

XML-Signatur für CDA-R2 Dokumente (Elektronische Signatur von Arztbriefen)

Erarbeitet im Auftrag von:



Bundesärztekammer



Ärztekammer Nordrhein



Ärztekammer Westfalen-Lippe

Jörg Apitzsch

bremen online services



bremen online services GmbH & Co. KG (bos KG)



- Die bos KG ist ein Software- und Beratungsunternehmen mit dem Schwerpunkt rechtsverbindliche und sichere Internetkommunikation in der Öffentlichen Verwaltung und Privatwirtschaft; hervorgegangen aus dem *MEDIA@komm*-Wettbewerb
- Unternehmensgründung: 1999
- Geschäftsführer: Dr. Stephan Klein
- Mitarbeiterinnen und Mitarbeiter derzeit: über 80
- Eigentümerstruktur: Public Private Partnership
 - Mehrheitseigentümerin: Freie Hansestadt Bremen
 - Gesellschafter u.a. Deutsche Telekom AG, Sparkasse Bremen, Brekom (EWE Gruppe)



Leistungsprofil – Was macht die bos KG?

- Produktarbeit - Entwicklung von Standard- und Individualsoftware
 - OSCI-Transport und OSCI-basierte Software
 - Governikus (Middleware, Sicherheitsinfrastruktur) 
 - Govello (auf OSCI basierender Nachrichten-Client) 
 - Derivate, u.a. EGVP für den elektronischen Rechtsverkehr

- Hosting - Betrieb von E-Government-Dienstleistungen
 - OSCI-Transport und OSCI-basierte Software
 - bos ist darauf spezialisiert, rechtsverbindliche, sichere und datenschutzgerechte Kommunikation über das Internet zu ermöglichen (z.B. Server- und Anwendungshosting)

- Projektarbeit - Planung, Umsetzung und Betreuung von rechtssicheren Online-Diensten
 - Consulting, IT-Servicedienstleistungen und IT-Support / Helpdesk

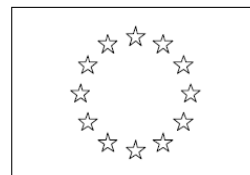
Gremien- /Standardisierungsarbeit

- Die bos KG engagiert sich in folgenden Gremien:



BMWA

Exportnetz



EUROPEAN COMMISSION
ENTERPRISE AND INDUSTRY DIRECTORATE-GENERAL

Basic and Design Industries, Tourism, IDABC
European eGovernment Services (IDABC)

Jörg Apitzsch

- Ausbildung: Diplom-Informatiker
- 1977-97 Erfahrungen mit IT-Systemen/Projekten für das Gesundheitswesen, u.a. leitende Stellung bei der GSD mbH Berlin
- 1997-2005 selbständiger Berater
 - IT-Integrations-Projekte, Web-Enabling (Handelsunternehmen)
 - Co-Autor E-Government-Standard OSCI Transport, Beratung bos bei der Realisierung von Infrastrukturen zur Verbreitung und Nutzung digitaler Signaturen
 - Chefarchitekt „Governikus“ - aka „Virtuelle Poststelle des Bundes“
 - Engagement in div. Standardisierungsgremien
- Seit Mitte 2005 zunächst Ltr. Produktmanagement, jetzt CTO bei bos
 - Aktuell Editor Weiterentwicklung OSCI Transport auf Basis WS-Stack
 - Mitarbeit IDABC: EU-weite Profilierung der relevanten internationalen Standards für sicheren und rechtsgültigen Daten- u. Dokumentenaustausch
 - Mitarbeit T7-Ag „QES“ (Umsetzung eCard-API für die Kartenprojekte der Bundesregierung)
 - Kundenprojekte: vornehmlich Technologie-/Architekturberatung

Signatur „Arztbriefe“: Rahmenbedingungen

- Aufgabe: Spezifikation / Policy für die Erstellung digitaler Signaturen für med. XML-Dokumente als Vorgabe für die Implementierung interoperabler Signaturanwendungskomponenten durch die SW-Hersteller
- Konsentierung des Konzepts mit der Fachöffentlichkeit, neben den Auftraggebern u.a. beteiligt:
 - gematik
 - HL7-Nutzergruppe (Abstimmung mit Dr. Heitmann)
 - VHitG (Dr. Gehlen, Duria EG)
 - Fraunhofer-Institute ISST, IBMT
 - DRV Bund
 - SAK-Hersteller

Grundsätzliche Anforderungen (1)

- Es sollen Signaturen nach XDSIG eingesetzt werden
 - Qualifizierte Signaturen nach SigG (zum Einsatz kommt die „Health Professional Card“ – HPC)
 - Profilierung der Signaturelemente gem. ISIS-MTT mit
 - Einschränkung „exklusive Kanonisierung“
 - Erweiterung „SHA-256“ ff.
 - Optionale Einbindung von Attributzertifikaten
- Konzept zunächst für den „Arztbrief“, aber applizierbar auch für andere med. Dokumente im XML-Format
 - Anlagen zu Arztbrief (Texte, Bilder) müssen (in späterer Version) als zum Dokument gehörig mitsigniert werden können
 - Mehrfachsignaturen zulässig
 - Konzept muss zukünftig geplante Signaturen von Fragmenten von XML-Dokumenten berücksichtigen

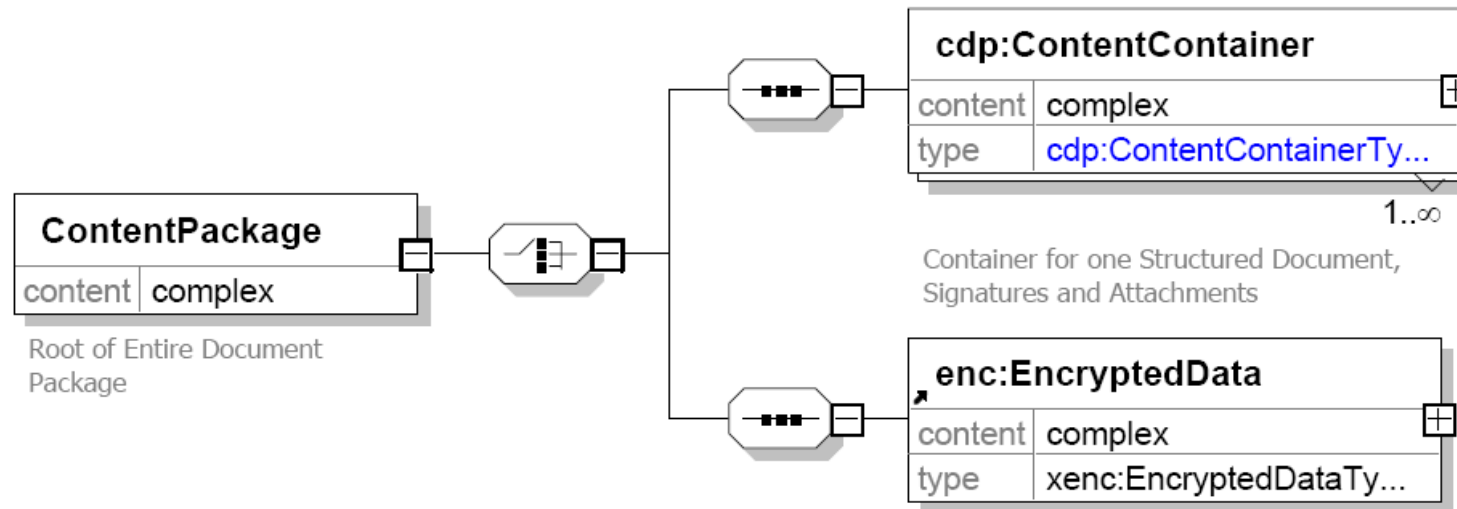
Grundsätzliche Anforderungen (2)

■ CDA-R2-Dokument:

- Darstellbar als normaler Brief, lesbar mit üblichen Browser durch Arzt und Patient
- Beliebig transportierbar, kopierbar, ablegbar, strukturiert zerlegbar und darstellbar in beliebigen Kontexten
- Qualifiziert signiert mit dem eA - ein Dokument mit zunächst ca. sechsjähriger „Haltbarkeit“, darstellbar in Viewer, z.B. im Browser mit speziellen Darstellungskomponenten

■ „Paketierbarkeit“

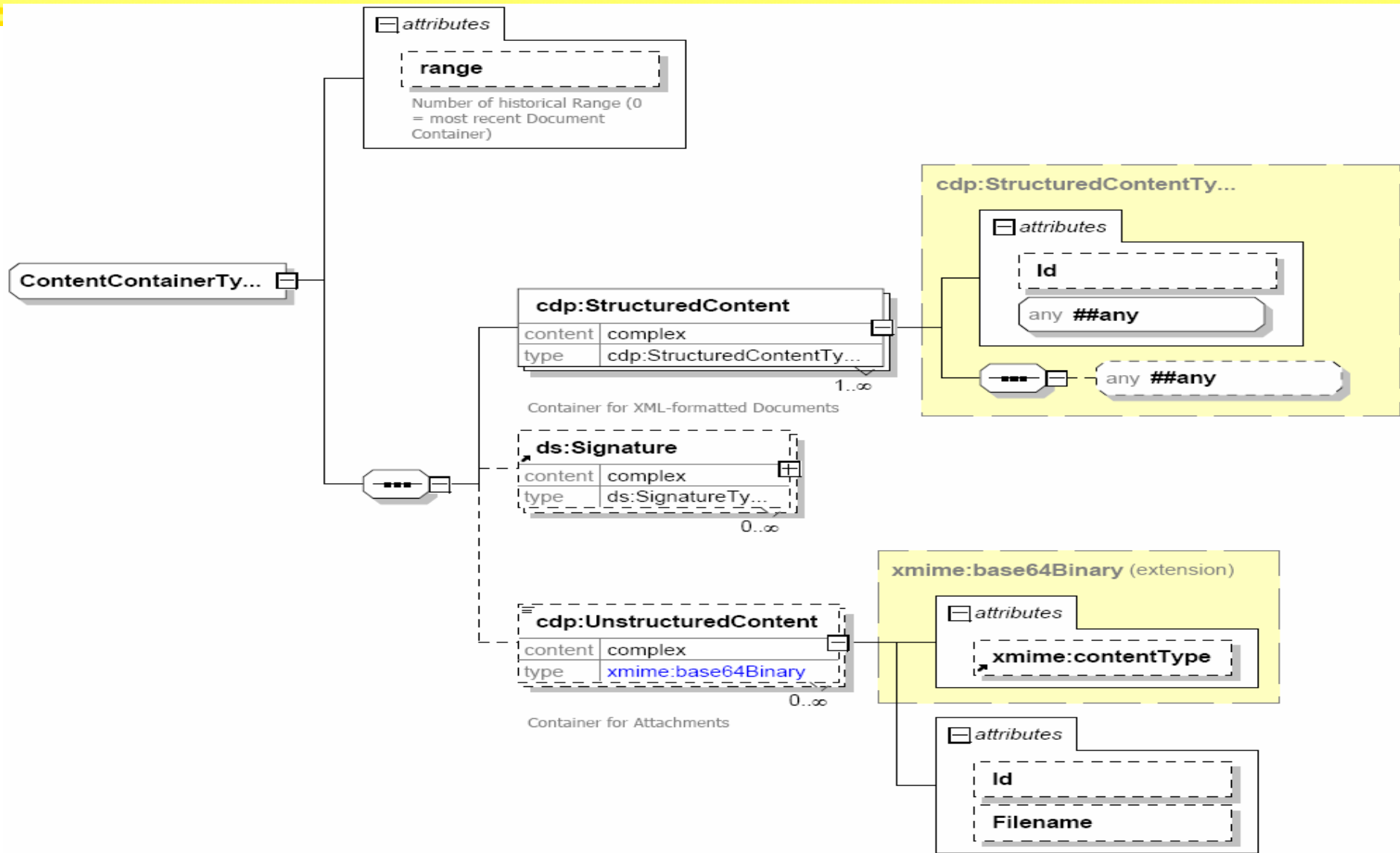
- Sicherung Zusammengehörigkeit von Signatur(en) und signierten Dokumenten in einer Struktur
- Optional auch zugehörige Attachments
- Optional auch CDA-R2-Dokumente der Episode des Falls



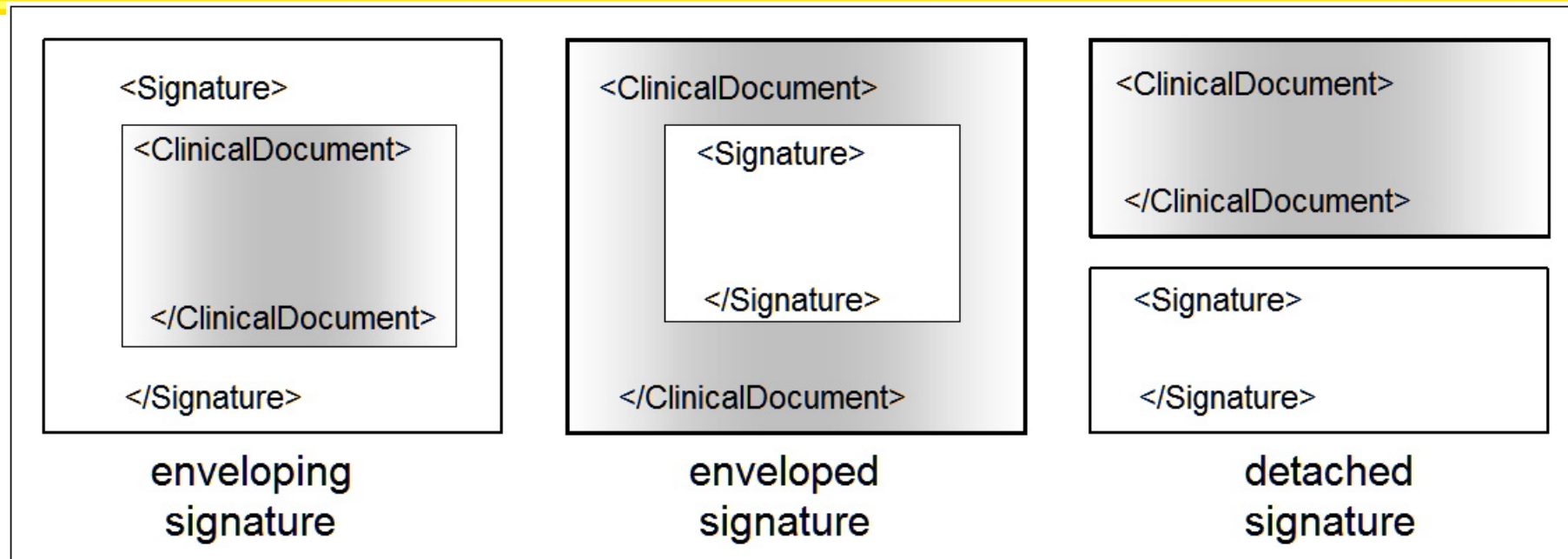
Das Root-Element enthält alternativ eine Sequenz von Elementen
<cdp:ContentContainer> zur Aufnahme von strukturierten Dokumenten,
Signaturen und Attachments
oder
<xenc:EncryptedData> - verschlüsselte **<cpd:ContentContainer>** gem. [xenc];
diese werden im Rahmen dieser Spezifikation nicht näher betrachtet.

► Hinweis: *Eine SAK kann die Ver- und Entschlüsselung unterstützen; ansonsten muss diese Funktionalität im Kontext der gewählten Telematik-Infrastruktur von den Transportkomponenten abgedeckt werden.*

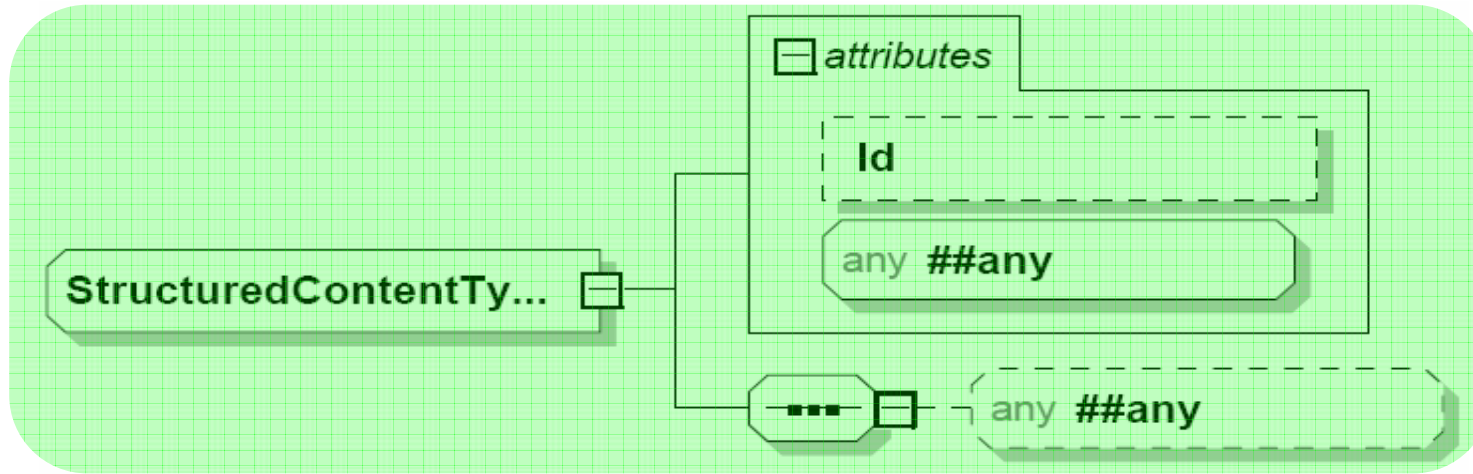
ContentContainer



XML Signature: Typen



- Gewählt wurde „Detached Signature“:
 - `<ClinicalDocument>` wird referenziert (Signatur Gesamtdokument)
 - Weiter der zugehörige `<LegalAuthenticator>` (auch `<Authenticator>` möglich)
 - Referenzierung generell über Id-Attribute gem. XML Schema



- Ein Element `<cdp:StructuredContent>` kann XML-Dokumente aus beliebigen Namensräumen aufnehmen, es wird ein Attribut `<Id>` vom Typ `<xs:ID>` geführt, welches dazu dienen kann, den gesamten Teilbaum (das gesamte Dokument) aus Signaturelementen des Containers heraus zu referenzieren
- Im Fall CDA-R2-Dokumente ist dies `<POCD_MT000040.ClinicalDocument>` aus dem Namensraum „urn:hl7-org:v3“, in diesem Fall führt das Root-Element `<ClinicalDocument>` selbst ein Id-Attribut.

In Version 1 der Signaturspezifikation für CDAR2-Dokumente sind nur Signaturen über das ganze Dokument zulässig. In einer zukünftigen Version sollen auch Signaturen möglich sein, die sich nur auf fachliche Fragmente des Dokuments erstrecken, für die ein bestimmter Autor verantwortlich zeichnet:

<cda:Section>, klammert einen fachlichen Abschnitt des CDA-R2-Dokuments, der von einem Authenticator signiert werden kann

<cda:Authenticator> enthält spezifische ergänzende Informationen zum jeweiligen Signator, der eine Signatur auf ein oder mehrere <cda:Section>-Elemente appliziert.

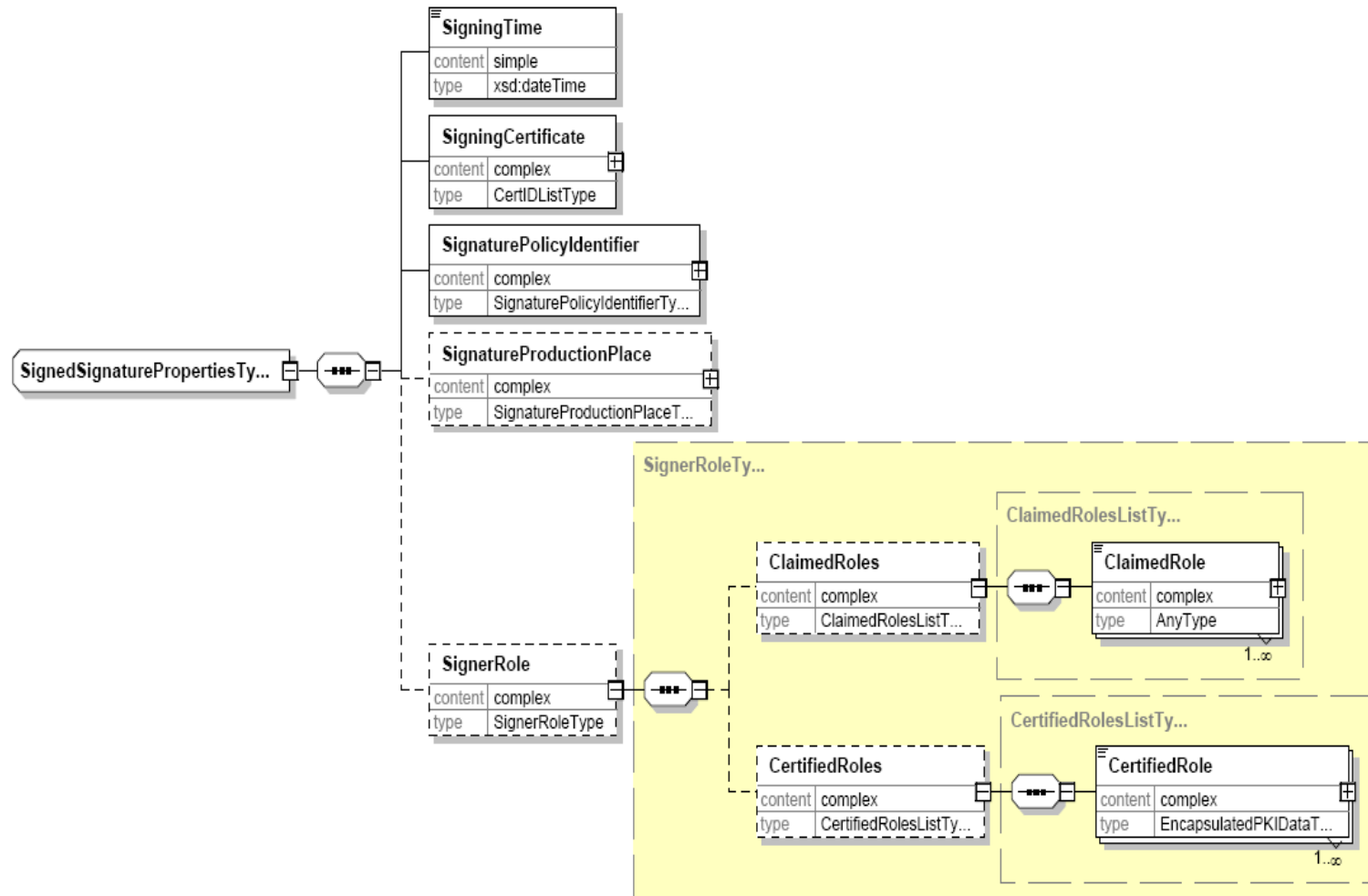
Eindeutige Id-Attribute erforderlich

- Da in der Gesamtstruktur <cdp:ContentPackage> auch ursprünglich selbstständige XML-Dokumente zusammengeführt werden können, ist sicherzustellen, dass die Eindeutigkeit der Werte der Id-Attribute auch dann gewährleistet ist
- Algorithmen zur Erzeugung von eindeutigen Identifiern stellt die Spezifikation „A Universally Unique Identifier (UUID) URN Namespace“ zur Verfügung [RFC4122]. Erzeugt wird dabei jeweils ein 128-Bit-String. SAK-Implementierungen müssen diesen Mechanismus unterstützen
- Die gematik schreibt eine Generierungsregel vor, die auch hier zum Einsatz kommen soll

Qualifizierende Angaben zur Signatur

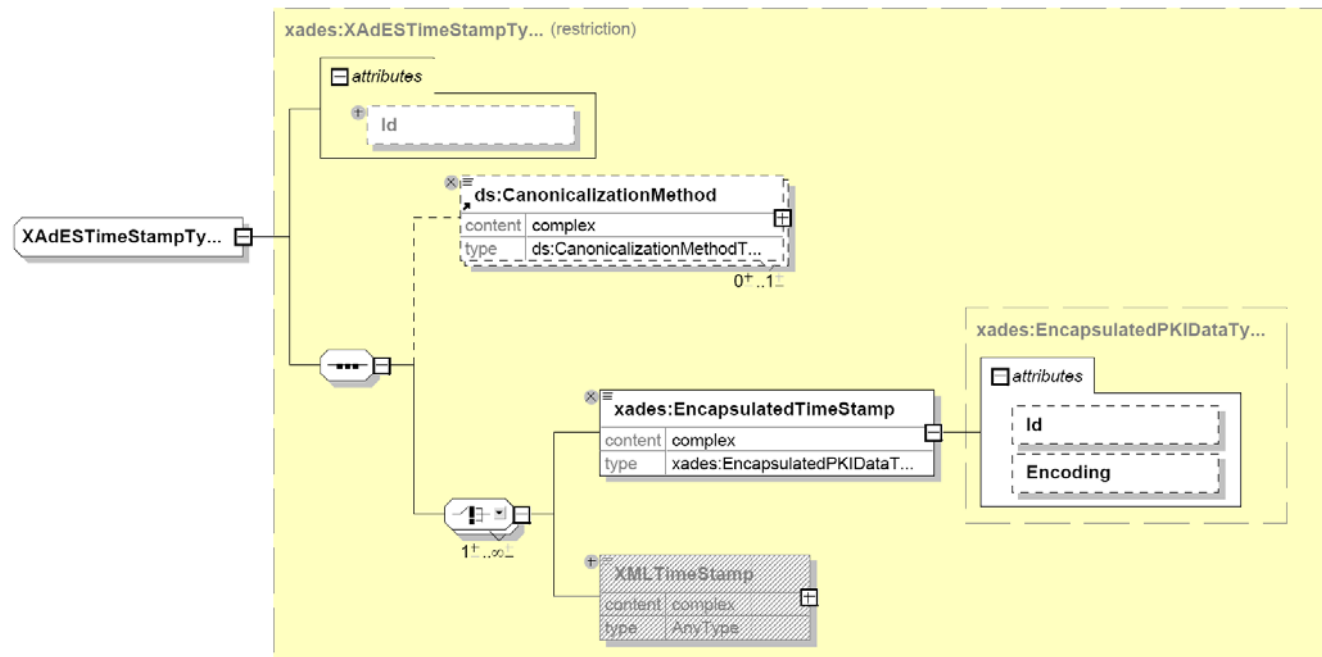
- Spezifikation XAdES des European Telecommunication Standards Institute (ETSI) definiert Erweiterungen zu xdsig, die in <xdsig:Object>-Elementen geführt werden. Diese werden ebenfalls in die Signaturberechnung einbezogen
- Hier sind dies:
 - <SignerRole>
 - Attributzertifikat („CertifiedRole“)
 - Verweis auf das zugeordnete <LegalAuthenticator>-Element („ClaimedRole“)
 - <SigningTime> (als Systemzeit)
 - Verweis auf das eingesetzte Signaturzertifikat (Hash, Ser-No)
 - <SignaturePolicy> - als URI, später ggf. als Link auf maschinenlesbare Policy
 - Eingesetztes Stylesheet für die Visualisierung (als URI in einem <Manifest>-Element)

<xades:SignedSignatureProperties>



Optionaler qual. Zeitstempel

Der qual. Zeitstempel wird nach der Signatur appliziert. Auch hier gilt eine entspr. XAdES-Erweiterung `<xades:SignatureTimestamp>`, die von folgendem Typ ist:



Konkretisierung: fiktives Beispiel

Ansicht strukt. Arztbrief (xml im Browser)

Klinisches Dokument - Maxthon Browser

Datei Bearbeiten Ansicht Favoriten Gruppen Optionen Extras Fenster Hilfe

Patient:	Paul Pappel	Patient-Nr:	6245
Kontakt:	Riedemannweg 59 13627 Berlin		
geb.:	17. Dezember 1955	Geschlecht:	männlich
Behandelnder Arzt:	Dr.med. Hans Topp-Glücklich Musterstr. 1 64283 Darmstadt Tel: 061511111111 (Arbeitsplatz) Fax: 061512222222 (Arbeitsplatz)	Erzeugt am:	31. Juli 2007

Klinisches Dokument

29.08.2005: Diagnosen mit ICD 10

Diagnose	ICD Code	Lokalisation	Zusatz
Allergisches Asthma	J45.0	--	G
Ausschluss Lungenemphysem	J43.9	--	A
V.a. Allergische Rhinopathie durch Pollen	J31.1	--	V

03.04.2007: Diagnosen mit ICD 10

Diagnose	ICD Code	Lokalisation	Zusatz
Kandidose der Haut und der Nägel re	B37.2	R	G

29.08.2005: Anamnese

Sei Jahren wiederholt chronische Bronchitiden besonders bei kalter Luft. Bei Anstrengung expiratorische Atemnot. Kontakt mit Haustieren.

29.08.2005: Befund

Pulmo: Basal diskrete RGs, Cor: oB Abdomen: weich, Peri:+++ , Muskulatur: atrophisch, Mundhöhle: Soor, Haarleukoplakie, Haut: blass, seborrhoisches Ekzem, Schleimhäute: blass, Hauttrrurgor herabgesetzt Neuro: herabgesetztes Vibrationsempfinden der Beine, distal betont, Parästesien der Beine, PSR, AST oB und seitengleich.

29.08.2005: Pricktest

Test	Ergebnis
Pricktest	
Brike	+++
Haselstrauch	+++
Erl	+
Hainbuche	+
Rotbuche	+
Eiche	+
Gräser-Mix	+++

Id-Attribute in <ClinicalDocument>

```

<?xml version="1.0" encoding="UTF-8"?>
<cdp:ContentPackage xsi:schemaLocation="http://ws.gematik.de/fa/cds/CDocumentPayload/v1.0
CDA_Package_V01.xsd" xmlns:cdp="http://ws.gematik.de/fa/cds/CDocumentPayload/v1.0"
xmlns:ds="http://www.w3.org/2000/09/xmldsig#" xmlns:xsi="http://www.w3.org/2001/XMLSchema-
instance" xmlns:xmime="http://www.w3.org/2005/05/xmlmime">
  <cdp:ContentContainer range="0">
    <cdp:StructuredContent>
      <!-- Clinical Document mit ID_1 ->
      <ClinicalDocument classCode="DOCCLIN" moodCode="EVN,,
id="ID-9af4ea90-65cf-11dc-9e28-00123fde8721" nullFlavor="OTH,,
xsi:schemaLocation="urn:hl7-org:v3 POCD_MT000040DE.xsd" xmlns="urn:hl7-org:v3"
xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance">
        .....
        <!-- legalAuthenticator mit ID_2 ->
        <legalAuthenticator id="ID-a4030810-65cf-11dc-bcda-00123fde8721">
          .....
          <assignedPerson>
            <name>
              <given>Robert</given>
              <family>Dolin</family>
              <suffix>MD</suffix>
            </name>
          </assignedPerson>
          .....
        </legalAuthenticator>
      </ClinicalDocument>
    </cdp:StructuredContent>
  
```

Signaturelement: Reference-Elemente

```

<!-- Signatur Element mit ID_3 (wird aus QualifyingProperties, Target referenziert) -->
<ds:Signature Id="ID-abbc1ce0-65cf-11dc-99b6-00123fde8721">
  <ds:SignedInfo>
    <ds:CanonicalizationMethod Algorithm="http://www.w3.org/TR/2001/10/xml-exc-c14n#"/>
    <ds:SignatureMethod Algorithm="http://www.w3.org/2001/04/xmldsig-more#rsa-sha256"/>
  <!-- Referenz auf ID_1 (ClinicalDocument) -->
    <ds:Reference URI="#ID-9af4ea90-65cf-11dc-9e28-00123fde8721">
      <ds:Transforms><ds:Transform Algorithm="http://www.w3.org/TR/2001/10/xml-exc-c14n#"/></ds:Transforms>
      <ds:DigestMethod Algorithm="http://www.w3.org/2001/04/xmlenc#sha256"/>
      <ds:DigestValue>UjBsR09EbGhjZ0dTQUxNQUFBUNBRU1tQ1p0dU1GUXhEUzhi</ds:DigestValue>
    </ds:Reference>
  <!-- Referenz auf ID_4 (SignedProperties in Object-Element 1) -->
    <ds:Reference URI="#ID-ad58b5e0-65cf-11dc-9f07-00123fde8721"
      Type="http://uri.etsi.org/01903/v1.3.2#SignedProperties">
      <ds:Transforms><ds:Transform Algorithm="http://www.w3.org/TR/2001/10/xml-exc-c14n#"/></ds:Transforms>
      <ds:DigestMethod Algorithm="http://www.w3.org/2001/04/xmlenc#sha256"/>
      <ds:DigestValue>UjBsR09EbGhjZ0dTQUxNQUFBUNBRU1tQ1p0dU1GUXhEUzhi</ds:DigestValue>
    </ds:Reference>
  <!-- Referenz auf ID_5 (Manifest in Object-Element 2) -->
    <ds:Reference URI="#ID-7e577810-65e5-11dc-a853-00123fde8721"
      Type="http://www.w3.org/2000/09/xmldsig#Manifest">
      <ds:Transforms><ds:Transform Algorithm="http://www.w3.org/TR/2001/10/xml-exc-c14n#"/></ds:Transforms>
      <ds:DigestMethod Algorithm="http://www.w3.org/2001/04/xmlenc#sha256"/>
      <ds:DigestValue>UjBsR09EbGhjZ0dTQUxNQUFBUNBRU1tQ1p0dU1GUXhEUzhi</ds:DigestValue>
    </ds:Reference>
  </ds:SignedInfo>
  <ds:SignatureValue>...</ds:SignatureValue> <ds:KeyInfo.../>

```

Object-Element 1: Signed Properties (1)

```
<ds:Object>
  <!-- Target zeigt auf ID_3 des Signaturelements -->
  <xades:QualifyingProperties Target="#ID-abbc1ce0-65cf-11dc-99b6-00123fde8721"
    xsi:schemaLocation="http://uri.etsi.org/01903/v1.3.2# xmlns:xades="http://uri.etsi.org/01903/v1.3.2#"
    xmlns:ds="http://www.w3.org/2000/09/xmldsig#" xmlns:xsi="http://www.w3.org/2001/XMLSchema-
    instance">
    <!-- SignedProperties haben Id-Attribut ID_4, referenziert aus SignedInfo -->
    <xades:SignedProperties Id="ID-ad58b5e0-65cf-11dc-9f07-00123fde8721">
      <xades:SignedSignatureProperties>
        <xades:SigningTime>2007-09-17T09:30:47.0Z</xades:SigningTime>
        <!-- Referenz auf das Signaturzertifikat -->
        <xades:SigningCertificate> <xades:Cert>
          <xades:CertDigest>
            <ds:DigestMethod Algorithm="http://www.w3.org/2001/04/xmlenc#sha256"/>
            <ds:DigestValue>
              UjBsR09EbGhjZ0dTQUxNQUFBUUNBRU1tQ1p0dU1GUXhEUzhi
            </ds:DigestValue>
          </xades:CertDigest>
          <xades:IssuerSerial><ds:X509IssuerName>teletrust</ds:X509IssuerName>
            <ds:X509SerialNumber>123</ds:X509SerialNumber>
          </xades:IssuerSerial> </xades:Cert>
        </xades:SigningCertificate>
        <!-- Signature Policy – hier: „implied“ ; in Zukunft Referenz auf eine maschinelesbare Policy geplant
        -->
        <xades:SignaturePolicyIdentifier>
          <xades:SignaturePolicyImplied/>
        </xades:SignaturePolicyIdentifier>
      </xades:SignedSignatureProperties>
    </xades:SignedProperties>
  </xades:QualifyingProperties>
</ds:Object>
```

Object-Element 1: Signed Properties (2)

```
<xades:SignerRole>
  <!-- Referenz auf zugeordnetes legalAuthenticator-Element (ID_2) -->
  <xades:ClaimedRoles>
    <xades:ClaimedRole>
      <ds:Reference URI="#ID-a4030810-65cf-11dc-bcda-00123fde8721">
        <ds:Transforms><ds:Transform
          Algorithm="http://www.w3.org/TR/2001/10/xml-exc-c14n#" /></ds:Transforms>
        <ds:DigestMethod Algorithm="http://www.w3.org/2001/04/xmlenc#sha256" />
        <ds:DigestValue>UjBsR09EbGhjZ0dTQUxNQUFBUUNBRU1tQ1p0dU1GUXhEUzhi</ds:DigestValue>
      </ds:Reference>
    </xades:ClaimedRole>
  </xades:ClaimedRoles>
  <!-- Attributzertifikat -->
  <xades:CertifiedRoles>
    <xades:CertifiedRole Encoding="http://www.w3.org/2000/09/xmlsig#base64">
      UjBsR09EbGhjZ0dTQUxNQUFBUUNBRU1tQ1p0dU1GUXhEUzhi</xades:CertifiedRole>
    </xades:CertifiedRoles>
  </xades:SignerRole>
</xades:SignedSignatureProperties>
</xades:SignedProperties>
</xades:QualifyingProperties>
</ds:Object>
```

Object-Element 2: Ref. auf Stylesheet

```
<ds:Object>
<!-- ds:Manifest haben Id-Attribut ID_5, referenziert aus SignedInfo -->
  <ds:Manifest Id="ID-7e577810-65e5-11dc-a853-00123fde8721"
    xmlns:ds="http://www.w3.org/2000/09/xmlsig#"
    xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance">
    <ds:Reference
      URI="http://www.e-arztausweis.de/stylesheets/earztbrief-1_0/vhitg-cda-v3-signed.xsl">
      <ds:Transforms>
        <ds:Transform Algorithm="http://www.w3.org/TR/2001/10/xml-exc-c14n"/>
      </ds:Transforms>
      <ds:DigestMethod Algorithm="http://www.w3.org/2001/04/xmlenc#sha256"/>
      <ds:DigestValue>UjBsR09EbGhjZ0dTQUxNQUFBUNBRU1tQ1p0dU1GUXhEUzhi
      </ds:DigestValue>
    </ds:Reference>
  </ds:Manifest>
</ds:Object>

</ds:Signature>
```

Noch nicht gelöst:

- „Trusted Viewer“ für XML-Dokumente, die mit einem Stylesheet transformiert werden
- Lt. BSI mangelt es auch noch an einem Konzept hierfür – bzw. Anforderungen aus der Bestätigung nach SigG sind nicht fixiert!

Vielen Dank für die Aufmerksamkeit!

Fragen und Anregungen ?

gerne an: Jörg Apitzsch, bos

ja@bos-bremen.de