

Introductie CreAim

- Introductie CreAim
 - Portaal & IDSP
 - Authenticatie en Autorisatie
 - De SBR Assurance oplossing
 - Impact op software ontwikkelaars
 - CreAim kan helpen
- ❧ Actief sinds 2001 en momenteel gevestigd in Zaandam (noord ring Amsterdam)
 - ❧ Internetspecialist op de gebieden authenticatie& autorisatie, m2m informatie-uitwisseling en SBR rendering.
 - ❧ Klanten: Intermediairs, overheidsdienstverleners (zoals de Belastingdienst) en MKB
 - ❧ Producten/ diensten:
 - ❧ Klantenportaal voor intermediairs
 - ❧ Softwarecomponenten voor softwareontwikkelaars
 - ❧ Identity Service Provider
 - ❧ Authenticatiemiddelen (bijv. eHerkenning en PKI certificaten)
 - ❧ Ondertekensoftware

Portaal & IDSP software

- Introductie CreAim
- Portaal & IDSP
- Authenticatie en Autorisatie
- De SBR Assurance oplossing
- Impact op software ontwikkelaars
- CreAim kan helpen

❧ Functionaliteiten Klantenportaal:

- ❧ Aangifte en jaarrekening management
- ❧ Machtigingen registratie en digitale ondertekeningen
- ❧ Elektronisch dossiervorming
- ❧ Koppelingen met (accountancy)applicaties
 - ❧ Financieel, fiscaal, CRM, rapportage

❧ Identity Service Provider

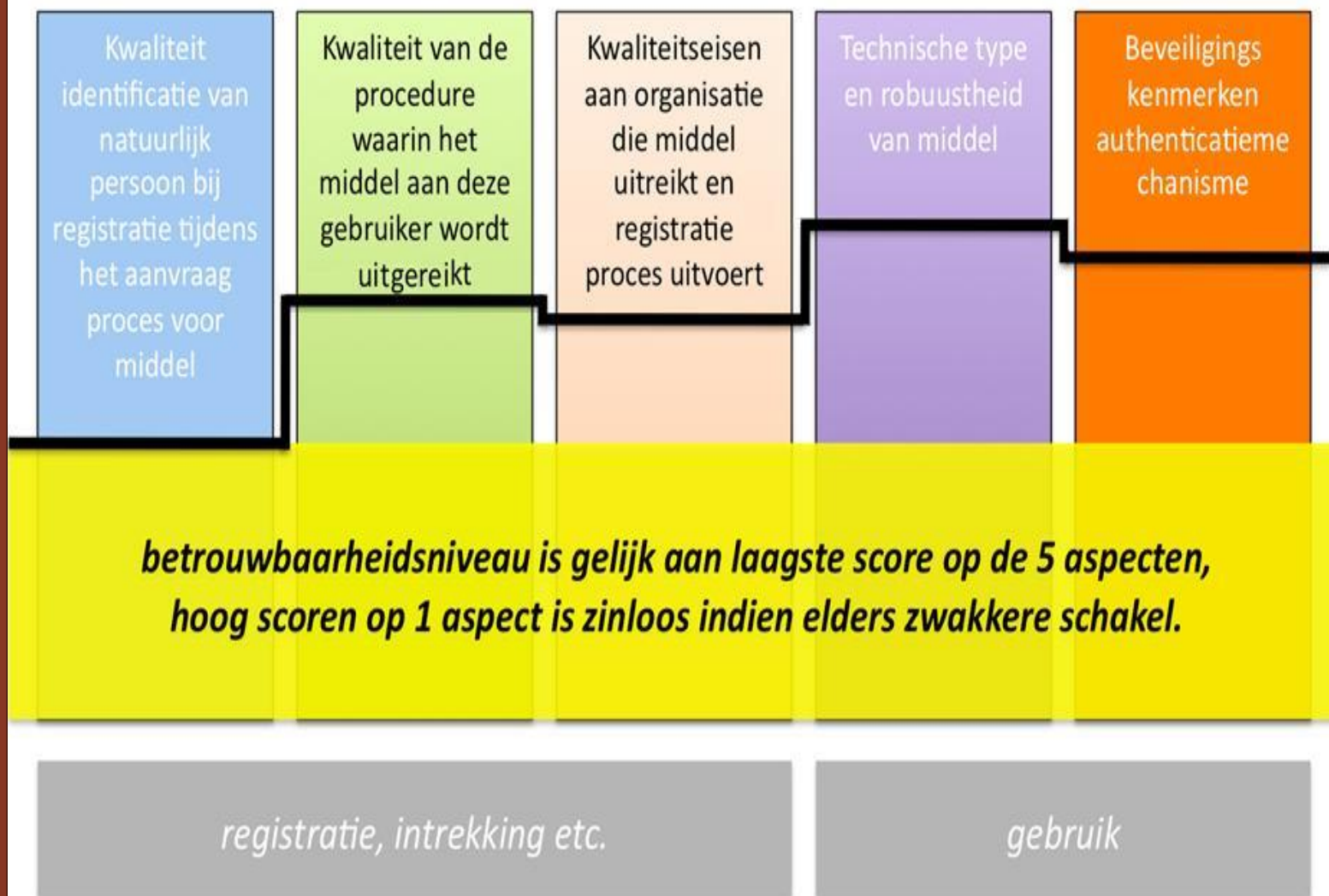
- ❧ Authenticatieschil om applicaties (zowel SaaS als backoffice)
- ❧ Single Sign On
- ❧ Hergebruik van authenticatiemiddelen

Authenticatie en Autorisatie (1)

- Introductie CreAim
 - Portaal & IDSP
 - Authenticatie en Autorisatie
 - De SBR Assurance oplossing
 - Impact op software ontwikkelaars
 - CreAim kan helpen
- ❧ PKIo services servercertificaten (t.b.v. Digipoort)
 - ❧ De partner van KPN in de accountantsmarkt
 - ❧ PKIo beroepscertificaten (voor RA's en AA's)
 - ❧ Oplageverklaring, Publicatiestukken, ondertekening brieven
 - ❧ eHerkenning en eID
 - ❧ Sinds 2011 in gebruik, in eerste instantie voor WBSO subsidies en vergunningen.
 - ❧ Snel toenemend aantal overheidsdienstverleners met eHerkenning.
 - ❧ Eerst alleen B2G, nu ook B2B met eHerkenning.
 - ❧ Sinds begin 2014 migratie naar eID, gereed medio 2015.
 - ❧ eID ook bij SBR (machtigingen).

Authenticatie en Autorisatie (2)

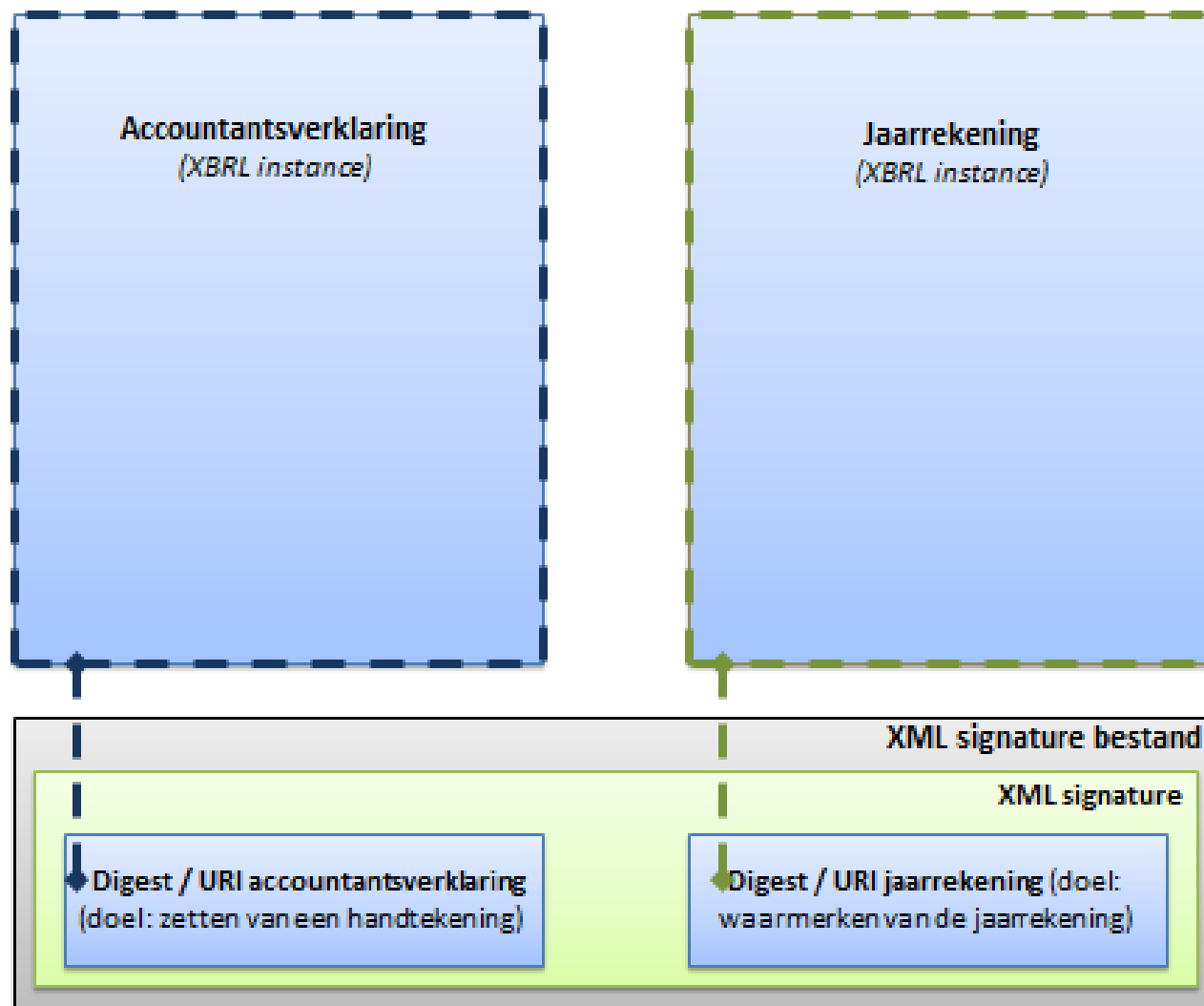
- Introductie CreAim
- Portaal & IDSP
- Authenticatie en Autorisatie
- De SBR Assurance oplossing
- Impact op software ontwikkelaars
- CreAim kan helpen





CREAIM Uitgangspunten van de SBR oplossing (1)

- Introductie CreAim
- Portaal & IDSP
- Authenticatie en Autorisatie
- De SBR Assurance oplossing
- Impact op software ontwikkelaars
- CreAim kan helpen



Uitgangspunten van de oplossing (2)

- Introductie CreAim
 - Portaal & IDSP
 - Authenticatie en Autorisatie
 - De SBR Assurance oplossing
 - Impact op software ontwikkelaars
 - CreAim kan helpen
- ❧ Twee taxonomieën en twee instance documenten
 - ❧ Elektronische handtekening met NBA beroepscertificaat
 - ❧ Geautomatiseerde controle op koppeling jaarverantwoording en verklaring
 - ❧ Aanlevering aan Digipoort system-to-system of via upload portaal

Impact op software ontwikkelaars

- Introductie CreAim
- Portaal & IDSP
- Authenticatie en Autorisatie
- De SBR Assurance oplossing
- Impact op software ontwikkelaars
- CreAim kan helpen

- ❧ SBR bestanden creëren
- ❧ SBR bestanden valideren
- ❧ Aanroepen verklaringengenerator
- ❧ PKIo certificaat
- ❧ Presenteren
- ❧ Linking & Signing
- ❧ Verzenden

NBA beroepscertificaat

- Introductie CreAim
- Portaal & IDSP
- Authenticatie en Autorisatie
- De SBR Assurance oplossing
- Impact op software ontwikkelaars
- CreAim kan helpen

✧ Uitgegeven door:

- ✧ KPN Corporate Market BV
- ✧ ESG de elektronische signatuur BV
- ✧ QuoVadis TrustLink BV
- ✧ Digidentity BV
- ✧ CreAim BV

- ✧ PKI met registercheck

Controle certificaat service

- Introductie CreAim
- Portaal & IDSP
- Authenticatie en Autorisatie
- De SBR Assurance oplossing
- Impact op software ontwikkelaars
- CreAim kan helpen

- ❧ NBA-beroepscertificaat?
 - ❧ Correcte uitgevers
- ❧ Is het certificaat niet ingetrokken?
- ❧ Is het certificaat nog geldig?

Presenteren

- Introductie CreAim
- Portaal & IDSP
- Authenticatie en Autorisatie
- De SBR Assurance oplossing
- Impact op software ontwikkelaars
- CreAim kan helpen

- ❧ Presenteren jaarrekening en controleverklaring
 - ❧ Renderen SBR bestanden
 - ❧ Afhankelijk van de uitkomsten werkgroep nominatieve presentatie
- ❧ Aandachtspunten:
 - ❧ Extensies
 - ❧ Dimensions

Stappen Linken en Signen

- Introductie CreAim
- Portaal & IDSP
- Authenticatie en Autorisatie
- De SBR Assurance oplossing
- Impact op software ontwikkelaars
- CreAim kan helpen

- ❧ Waarmerken van de Jaarverantwoording
 - ❧ Subset bepalen met Xpath
 - ❧ Exclusive XML Canonicalization (C14N)
 - ❧ Berekenen hash waarde (SHA2)
- ❧ Opnemen hash waarde/functie in verklaring
 - ❧ nba-i:HashFunctionType
 - ❧ nba-i:HashValueSubjectMatter
- ❧ Ondertekenen accountantsverklaring
 - ❧ Canonicalization (C14N)
 - ❧ XMLDSig
 - ❧ XAdES detached signature
 - ❧ Uitgangspunten ondertekening

Uitgangspunten ondertekening

- Introductie CreAim
- Portaal & IDSP
- Authenticatie en Autorisatie
- De SBR Assurance oplossing
- Impact op software ontwikkelaars
- CreAim kan helpen

- ✧ In het kader van het zetten van de XML signature vormen de onderstaande uitgangspunten de basis, aangezien dit best practices of reeds vastgelegde keuzes zijn:
 - ✧ Gebruik van een X.509 NBA beroepscertificaat
 - ✧ Gebruik van een externally detached XML signature
 - ✧ Gebruik van de XAdES standaard
 - ✧ Gebruik van een RSA algoritme met modulus lengte 2048
 - ✧ Gebruik van (minimaal) SHA-256 versleuteling
 - ✧ Gebruik van de canoncalization methode c14n of ext-c14n



CREAIM Waarmerken van de Jaarverantwoording

- Introductie CreAim
- Portaal & IDSP
- Authenticatie en Autorisatie
- De SBR Assurance oplossing
- Impact op software ontwikkelaars
- CreAim kan helpen

❧ Subset bepalen met Xpath

- ❧ Bepalen welke elementen van de Jaarverantwoording gewaarmerkt moeten worden.
- ❧ Twee logische methodes voor Xpath query
 - ❧ Uitsluiten *DocumenAdoption*-elementen
 - ❧ Uitgebreider excluden
 - ❧ Toevoegen ID's aan instance

Waarmerken Jaarverantwoording

- Introductie CreAim
- Portaal & IDSP
- Authenticatie en Autorisatie
- De SBR Assurance oplossing
- Impact op software ontwikkelaars
- CreAim kan helpen

❧ Exclusive XML Canonicalization (C14N)

- ❧ Het document wordt gecodeerd in UTF-8
- ❧ Linebreak normalisatie naar #xA voor het parsen
- ❧ Attribuut waarden worden genormaliseerd
- ❧ Karakters en entiteit referenties worden vervangen
- ❧ CDATA secties worden vervangen door hun karakter inhoud
- ❧ XML declaratie wordt verwijderd
- ❧ Lege elementen worden geconverteerd naar begin en eind elementparen
- ❧ Witruimte buiten en tussen de begin en eind tags wordt genormaliseerd
- ❧ Witruimte in de inhoud is behouden
- ❧ Attribuut waardes worden ontsloten met dubbel quotes
- ❧ Speciale tekens in attributen en elementen worden vervangen door karakter referenties
- ❧ Overbodige namespace declaraties worden verwijderd
- ❧ Standaard attributen worden toegevoegd aan ieder element
- ❧ Lexicografische volgorde wordt opgelegd aan de namespace declaraties en eigenschappen van elk element

Waarmerken Jaarverantwoording

- Introductie CreAim
- Portaal & IDSP
- Authenticatie en Autorisatie
- De SBR Assurance oplossing
- Impact op software ontwikkelaars
- CreAim kan helpen

❧ Berekenen hash waarde (SHA2)

- ❧ Het doel van deze algoritmen is het berekenen van een verkorte versie van een reeks tekens, een "samenvatting" (Engels: digest), die met een hoge mate van waarschijnlijkheid uniek is voor een gegeven tekenreeks, de "boodschap" (Engels: message)

Voorbeeld SHA256 hash als HEX waarde:

3c7ec5c87c6a88cc9324279d5b71f5a4e0cc0fda27486e650e6382d753bb480f

Waarmerken Jaarverantwoording

- Introductie CreAim
- Portaal & IDSP
- Authenticatie en Autorisatie
- De SBR Assurance oplossing
- Impact op software ontwikkelaars
- CreAim kan helpen

❧ Berekenen hash waarde (SHA2)

- ❧ Het doel van deze algoritmen is het berekenen van een verkorte versie van een reeks tekens, een "samenvatting" (Engels: digest), die met een hoge mate van waarschijnlijkheid uniek is voor een gegeven tekenreeks, de "boodschap" (Engels: message)

Voorbeeld SHA256 hash als HEX waarde:

3c7ec5c87c6a88cc9324279d5b71f5a4e0cc0fda27486e650e6382d753bb480f

Opnemen hash waarde/functie in verklaring

- Introductie CreAim
- Portaal & IDSP
- Authenticatie en Autorisatie
- De SBR Assurance oplossing
- Impact op software ontwikkelaars
- CreAim kan helpen

✧ nba-i:HashFunctionType

- ✧ Geeft aan welke hash functie is gebruikt voor het waarmerken van de Jaarverantwoording

Jaarverantwoording:

```
<nba-i:HashFunctionType>SHA2</nba-i:HashFunctionType>
```

NBA taxonomie:

```
<xs:complexType name="hashFunctionItemType">  
  <xs:simpleContent>  
    <xs:restriction base="xbrli:stringItemType">  
      <xs:enumeration id="nba-codes_SHA2" value="SHA2"/>  
    </xs:restriction>  
  </xs:simpleContent>  
</xs:complexType>
```

Opnemen hash waarde/functie in verklaring

- Introductie CreAim
- Portaal & IDSP
- Authenticatie en Autorisatie
- De SBR Assurance oplossing
- Impact op software ontwikkelaars
- CreAim kan helpen

✂ nba-i:HashValueSubjectMatter

- ✂ Bevat de hexidecimale representatie van de waarde die uit de hashfunctie gekomen is. Dit is een samenvatting/digest van de Jaarverantwoording

Jaarverantwoording:

<nba-i:HashValueSubjectMatter>

159DE7570F85A0BE19375E2F4AFDAB0F20C1DBB6

</nba-i:HashValueSubjectMatter>

Ondertekenen Accountantsverklaring

- Introductie CreAim
- Portaal & IDSP
- Authenticatie en Autorisatie
- De SBR Assurance oplossing
- Impact op software ontwikkelaars
- CreAim kan helpen

☞ Canonicalization

- ☞ Dit is dezelfde methode om te normaliseren als in de vorige stap bij de Jaarverantwoording

- Introductie CreAim
- Portaal & IDSP
- Authenticatie en Autorisatie
- De SBR Assurance oplossing
- Impact op software ontwikkelaars
- CreAim kan helpen

✎ XMLDSig

- ✎ XMLDSig beschrijft een methode om XML documenten te voorzien van een digitale handtekening. Deze standaard is gedefinieerd in de W3C recommendation XML Signature Syntax and Processing standaard.

Het uiterlijk van een XMLDSig ondertekening

```
<Signature>
  <SignedInfo>
    <CanonicalizationMethod />
    <SignatureMethod />
    <Reference>
      <Transforms>
        <DigestMethod>
          <DigestValue>
        </DigestMethod>
      </Transforms>
    </Reference>
  </SignedInfo>
  <SignatureValue />
  <KeyInfo />
  <Object />
</Signature>
```

XAdES detached signature

- Introductie CreAim
- Portaal & IDSP
- Authenticatie en Autorisatie
- De SBR Assurance oplossing
- Impact op software ontwikkelaars
- CreAim kan helpen

✂ XAdES (XML Advanced Electronic Signatures) is een set van extensies op de XMLDSig standaard welke deze standaard geschikt maakt voor geavanceerde elektronische handtekeningen

XAdES detached signature (Basis)

- Introductie CreAim
- Portaal & IDSP
- Authenticatie en Autorisatie
- De SBR Assurance oplossing
- Impact op software ontwikkelaars
- CreAim kan helpen

∞ De basis ziet er uit als een XMLDSig handtekening:

```
<Signature>
  <SignedInfo>
    <CanonicalizationMethod />
    <SignatureMethod />
    <Reference>
      <Transforms>
        <DigestMethod>
          <DigestValue>
        </DigestValue>
      </Transforms>
    </Reference>
    <Reference />
  </SignedInfo>
  <SignatureValue />
  <KeyInfo />
  <Object />
</Signature>
```

∞ De inhoud van het **<SignedInfo>** element op volgende slide >>>

XAdES detached signature <SignedInfo>

- Introductie CreAim
- Portaal & IDSP
- Authenticatie en Autorisatie
- De SBR Assurance oplossing
- Impact op software ontwikkelaars
- CreAim kan helpen

☞ Het SignedInfo element:

<SignedInfo>

<Reference>

<Transforms>

<Transform>xpath</Transform>

</Transforms>

<DigestMethod/>

<DigestValue/>

</Reference>

</SignedInfo>

☞ Het <Transform> element bevat de Xpath query die de subset van het document selecteerd.

XAdES detached signature (Basis)

- Introductie CreAim
- Portaal & IDSP
- Authenticatie en Autorisatie
- De SBR Assurance oplossing
- Impact op software ontwikkelaars
- CreAim kan helpen

☞ Terug naar de basis

```
<Signature>
  <SignedInfo>
    <CanonicalizationMethod />
    <SignatureMethod />
    <Reference>
      <Transforms>
        <DigestMethod>
          <DigestValue>
        </DigestValue>
      </Transforms>
    </Reference>
  </SignedInfo>
  <SignatureValue />
  <KeyInfo />
  <Object />
</Signature>
```

☞ De inhoud van het **<Object>** element op volgende slide >>>

XAdES detached signature <Object>

- Introductie CreAim
- Portaal & IDSP
- Authenticatie en Autorisatie
- De SBR Assurance oplossing
- Impact op software ontwikkelaars
- CreAim kan helpen

☞ Het Object element:

<Object>

<QualifyingProperties>

<SignedProperties>

<SignedSignatureProperties/>

<SignedDataObjectProperties/>

</SignedProperties>

</QualifyingProperties>

</Object>

☞ De inhoud van het <SignedDataObjectProperties> element op volgende slide >>>

XAdES detached signature <SignedDataObjectProperties>

- Introductie CreAim
- Portaal & IDSP
- Authenticatie en Autorisatie
- De SBR Assurance oplossing
- Impact op software ontwikkelaars
- CreAim kan helpen

☞ Het SignedDataObjectProperties element:

```
<SignedDataObjectProperties>
  <DataObjectFormat>
    <Description/>
    <ObjectIdentifier>
      <Identifier>#naam</Identifier>
    </ObjectIdentifier>
    <MimeType/>
    <Encoding/>
  </DataObjectFormat>
  <CommitmentTypeIndication>
    <CommitmentTypeId>
      <Identifier>#naam</Identifier>
    </CommitmentTypeId>
    <ObjectReference/>
  </CommitmentTypeIndication>
</SignedDataObjectProperties>
```

Aanleverservice

- Introductie CreAim
- Portaal & IDSP
- Authenticatie en Autorisatie
- De SBR Assurance oplossing
- Impact op software ontwikkelaars
- CreAim kan helpen

- ❧ WUS voor bedrijven v1.2 aanlevering
 - ❧ Verzenden
 - ❧ Ophalen statusinformatie
- ❧ Bijlagen worden verplicht
 - ❧ 1x XBRL > Accountantsverklaring
 - ❧ 1x XML > Detached Signature



CreAim kan helpen

- Introductie CreAim
- Portaal & IDSP
- Authenticatie en Autorisatie
- De SBR Assurance oplossing
- Impact op software ontwikkelaars
- CreAim kan helpen

☞ Wat kunnen wij leveren:

- ☞ Viewer (rendertool)
- ☞ PKIoverheid certificaten
- ☞ Ondertekendienst/linking & signing tool
- ☞ Digipoort Connector 2.0

☞ Voor meer informatie:

- ☞ Frank Jonker
- ☞ info@creaim.nl
- ☞ 075-6312709