SIDKiG
Arbeitskreis
„Sichere Identifikation, Datenübertragung und Kommunikation im Gesundheitswesen“
CCESigG
Competence Center für die Elektronische Signatur im Gesundheitswesen e.V.

timeproof secure transactions and documents

accellonet wir finden eine Lösung

CCESigG Arbeitskreise **SIDKiG** (**S**ichere **I**dentifikation, **D**atenübertragung und **K**ommunikation **i**m **G**esundheitswesen)

Einsatz digitaler Signaturverfahren in IHE-konformen Kommunikations- und Archivierungsumgebungen.

24.04.2017 Dr. Jürgen Weidner, accellonet

Olaf Feller, timeproof

SIDKiG
Arbeitskreis „Sichere Identifikation, Datenübertragung und Kommunikation im Gesundheitswesen“
CCESiGG
Competence Center für die Elektronische Signatur im Gesundheitswesen e.V.

timeproof secure transactions and documents

accellonet wir finden eine Lösung

Aufgabenstellung des Arbeitskreises

Erarbeitung praktikabler Empfehlungen für die sichere Intersektorale Kommunikation im Gesundheitswesen:

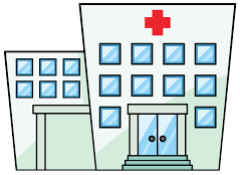
- über vom Gesetzgeber zugelassene Infrastrukturen
- unter Nutzung standardisierter Übertragungstechnologien
- mit geeigneten Methoden (Evidence Record, Zeitstempel, Signatur, Siegel) sichergestellten Erhaltung der Verkehrsfähigkeit (Authentizität, Integrität).

Der Arbeitskreis hat von IHE Deutschland den Prüfauftrag erhalten, das IHE Profil DSG auf aktuellen Stand der Technik und insbesondere eIDAS Kompatibilität zu prüfen.

Intersektorale Kommunikation analog

- Ausgetauscht werden Informationen aus den jeweiligen (unterschiedlichen) Patientenakten
- Befunde, Überweisungen, Arztbriefe, etc.
- Push- Übertragung ohne Aufforderung
- Pull- die Informationen werden angefragt

- Die Information muss für den Austausch ***verkehrsfähig*** gemacht werden



Patienten-akte

Krankenhaus

Patienten-akte

Arzt

Patienten-akte

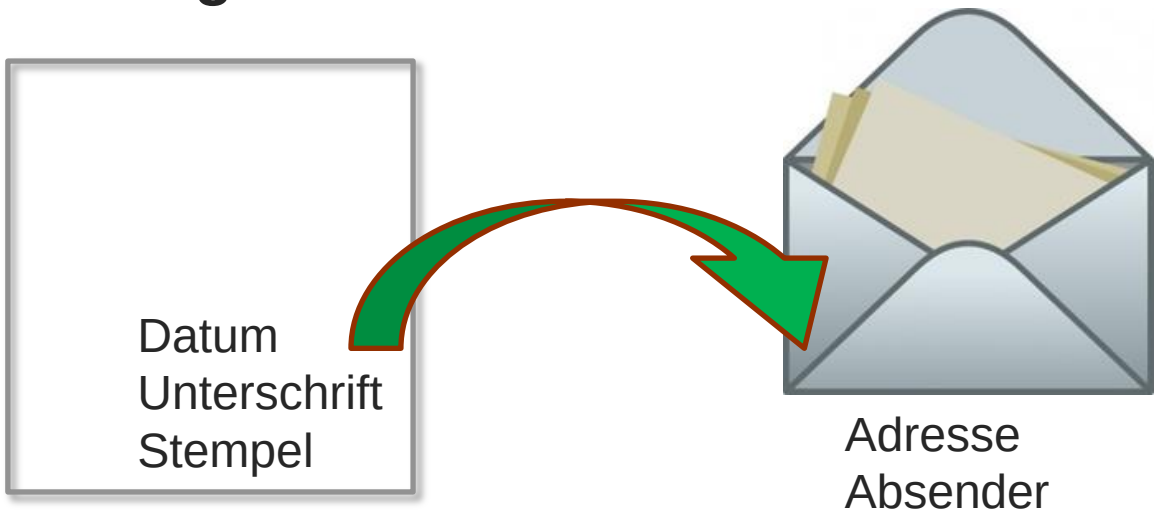
Facharzt

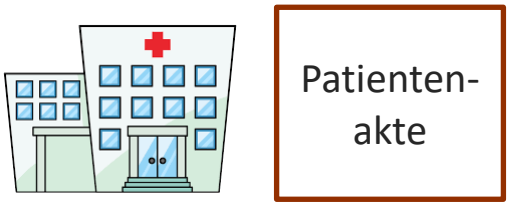
SIDKiG
Arbeitskreis „Sichere Identifikation, Datenübertragung und Kommunikation im Gesundheitswesen“
CCESigG
Competence Center für die Elektronische Signatur im Gesundheitswesen e.V.

timeproof secure transactions and documents

accellonet wir finden eine Lösung

Verkehrsfähige Information:





Krankenhaus

Arzt

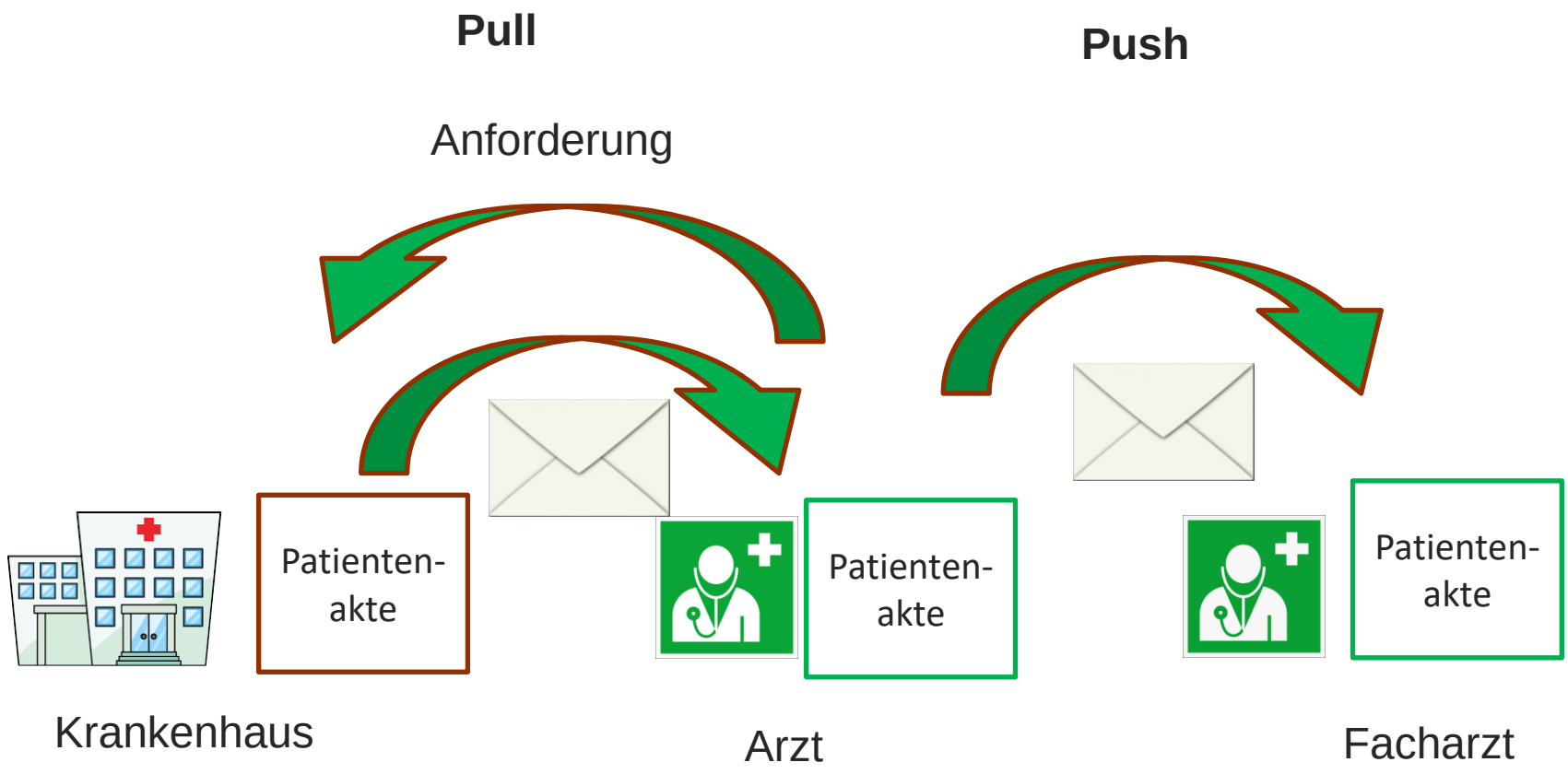
Facharzt

SIDKiG
Arbeitskreis „Sichere Identifikation, Datenübertragung und Kommunikation im Gesundheitswesen“
CCESigG
Competence Center für die Elektronische Signatur im Gesundheitswesen e.V.

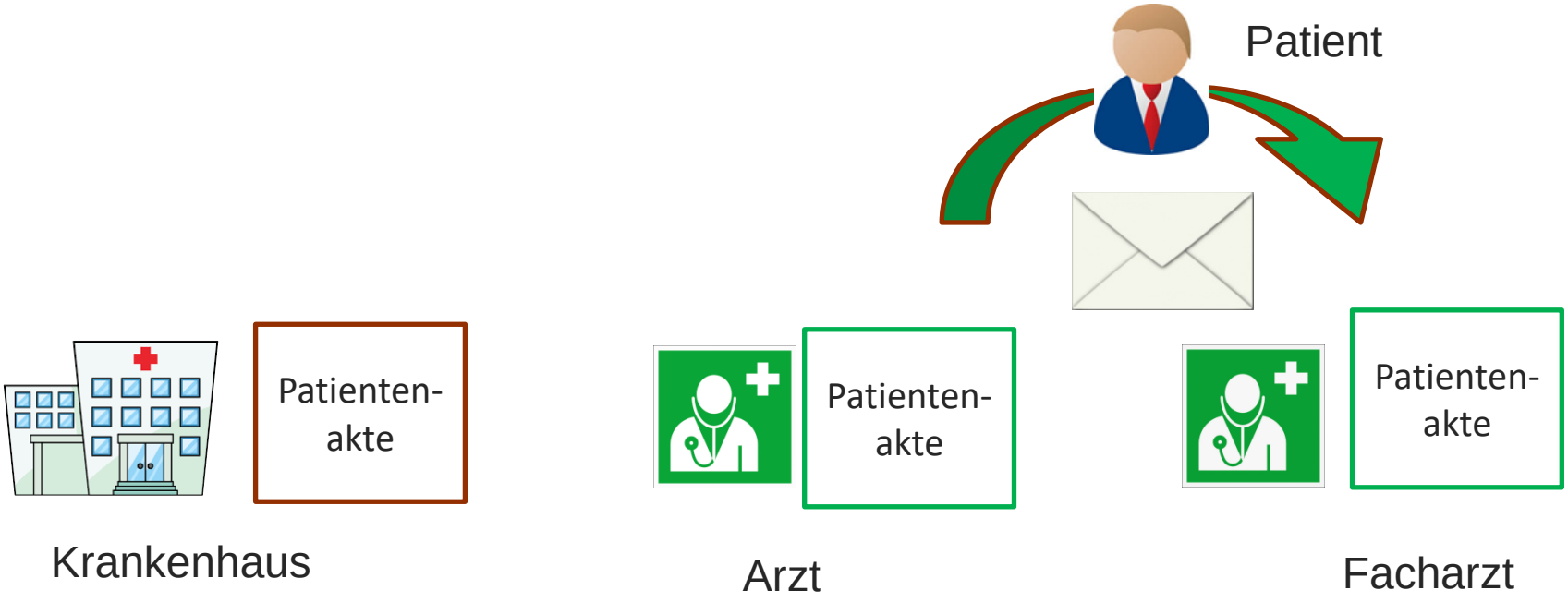
timeproof secure transactions and documents

accellonet wir finden eine Lösung

Übertragung:



Übertragung:



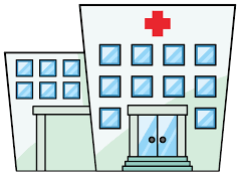
SIDKiG
Arbeitskreis „Sichere Identifikation, Datenübertragung und Kommunikation im Gesundheitswesen“
CCESigG
Competence Center für die Elektronische Signatur im Gesundheitswesen e.V.

timeproof secure transactions and documents

accellonet wir finden eine Lösung

Information elektronisch:

Datei … eAkte



Patienten-akte

Krankenhaus

Patienten-akte

Arzt

Patienten-akte

Facharzt

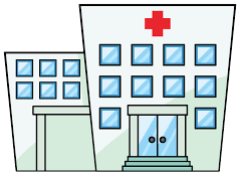
Verkehrsfähige Information elektronisch:

Datei … eAkte

Evidence Record
Zeitstempel
Signatur
Siegel

Container mit Metadaten
Adresse, Absender, MPI.

Standardisiertes Format:
z.B. IHE- kompatible Datenstrukturen



Patienten-akte

Krankenhaus

Patienten-akte

Arzt

Patienten-akte

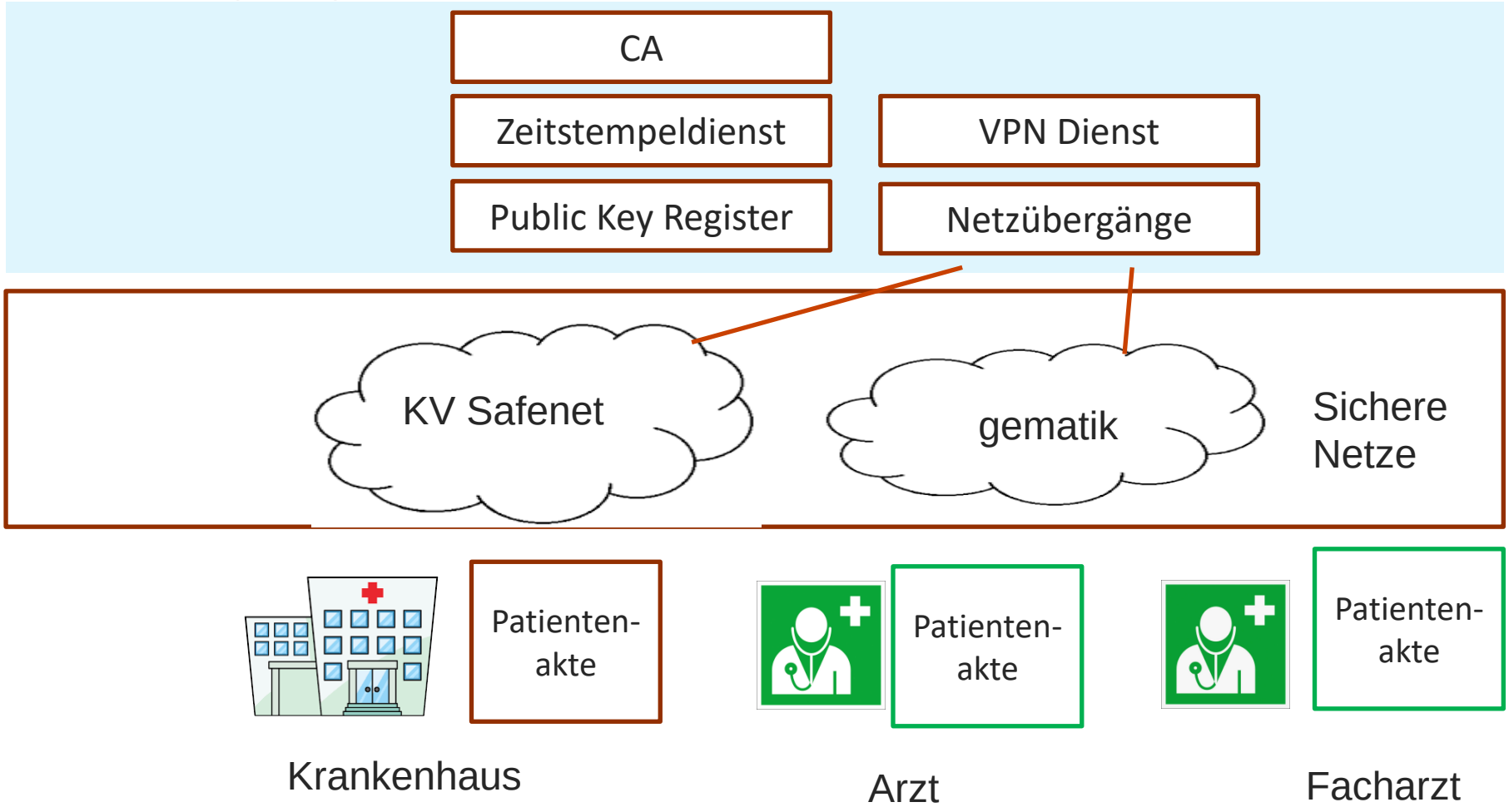
Facharzt

SIDKiG
Arbeitskreis „Sichere Identifikation, Datenübertragung und Kommunikation im Gesundheitswesen“
CCESigG
Competence Center für die Elektronische Signatur im Gesundheitswesen e.V.

timeproof secure transactions and documents

accellonet wir finden eine Lösung

Übertragung elektronisch



SIDKiG
Arbeitskreis „Sichere Identifikation, Datenübertragung und Kommunikation im Gesundheitswesen“
CCESigG
Competence Center für die Elektronische Signatur im Gesundheitswesen e.V.

timeproof secure transactions and documents

accellonet wir finden eine Lösung

Anforderungen

- Dezentrales Kommunikationsmodell
- Einzeldokumente und Dokumentenstrukturen (eAkten) übertragbar
- IHE- kompatible Datenstrukturen
- Verkehrsfähige Dokumente und eAkten
- eIDAS konform
- Direkte Einbindung in IHE-kompatible Umgebungen
- Direkte Archivierung nach TR-ESOR

SIDKiG
Arbeitskreis „Sichere Identifikation, Datenübertragung und Kommunikation im Gesundheitswesen“
CCESigG
Competence Center für die Elektronische Signatur im Gesundheitswesen e.V.

timeproof secure transactions and documents

accellonet wir finden eine Lösung

IHE Domänen

IT Infrastruktur

- Pathologie
- Kardiologie
- Augenheilkunde
- Labormedizin
- Einrichtungsübergreifende Behandlungsketten
- Gerätekommunikation von PCD-Daten
- Pharmazie
- Qualitätssicherung, Forschung, Meldewesen
- Strahlentherapie
- Radiologie inklusive Mammographie

SIDKiG
Arbeitskreis
„Sichere Identifikation, Datenübertragung und Kommunikation im Gesundheitswesen“
CCESigG
Competence Center für die Elektronische Signatur im Gesundheitswesen e.V.

timeproof secure transactions and documents

accellonet
wir finden eine Lösung

IHE - IT Infrastruktur Profile:

Sicherheit:
ATNA - Audit Trail and Node Authentication
CT - Consistent Time

Patientenadministration:
PAM - Patient Administration Management
PDQ - Patient Demographic Query

Document Sharing:
XDS - Cross-Enterprise Sharing of Scanned Documents
XDM - Cross-Enterprise Document Media Interchange
XDR - Cross-Enterprise Document Reliable Interchange
XCA - Cross-Community Access

Erweiterung:
DSG - Document Digital Signature

SIDKiG
Arbeitskreis
„Sichere Identifikation, Datenübertragung und Kommunikation im Gesundheitswesen“
CCESigG
Competence Center für die Elektronische Signatur im Gesundheitswesen e.V.

timeproof secure transactions and documents

accellonet
wir finden eine Lösung

IHE - IT Infrastruktur Profile:

Sicherheit:
ATNA - Audit Trail and Node Authentication
CT - Consistent Time

Patientenadministration:
PAM - Patient Administration Management
PDQ - Patient Demographic Query

Document Sharing:
XDS - Cross-Enterprise Sharing of Scanned Documents
XDM - Cross-Enterprise Document Media Interchange
XDR - Cross-Enterprise Document Reliable Interchange
XCA - Cross-Community Access

Content Profile:
DSG - Document Digital Signature

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“

SIDKiG
Arbeitskreis „Sichere Identifikation, Datenübertragung und Kommunikation im Gesundheitswesen“
CCESigG
Competence Center für die Elektronische Signatur im Gesundheitswesen e.V.

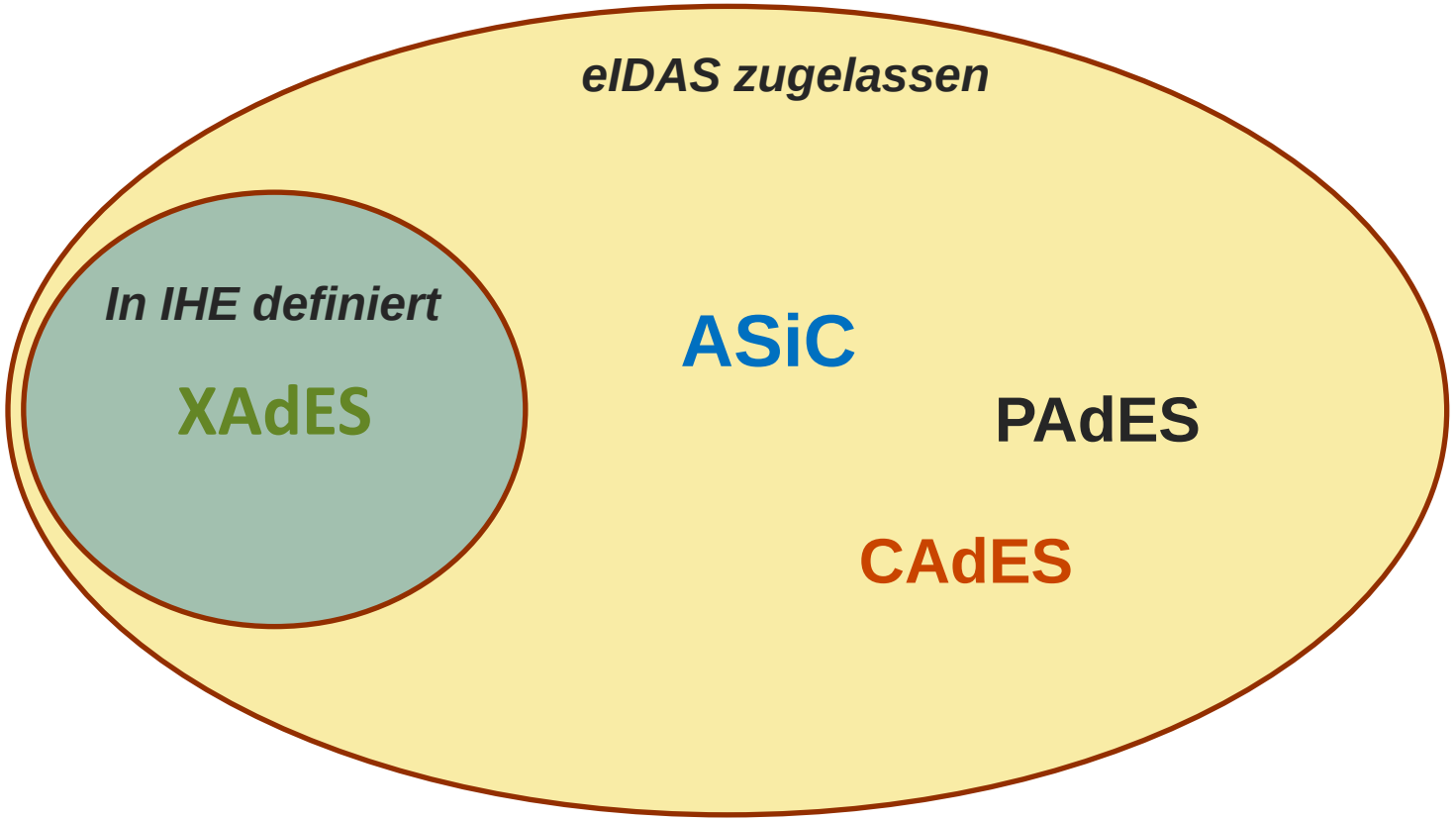
timeproof secure transactions and documents

accellonet wir finden eine Lösung

eIDAS - zugelassene elektronische Signaturen-Formate

- **CAdES** – CMS basierte elektronische Signatur
  (z.B. S/Mine)
- **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
  (In Normung ISO 21320 begriffen. 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



SIDKiG
Arbeitskreis „Sichere Identifikation, Datenübertragung und Kommunikation im Gesundheitswesen“
CCESigG
Competence Center für die Elektronische Signatur im Gesundheitswesen e.V.

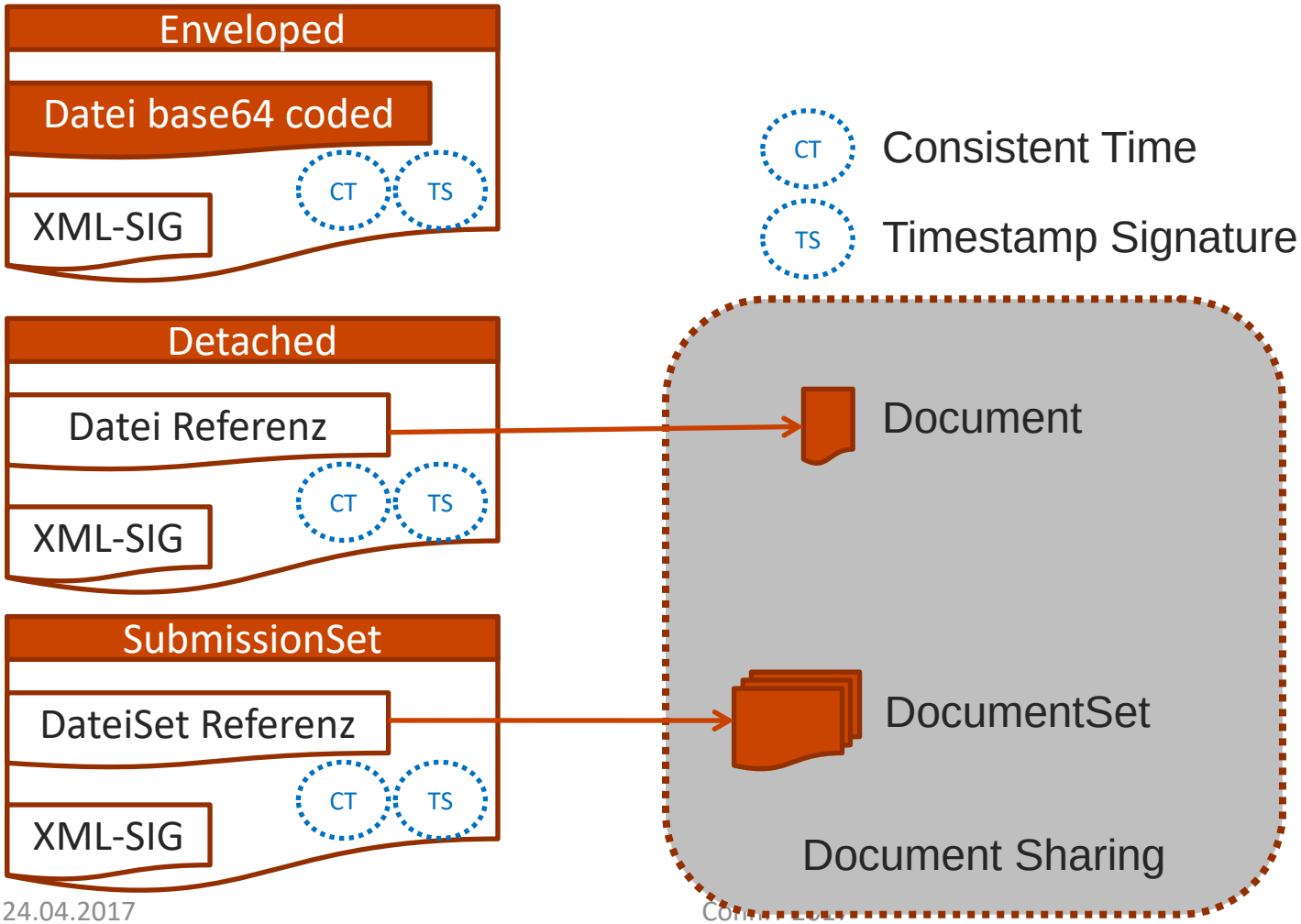
timeproof secure transactions and documents

accellonet wir finden eine Lösung

XAdES erlaubt 3 Datenstrukturen:

- **Enveloping** signierter Content ist in die Signature XML-Syntax eingebettet (Content ist base64 codiert)
- **Detached** verwaltet die Signatur als ein Manifest, das auf unabhängig verwalteten Content verweist (Üblicherweise sind Signatur und Daten in zwei Datenobjekten abgelegt, aber auch als „Geschwisterpaar“ in einer XML-Datei z.B. in W3C XMLDSIG)
- **SubmissionSet** ist eine Detached Signatur, die auf eine Dokumentengruppe und deren Dokumente referenziert, deren Hashwerte enthält und eine XML Digital Signature verwendet.

IHE DSG mit und ohne Document Sharing



SIDKiG
Arbeitskreis „Sichere Identifikation, Datenübertragung und Kommunikation im Gesundheitswesen“
CCESigG
Competence Center für die Elektronische Signatur im Gesundheitswesen e.V.

timeproof secure transactions and documents

accellonet wir finden eine Lösung

Einschätzung IHE DSG

- **DSG nutzt XAdES und ist damit eIDAS konform**
- Eine Akte ist nur in 1 von 3 DSG-Ausprägungen ansatzweise abbildbar (SubmissionSet), ansonsten nur Einzeldokumente
- Keine verkehrsfähige Akte im gegenwärtigen Profil

- **XAdES** nutzt Archivzeitstempel überwiegend im 1:1-Verhältnis an einer Einzelsignatur, d.h. enormer Aufwand bei Signatur- und Zeitstempelerneuerung
- eIDAS Signaturcontainer ASiC - Nutzung von Hashbäumen zur Signaturerneuerung geschaffen. Beweisdokument (Evidence Record) wird im Signaturcontainer abgelegt.
  ISO Norm in Vorbereitung. TR-ESOR integrierbar.

SIDKiG
Arbeitskreis „Sichere Identifikation, Datenübertragung und Kommunikation im Gesundheitswesen“
CCESigG
Competence Center für die Elektronische Signatur im Gesundheitswesen e.V.

timeproof secure transactions and documents

accellonet wir finden eine Lösung

Was ist umsetzbar ?

- Dokument-Austausch per XAdES Enveloping auch ohne Shared Document Infrastructur möglich.
- Für DokumentenSet-Austausch mit XAdES SubmissionSet starten.
- Wenn Shared Document Infrastrutur vorhanden, dann vorzugsweise mit XAdES Detached Dokumente austauschen.
- eIDAS Signaturcontainer ASiC mit TR-ESOR Funktionalität in IHE einbringen, um Aktenabbildung und –verwaltung (Anlegen, Updaten, Löschen, Versionieren, LTA) vollständig abzubilden. CCESigG wird dies im Kommentar zum DSG Profil im Juni 2017 bei IHE-D ausführen.

SIDKiG
Arbeitskreis
„Sichere Identifikation, Datenübertragung und Kommunikation im Gesundheitswesen“
CCESigG
Competence Center für die Elektronische Signatur im Gesundheitswesen e.V.

timeproof secure transactions and documents

accellonet wir finden eine Lösung

Vielen Dank für Ihre Aufmerksamkeit!

Referent: Dr. Jürgen Weidner, Geschäftsführer accellonet
Co-Referent: Olaf Feller, Geschäftsführer timeproof