

Stefan Müller-Mielitz:

- Aktuelles aus der IHE AG ValueSet
- IHE Kernelemente
- Aufgabe eAktenstruktur
- Aufgabe Systematisierung der ePA-Konzepte
- Lösungsansatz

Olaf Feller:

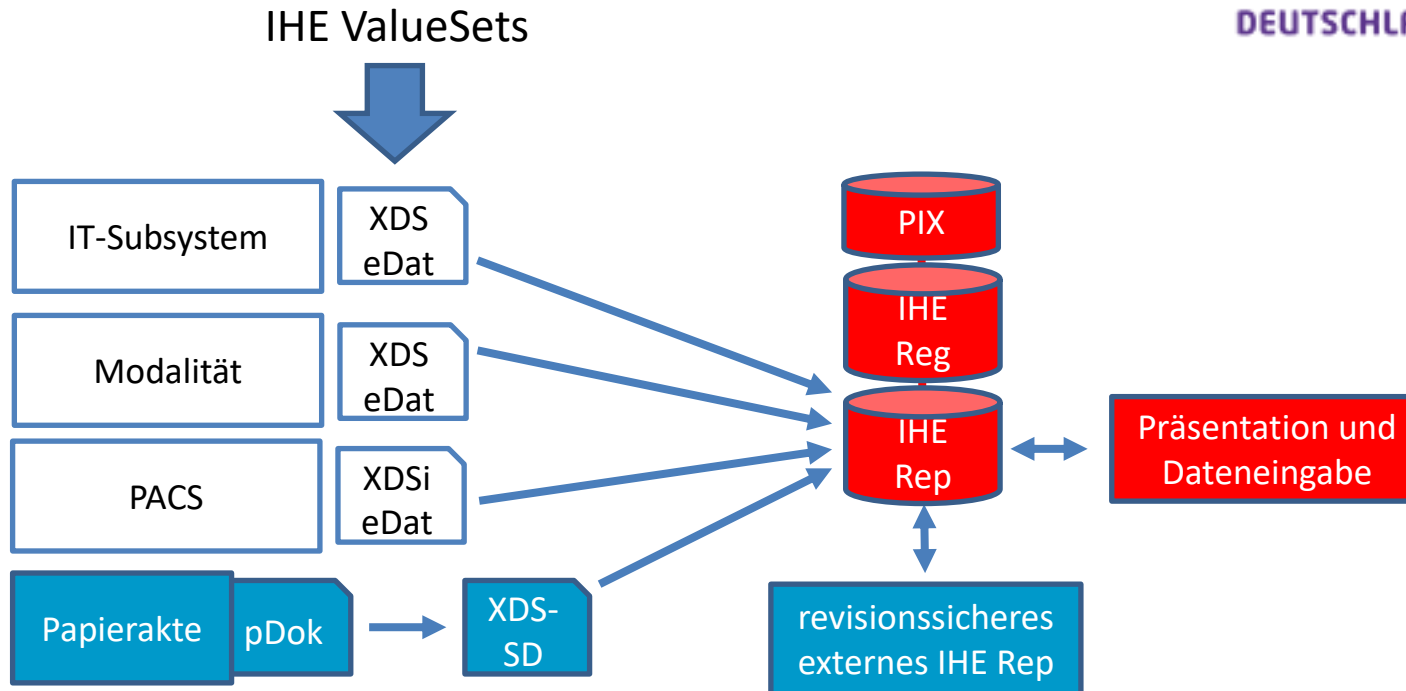
- Aufgabe Verkehrsfähigkeit und Revisonssicherheit
- Lösungsansatz

Bisherige Ergebnisse:

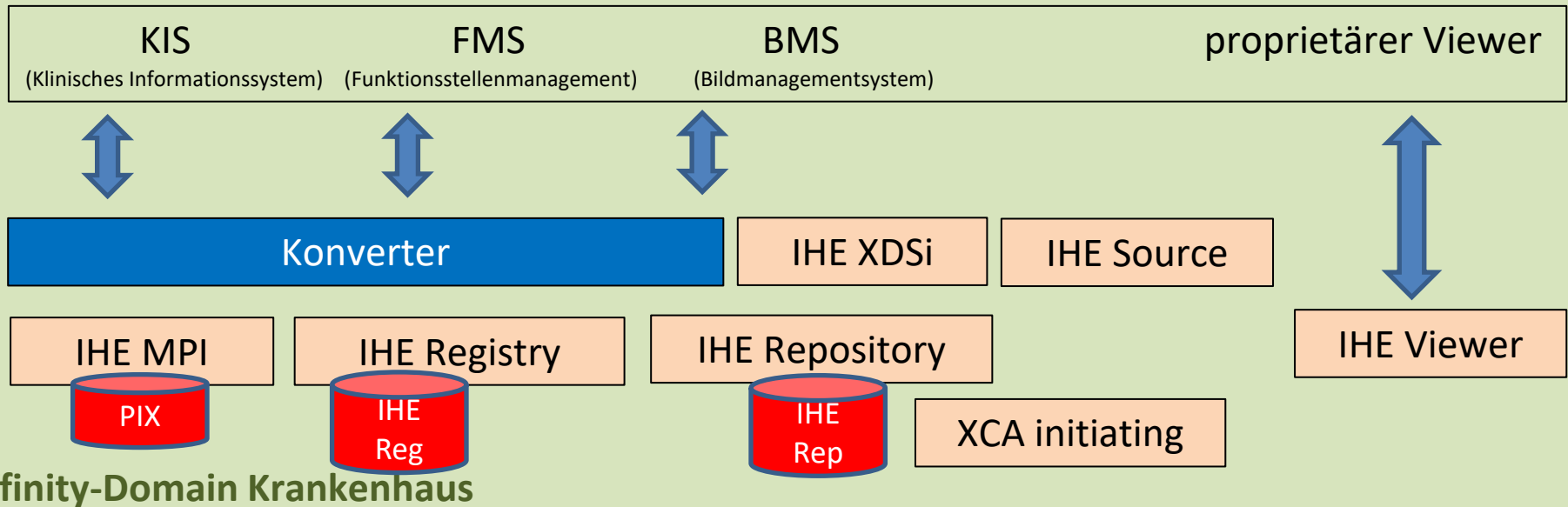
<http://www.ihe-d.de/projekte/xds-value-sets-fuer-deutschland/>

Zur Kommentierung standen:

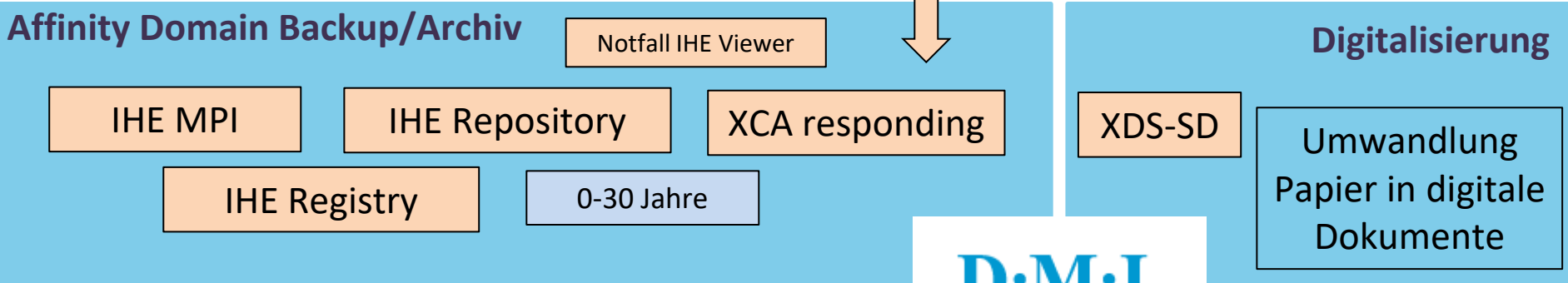
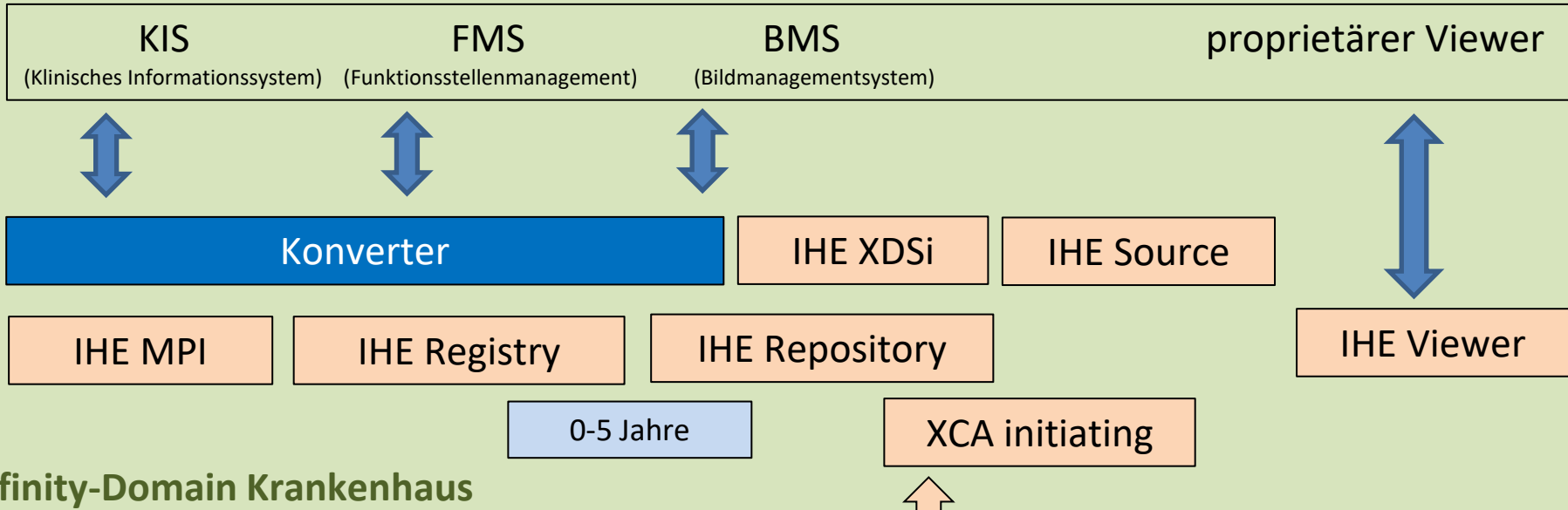
- ✓ Einrichtungsart (DocumentEntry.healthcareFacilityTypeCode)
- ✓ Fachrichtung (DocumentEntry.practiceSettingCode)
- ✓ Dokumentenklasse (DocumentEntry.classCode)
- ✓ Dokumententyp (DocumentEntry.typeCode)
- ✓ Dokumentenformat (DocumentEntry.formatCode)
- ✓ Dokumentensprache (DocumentEntry.languageCode)
- ✓ Ordnerklassifizierung (Folder.codeList)



Anforderungen an IHE-Archive



IHE konforme Langzeitarchivierung



Revisions sichere Langzeitarchivierung und Rohdatenspeicherung



Revisionsdienst

Langzeitarchivierung

Aktuelle Arbeiten/Diskussionpunkte der IHE AG „ValueSets“

DocumentEntry.AuthorRole

Das AuthorRole Element beschreibt die Rolle, die der inhaltliche Autor des Dokuments zum Zeitpunkt der Dokumentation innehatte

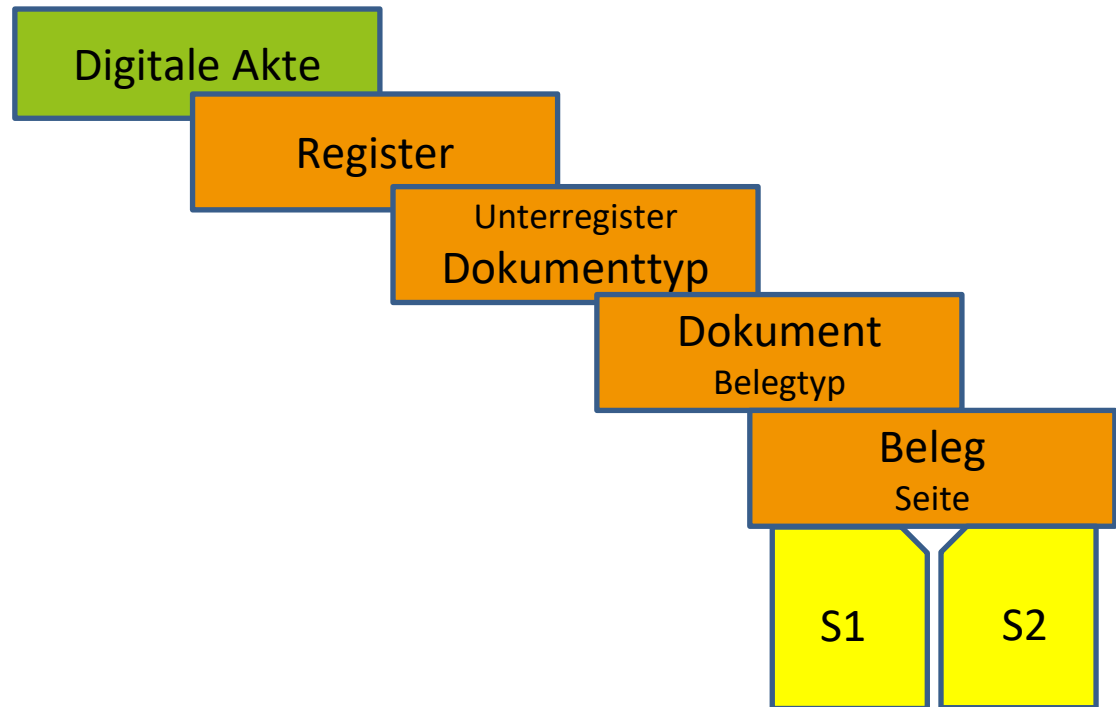
DocumentEntry.authorSpeciality

DocumentEntry.confidentialityCode

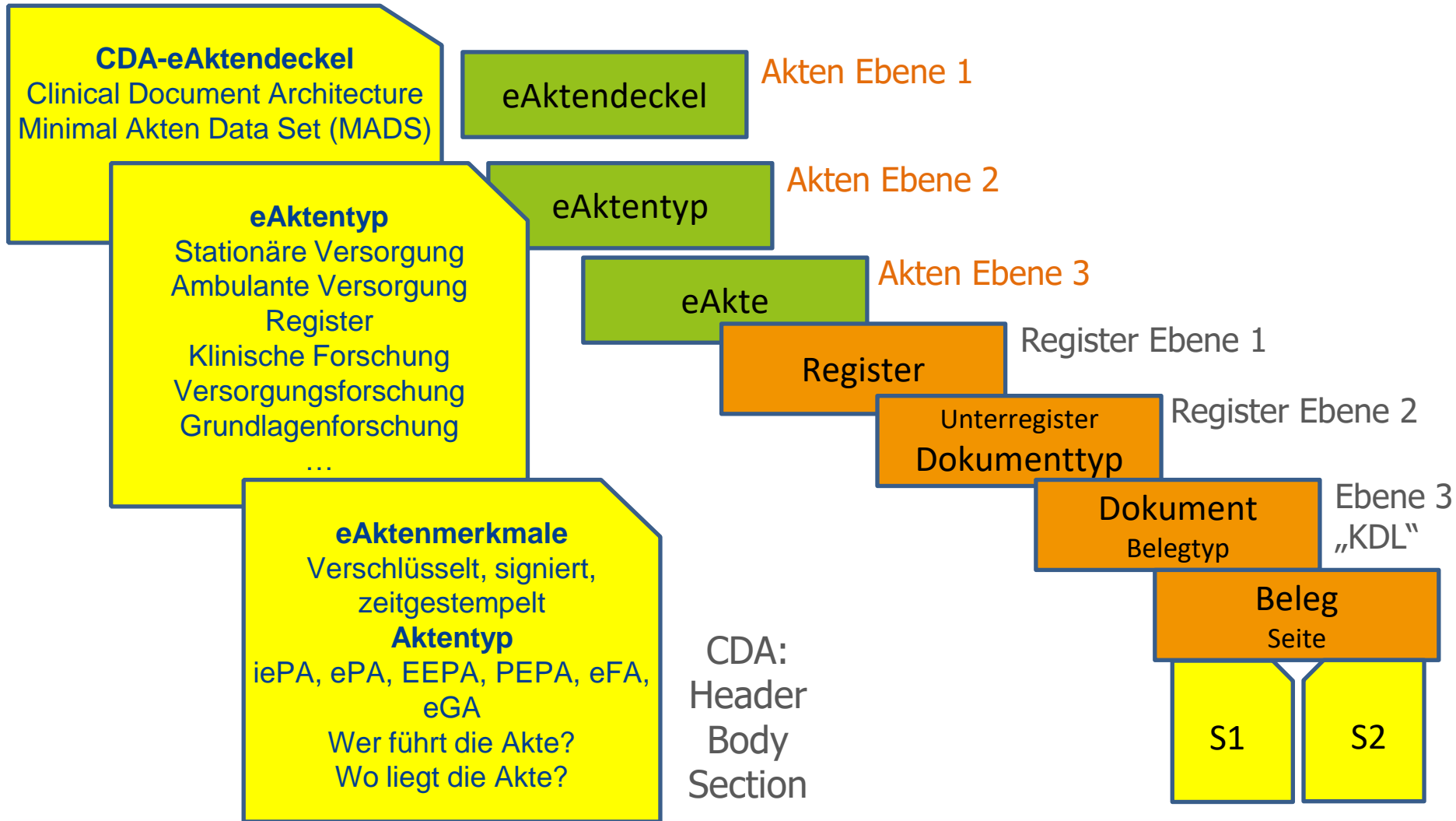
DocumentEntry.eventCodeList

SubmissionSet.contentTypeCode

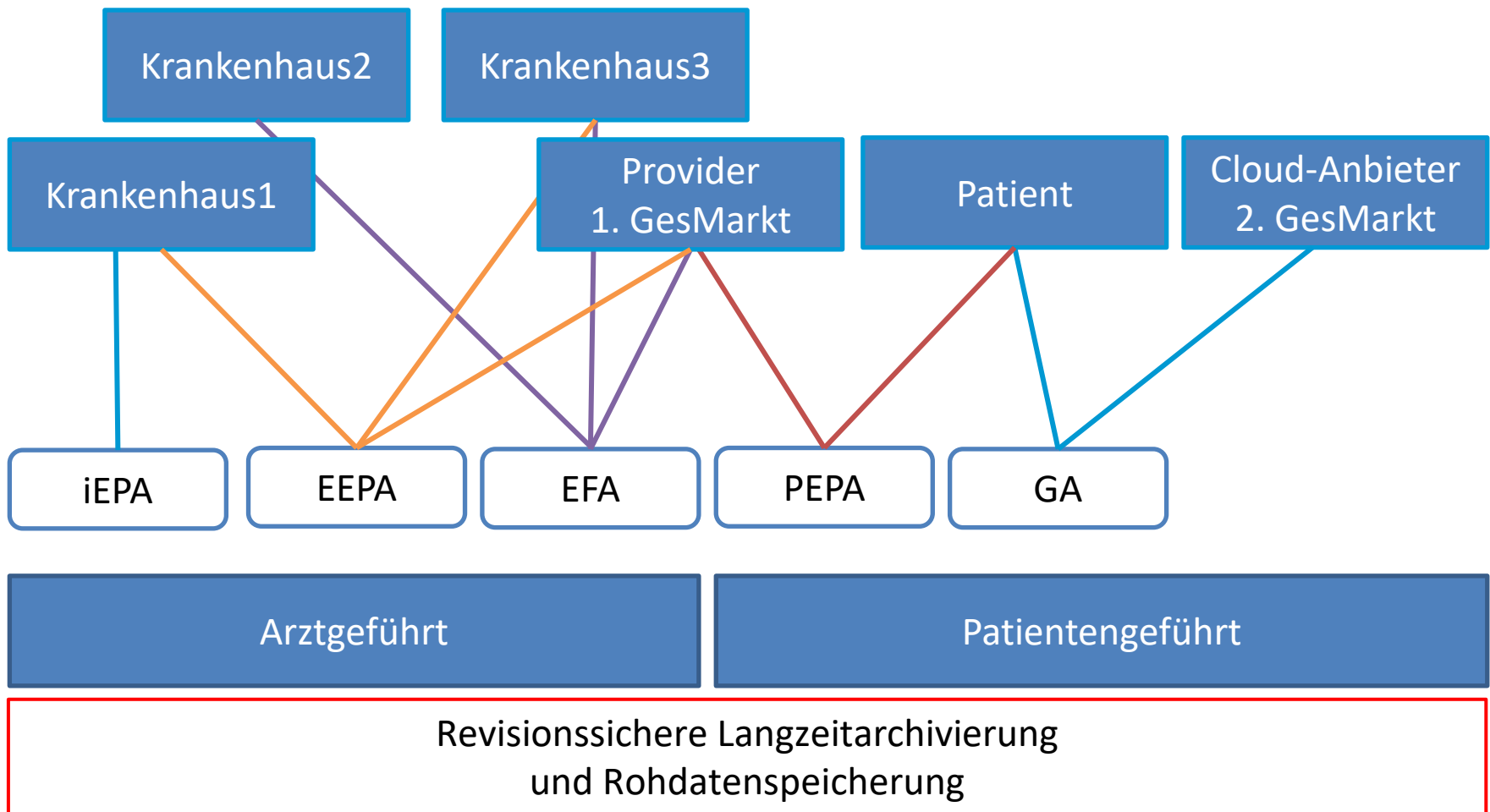
IHE Value Sets definieren Metainformationen von Dokumenten – keine Akten



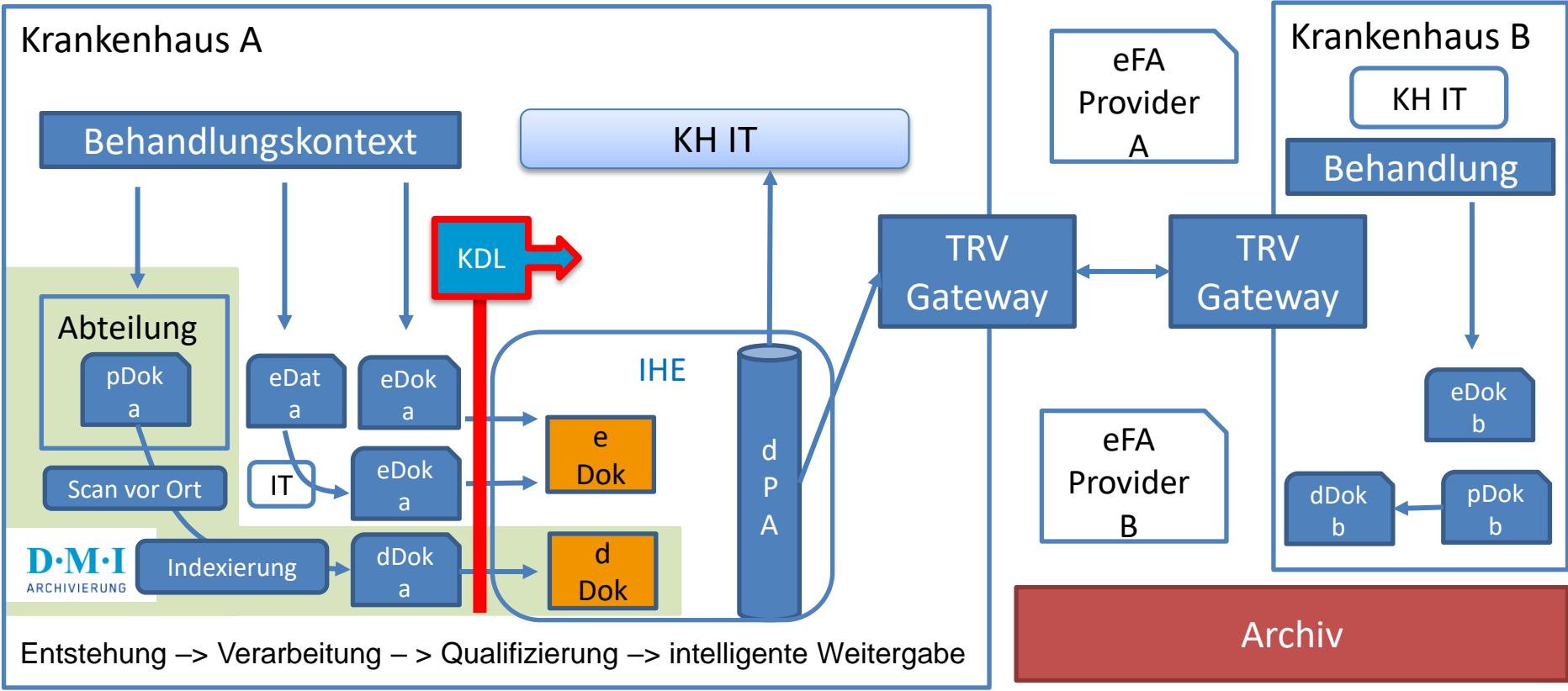
Aufgabe „eAktenstruktur“ – Lösungsweg über eAktendeckel



Aufgabe: Systematisierung der ePA-Konzepte



Lösungen für FALKO.NRW: fallorientierte Kommunikation - Verlegung



EUROPÄISCHE UNION
Investition in unsere Zukunft
Europäischer Fonds
für regionale Entwicklung

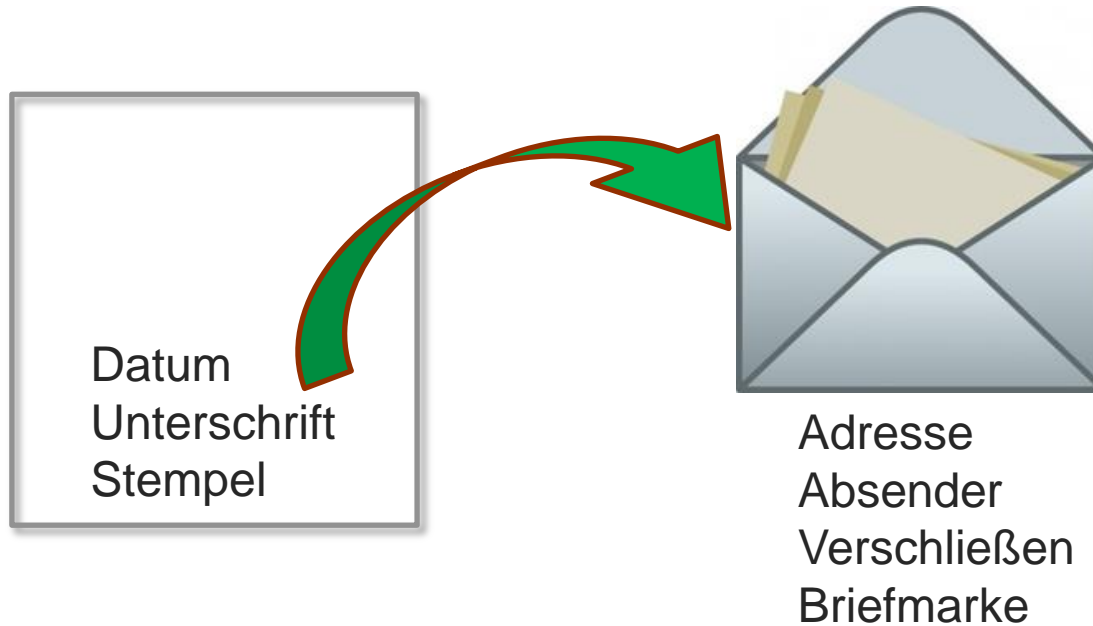


EFRE.NRW
Investitionen in Wachstum
und Beschäftigung

Ministerium für Wirtschaft, Energie,
Industrie, Mittelstand und Handwerk
des Landes Nordrhein-Westfalen



Analoge verkehrsfähige Information



Patienten-
akte

Krankenhaus



Patienten-
akte

Arzt

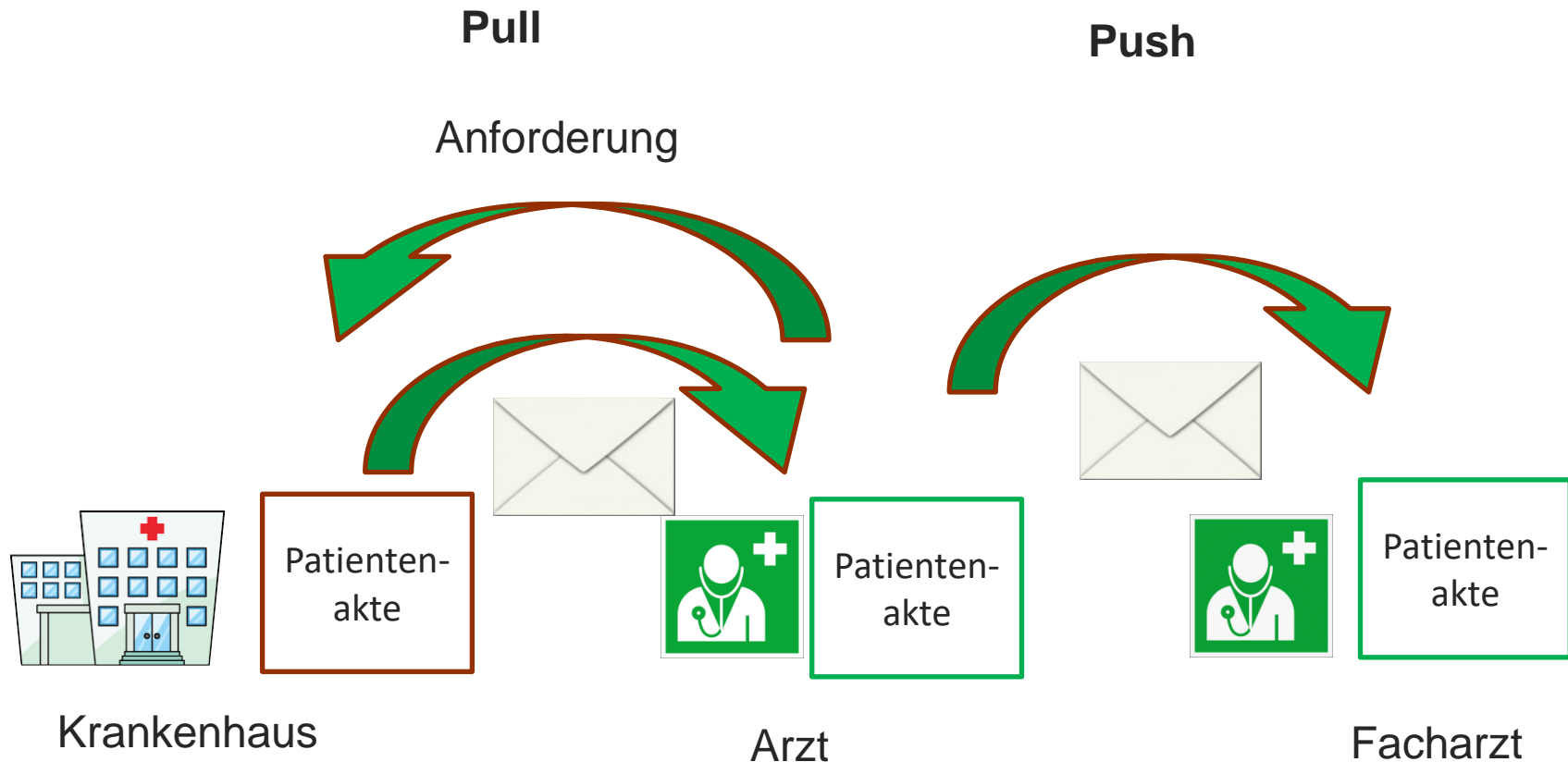


Patienten-
akte

Facharzt

Analoge Übertragung

Sichere Übertragung - Postdienst



Information elektronisch

Datei ... eAkte



Patienten-
akte

Krankenhaus



Patienten-
akte

Arzt



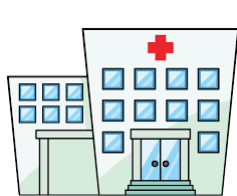
Patienten-
akte

Facharzt

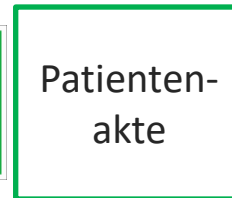
Verkehrsfähige Information elektronisch



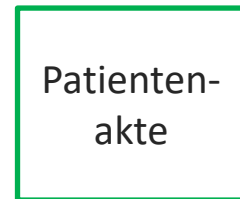
Standardisiertes Format:
 z.B. IHE- kompatible Datenstrukturen



Krankenhaus

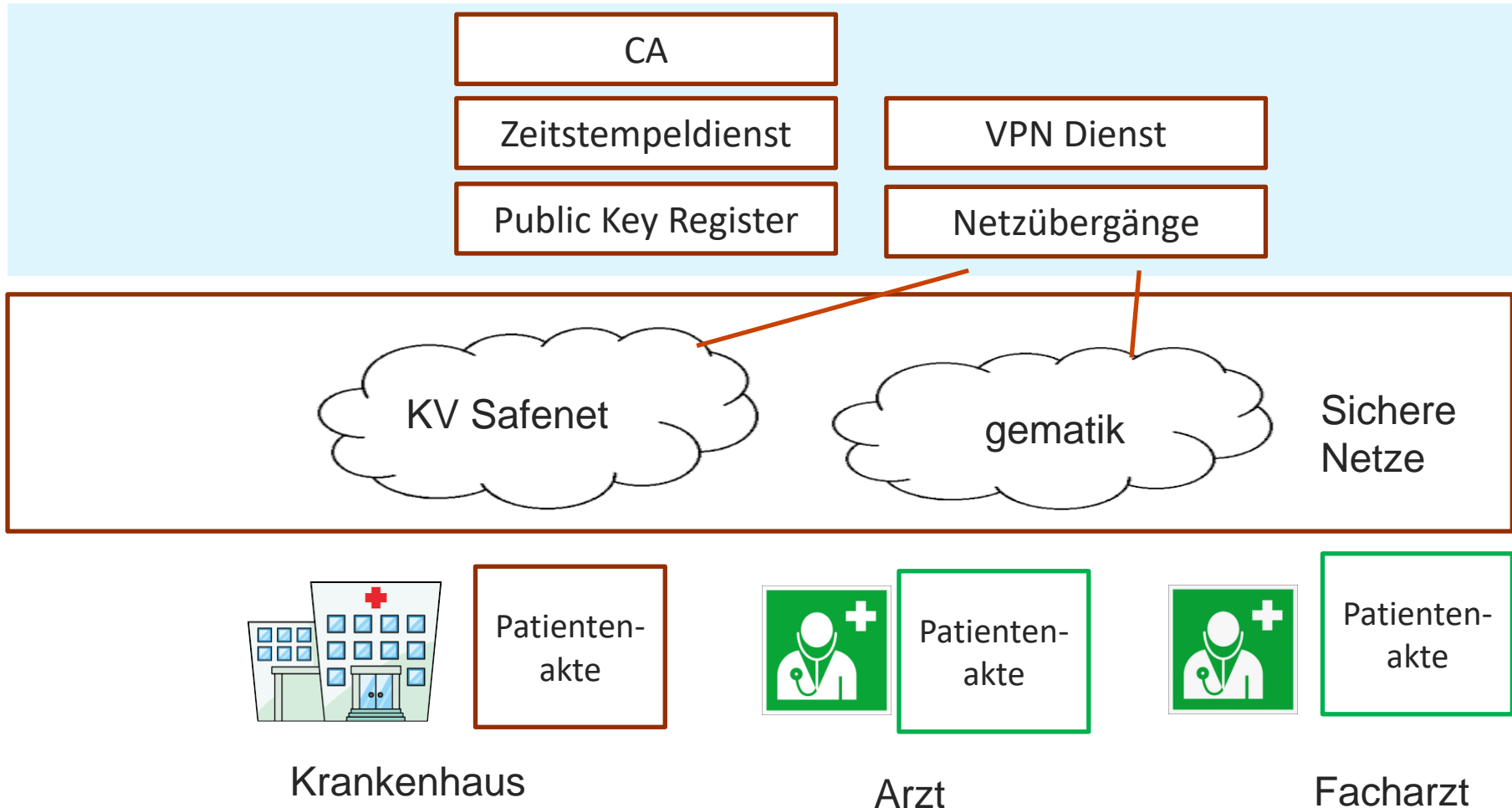


Arzt



Facharzt

Logistik elektronisch





Gibt es das schon?

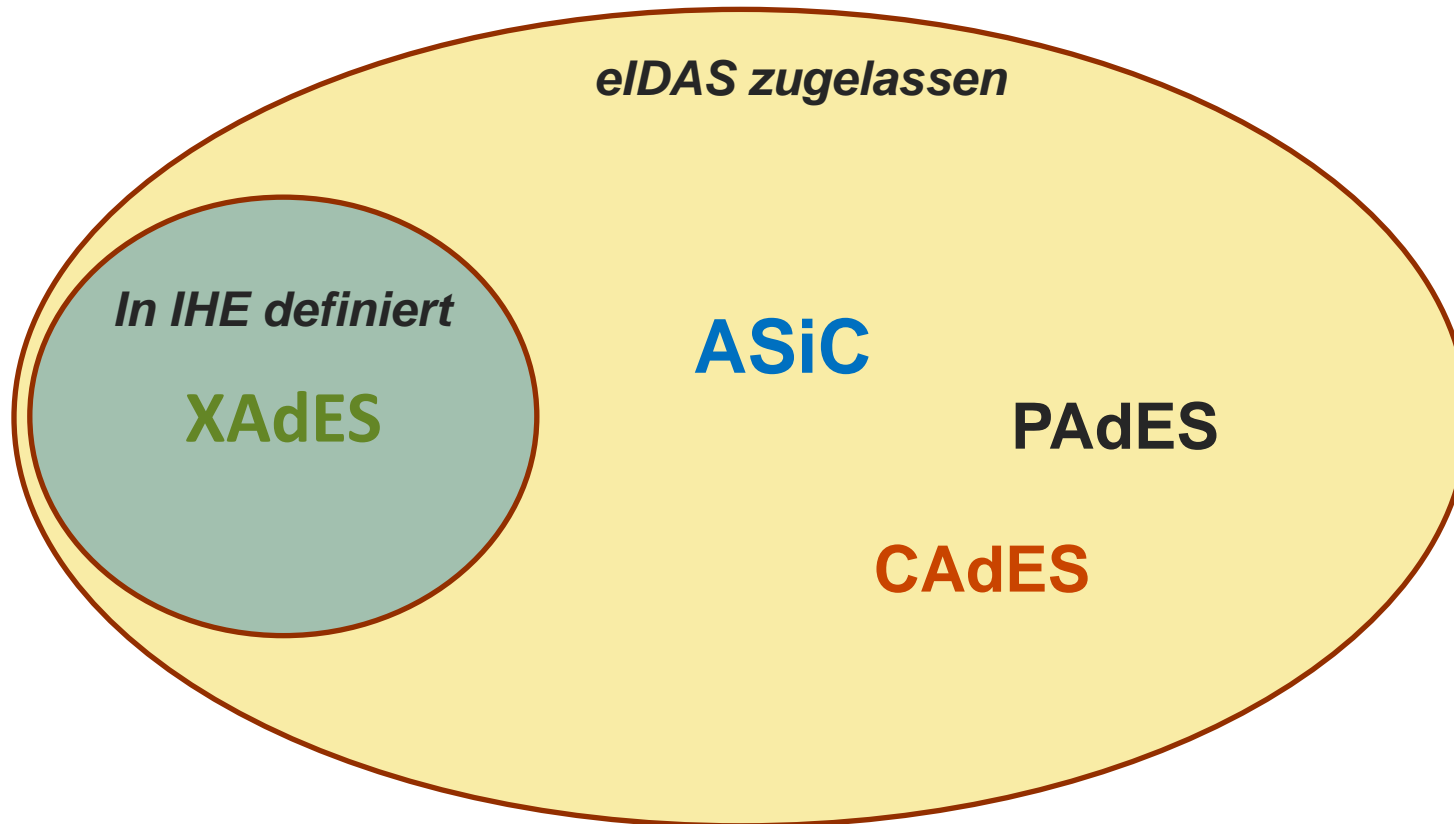
IHE DSG – Document Digital Signature (Rev. 2.2 – 2016-09-09)

- Ist ein „Document Content Profile“ basierend auf **XAdES**
- Eingesetzt vor allem in Document Sharing Infrastrukturen (im Besonderen XDS, XDR, XDM, XCA)
- Format der Signaturen ist XAdES (XML Advanced Electronic Signatures)
 - XML basierte elektronische Signatur, basierend auf W3C Empfehlung und konform zur EU eIDAS Verordnung
 - Ausprägungen für Nutzung von qualifizierten Zeitstempel „XAdES-T“ und Langzeitspeicherung „XAdES-LTA“

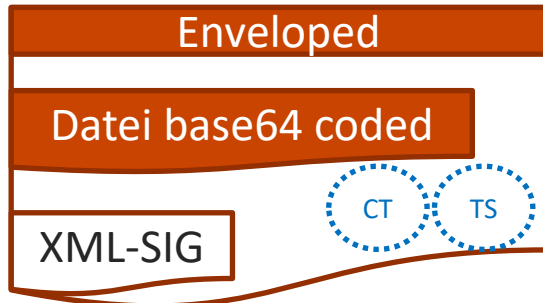
eIDAS - zugelassene elektronische Signaturen-Formate

- CAdES – CMS basierte elektronische Signatur
(z.B. S/Mime)
- **XAdES** – XML basierte elektronische Signatur
(Deutschland: TR-ESOR kann mittels partiellen Hashbäumen auf
XAdES abgebildet werden, so das eine eIDAS konforme Realisierung
erfolgt.)
- PAdES – PDF basierte elektronische Signatur
- **ASiC** – ZIP basierter Signatur Container
(EU ETSI-Norm EN 319 162-1, gültig ab 01.01.2017. Neben dem reinen
Signaturformat kann ASiC auch als standardisierter Datencontainer zur
beweiswerterhaltenden Langzeitspeicherung sowie zum
Datenaustausch verwendet werden.)

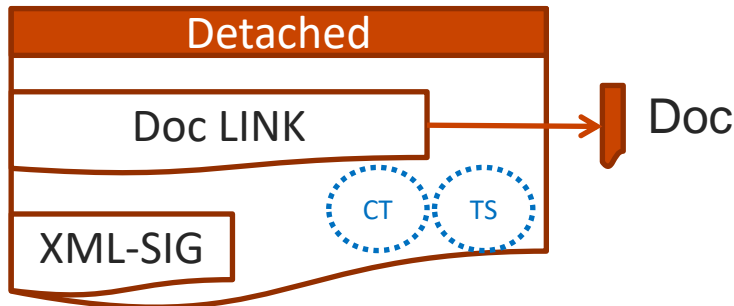
IHE DSG und eIDAS konform ist zurzeit nur XAdES



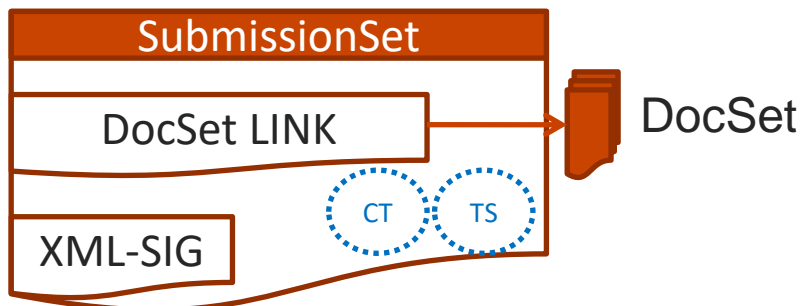
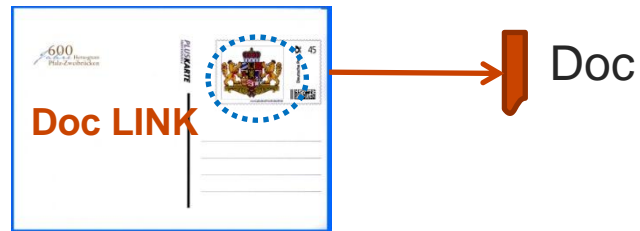
IHE DSG Profil Entsprechungen im Postverkehr



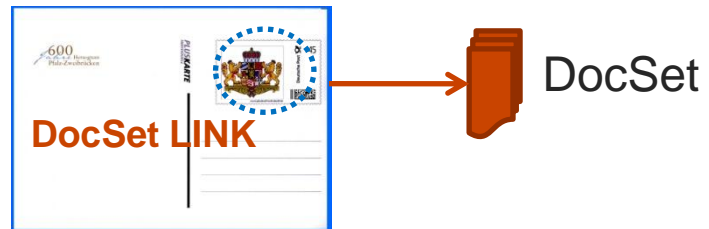
Postkarte mit Datei Inhalt



Postkarte mit Link auf Datei

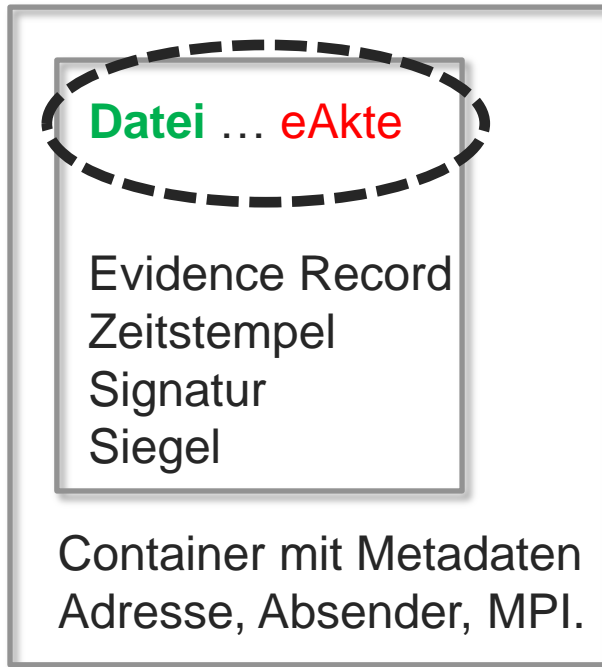


Postkarte mit Link auf Datei-Stapel

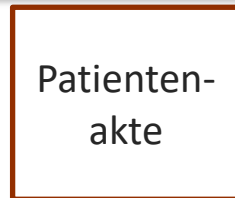


- **DSG nutzt XAdES und ist damit eIDAS konform**
- Eine Akte ist nur in 1 von 3 DSG-Ausprägungen ansatzweise abbildbar (SubmissionSet, nur Liste von Dokumenten, keine Strukturen), ansonsten nur Einzeldokumente
- **Keine verkehrsfähige Akte (Dokumentenstruktur) im gegenwärtigen Profil**
- **XAdES nutzt Archivzeitstempel im 1:1-Verhältnis an einer Einzelsignatur, d.h. enormer Aufwand bei Signatur- und Zeitstempelerneuerung**
- **Alternativ:** eIDAS Signaturcontainer ASiC - Nutzung von Hashbäumen zur Signaturerneuerung. Beweisdokument (Evidence Record) wird im Signaturcontainer abgelegt. Erfüllt EU ETSI-Norm EN 319 162-1 (2016-04) und DE TR-ESOR.

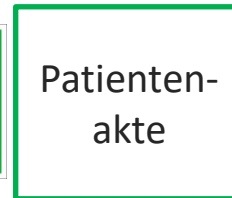
DSG ist derzeit nur auf Dokumenten-Ebene verkehrsfähig



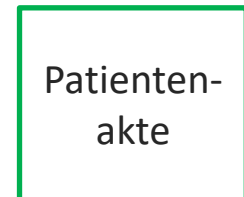
Standardisiertes Format:
 z.B. IHE- kompatible Datenstrukturen



Krankenhaus

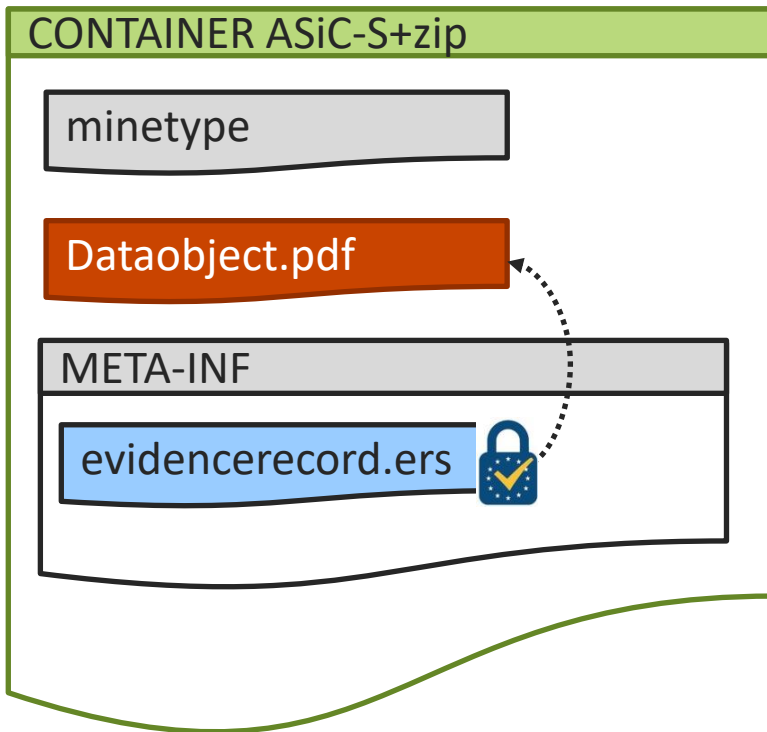


Arzt



Facharzt

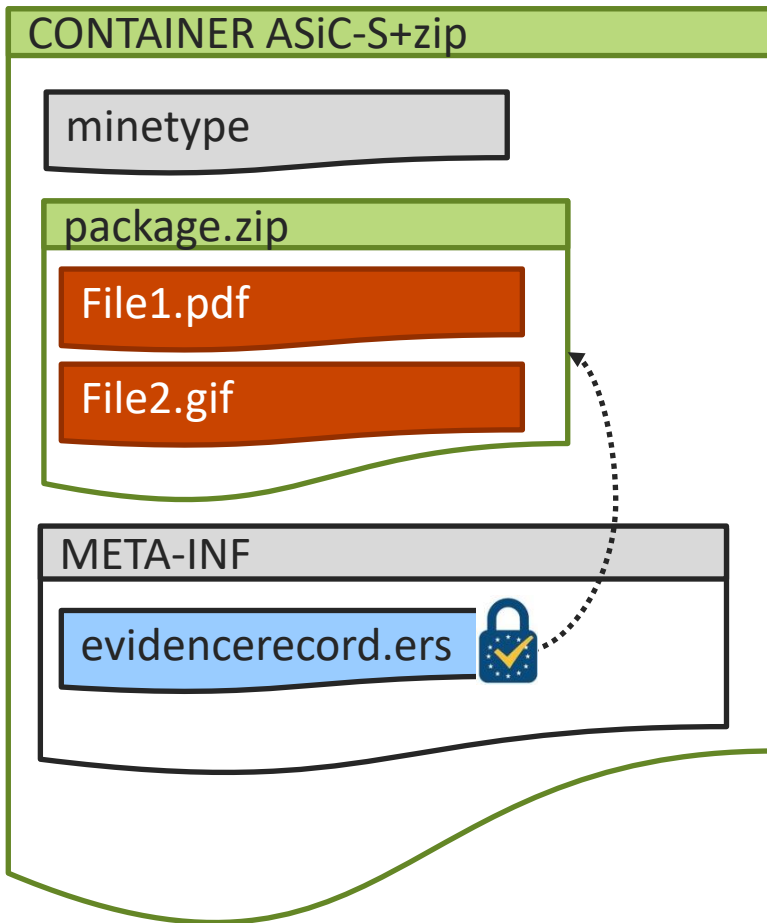
ASiC-S Beispiel 1 – einfache Datei versiegelt



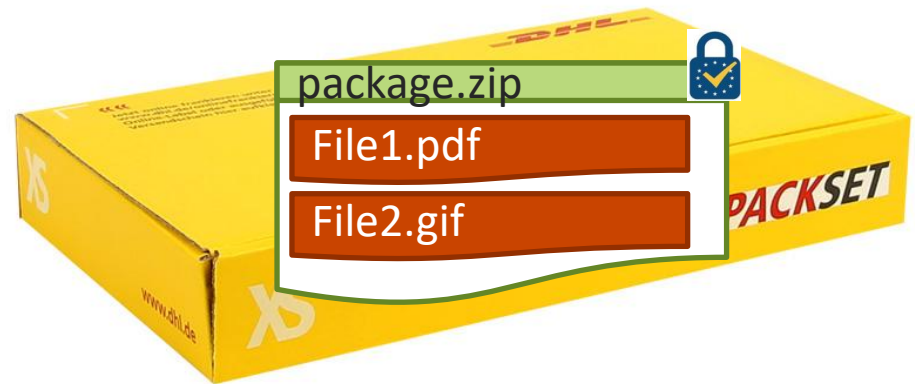
Päckchen mit Datei versiegelt



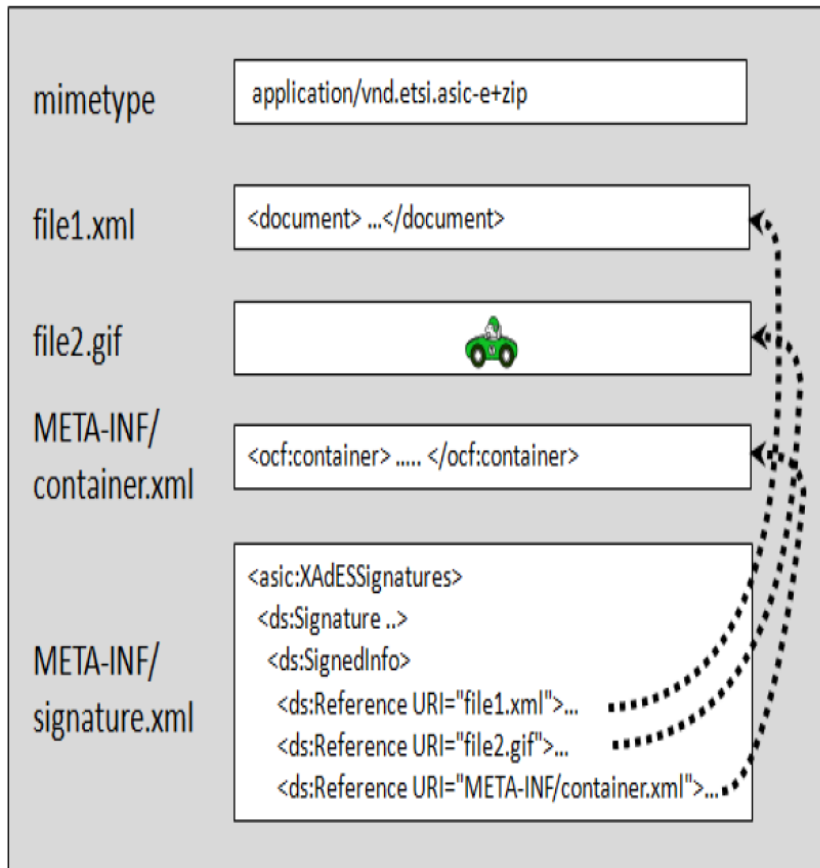
ASiC-S Beispiel 2 – Dateistapel als Ganzes versiegelt



Päckchen mit Dateistapel als Ganzes versiegelt



ASiC-E Beispiel 5 – Akte mit Metadaten als Ganzes versiegelt

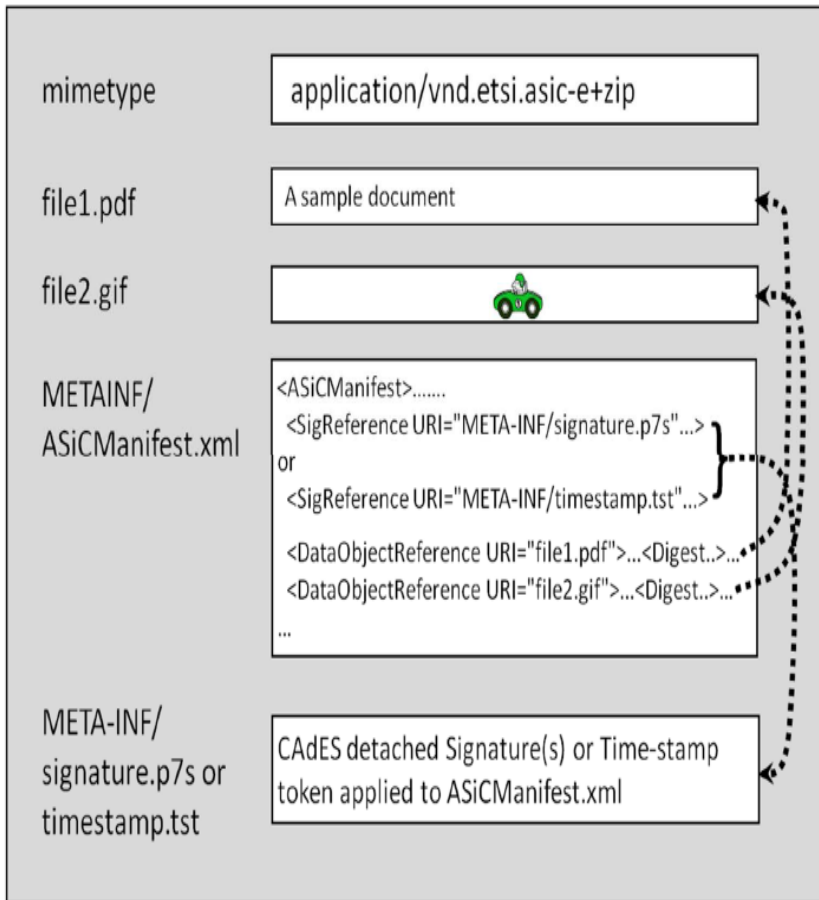


Paket mit Akte und Lieferschein als Ganzes versiegelt



Figure 5: ASiC-E with XAdES and direct ds:reference usage

ASiC-E Beispiel 6 – Akte mit versiegelten Metadaten

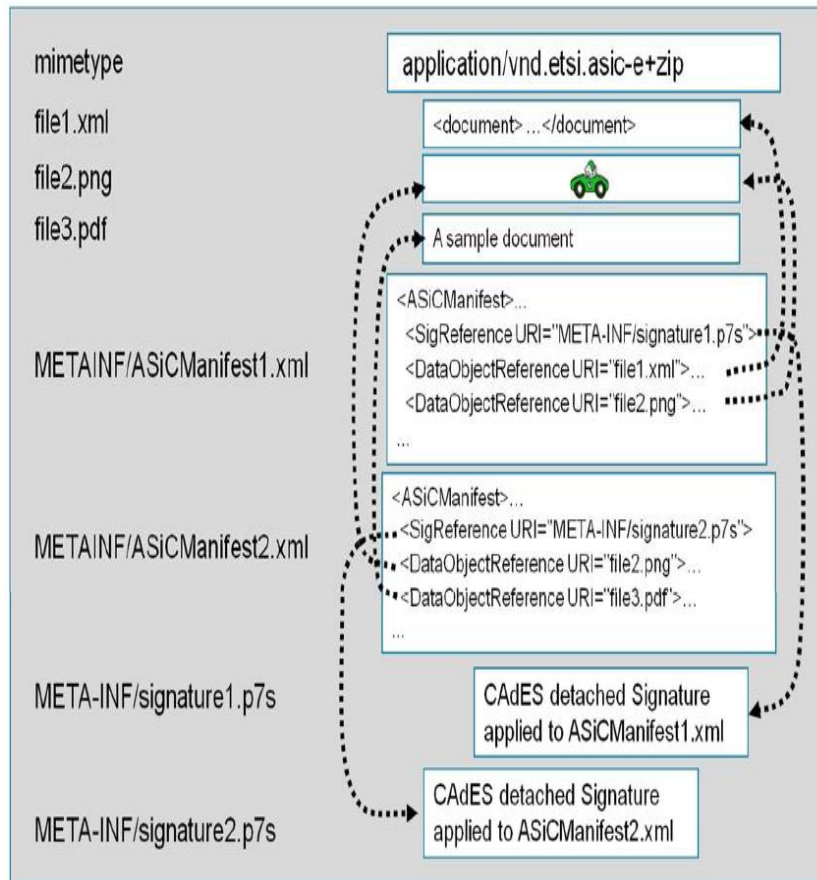


Paket mit Akte und versiegeltem Lieferschein



Figure 6: ASiC-E with CADES signature or time-stamp token

ASiC-E Beispiel 7 – Akte mit 2 Kapiteln, jedes Kapitel einzeln versiegelt



Paket mit Akte und 2 versiegelten Lieferscheinen



Figure 7: ASiC-E with CAES containing different signatures

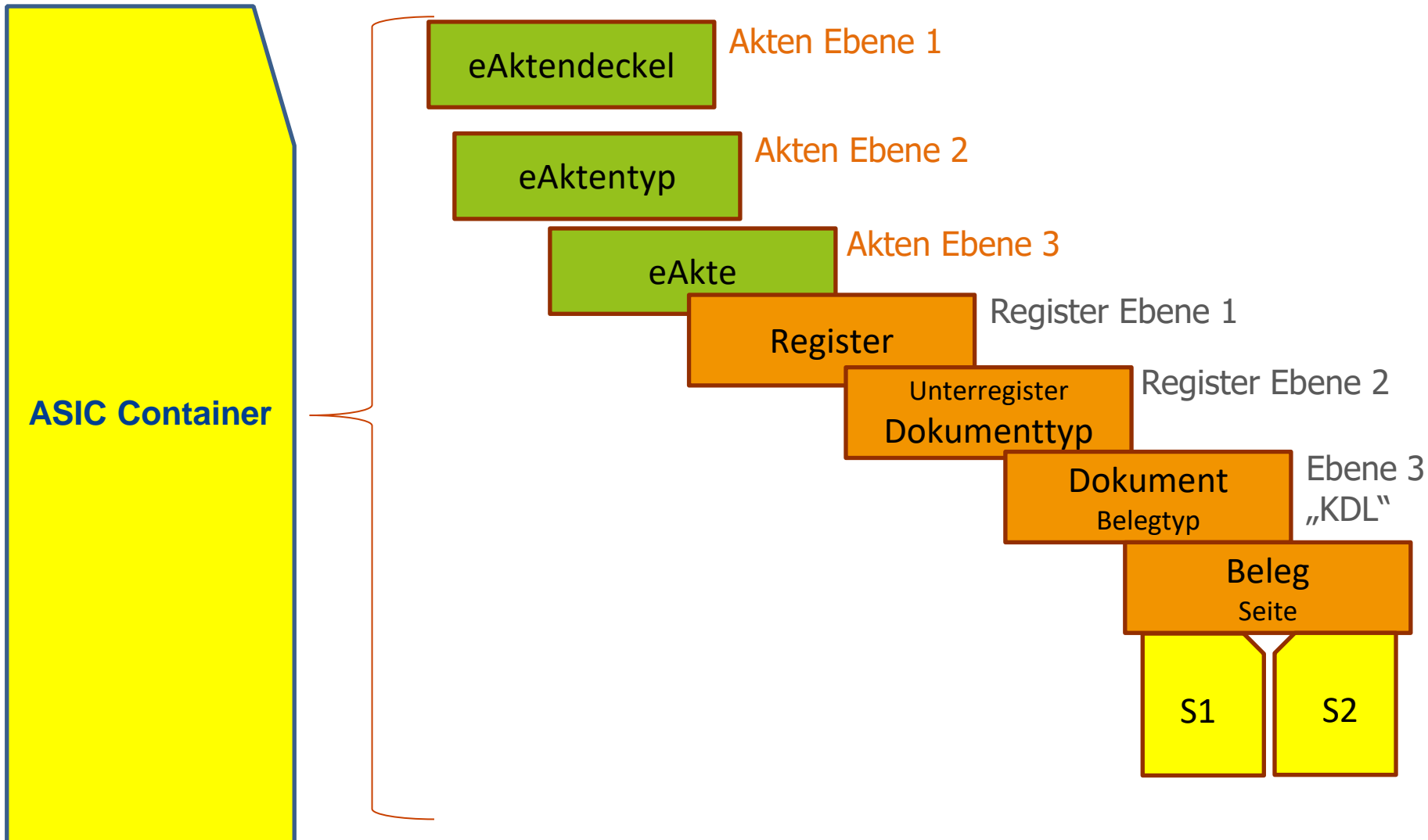


ASiC-E Container können verschachtelt werden !!!

Was ermöglicht die ASiC-E Verschachtelung im IHE Kontext?

- **Virtuelles Dateisystem** mit beliebiger Tiefe in den Ordner-Strukturen
- **Aktenplan** Abbildung ist damit gesichert
- Übertragung einer **Fallakte** in einem ASiC-E Container
- Übertragung einer **Lebensakte** in einem ASiC-E Container
- Selbstverständlich auch Übertragung von **Einzelbelegen**
- ASiC-E ist also eine **All-in-One Lösung** für den Dokumenten- und eAkten-Transfer

eIDAS ASIC Transport der „eAktenstruktur“



Zusammenfassung

- Übertragung von Dokumenten eAkten ist mit ASiC garantiert
- **Verschlüsselung** ist nicht Bestandteil von ASiC
- **Zugriffsschutz** ist nicht Bestandteil von ASiC
- Für den Transport über ungesicherte Netze ist auf jeden Fall ein weiterer umhüllender geschützter Container erforderlich, der die Document Sharing X-Protokolle (XDS, XDM, XDR, XCA) nutzt.
- Alternativ kann ein weiteres generisches Protokoll für gesicherten Transport definiert werden.



Stefan Müller-Mielitz
DMI Angewandte Forschung

stefan.mueller-mielitz@dmi.de

Olaf Feller
Geschäftsführer timeproof

olaf.feller@timeproof.de



Jürgen Bosk
Geschäftsführer CCESigG

info@ccesigg.de

Jürgen Weidner
**Geschäftsführer accellonet
consulting**

juergen.weidner@accellonet.com

