

Pushing IT forward!

Anforderungen des eANV an die komplexe Infrastruktur von Otto Dörner

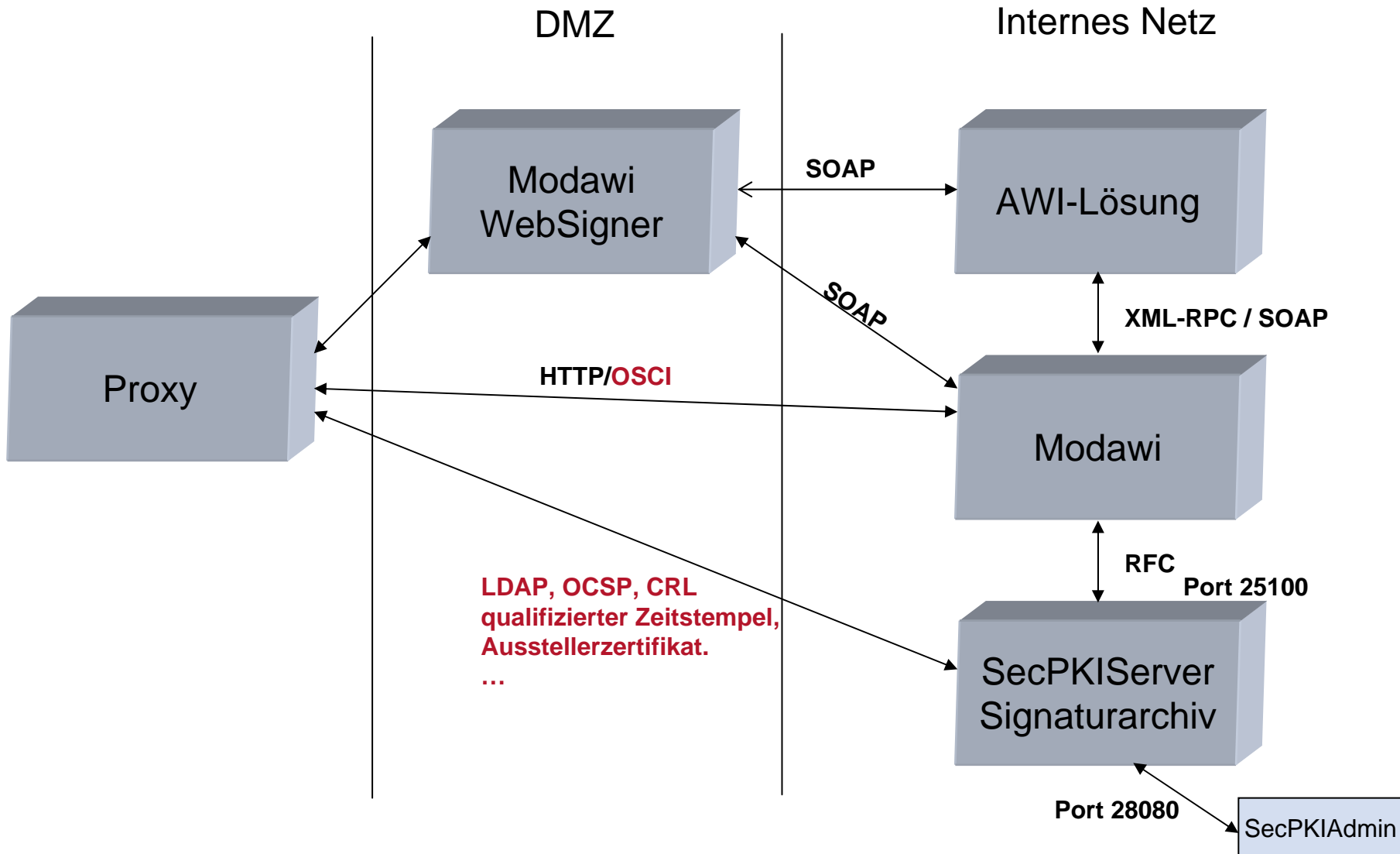


24.02.2010, Modawi Infotag, Matthias Bauer

- eANV im Unternehmensnetz
 - Ports und Protokolle
 - Neue Begrifflichkeiten
 - Signaturprüfung / Zertifikatsprüfung
- Signatur im BMU-Dokument – Technische Darstellung
 - Layertechnik – Was unterschreibe ich wirklich?

- Proxy
- OSCI – Online Service Computer Interface
- vertrauenswürdiges Ausstellerzertifikat
- OCSP – Online Certificate Status Protocol
- LDAP – Lightweight Directory Access Protocol
- CRL – Certificate Revocation List
- Qualifizierter Zeitstempel / Signaturarchiv / Beweiskrafterhaltung

eANV-Netzwerkdarstellung am Beispiel Otto Dörner

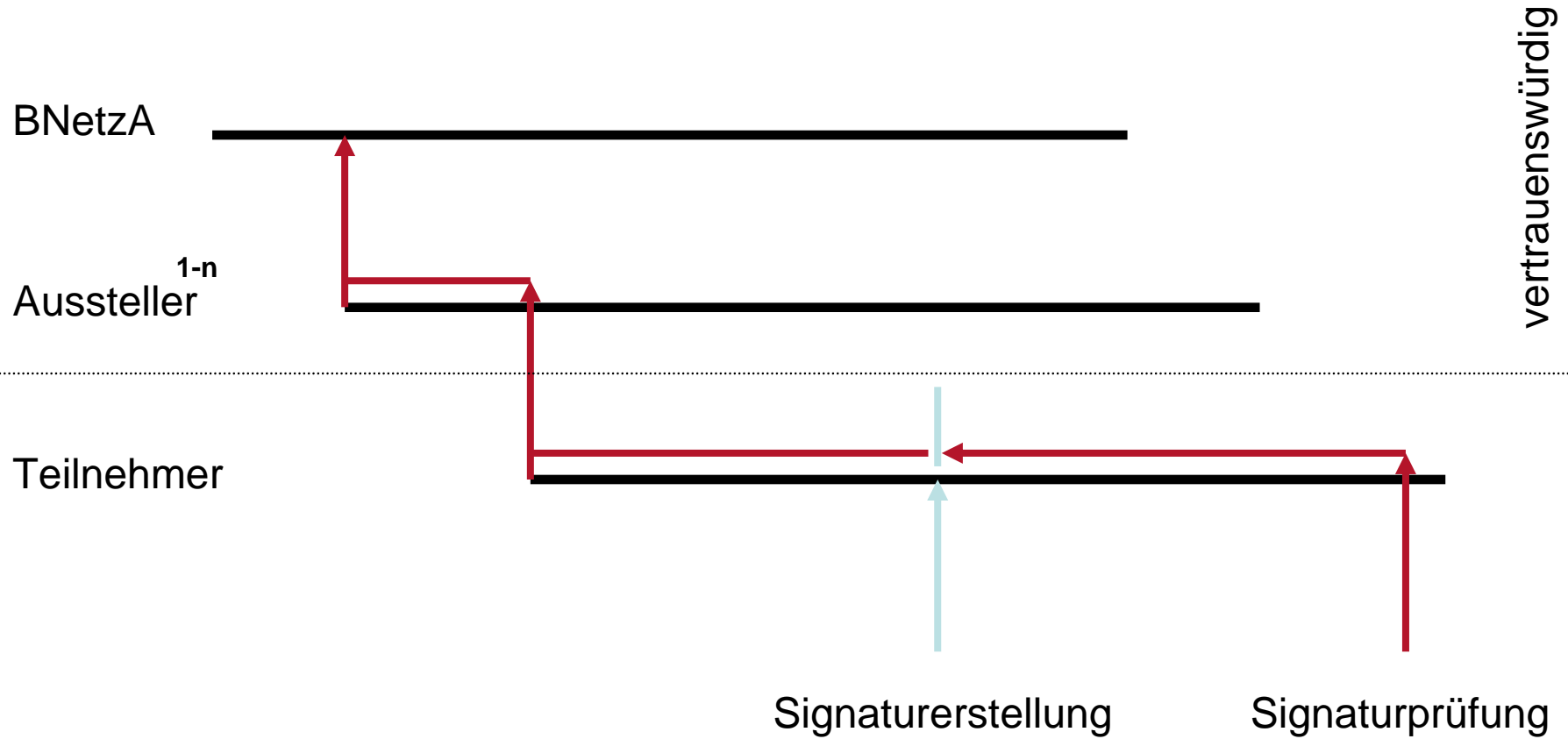


- Proxy 
 - Vermittler zwischen zwei Netzwerken
- OSCI – Online Service Computer Interface 
 - Kommunikationsprotokoll des eGovernment 2.0
- vertrauenswürdiges Ausstellerzertifikat
- OCSP – Online Certificate Status Protocol
- LDAP – Lightweight Directory Access Protocol
- CRL – Certificate Revocation List
- Qualifizierter Zeitstempel / Signaturarchiv / Beweiskrafterhaltung

Voraussetzungen für eine QES nach SigG - Auszug

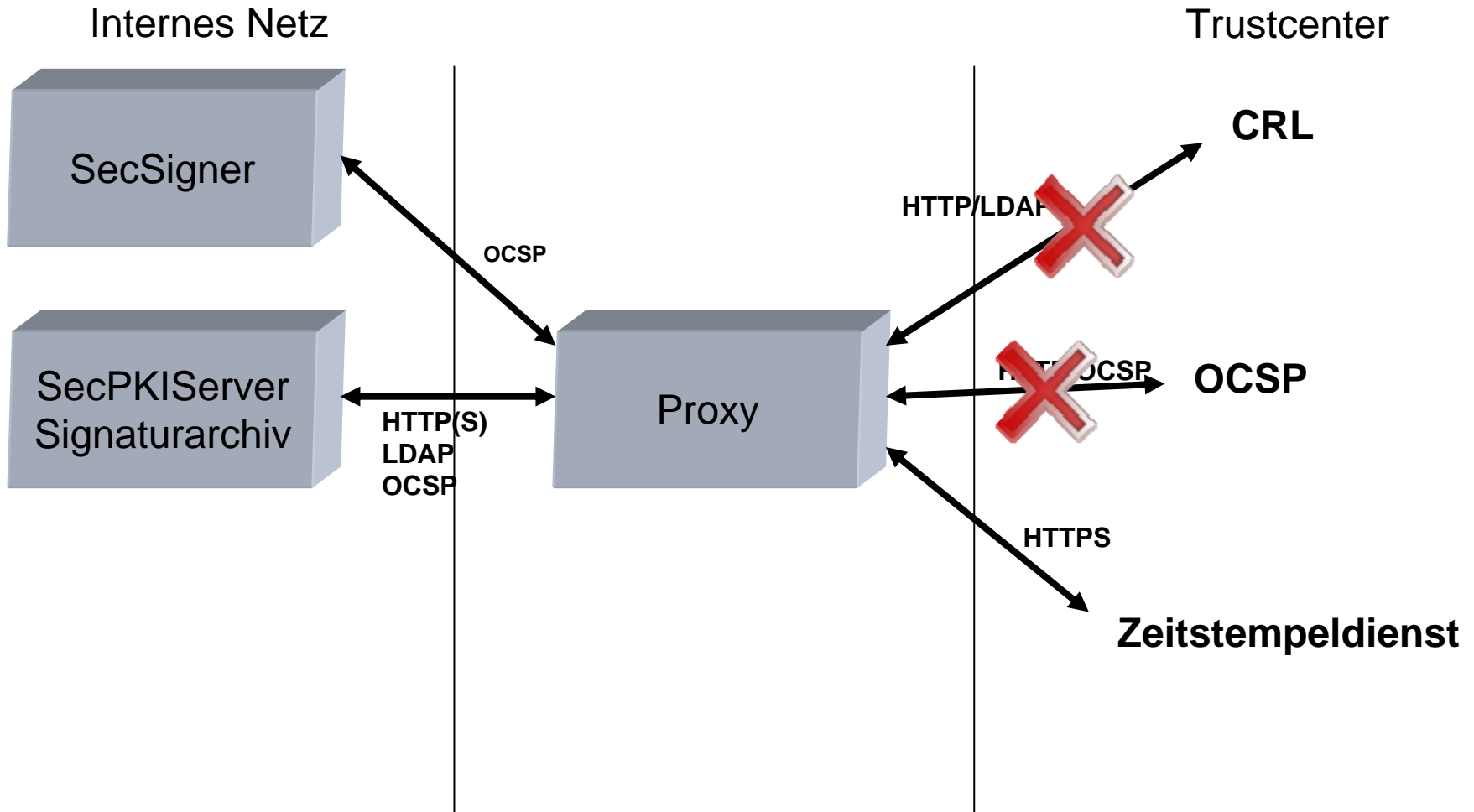
- Qualifizierte Signatur gemäß SigG:
 - muss auf einem zum Zeitpunkt der Signatur gültigen Zertifikat beruhen
- ➔ Signaturzeitpunkt muss ermittelbar sein
- ➔ Zertifikat muss zum Signaturzeitpunkt gültig sein / gewesen sein - Zertifikatsprüfung

Verfahren der Zertifikatsprüfung



- Proxy ✓
 - Vermittler zwischen zwei Netzwerken
- OSCI – Online Service Computer Interface ✓
 - Kommunikationsprotokoll des eGovernment 2.0
- vertrauenswürdigen Ausstellerzertifikat ✓
- OCSP – Online Certificate Status Protocol
- LDAP – Lightweight Directory Access Protocol
- CRL – Certificate Revocation List
- Qualifizierter Zeitstempel / Signaturarchiv / Beweiskrafterhaltung

Die SAK und die Aussenwelt

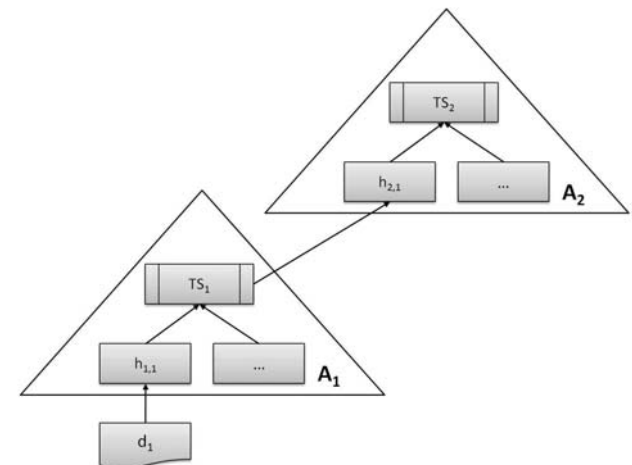


■ BSI bestimmt den Gültigkeitszeitraum der kryptographischen Algorithmen auf denen die Signatur beruht

„wenn diese für längere Zeit in signierter Form benötigt werden, als die für ihre Erzeugung und Prüfung eingesetzten Algorithmen und zugehörigen Parameter als geeignet beurteilt sind. In diesem Falle sind die Daten vor dem Zeitpunkt des Ablaufs der Eignung der Algorithmen oder der zugehörigen Parameter mit einer neuen qualifizierten elektronischen Signatur zu versehen. Diese muss mit geeigneten neuen Algorithmen oder zugehörigen Parametern erfolgen, frühere Signaturen einschließen und einen qualifizierten Zeitstempel tragen.“ §17 SigV

■ Beweiskrafterhaltung einer Signatur nach Ablauf der Gültigkeit der Algorithmen mittels:

- Übersignatur/Beweiskrafterhaltung
 - ArchiSig – Konzept
- Qualifiziertem Zeitstempel



- Proxy ✓
 - Vermittler zwischen zwei Netzwerken
- OSCI – Online Service Computer Interface ✓
 - Kommunikationsprotokoll des eGovernment 2.0
- vertrauenswürdiges Ausstellerzertifikat ✓
- OCSP – Online Certificate Status Protocol ✓
 - Online Statusabfrage von Zertifikaten
- LDAP – Lightweight Directory Access Protocol ✓
- CRL – Certificate Revocation List ✓
 - Zertifikats-Sperlliste
- Qualifizierter Zeitstempel / Signaturarchiv / Beweiskrafterhaltung ✓
 - „Vom Trustcenter bestätigte Uhrzeit“

Signatur um BMU-Dokument – Technische Darstellung

Ausserhalb eANV

```
<Dokument>
  <Datensatz1>
    <Signatur1>
  </Datensatz1>
  <Datensatz2>
    <Signatur2>
  </Datensatz2>
</Dokument>
```

eANV

```
<BGSDokument>
  <ENTLayer>
    <BEFLayer>
      <ERZLayer>
        <Daten>
          <SignaturERZ>
        </ERZLayer>
      <Daten>
        <SignaturBEF>
      </BEFLayer>
    <Daten>
      </SignaturENT>
    </ENTLayer>
  </BGSDokument>
```

Signatur um BMU-Dokument – Technische Darstellung

BGS

```
<BGSDokument>  
  <ENTLayer>  
    <BEFLayer>  
      <ERZLayer>  
        <Daten>  
          <SignaturERZ>  
        </ERZLayer>  
      <Daten>  
        <SignaturBEF>  
      </BEFLayer>  
    <Daten>  
      </SignaturENT>  
    </ENTLayer>  
  
</BGSDokument>
```

EGF

```
<EGFDokument>  
  
  <Bevollmächtigung>  
    <Signatur1>  
  </Bevollmächtigung>  
  <Beauftragung>  
    <Signatur2>  
  </Beauftragung>  
  <SignaturERZ>  
  <SignaturBEH>  
  
</EGFDokument>
```

Layertechnik – Was unterschreibe ich wirklich?

- Technisch gesehen unterschreibt jeder den Inhalt seines Layers

Durch die inkrementiell wachsende Layertechnik:

- ➔ der BEF unterschreibt den Inhalt des ERZLayers mit
- ➔ der ENT unterschreibt den Inhalt des BEFLayers und des ERZLayers mit

Pushing IT forward!

CONSIST
Business Information Technology

Herzlichen Dank für Ihre Aufmerksamkeit!

Haben Sie Fragen?

CONSIST