Signatur-Workshop

Neue Signaturformate und ausländische Zertifikate in MOA-SPSS

Klaus Stranacher

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

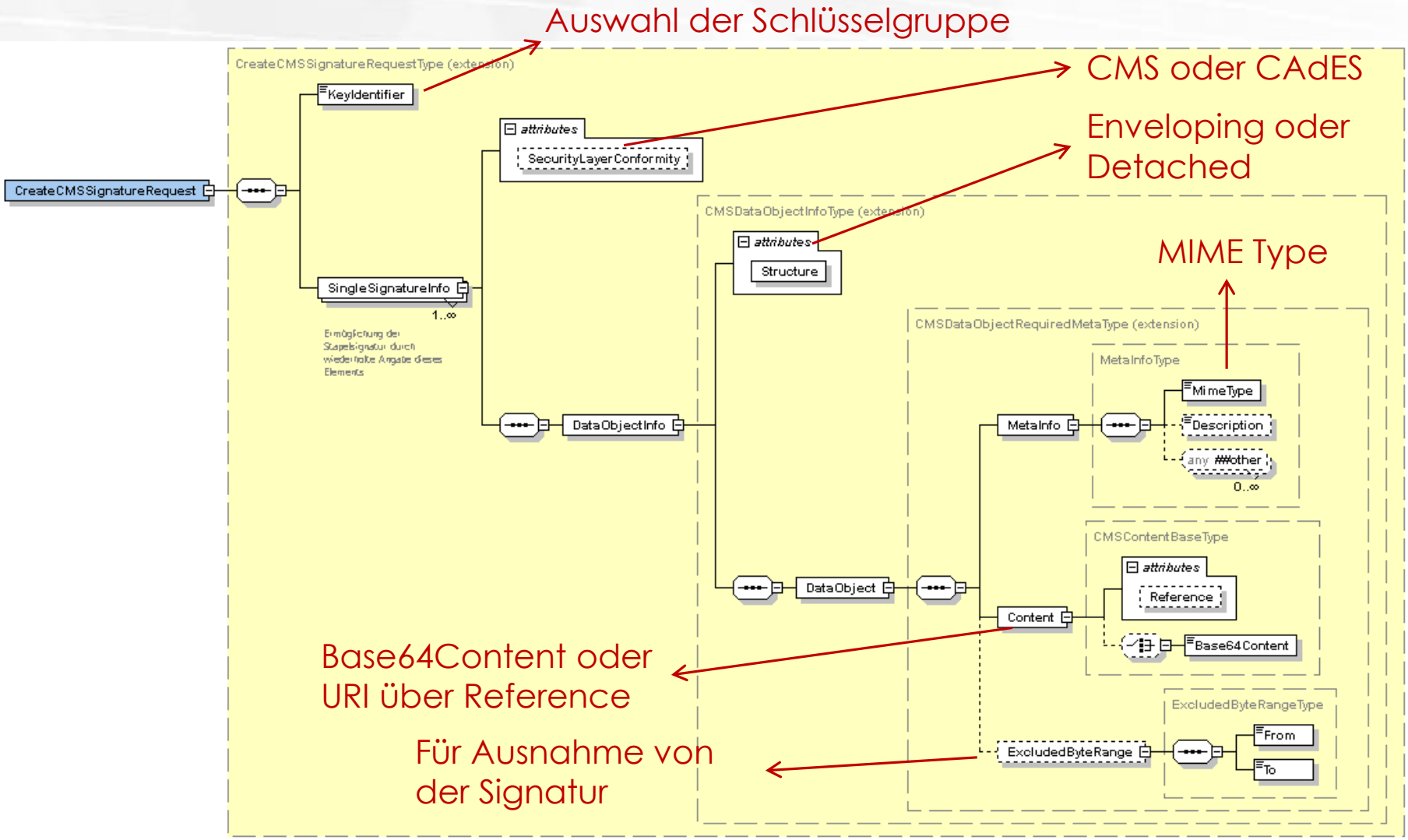
Überblick

- MOA-SS
  - Neue Signaturformate
    - CAdES: CreateCMSSignatureRequest
    - XAdES: Konfiguration
  - Beispiel
- MOA-SP
  - Ausländische Zertifikate in MOA-SP
    - Warum notwendig?
    - Trust-service Status List (TSL)
    - Integration von TSLs in MOA-SP
    - Konfiguration
  - Beispiel

MOA-SS

- CAdES:
  - Neuer `<CreateCMSSignatureRequest>`
    - Basierend auf Security Layer Neu
  - CMS oder CAdES möglich (über Attribut `SecurityLayerConformity` steuerbar)
  - Keine CAdES-spezifische Konfiguration notwendig
  - Verifikation bisher schon möglich über `<VerifyCMSSignatureRequest>`

CreateCMSSignaturRequest



CAdES Beispiel-Request/Response

```
<CreateCMSSignatureRequest xmlns="http://reference.e-government.gv.at/namespace/moa/20020822#">
  <KeyIdentifier>KG_allgemein</KeyIdentifier>
  <SingleSignatureInfo SecurityLayerConformity="true">
    <DataObjectInfo Structure="enveloping">
      <DataObject>
        <MetaInfo>
          <MimeType>text/plain</MimeType>
        </MetaInfo>
        <Content>
          <Base64Content>RGFzIGlzdCBlaW4gQmVpc3BpZWx0ZXh0Lg==</Base64Content>
        </Content>
      </DataObject>
    </DataObjectInfo>
  </SingleSignatureInfo>
</CreateCMSSignatureRequest>
```

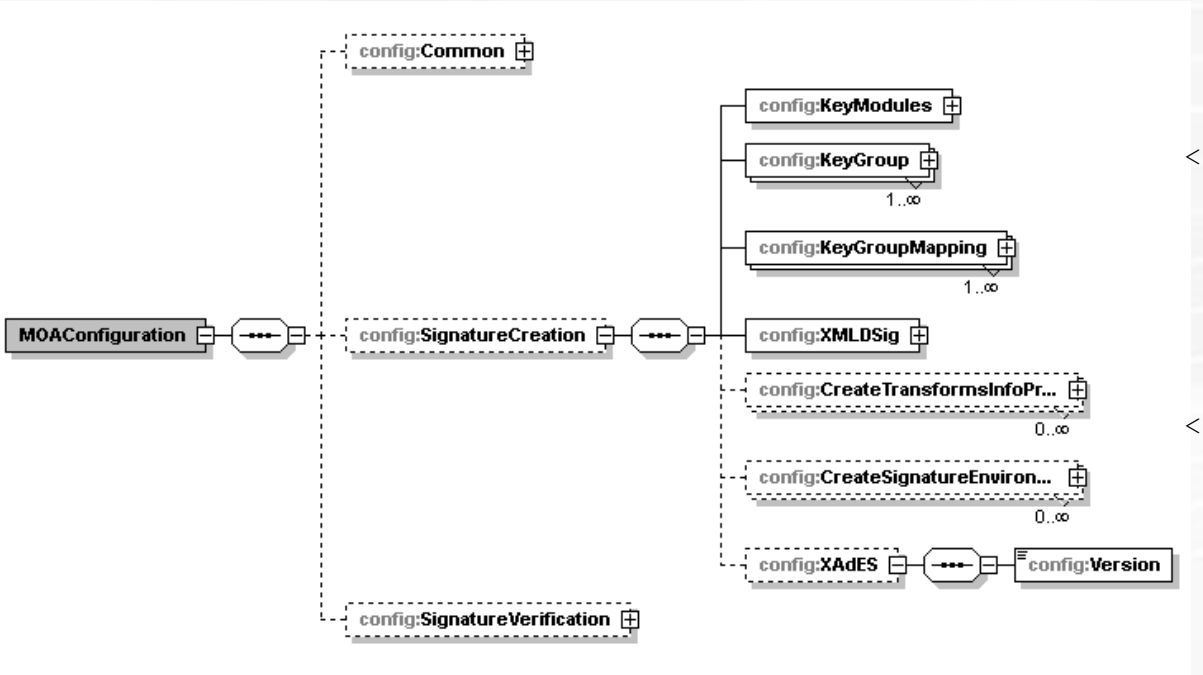
```
<CreateCMSSignatureResponse xmlns="http://reference.e-government.gv.at/namespace/moa/20020822#">
  <CMSSignature>MIAGCSqGSIb3DQEHAqCAMIACAQExDTALBglghkgBZQMEAgMwgAYJKoZIhvcNAQcB
oIAkgAQBRAQBYQQBcwQBIAQBaQQBcwQBdAQBIAQBZQQBaQQBbgQBIAQBQgQBZQQBaQQBcwQBcAQBaQQBZQQBbAQBdAQBZQQBeAQBdAQBLgAAAAAAAKwggQrMIID
lKADAgECAgZjq1d98CYwDQYJKoZIhvcNAQEFBQAwQDEiMCAGA1UEAxMZSUFJSyBUZXN0IEludGVybWVkaWF0ZSBDQTENMAsGA1UEChMESUFJSzELMAEBhMCQVQw
[...]
CwYJYIZIAWUDBAIDoIIBXDAWBgYEAI1FAgExDAwKdGV4dC9wbGFpbjAYBgkqhkiG9w0BCQMxCwYJKoZIhvcNAQcBMBwGCSqGSIb3DQEJBTEPFw0xMzxMzE1MzVa
ME8GCSqGSIb3DQEJBDFCBEARQZLBFtFyOdsapeHhnc/QUEs4pI9yAxPZQSS3SGHvfEceS78doiGsBlm4gJb5nU8osGANq2uNH2WTmoDzrLxlMIG4BgG9w0BCRAC
LzGBqDCBpTCBojCBnzALBglghkgBZQMEAgMEQHEQSWwiCtIPwqCdmTzy6iaKpYQS9agy59B7ryXvPX+phff1ouUPZKGkeiWQj4Qzkm65YzrvwIAl2Q8qbwwTjBE
pEIwQDEiMCAGA1UEAxMZSUFJSyBUZXN0IEludGVybWVkaWF0ZSBDQTENMAsGA1UEChMESUFJSzELMAkGA1UEBhMCQVQCBmOrV33wJjALBgkqhkiG9wEggEAcddc
Sd4WJHeak6aPU7VfwYynjJtSN1ec/qF6aWSshGRWzFZagKKEAj8CVEdJI7429IlH2Fgp349YMa1SZaZCuloe4ljdsLBGVdvmV5tYIC3AnQUY483MiUhye4mlhWd
MWWzgU6kg3xIYQe0FQepWKm4O+s7VM0Jks7T68LvXPmYLhkJD7DDGCK5ZDDWvjijLY/ncfrK0ayysR2GneLBDZiZ6cTV7rSPTrq3XCmtFAdxra8vQU1GWT5HsAQ
OXZXfEN7Y8U1kvm8E/eiEhHa9o5fuSz9O84DWzTubcML6R9ZovUsK4dcs3EXm/K6rUWH+UQM2AeWbgKe2gAAAAAAAA==</CMSSignature>
</CreateCMSSignatureResponse>
```

MOA-SS

- XAdES:
  - Bisher: MOA-SS erstellt bei `SecurityLayerConformity=true` eine XAdES Version 1.1.1 Signatur
  - Referenzformat aus Kommissions-Entscheidung aber: XAdES Version 1.4.2
  - → Konfigurationselement zur Festlegung der XAdES-Signatur
    - `cfg:SignatureCreation/cfg:XAdES`
  - Der Request bleibt unverändert!
  - Verifikation bisher schon möglich über `<VerifyXMLSignatureRequest>`

MOA-SS

» Konfiguration XAdES-Version




```
<cfg:MOAConfiguration>
  <cfg:SignatureCreation>
    [..]
    <cfg:XAdES>
      <cfg:Version>1.4.2</cfg:Version>
    </cfg:XAdES>
  </cfg:SignatureCreation>
  [...]
</cfg:MOAConfiguration>
```

XAdES 1.4.2 Beispiel-Request

```
<CreateXMLSignatureRequest xmlns="http://reference.e-government.gv.at/namespace/moa/20020822#"
xmlns:dsig="http://www.w3.org/2000/09/xmldsig#">
  <KeyIdentifier>KG_allgemein</KeyIdentifier>
  <SingleSignatureInfo SecurityLayerConformity="true">
    <DataObjectInfo Structure="enveloping">
      <DataObject>
        <XMLContent>Diese Daten werden signiert.</XMLContent>
      </DataObject>
      <CreateTransformsInfoProfile>
        <CreateTransformsInfo>
          <FinalDataMetaInfo>
            <MimeType>text/xml</MimeType>
          </FinalDataMetaInfo>
        </CreateTransformsInfo>
      </CreateTransformsInfoProfile>
    </DataObjectInfo>
  </SingleSignatureInfo>
</CreateXMLSignatureRequest>
```

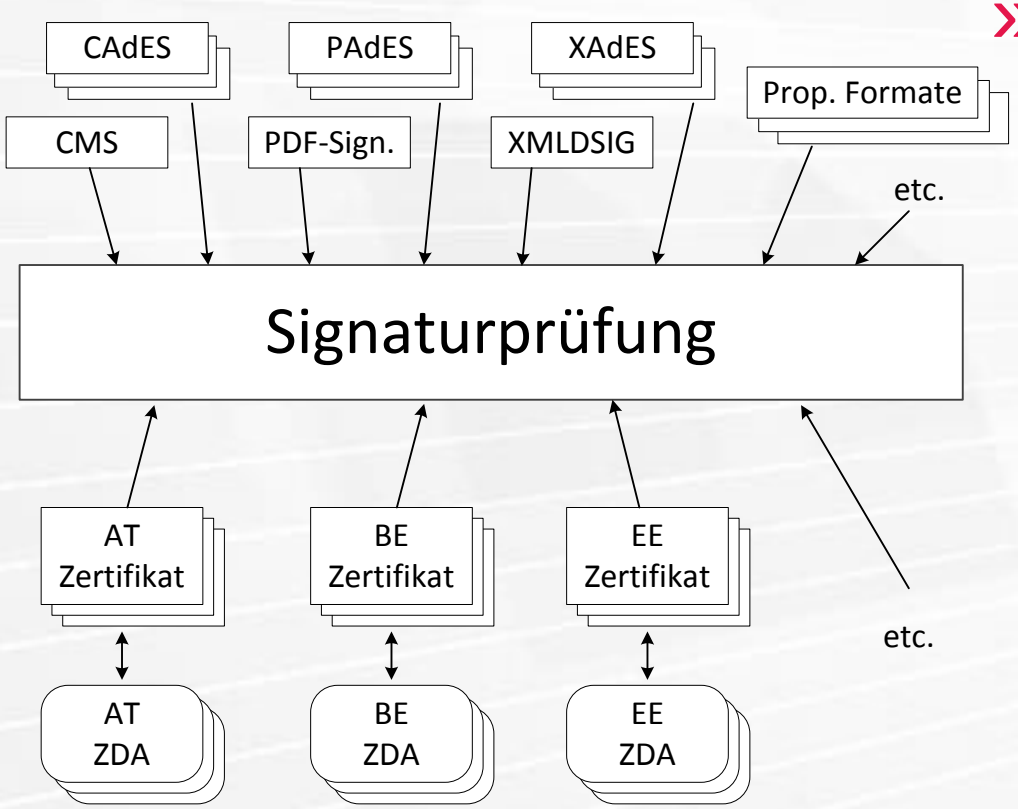
XAdES 1.4.2 Beispiel-Response

```
<CreateXMLSignatureResponse xmlns="http://reference.e-government.gv.at/namespace/moa/20020822#" xmlns:dsig="http://www.w3.org/2000/09/xmldsig#">
  <SignatureEnvironment>
    <dsig:Signature Id="signature-1-1">
      <dsig:SignedInfo>
        <dsig:CanonicalizationMethod Algorithm="http://www.w3.org/TR/2001/REC-xml-c14n-20010315"/>
        <dsig:SignatureMethod Algorithm="http://www.w3.org/2001/04/xmldsig-more#rsa-sha512"/>
        <dsig:Reference Id="reference-1-1" URI="#signed-data-1-1-1">
          <dsig:Transforms>
            <dsig:Transform Algorithm="http://www.w3.org/2002/06/xmldsig-filter2">
  <xf2:XPath Filter="intersect" xmlns:xf2="http://www.w3.org/2002/06/xmldsig-filter2">id('signed-data-1-1-1')/node()</xf2:XPath>
            </dsig:Transform>
          </dsig:Transforms>
          <dsig:DigestMethod Algorithm="http://www.w3.org/2001/04/xmlenc#sha512"/>
          <dsig:DigestValue>GkACyffvS/bnMWub9yKEZl3iuhHk...fJpqwc7uGZ8Mu95Dw==</dsig:DigestValue>
        </dsig:Reference>
        <dsig:Reference Type="http://uri.etsi.org/01903#SignedProperties" URI="#etsi-signed-1-1">
          <dsig:DigestMethod Algorithm="http://www.w3.org/2001/04/xmlenc#sha512"/>
          <dsig:DigestValue>jzgMMtsclCMX7DSOTLn8UKdqkVr2...kGQdPBTJSrXSXGZkg==</dsig:DigestValue>
        </dsig:Reference>
      </dsig:SignedInfo>
      <dsig:SignatureValue>jIizJSZj+TTLSNntTouyykLB7T7tc2...h1p3mgEyKPdOrFN5FaX3AckA==</dsig:SignatureValue>
      <dsig:KeyInfo><dsig:X509Data><dsig:X509Certificate>MIIEKz...T8VGS0wG</dsig:X509Certificate></dsig:X509Data></dsig:KeyInfo>
      <dsig:Object Id="signed-data-1-1-1">Diese Daten werden signiert.</dsig:Object>
      <dsig:Object>
        <etsi:QualifyingProperties Target="#signature-1-1" xmlns:etsi="http://uri.etsi.org/01903/v1.3.2#">
          <etsi:SignedProperties Id="etsi-signed-1-1">
            <etsi:SignedSignatureProperties>
              <etsi:SigningTime>2013-11-26T10:46:27+01:00</etsi:SigningTime>
              <etsi:SigningCertificate><etsi:Cert>
                <etsi:CertDigest>... </etsi:CertDigest>
                <etsi:IssuerSerial>... </etsi:IssuerSerial>
              </etsi:Cert></etsi:SigningCertificate>
              <etsi:SignaturePolicyIdentifier><etsi:SignaturePolicyImplied/></etsi:SignaturePolicyIdentifier>
            </etsi:SignedSignatureProperties>
            <etsi:SignedDataObjectProperties>
              <etsi:DataObjectFormat ObjectReference="#reference-1-1"><etsi:MimeType>text/xml</etsi:MimeType></etsi:DataObjectFormat>
            </etsi:SignedDataObjectProperties>
          </etsi:SignedProperties>
        </etsi:QualifyingProperties>
      </dsig:Object>
    </dsig:Signature>
  </SignatureEnvironment>
</CreateXMLSignatureResponse>
```

Überblick

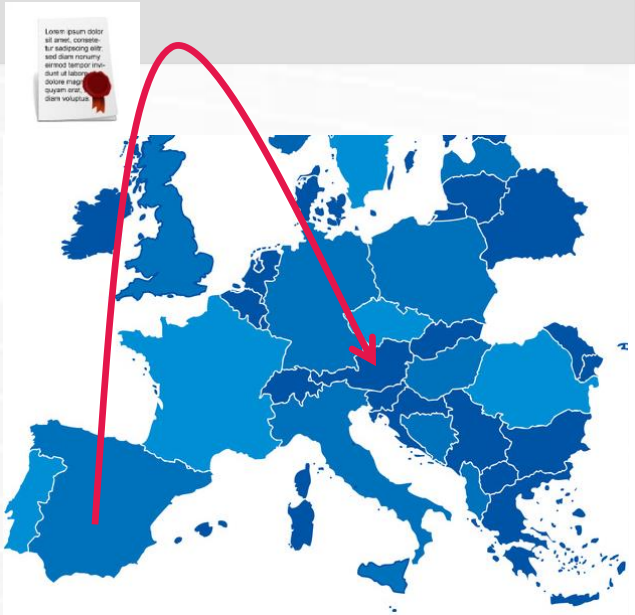
- MOA-SS
  - Neue Signaturformate
    - CAdES
    - XAdES
  - Beispiel
- MOA-SP
  - Ausländische Zertifikate in MOA-SP
    - Warum notwendig?
    - Trust-service Status List (TSL)
    - Integration von TSLs in MOA-SP
    - Konfiguration
  - Beispiel

Signaturverifikation



- Qualifizierte elektronische Signatur =
  - Fortgeschrittene Signatur +
  - Qualifiziertes Zertifikat (QC) +
  - Sichere Signaturerstellungs-einheit (SSCD)

Signaturverifikation



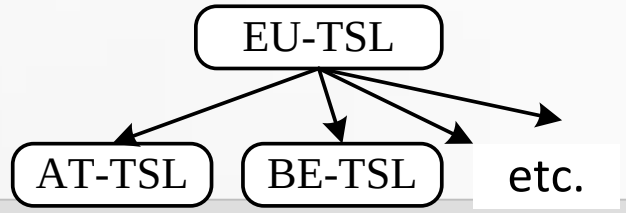
- Grenzüberschreitende Prüfung
  - Wie erkenne ich Befähigung eines ausländischen ZDAs?
- EU Kommissionsentscheidung 2013/662/EU („Trustlisten-Entscheidung“)

Artikel 2

(1) Jeder Mitgliedstaat sorgt entsprechend den im Anhang festgelegten technischen Spezifikationen für die Erstellung, Führung und Veröffentlichung einer „vertrauenswürdigen Liste“, die mindestens Angaben zu den von ihm beaufsichtigten bzw. akkreditierten Zertifizierungsdiensteanbietern enthält, die öffentlich qualifizierte Zertifikate ausstellen.

Trust-service Status Lists

- ETSI Standard (TS 102 231)
- TSL ermöglichen die strukturierte Angabe (XML) von Statusinformationen über Trust-service Provider (TSP) → im Fall von Signaturprüfung ist TSP=ZDA
- Logischer Aufbau
  - Allgemeine Informationen zur TSL
  - Information über den TSP und welche Dienste er anbietet
  - Für jeden Dienst:
    - Information über den momentanen Status (ZDA unter Aufsicht, akkreditiert, Akkreditierung widerrufen, etc.), das entsprechende Zertifikat zum Dienst,…
    - Historische Statusinformationen
  - Signatur von TSL-Aussteller
- Signierte EU-TSL verweist auf nationale signierte TSLs (die beaufsichtigte bzw. akkreditierte ZDA, die qualifizierte Zertifikate ausstellen beinhalten)



Signaturverifikation

```
<tsl:TrustServiceStatusList>
  <tsl:SchemeInformation>
    [...]
    <tsl:SchemeOperatorName>
      <tsl:Name xml:lang="en">Rundfunk und Telekom Regulierungs-GmbH</tsl:Name>
    </tsl:SchemeOperatorName>
    <tsl:SchemeOperatorAddress>...</tsl:SchemeOperatorAddress>
    [...]
  </tsl:SchemeInformation>
  <tsl:TrustServiceProviderList>
    <tsl:TrustServiceProvider>
      <tsl:TSPInformation>
        <tsl:TSPName>
          <tsl:Name xml:lang="en">A-Trust Gesellschaft für Sicherheitssysteme im elektronischen Datenverkehr GmbH</tsl:Name>
        </tsl:TSPName>
        <tsl:TSPAddress>...</tsl:TSPAddress>
        [...]
      </tsl:TSPInformation>
      <tsl:TSPServices>
        [...]
        <tsl:TSPService>
          <tsl:ServiceInformation>
            <tsl:ServiceTypeIdentifier>http://uri.etsi.org/TrstSvc/Svctype/CA/QC</tsl:ServiceTypeIdentifier>
            <tsl:ServiceName><tsl:Name xml:lang="en">a-sign-Premium-Sig-03 (primary system, 1st certificate)</tsl:Name>
            </tsl:ServiceName>
            <tsl:ServiceDigitalIdentity>
              <tsl:DigitalId><tsl:X509Certificate>MIIEgzCCA2u...t+A==</tsl:X509Certificate></tsl:DigitalId>
              <tsl:X509SubjectName>CN=a-sign-Premium-Sig-03,...</tsl:X509SubjectName>
            </tsl:ServiceDigitalIdentity>
            <tsl:ServiceStatus>http://uri.etsi.org/TrstSvc/eSigDir-1999-93-EC-TrustedList/Svcstatus/accredited</tsl:ServiceStatus>
            <tsl:StatusStartingTime>2008-04-28T22:00:00Z</tsl:StatusStartingTime>
          </tsl:ServiceInformation>
        </tsl:TSPService>
      </tsl:TSPServices>
    </tsl:TrustServiceProvider>
  <dsig:Signature>...</dsig:Signature>
</tsl:TrustServiceStatusList>
```

Betreiber der TSL (RTR)

TSP = ZDA (A-Trust)

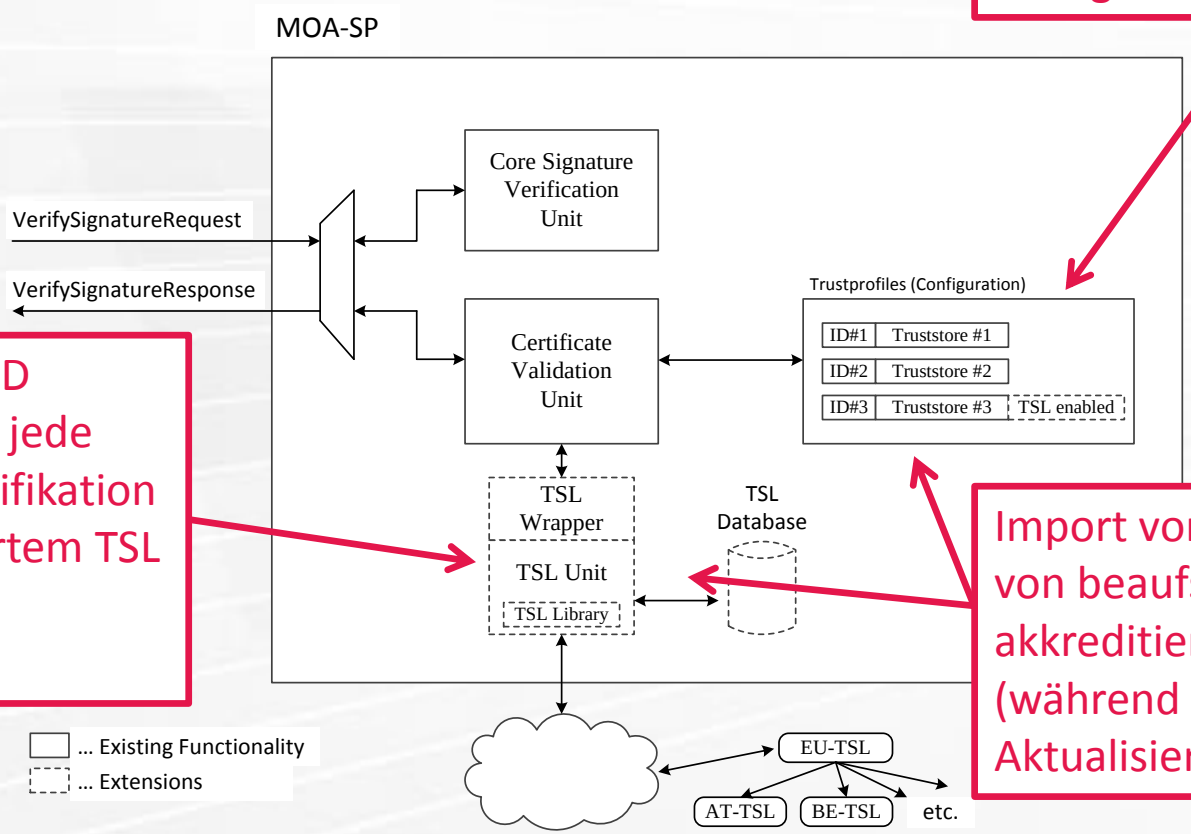
Von A-Trust betriebener Dienst

TSL signiert von RTR

http://www.signatur.rtr.at/currenttsl.xml

Erweiterte Architektur MOA-SP

TSL Support für Trustprofile konfigurierbar

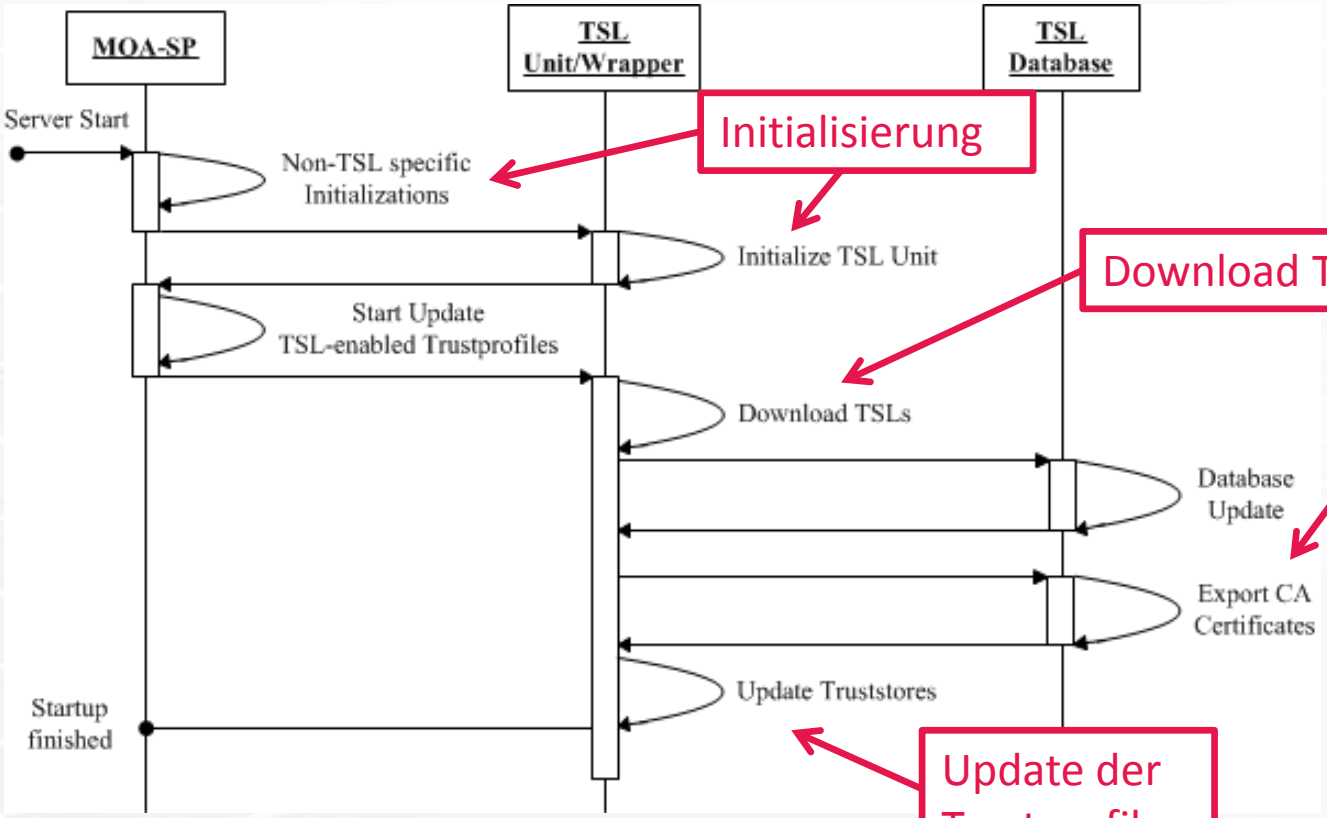


QC und SSCD Prüfung für jede Signaturverifikation (bei aktiviertem TSL Support in Trustprofil)

Import von CA Zertifikaten von beaufsichtigten bzw. akkreditierten ZDAs (während Startup und Aktualisierungen)

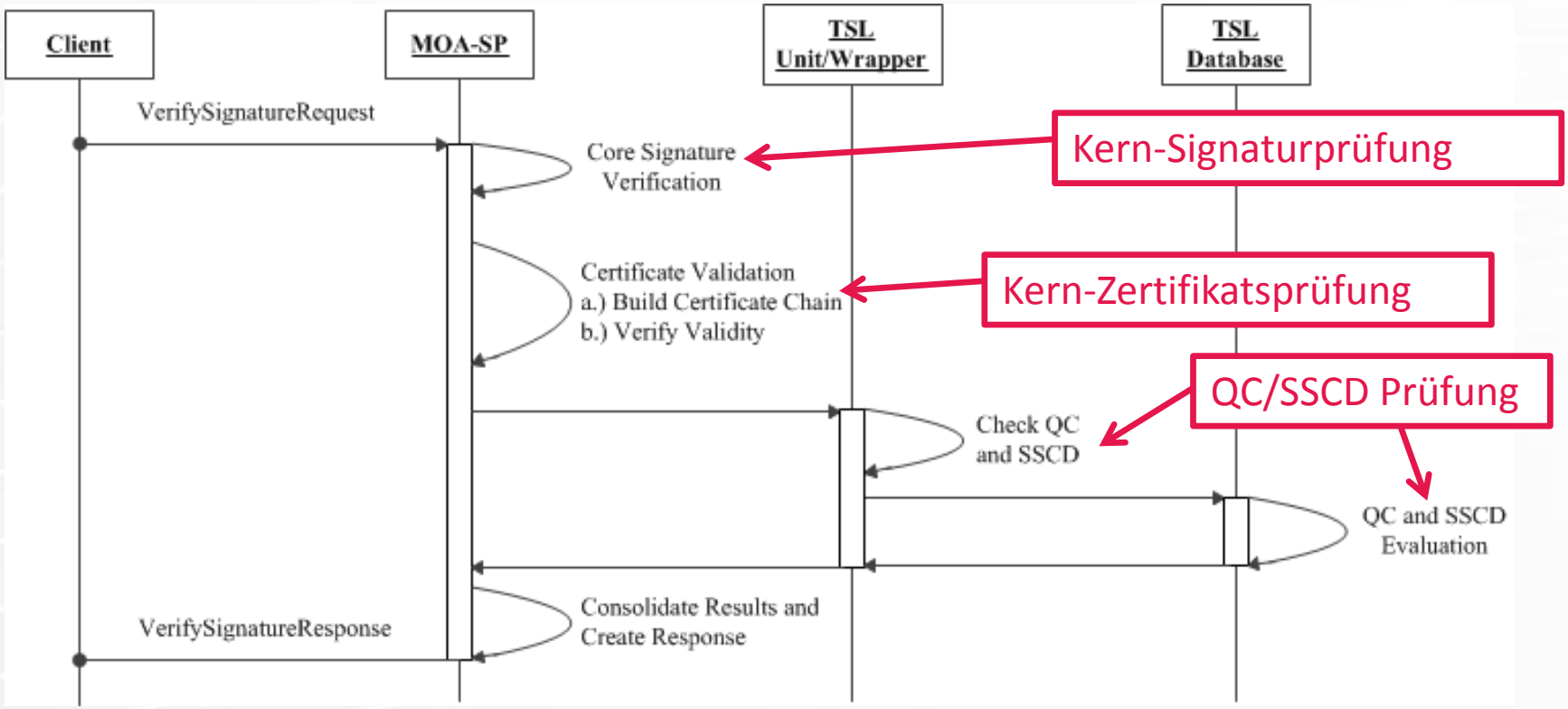
Prozessfluss

» Server-Startup und Aktualisierung



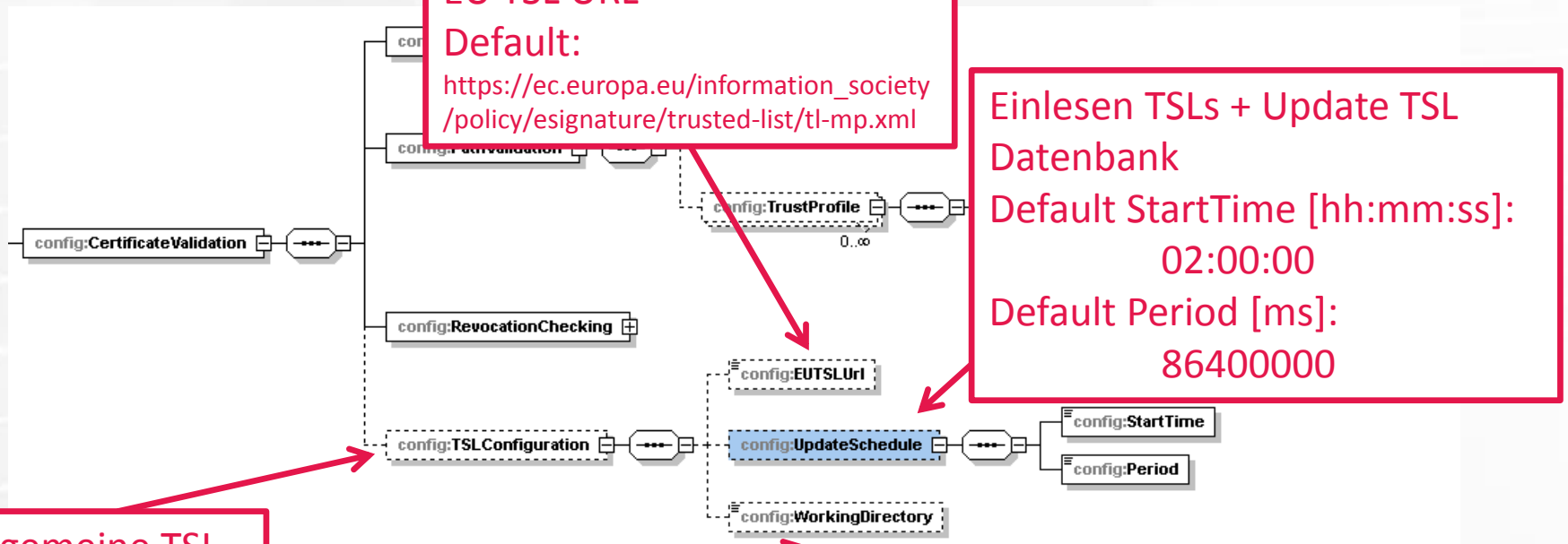
Prozessfluss

» Bei Signaturprüfung



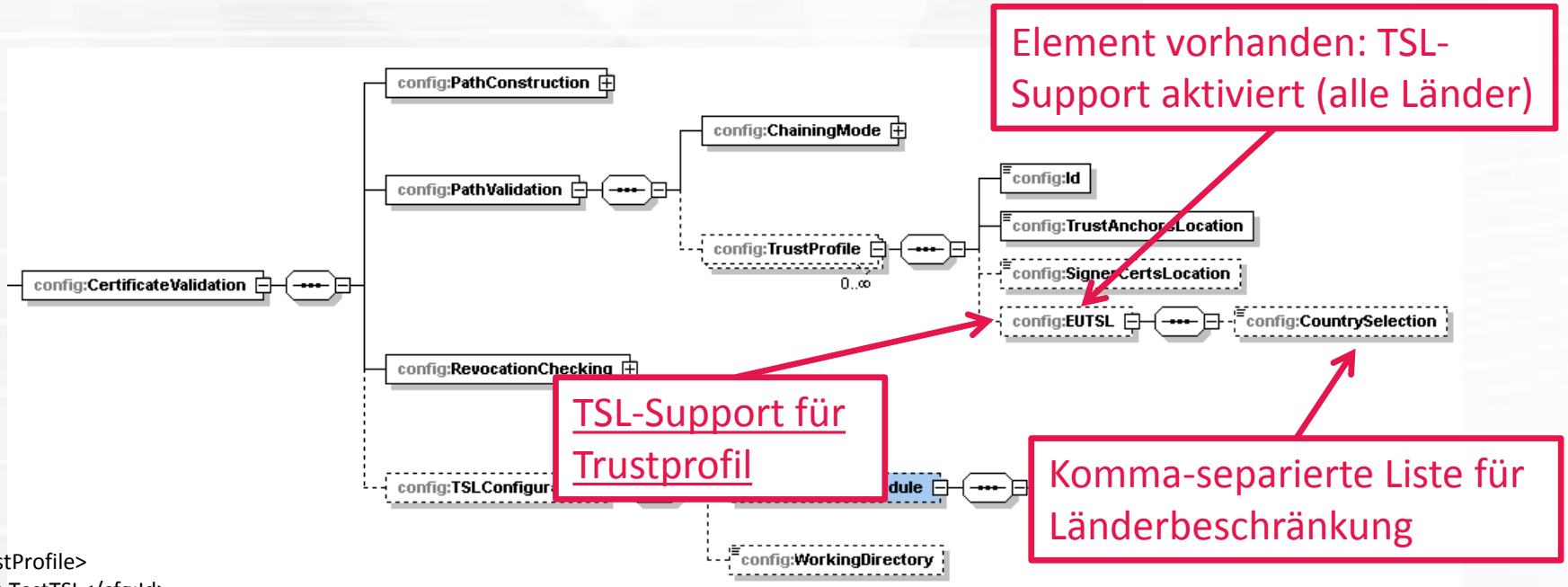
TSL Konfiguration

» Unter `MOAConfiguration/SignatureVerification`



TSL Konfiguration

» Unter `MOAConfiguration/SignatureVerification`




```
<cfg:TrustProfile>
  <cfg:Id>TestTSL</cfg:Id>
  <cfg:TrustAnchorsLocation>trustProfiles/testTSL</cfg:TrustAnchorsLocation>
  <cfg:EUTSL>
    <!--<cfg:CountrySelection>AT,BE</cfg:CountrySelection>-->
  </cfg:EUTSL>
</cfg:TrustProfile>
```

Signaturverifikation

» Beispiel MOA-SP Response

```
<VerifyXMLSignatureResponse>
  <SignerInfo>
    <dsig:X509Data>
      <dsig:X509SubjectName>CN=Klaus Stranacher,C=AT...</dsig:X509SubjectName>
      <dsig:X509IssuerSerial>
        <dsig:X509IssuerName>CN=a-sign-Premium-Sig-02... </dsig:X509IssuerName>
        <dsig:X509SerialNumber>519543</dsig:X509SerialNumber>
      </dsig:X509IssuerSerial>
      <dsig:X509Certificate>MIIEKzCCA5...tNGS0wG</dsig:X509Certificate>
      <QualifiedCertificate Source="TSL" />
      <SecureSignatureCreationDevice Source="Certificate"/>
      <IssuerCountryCode>AT</IssuerCountryCode>
    </dsig:X509Data>
  </SignerInfo>
  <SignatureCheck>
    <Code>0</Code>
  </SignatureCheck>
  [...]
  <CertificateCheck>
    <Code>0</Code>
  </CertificateCheck>
</VerifyXMLSignatureResponse>
```

Informationen zum Signator
Inkl. QC/SSCD/IssuerCountry

Ergebnis kryptographische Prüfung

Ergebnis Zertifikatsprüfung

Zusammenfassung

- Unterstützung der Referenzformate CAdES und XAdES in MOA-SS und SP
- Integration von TSL
  - Für Trustprofile
  - QC und SSCD Prüfung

Vielen Dank für Ihre Aufmerksamkeit!

Klaus Stranacher– klaus.stranacher@egiz.gv.at
www.egiz.gv.at

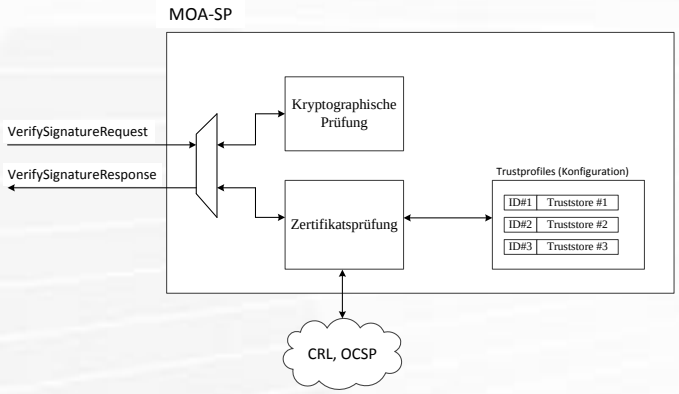
Follow us on Twitter
https://twitter.com/egov_egiz

EGIZ
E-Government Innovationszentrum

Backup Folien

Signaturverifikation

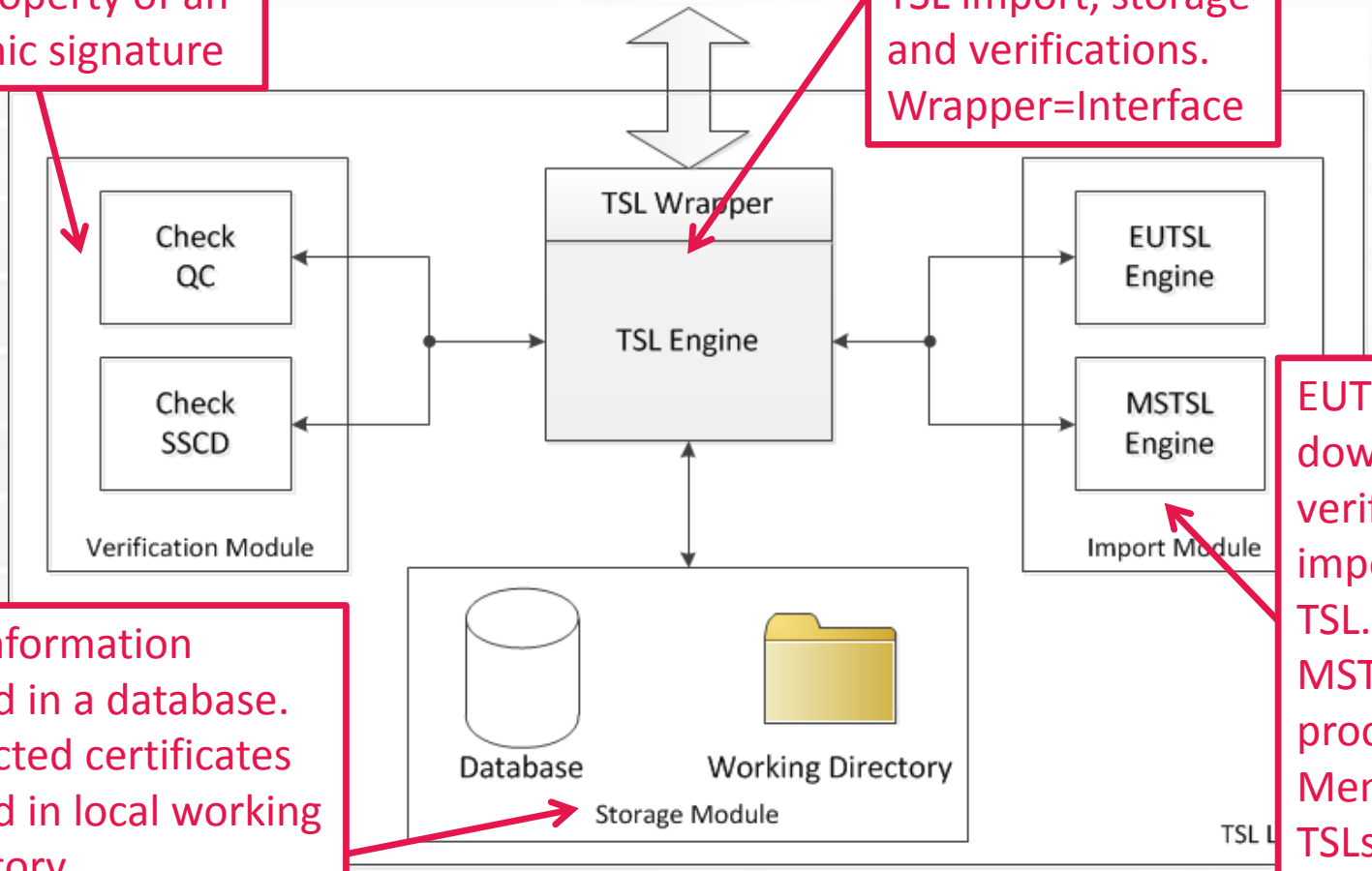
- Kryptographischer Prüfung:
  - Wie gehabt (siehe bspw. XAdES-Verifikation)
- Zertifikatsprüfung:
  - (1) Zertifikatskettenbildung
    - von Signatorzertifikat zu Wurzelzertifikat
  - (2) Für jedes Zertifikat in der Kette:
    - Überprüfung der zeitlichen Gültigkeit
    - Prüfung auf Widerruf via CRL/OCSP
      - CRL: Certificate Revocation List
      - OCSP: Online Certificate Status Protocol
  - (3) Überprüfung ob eines der Zertifikat in der Kette im angegebenen Trustprofil enthalten ist
  - (4) Überprüfung des Signatorzertifikats auf qualifiziertes Zertifikat (QC) bzw. sichere Signaturerstellungseinheit (SSCD)



TSL Library Implementation

Verifies the QC or SSCD property of an electronic signature

Key component. Coordinates the TSL import, storage and verifications. Wrapper=Interface

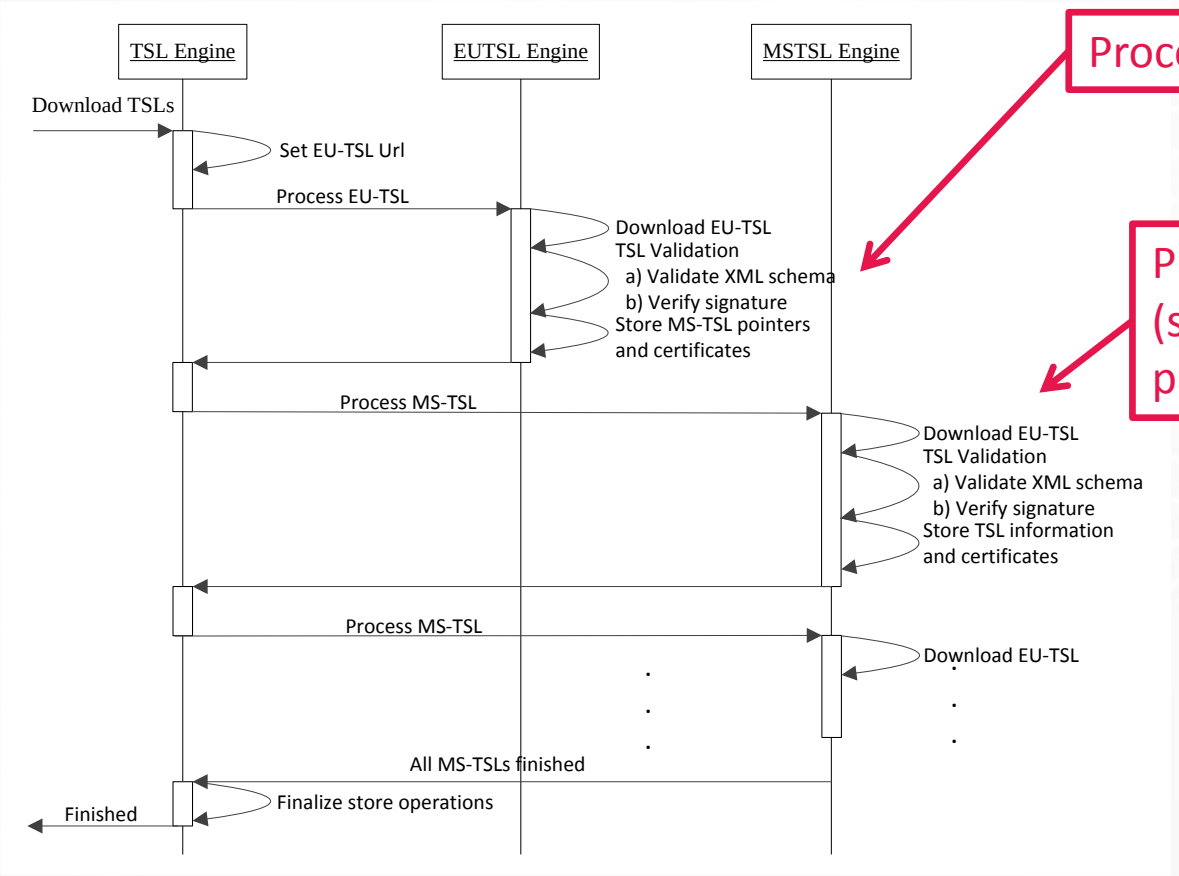


TSL information stored in a database. Extracted certificates stored in local working directory

EUTSL Engine, downloads, verifies and imports the EU-TSL.
MSTSL Engine processes the Member States TSLs

TSL Library Implementation

» Process flow „TSL Import“



TSL Library Implementation

» Process flow „QC/SSCD Verification“