Signatur-Workshop

Neue Signaturformate
SecurityLayer, MOCCA, PDF-AS

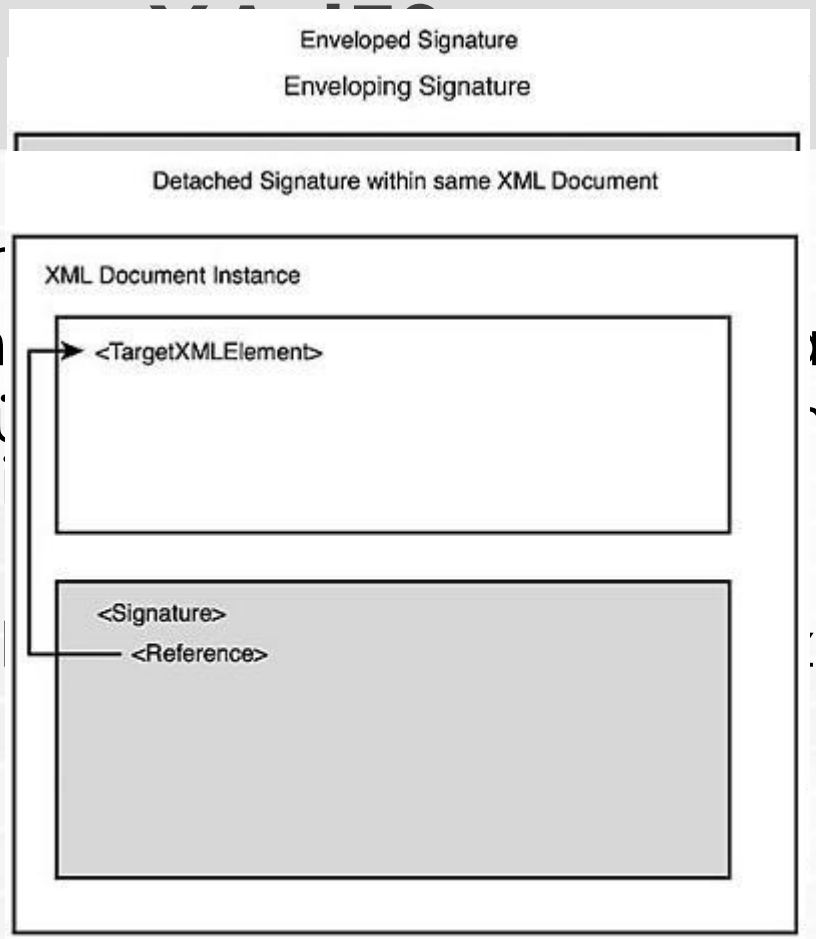
Tobias Kellner

Wien, 05.12.2013

EGIZ
E-Government Innovationszentrum

Das E-Government Innovationszentrum ist
eine gemeinsame Einrichtung des
Bundeskanzleramtes und der TU Graz

TU Graz
BUNDESKANZLERAMT ÖSTERREICH



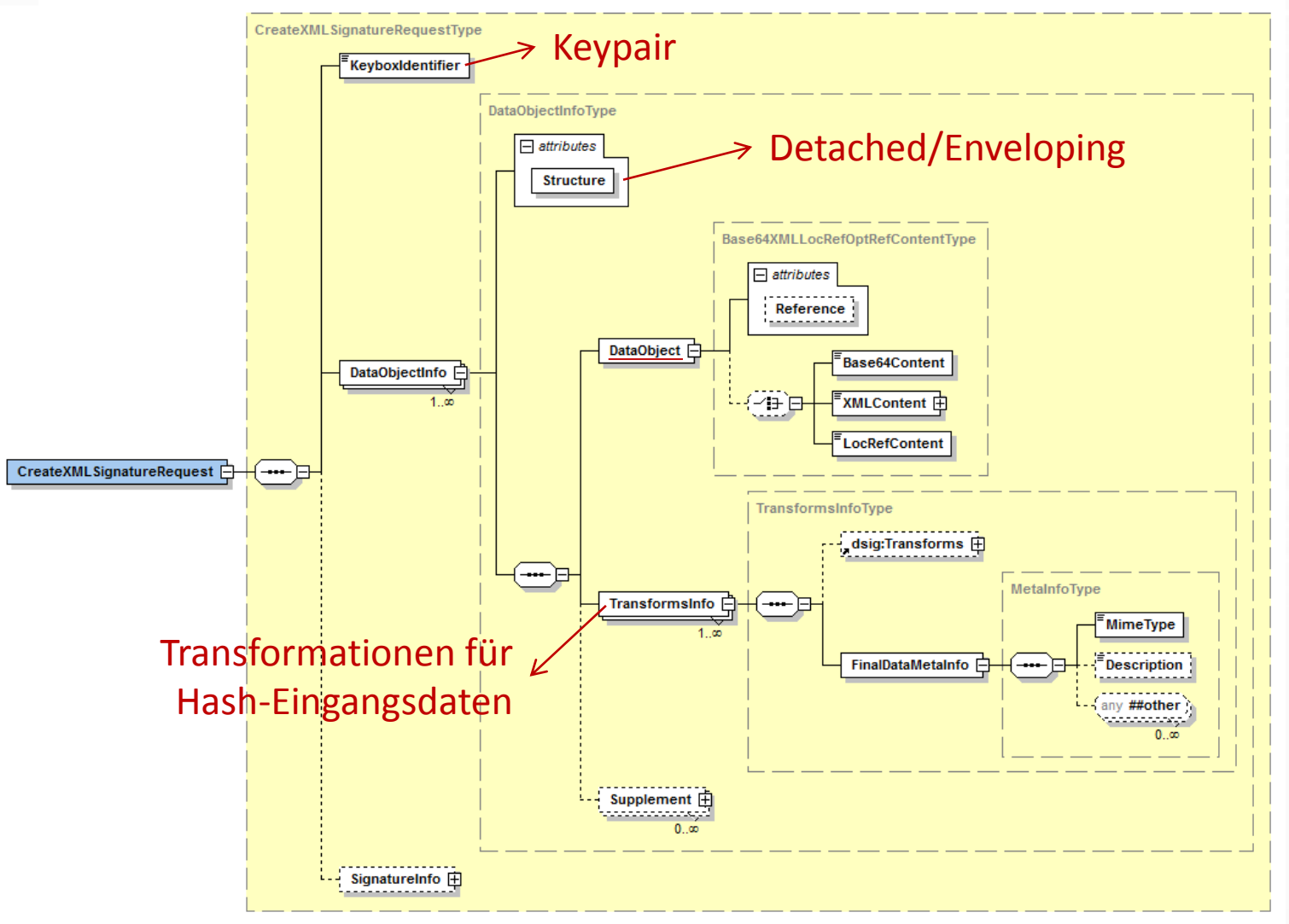
- Erweiterunger
  - Für fortgesch ...turen
  - Dokument gü ...nen gebrochen s
- XML-DSig
  - <Signature>- ...U signierendes
    - Enveloping
    - Enveloped
    - Detached
- XAdES: QualifyingProperties
  - SigningCertificate
  - SigningTime, etc.

Quelle: *Securing Web Services Security with WS-Security* (Sams, 2004, ISBN: 0672326515)

XAdES SecurityLayer Änderung

- `CreateXMLSignature` muss XAdES 1.4.2-kompatible Signatur erzeugen
- Kleinere Ergänzungen und Korrekturen

CreateXMLSignature Request



XAdES 1.4.2 Signatur

```
<?xml version="1.0" encoding="UTF-8"?>
<dsig:Signature Id="Signature-1" xmlns:dsig="http://www.w3.org/2000/09/xmldsig#">
  <dsig:SignedInfo Id="SignedInfo-1">
    <dsig:Object Id="Object-2">
      <xades:QualifyingProperties Target="#Signature-1" xmlns:ns3=".../v1.4.1#" xmlns:xades=".../v1.3.2#">
        <xades:SignedProperties Id="SignedProperties-1">
          <xades:SignedSignatureProperties>
            <xades:SigningTime>2013-12-04T20:43:56Z</xades:SigningTime>
            <xades:SigningCertificate>
              <xades:Cert>
                <xades:CertDigest>
                  <dsig:DigestMethod Algorithm="http://www.w3.org/2001/04/xmlenc#sha256"/>
                  <dsig:DigestValue>r5s0</dsig:DigestValue>
                </xades:CertDigest>
                <xades:IssuerSerial>
                  <dsig:X509IssuerName>CN=a-sign-Premium-Sig-02,...</dsig:X509IssuerName>
                  <dsig:X509SerialNumber>12345</dsig:X509SerialNumber>
                </xades:IssuerSerial>
              </xades:Cert>
            </xades:SigningCertificate>
            <xades:SignaturePolicyIdentifier>
              <xades:SignaturePolicyImplied/>
            </xades:SignaturePolicyIdentifier>
          </xades:SignedSignatureProperties>
          <xades:SignedDataObjectProperties>
            <xades:DataObjectFormat ObjectReference="#Reference-1">
              <xades:MimeType>text/plain</xades:MimeType>
            </xades:DataObjectFormat>
          </xades:SignedDataObjectProperties>
        </xades:SignedProperties>
      </xades:QualifyingProperties>
    </dsig:Object>
  </dsig:Signature>
```

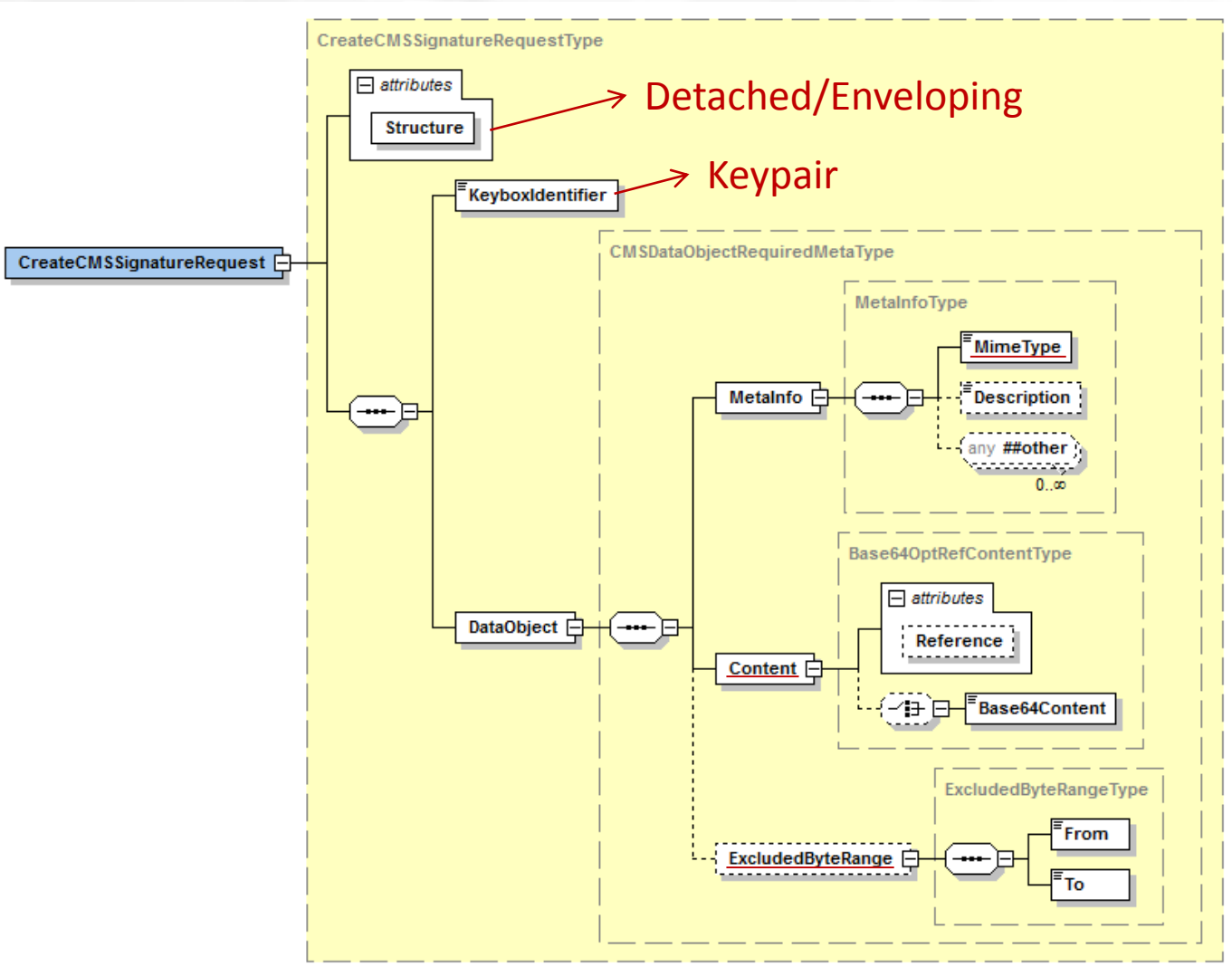
CAdES

- Erweiterung von CMS
  - Für fortgeschrittene elektronische Signaturen
  - Dokument gültig, auch wenn Algorithmen gebrochen sind
- CMS
  - Basiert auf PKCS #7
  - ASN.1-Struktur
  - Kann beliebige Daten enthalten
  - Signatur
- CAdES: weitere signierte Attribute
  - Signing-certificate
  - Content-Type, Message-digest
  - Signing-time, etc.

CAdES SecurityLayer Änderung

- `CreateCMSSignature` muss CAdES 2.2.1-kompatible Signatur erzeugen
  - Profil CAdES-BES
- Optional kann `ExcludedByteRange` angegeben werden
  - Wird nicht mitsigniert
  - Wird bei Anzeige in der BKU mit 0x00 ausgefüllt

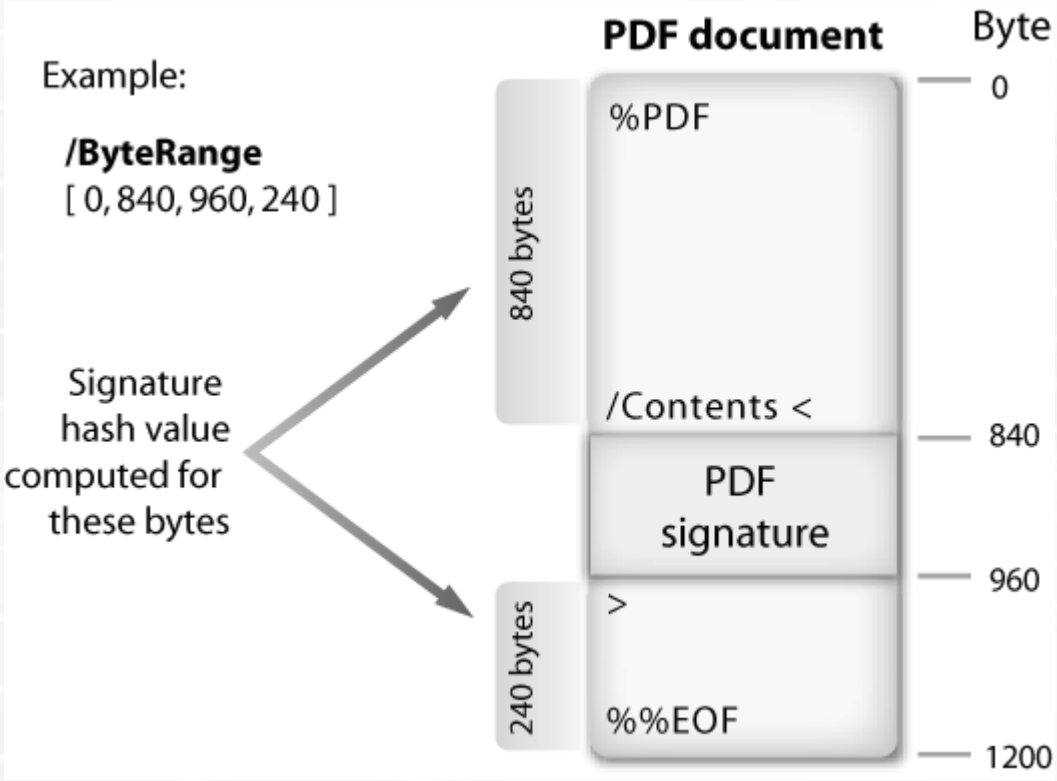
CreateCMSSignature request



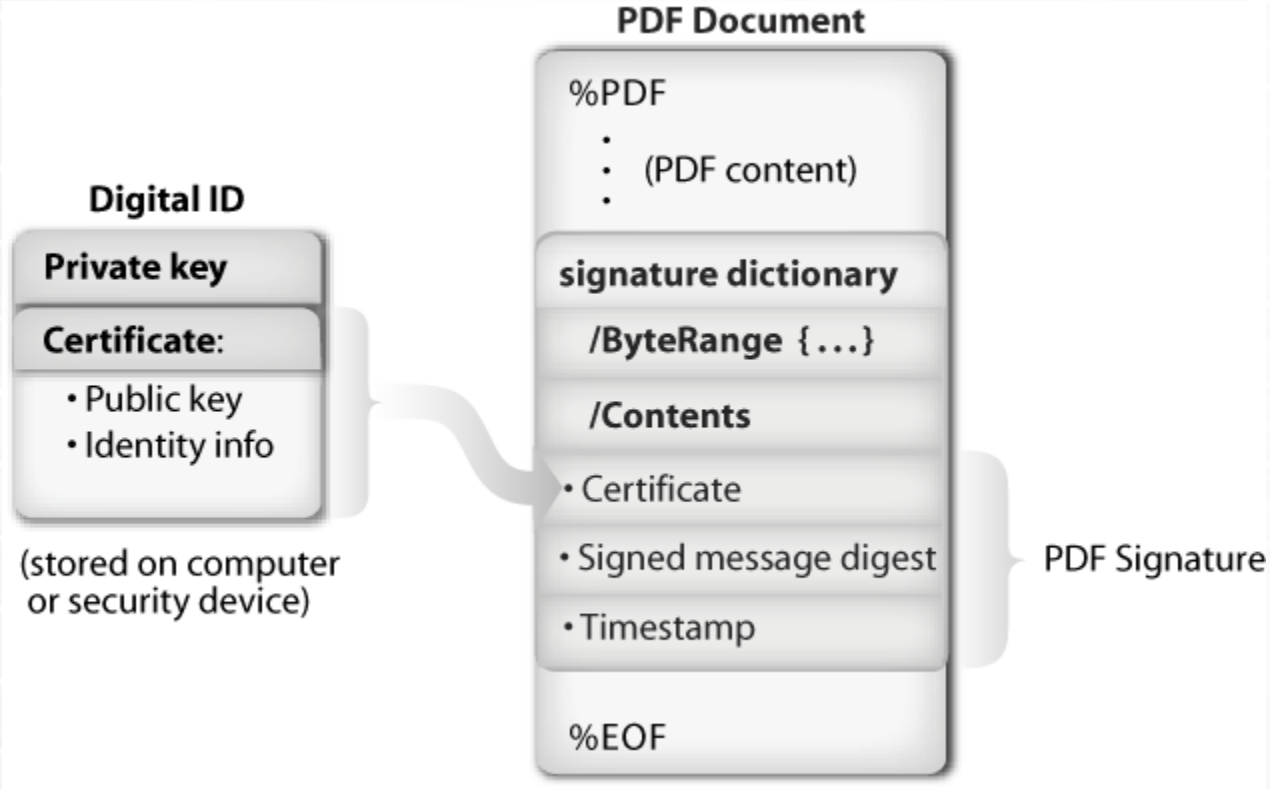
PAdES

- PDF unterstützt elektronische Signaturen
  - Unter anderem PKCS#7
- PAdES: Einschränkungen und Erweiterungen für PDF-Signaturen
  - Für fortgeschrittene elektronische Signaturen
  - Dokument gültig, auch wenn Algorithmen gebrochen sind
- CAdES-Signatur wird eingebettet
  - Das gesamte Dokument exklusive der Signatur selbst wird signiert
  - `ByteRange`

PDF-Signatur



PDF-Signatur



PDF-AS Änderungen

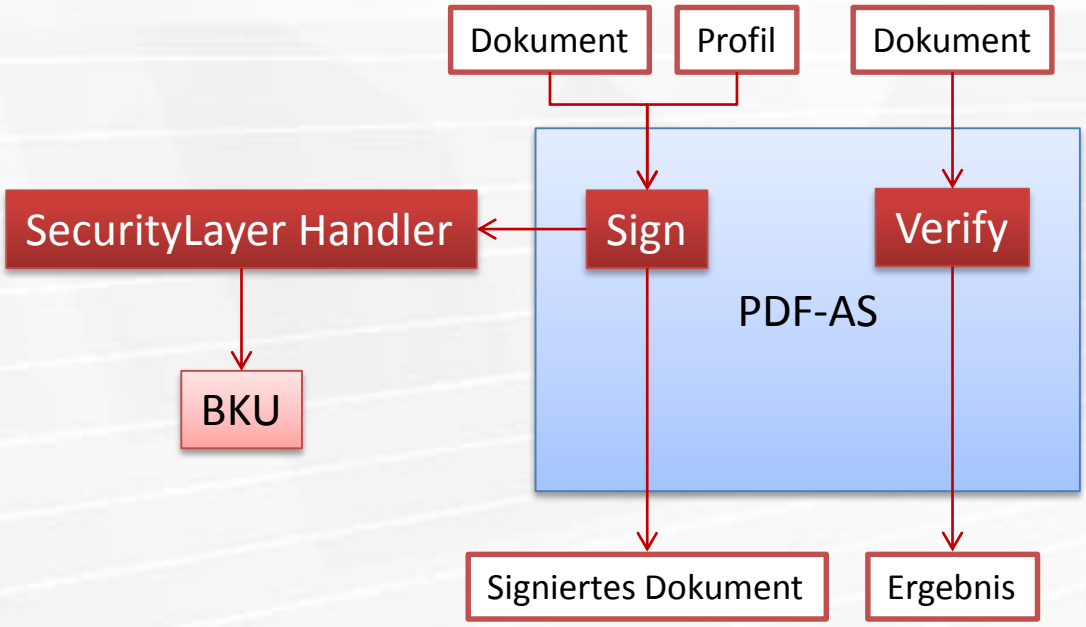
- PAdES-Signaturen
- Signatur nur mehr binär
- Signaturblock
  - Kein Signaturwert
- Ablauf
  - Mehrere SecurityLayer Requests

PDF-AS Ablauf neu

- Signaturblock muss vor Signaturvorgang feststehen
  - Wird vor Signaturvorgang eingebettet und mitsigniert
  - Signaturwert nicht bekannt
- Ablauf neu
  - Signator-Zertifikat auslesen
  - Signaturblock einfügen
  - CAdES-Signatur mittels BKU erstellen
  - Signatur einfügen

SIGNATURINFORMATIONEN		
	Unterzeichner	Tobias Kellner
	Aussteller-Zertifikat	CN=a-sign-Premium-Sig-02,OU=a-sign-Premium-Sig-02,O=A-Trust Ges. f. Sicherheitssysteme im elektr. Datenverkehr GmbH,C=AT
	Serien-Nr.	529366
	Methode	urn:pdfsigfilter:bka.gv.at:binaer:v1.1.0
	Parameter	etsi-moc-1.1:ecdsa-sha256@4e9bae38
Prüfinformation	Signaturpruefung unter: http://www.signaturpruefung.gv.at	
Hinweis	Dieses mit einer qualifizierten elektronischen Signatur versehene Dokument ist gemäß § 4 Abs. 1 Signaturgesetz einem handschriftlich unterschriebenen Dokument grundsätzlich rechtlich gleichgestellt.	
Datum/Zeit-UTC	2013-12-05T01:59:48Z	

PDF-AS API neu



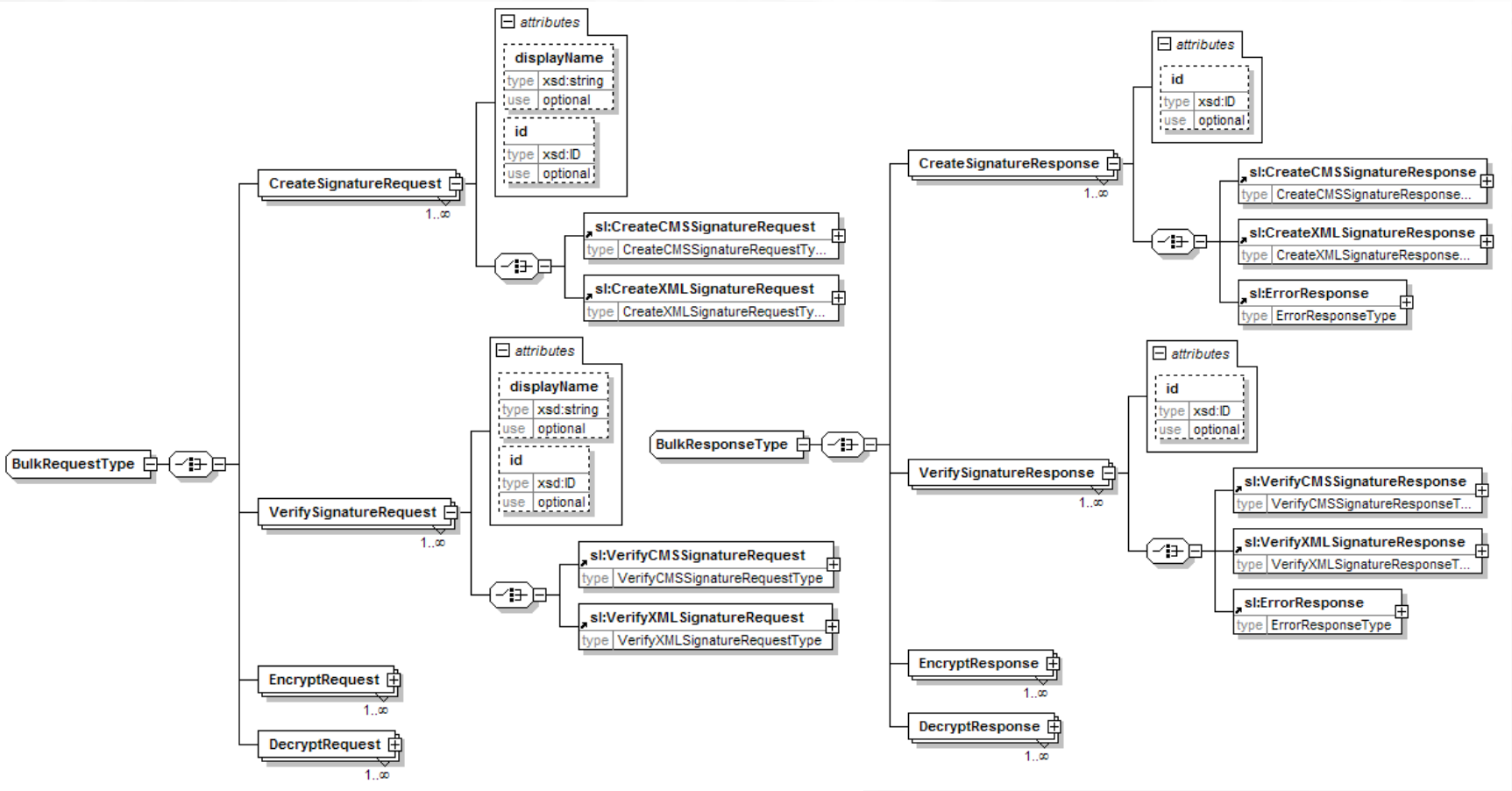
PDF-AS Kompatibilitäts-Wrapper

- Ziel:
  - Schnelle Migration von Produktiv-Applikationen
- Wrapper
  - Emuliert Verhalten des alten PDF-AS API
  - Bildet Requests auf das neue API ab
  - Übernimmt BKU-Kommunikation

Stapelsignaturen

- Mehrere unabhängige Signaturen
- Ein Schlüsselpaar
- Einmalige Authorisierung (PIN)

Stapelsignaturen



Vielen Dank für die Aufmerksamkeit!

Tobias Kellner – tobias.kellner@egiz.gv.at
www.egiz.gv.at

EGIZ
E-Government Innovationszentrum

XAdES-Profile

- **XAdES**, basic form just satisfying Directive legal requirements for advanced signature;
- **XAdES-T** (timestamp), adding timestamp field to protect against repudiation;
- **XAdES-C** (complete), adding references to verification data (certificates and revocation lists) to the signed documents to allow off-line verification and verification in future (but does not store the actual data);
- **XAdES-X** (extended), adding timestamps on the references introduced by XAdES-C to protect against possible compromise of certificates in chain in future;
- **XAdES-X-L** (extended long-term), adding actual certificates and revocation lists to the signed document to allow verification in future even if their original source is not available;
- **XAdES-A** (archival), adding possibility for periodical timestamping (e.g. each year) of the archived document to prevent compromise caused by weakening signature during long-time storage period.

CAdES-Profile

- **CAdES**, basic form just satisfying Directive legal requirements for advanced signature;
- **CAdES-T** (timestamp), adding timestamp field to protect against repudiation;
- **CAdES-C** (complete), adding references to verification data (certificates and revocation lists) to the signed documents to allow off-line verification and verification in future (but does not store the actual verification data);
- **CAdES-X** (extended), adding timestamps on the references introduced by CAdES-C to protect against possible compromise of certificates in chain in future;
- **CAdES-X-L** (extended long-term), adding actual certificates and revocation lists to the signed document to allow verification in future even if their original source is not available;
- **CAdES-A** (archival), adding possibility for periodical timestamping (e.g. each year) of the archived document to prevent compromise caused by weakening signature during long-time storage period.