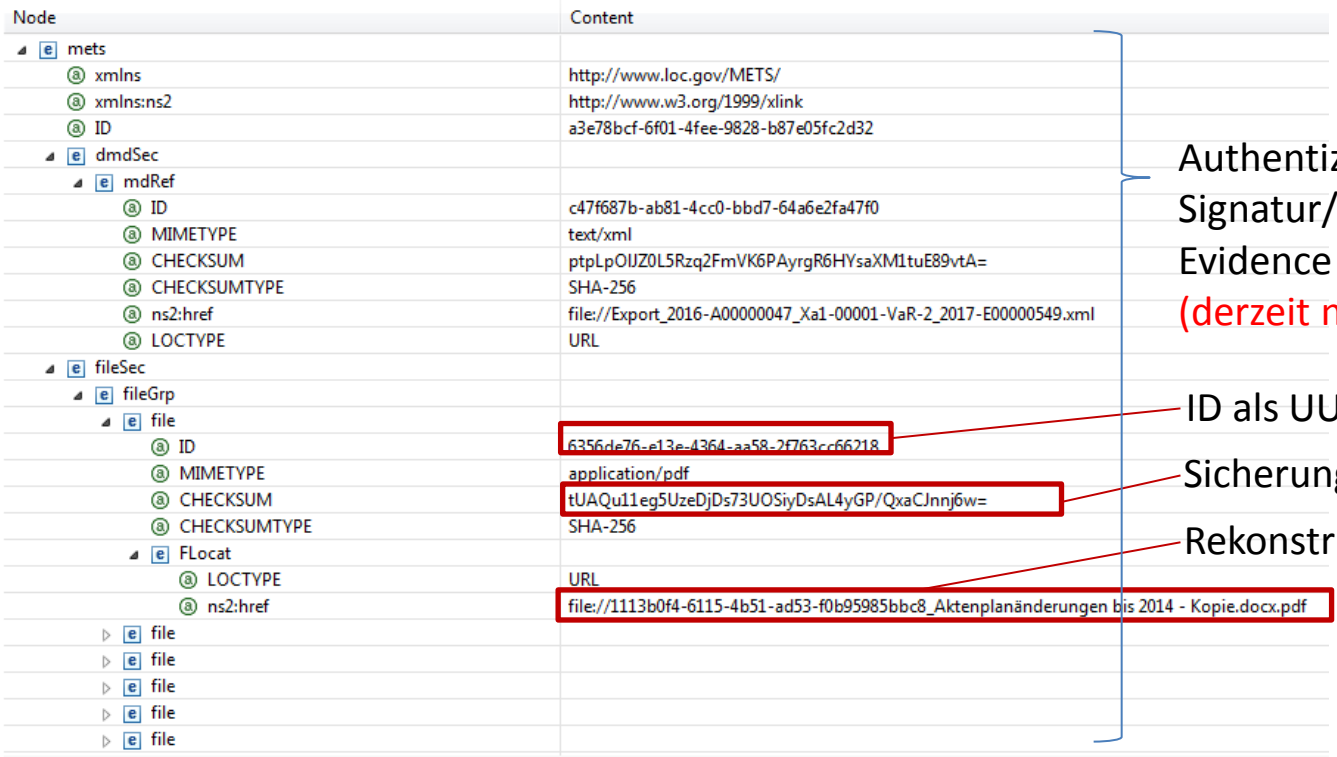
Quelle: T. Kusber, U. Korte, D. Hühnlein, M. Prechtl und B. Wild: Datenpakete zur Informations- und Beweiswerterhaltung. Ein Vergleich. DACH-Security 2017. Frechen 2017 S. 291-303

Anforderungen AIP-Formate 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

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

E-Ark SIP im Kontext XDOMEA und DZAB



Node	Content
mets	
xmlns	http://www.loc.gov/METS/
xmlns:ns2	http://www.w3.org/1999/xlink
ID	a3e78bcf-6f01-4fee-9828-b87e05fc2d32
dmdSec	
mdRef	
ID	c47f687b-ab81-4cc0-bbd7-64a6e2fa47f0
MIMETYPE	text/xml
CHECKSUM	ptpLpOIJZ0L5Rzq2FmVK6PAyrgR6HYsaXM1tuE89vtA=
CHECKSUMTYPE	SHA-256
ns2:href	file://Export_2016-A00000047_Xa1-00001-VaR-2_2017-E00000549.xml
LOCTYPE	URL
fileSec	
fileGrp	
file	
ID	6356de76-e13e-4364-aa58-2f763cc66218
MIMETYPE	application/pdf
CHECKSUM	tUAQu11eg5UzeDjDs73UOSiyDsAL4yGP/QxaCJnnj6w=
CHECKSUMTYPE	SHA-256
FLocat	
LOCTYPE	URL
ns2:href	file://1113b0f4-6115-4b51-ad53-f0b95985bbc8_Aktenplanänderungen bis 2014 - Kopie.docx.pdf
file	
file	
file	
file	
file	

Authentizität, Integrität durch Signatur/Siegel/Zeitstempel/ Evidence Records (derzeit nicht unterstützt)

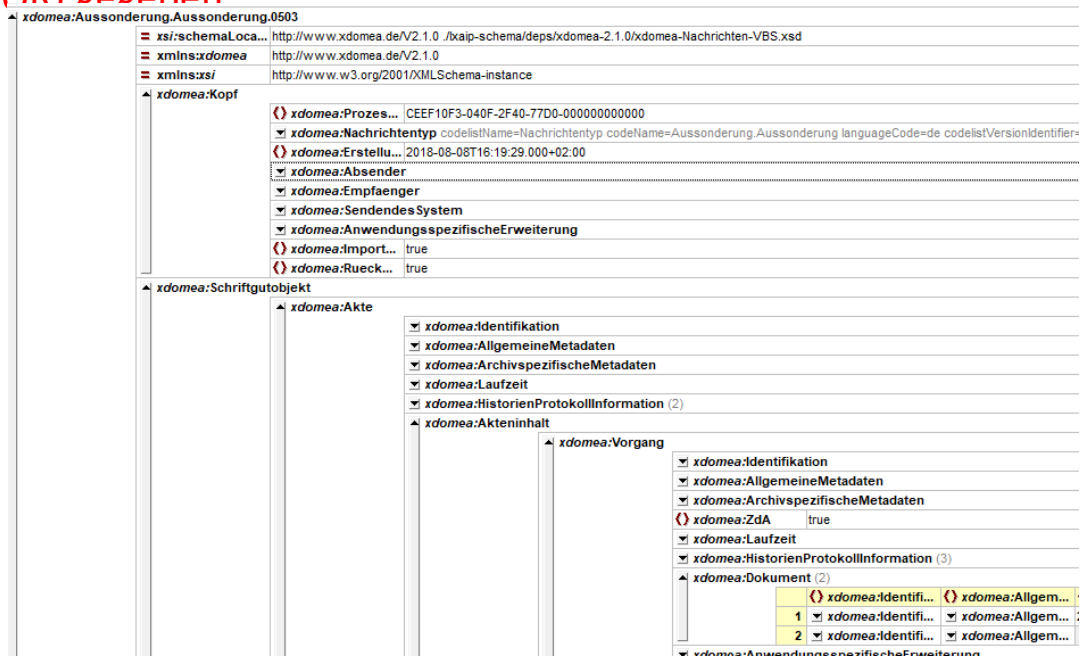
ID als UUIDv4 = AOID/COID

Sicherung der Referenz

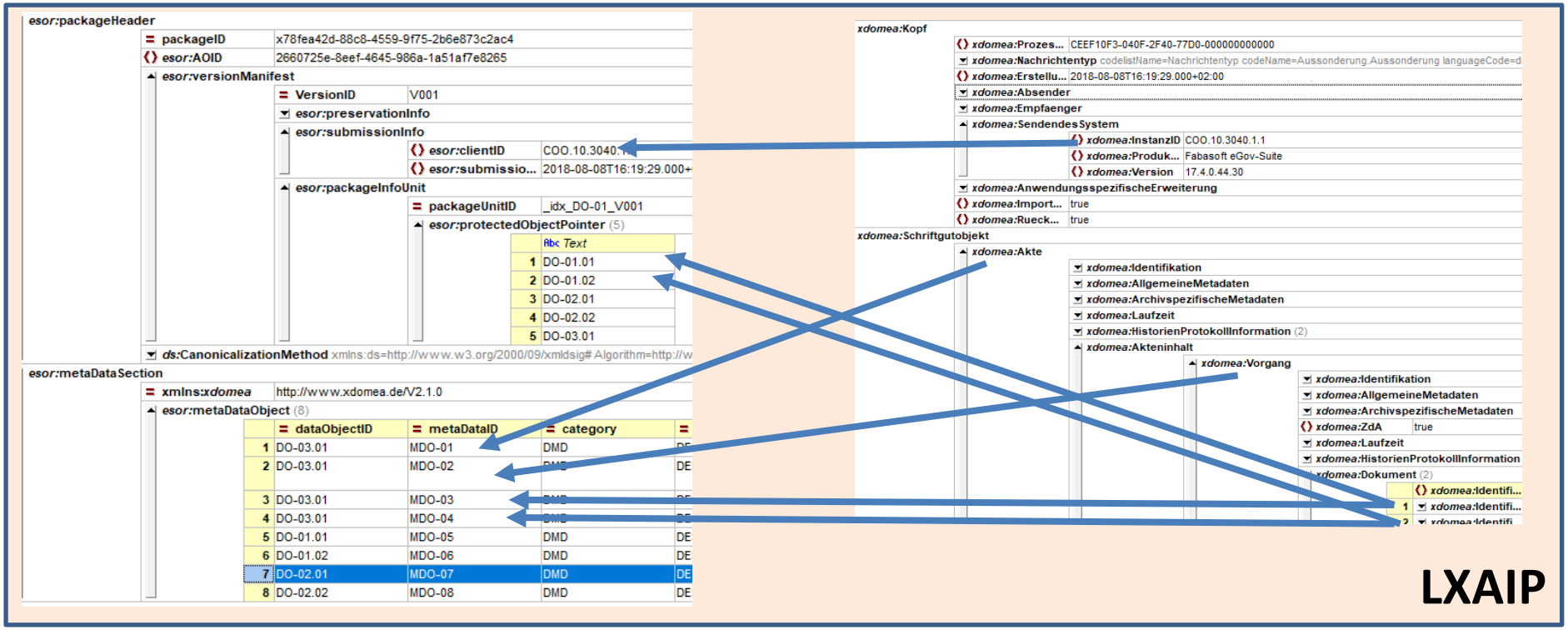
Rekonstruktion des XDOMEA

Verwendung von (L-) XAIP gem. TR-ESOR als Container (1/3)

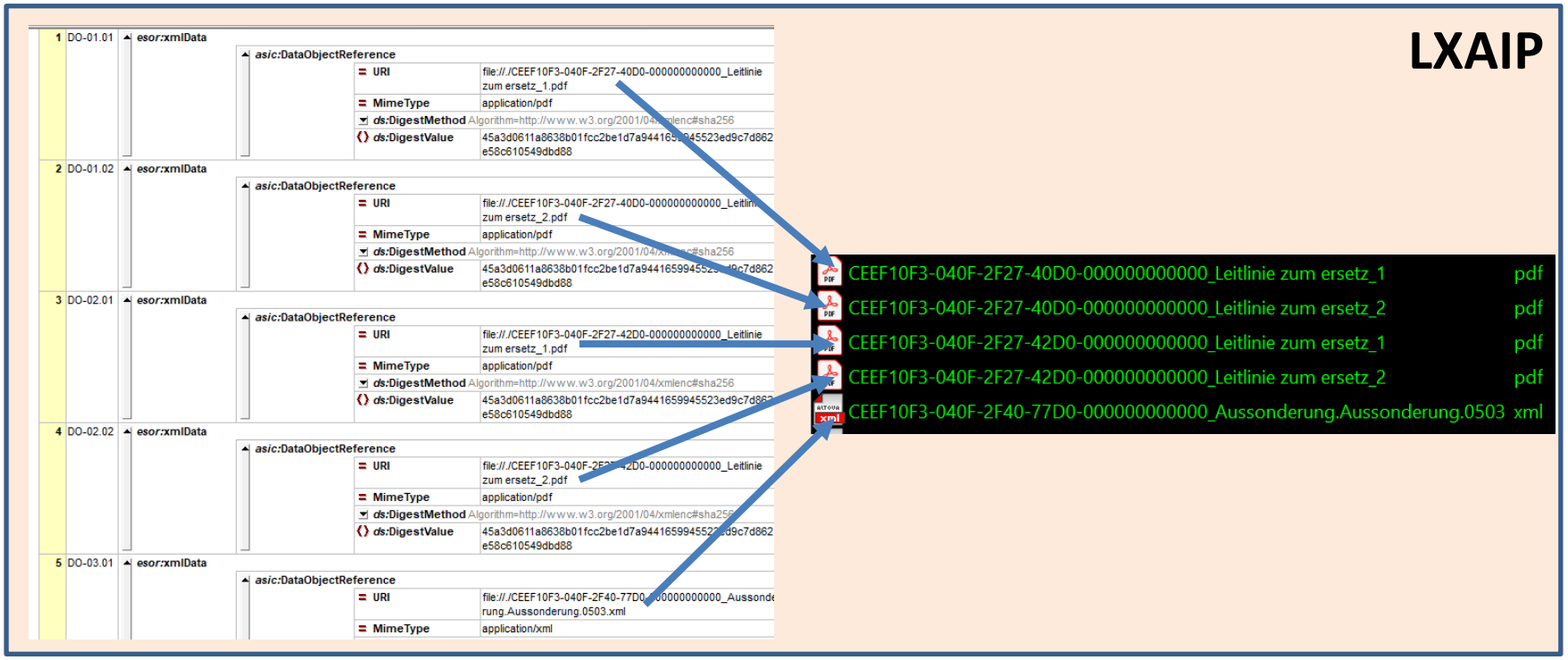
- Referenzen auf die einzelne Datenobjekte als Protected Pointer im Header
- Ablage der XDOMEA-Struktur in *metaDataSection* oder *dataObjectsSection*
  - Der wesentlichen Teile in *metaDataSection* und ganz in *dataObjectsSection*
  - Authentizität, Integrität durch Signaturen/Siegel/Zeitstempel/Evidence Records nach geltender Rechtslage (eIDAS/VDG) auf Basis internationaler Standards (ETSI, DIN, TR-ESOR) gegeben



Verwendung von (L-) XAIP gem. TR-ESOR als Container (2/3)



Verwendung von (L-) XAIP gem. TR-ESOR als Container (3/3)



Zusammenfassung und Ausblick

eARK	(L-)XAIP gem. TR-ESOR
•Derzeit keine Beweiswerterhaltung unterstützt •Anpassung im Rahmen weiterer Standardisierungsarbeiten möglich •Integration in bestehende Standards wie TR-ESOR/ETSI TS 119 512 ist mit geringem Aufwand bereits jetzt möglich	•Beweiswert- und Informationserhaltung werden auf Basis internationaler Standard unterstützt •Integration weiterer Formate wie z.B. eARK ist mit geringem Aufwand möglich

- Laufender Austausch zwischen Bundesarchiv sowie dem BSI zum DZAB
- Austausch mit eARK-Projekt und BSI zur Beweiswerterhaltung in eARK, um Synergien zu nutzen, wäre möglich