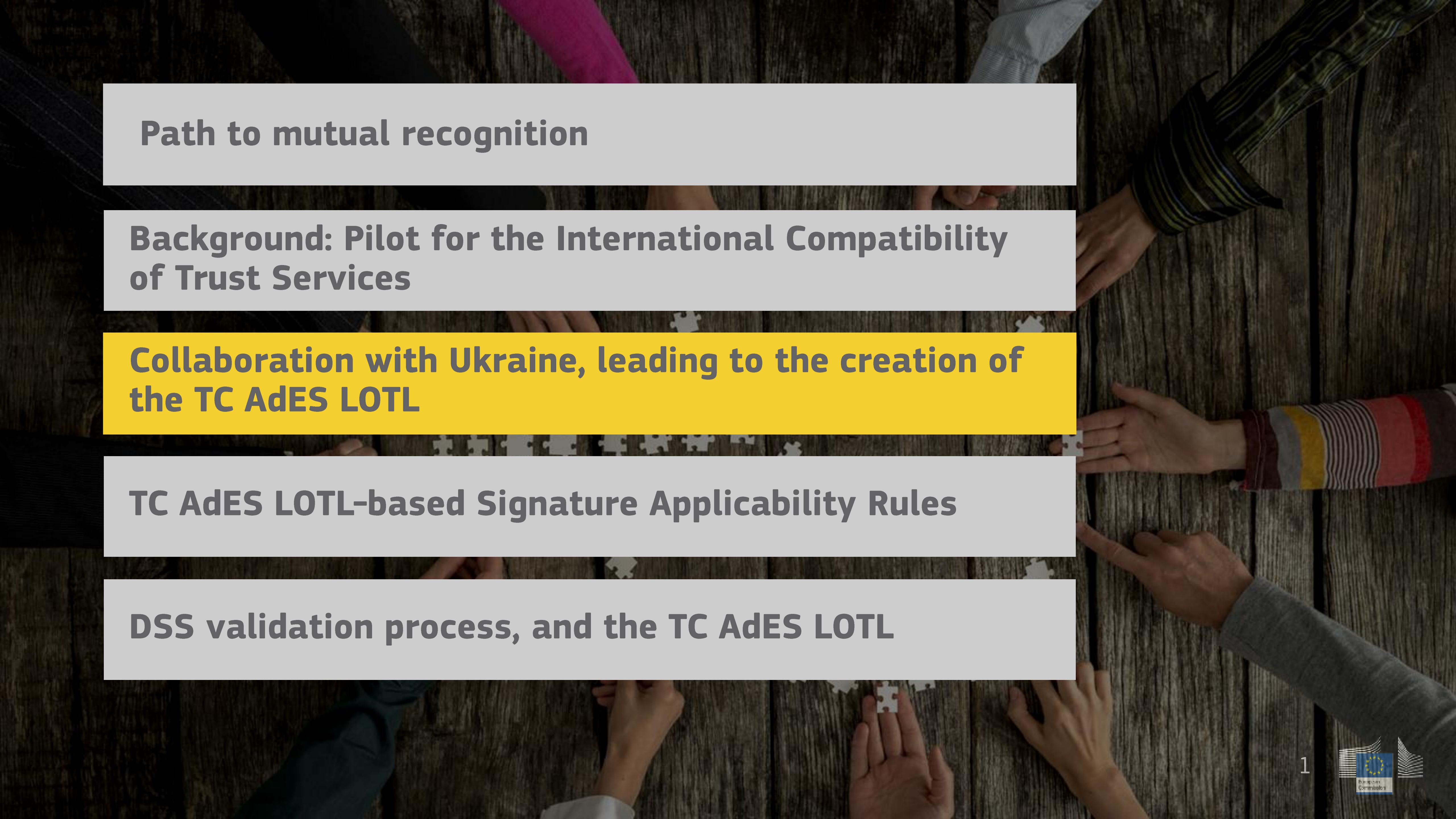


Path to mutual recognition

Background: Pilot for the International Compatibility of Trust Services

Collaboration with Ukraine, leading to the creation of the TC AdES LOTL

TC AdES LOTL-based Signature Applicability Rules

DSS validation process, and the TC AdES LOTL

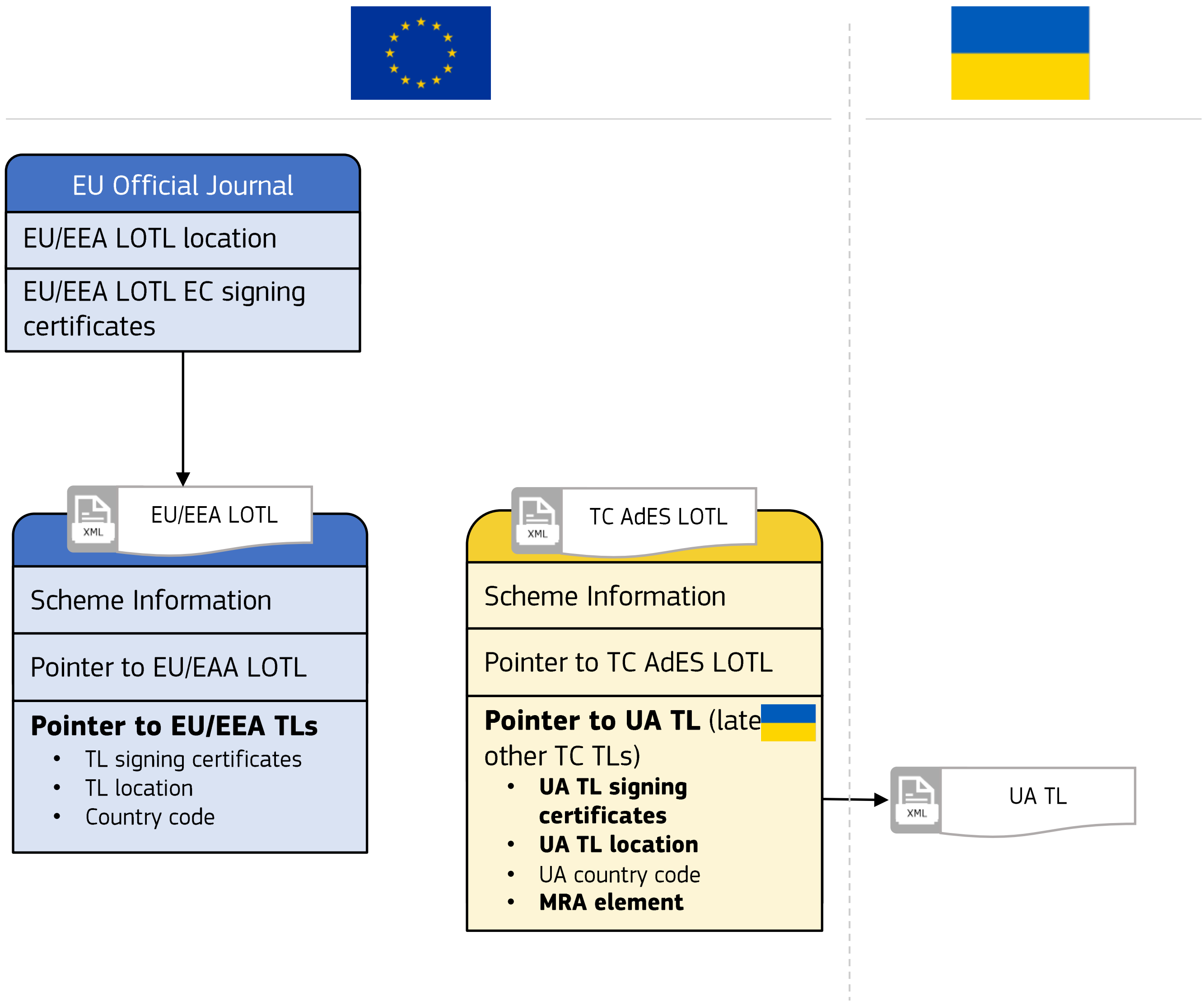
MRA-Info element

Usage n°2: Recognition of electronic signatures from Ukraine as EU advanced electronic signatures

Publication of **TC AdES LOTL** pointing to UA Trusted List (TL)

To allow Member States on a **voluntary** basis to:

- Download and authenticate the TC trusted list;
- Validate **UA-QES as eIDAS AdES**, using the Mutual Recognition Agreement (MRA) element.



EU Official Journal

EU/EEA LOTL location

EU/EEA LOTL EC signing certificates

Scheme Information

Pointer to EU/EAA LOTL

Pointer to EU/EEA TLs

- TL signing certificates
- TL location
- Country code

Scheme Information

Pointer to TC AdES LOTL

Pointer to UA TL (late other TC TLs)

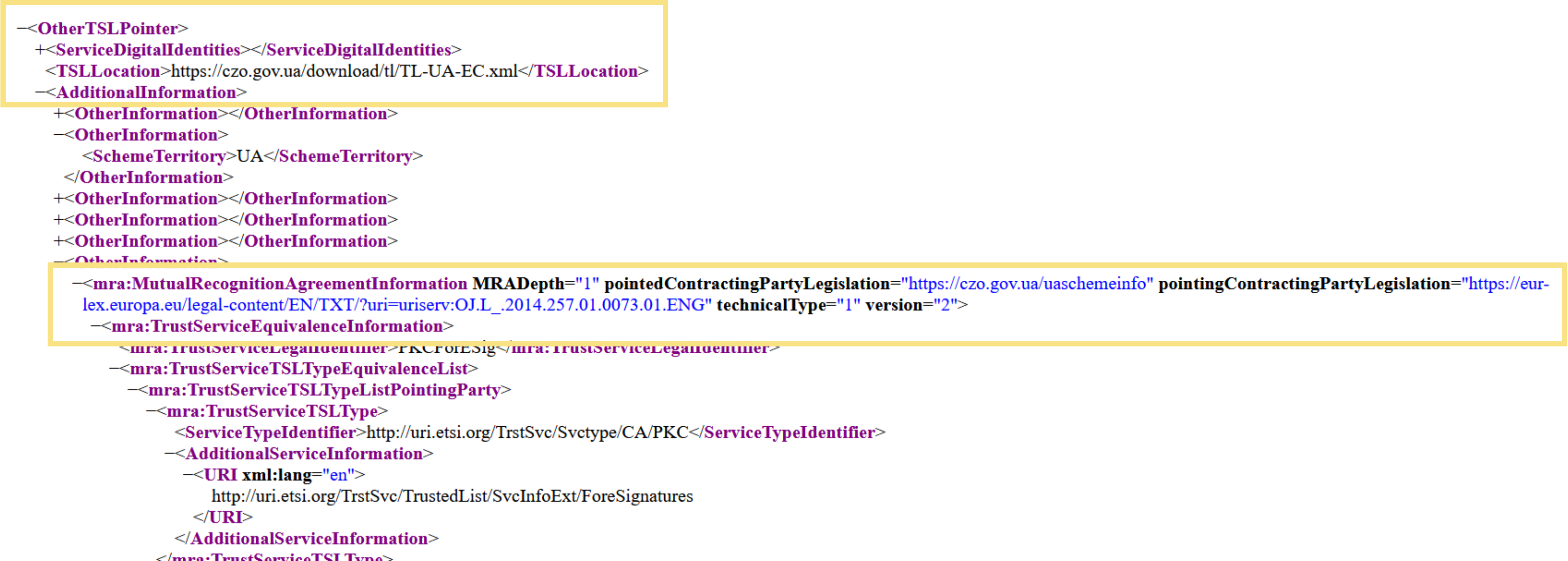
- **UA TL signing certificates**
- **UA TL location**
- UA country code
- **MRA element**

MRA-Info element specifications

Illustration based on the TC AdES LOTL

`MutualRecognitionAgreementInformation` element as an additional information included to the `OtherTSLPointer` element of the “Pointers to other TSLs”.

This MRA Info element contains a sequence of `TrustServiceEquivalenceInformation` element.



```
–<OtherTSLPointer>
  +<ServiceDigitalIdentities></ServiceDigitalIdentities>
   <TSLLocation>https://czo.gov.ua/download/tl/TL-UA-EC.xml</TSLLocation>
  –<AdditionalInformation>
    +<OtherInformation></OtherInformation>
    –<OtherInformation>
        <SchemeTerritory>UA</SchemeTerritory>
     </OtherInformation>
    +<OtherInformation></OtherInformation>
    +<OtherInformation></OtherInformation>
    +<OtherInformation></OtherInformation>
    –<OtherInformation>
      –<mra:MutualRecognitionAgreementInformation MRADepth="1" pointedContractingPartyLegislation="https://czo.gov.ua/uaschemeinfo" pointingContractingPartyLegislation="https://eur-
       lex.europa.eu/legal-content/EN/TXT/?uri=uriserv:OJ.L_.2014.257.01.0073.01.ENG" technicalType="1" version="2">
        –<mra:TrustServiceEquivalenceInformation>
           <mra:TrustServiceLegalIdentifier>PKCForESig</mra:TrustServiceLegalIdentifier>
          –<mra:TrustServiceTSLTypeEquivalenceList>
            –<mra:TrustServiceTSLTypeListPointingParty>
              –<mra:TrustServiceTSLType>
                 <ServiceTypeIdentifier>http://uri.etsi.org/TrstSvc/Svctype/CA/PKC</ServiceTypeIdentifier>
                –<AdditionalServiceInformation>
                  –<URI xml:lang="en">
                      http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/ForeSignatures
                    </URI>
                 </AdditionalServiceInformation>
               </mra:TrustServiceTSLType>
```

MRA-Info element specifications

Trust Service Equivalence Information

That contain information about the equivalence mapping :

TrustService**LegalIdentifier**

TrustService**TSLType**EquivalenceList

TrustService**TSLStatus**EquivalenceList

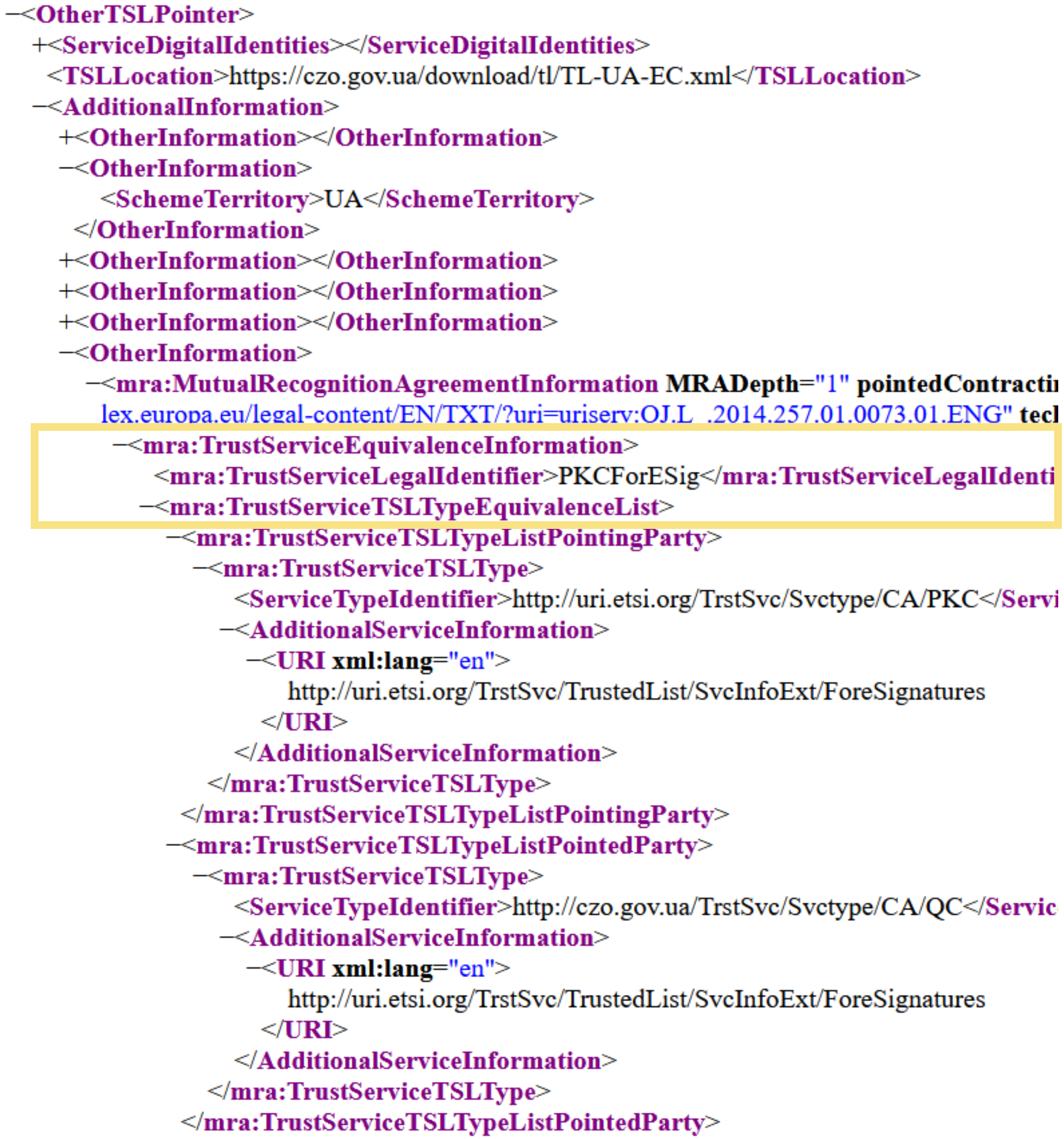
TrustService**TSLQualificationExtension**EquivalenceList

CertificateContentReferencesEquivalenceList

TrustService**EquivalenceStatus**

TrustServiceEquivalenceStatus**StartingTime**

TrustServiceEquivalence**History**



```
–<OtherTSLPointer>
  +<ServiceDigitalIdentities></ServiceDigitalIdentities>
   <TSLLocation>https://czo.gov.ua/download/tl/TL-UA-EC.xml</TSLLocation>
  –<AdditionalInformation>
    +<OtherInformation></OtherInformation>
    –<OtherInformation>
       <SchemeTerritory>UA</SchemeTerritory>
     </OtherInformation>
    +<OtherInformation></OtherInformation>
    +<OtherInformation></OtherInformation>
    +<OtherInformation></OtherInformation>
    –<OtherInformation>
      –<mra:MutualRecognitionAgreementInformation MRADepth="1" pointedContracti
       lex.europa.eu/legal-content/EN/TXT/?uri=uriserv:OJ.L_.2014.257.01.0073.01.ENG" tecl
        –<mra:TrustServiceEquivalenceInformation>
           <mra:TrustServiceLegalIdentifier>PKCForESig</mra:TrustServiceLegalIdenti
          –<mra:TrustServiceTSLTypeEquivalenceList>
            –<mra:TrustServiceTSLTypeListPointingParty>
              –<mra:TrustServiceTSLType>
                 <ServiceTypeIdentifier>http://uri.etsi.org/TrstSvc/Svctype/CA/PKC</Servi
                –<AdditionalServiceInformation>
                  –<URI xml:lang="en">
                     http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/ForeSignatures
                   </URI>
                 </AdditionalServiceInformation>
               </mra:TrustServiceTSLType>
             </mra:TrustServiceTSLTypeListPointingParty>
            –<mra:TrustServiceTSLTypeListPointedParty>
              –<mra:TrustServiceTSLType>
                 <ServiceTypeIdentifier>http://czo.gov.ua/TrstSvc/Svctype/CA/QC</Servic
                –<AdditionalServiceInformation>
                  –<URI xml:lang="en">
                     http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/ForeSignatures
                   </URI>
                 </AdditionalServiceInformation>
               </mra:TrustServiceTSLType>
             </mra:TrustServiceTSLTypeListPointedParty>
```

MRA-Info element specifications

Equivalences between information in the **Pointing Party** and information in the **Pointed Party**

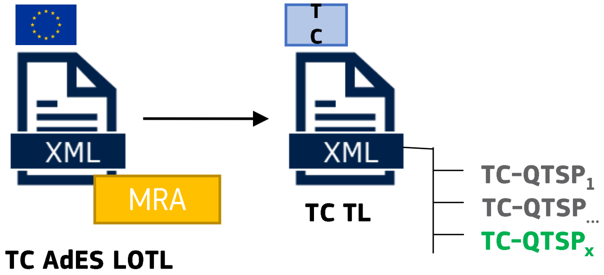
TrustService**TSLType**EquivalenceList

- Identifies the type of TC-QTS issuing TC-QC_for_eSig

CertificateContentReferencesEquivalenceList

- Identies QcCompliance, QcType and QcCClegislation statements declaring they are TC-QC_for_eSig
- Either QcSSCD (EU QSCD) or specific CP OID (TC-TL confirmed) declaring use of TC-QSCD meeting similar requirements applicable to EU-QSCD

**PointingParty - **PointedParty

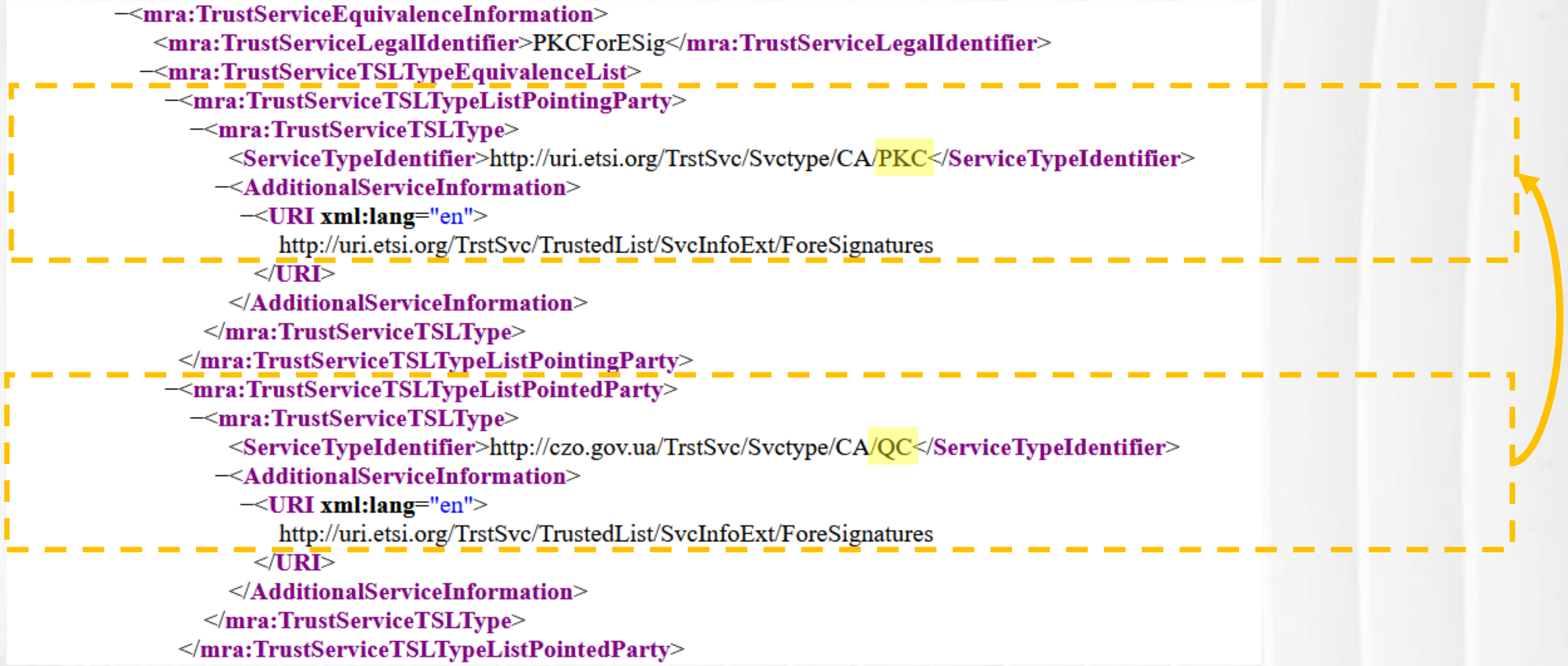


TC AdES LOTL

MRA element content – Trust services types

MRA element makes **equivalence** between the UA framework (PointedParty) and the eIDAS framework (PointingParty)

When in Ukraine: trust service is “Issuance of **qualified** certificates for eSig” (`CA/QC`)
Then in EU/EEA: trust service is “Issuance of **non-qualified** certificates for eSig” (`CA/PKC`)

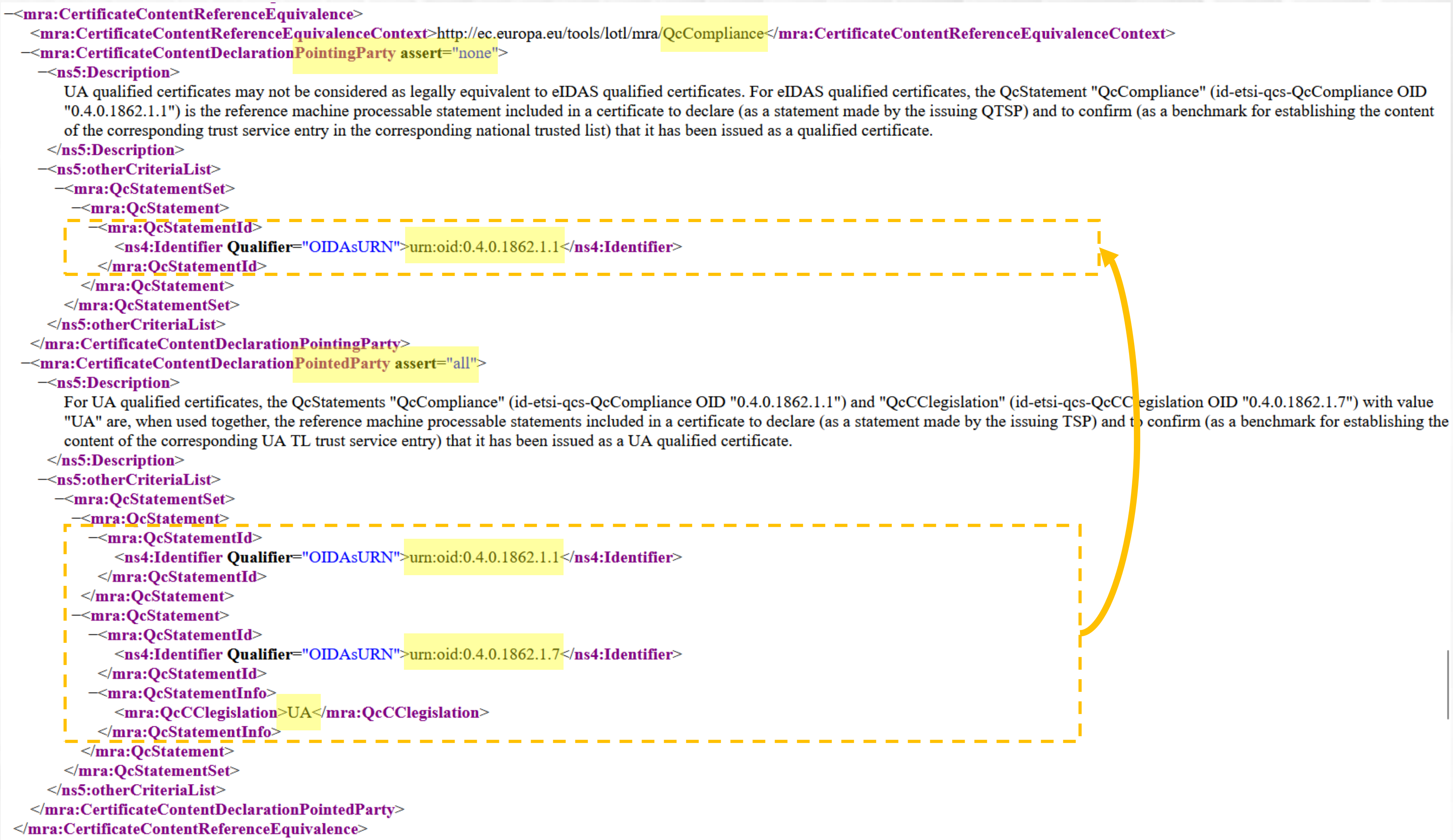


```
–<mra:TrustServiceEquivalenceInformation>
   <mra:TrustServiceLegalIdentifier>PKCForESig</mra:TrustServiceLegalIdentifier>
  –<mra:TrustServiceTSLTypeEquivalenceList>
    –<mra:TrustServiceTSLTypeListPointingParty>
      –<mra:TrustServiceTSLType>
         <ServiceTypeIdentifier>http://uri.etsi.org/TrstSvc/Svctype/CA/PKC</ServiceTypeIdentifier>
        –<AdditionalServiceInformation>
          –<URI xml:lang="en">
             http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/ForeSignatures
           </URI>
         </AdditionalServiceInformation>
       </mra:TrustServiceTSLType>
     </mra:TrustServiceTSLTypeListPointingParty>
    –<mra:TrustServiceTSLTypeListPointedParty>
      –<mra:TrustServiceTSLType>
         <ServiceTypeIdentifier>http://czo.gov.ua/TrstSvc/Svctype/CA/QC</ServiceTypeIdentifier>
        –<AdditionalServiceInformation>
          –<URI xml:lang="en">
             http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/ForeSignatures
           </URI>
         </AdditionalServiceInformation>
       </mra:TrustServiceTSLType>
     </mra:TrustServiceTSLTypeListPointedParty>
```

TC AdES LOTL

MRA element content – **Qualified** status of certificates

MRA element makes **equivalence** between the UA framework (PointedParty) and the eIDAS framework (PointingParty)

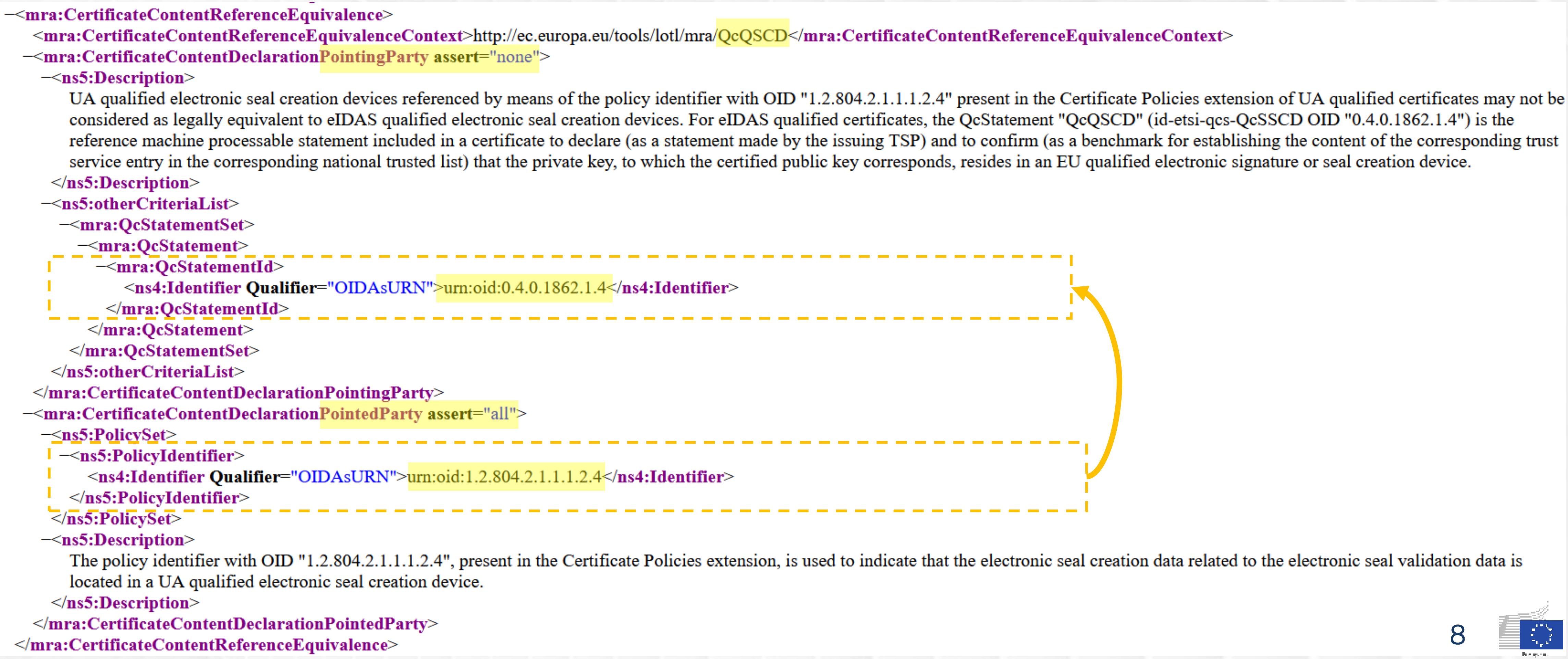


```
−<mra:CertificateContentReferenceEquivalence>
   <mra:CertificateContentReferenceEquivalenceContext>http://ec.europa.eu/tools/lotl/mra/QcCompliance</mra:CertificateContentReferenceEquivalenceContext>
  −<mra:CertificateContentDeclarationPointingParty assert="none">
    −<ns5:Description>
       UA qualified certificates may not be considered as legally equivalent to eIDAS qualified certificates. For eIDAS qualified certificates, the QcStatement "QcCompliance" (id-etsi-qcs-QcCompliance OID
       "0.4.0.1862.1.1") is the reference machine processable statement included in a certificate to declare (as a statement made by the issuing QTSP) and to confirm (as a benchmark for establishing the content
       of the corresponding trust service entry in the corresponding national trusted list) that it has been issued as a qualified certificate.
     </ns5:Description>
    −<ns5:otherCriteriaList>
      −<mra:QcStatementSet>
        −<mra:QcStatement>
          −<mra:QcStatementId>
             <ns4:Identifier Qualifier="OIDAsURN">urn:oid:0.4.0.1862.1.1</ns4:Identifier>
           </mra:QcStatementId>
         </mra:QcStatement>
       </mra:QcStatementSet>
     </ns5:otherCriteriaList>
   </mra:CertificateContentDeclarationPointingParty>
  −<mra:CertificateContentDeclarationPointedParty assert="all">
    −<ns5:Description>
       For UA qualified certificates, the QcStatements "QcCompliance" (id-etsi-qcs-QcCompliance OID "0.4.0.1862.1.1") and "QcCClegislation" (id-etsi-qcs-QcCClegislation OID "0.4.0.1862.1.7") with value
       "UA" are, when used together, the reference machine processable statements included in a certificate to declare (as a statement made by the issuing TSP) and to confirm (as a benchmark for establishing the
       content of the corresponding UA TL trust service entry) that it has been issued as a UA qualified certificate.
     </ns5:Description>
    −<ns5:otherCriteriaList>
      −<mra:QcStatementSet>
        −<mra:QcStatement>
          −<mra:QcStatementId>
             <ns4:Identifier Qualifier="OIDAsURN">urn:oid:0.4.0.1862.1.1</ns4:Identifier>
           </mra:QcStatementId>
         </mra:QcStatement>
        −<mra:QcStatement>
          −<mra:QcStatementId>
             <ns4:Identifier Qualifier="OIDAsURN">urn:oid:0.4.0.1862.1.7</ns4:Identifier>
           </mra:QcStatementId>
          −<mra:QcStatementInfo>
             <mra:QcCClegislation>UA</mra:QcCClegislation>
           </mra:QcStatementInfo>
         </mra:QcStatement>
       </mra:QcStatementSet>
     </ns5:otherCriteriaList>
   </mra:CertificateContentDeclarationPointedParty>
 </mra:CertificateContentReferenceEquivalence>
```

TC AdES LOTL

MRA element content – **QSCD** recognition

MRA element makes **equivalence** between the UA framework (PointedParty) and the eIDAS framework (PointingParty)

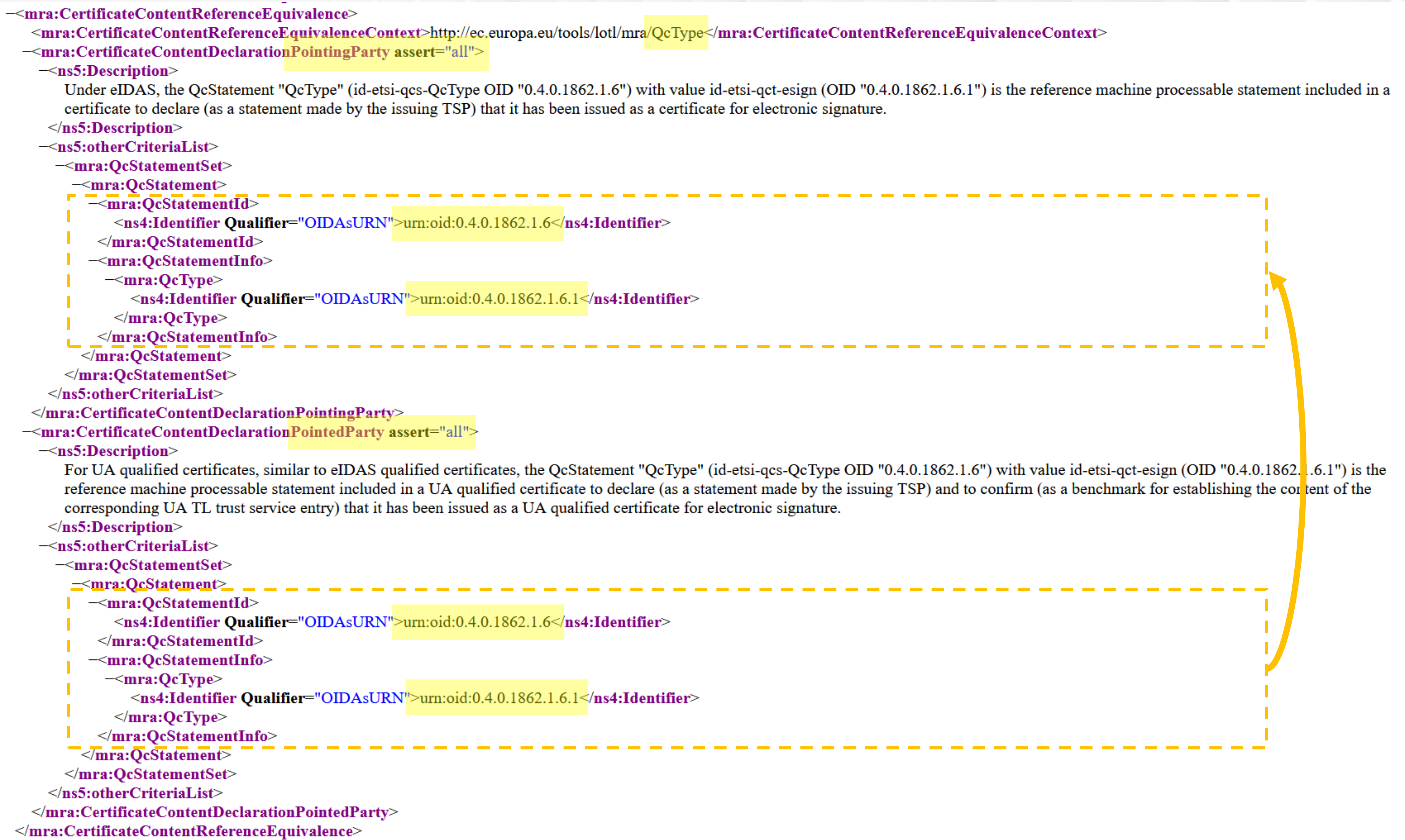


```
-<mra:CertificateContentReferenceEquivalence>
   <mra:CertificateContentReferenceEquivalenceContext>http://ec.europa.eu/tools/lotl/mra/QcQSCD</mra:CertificateContentReferenceEquivalenceContext>
  -<mra:CertificateContentDeclarationPointingParty assert="none">
    -<ns5:Description>
       UA qualified electronic seal creation devices referenced by means of the policy identifier with OID "1.2.804.2.1.1.1.2.4" present in the Certificate Policies extension of UA qualified certificates may not be
       considered as legally equivalent to eIDAS qualified electronic seal creation devices. For eIDAS qualified certificates, the QcStatement "QcQSCD" (id-etsi-qcs-QcSSCD OID "0.4.0.1862.1.4") is the
       reference machine processable statement included in a certificate to declare (as a statement made by the issuing TSP) and to confirm (as a benchmark for establishing the content of the corresponding trust
       service entry in the corresponding national trusted list) that the private key, to which the certified public key corresponds, resides in an EU qualified electronic signature or seal creation device.
     </ns5:Description>
    -<ns5:otherCriteriaList>
      -<mra:QcStatementSet>
        -<mra:QcStatement>
          -<mra:QcStatementId>
             <ns4:Identifier Qualifier="OIDAsURN">urn:oid:0.4.0.1862.1.4</ns4:Identifier>
           </mra:QcStatementId>
         </mra:QcStatement>
       </mra:QcStatementSet>
     </ns5:otherCriteriaList>
   </mra:CertificateContentDeclarationPointingParty>
  -<mra:CertificateContentDeclarationPointedParty assert="all">
    -<ns5:PolicySet>
      -<ns5:PolicyIdentifier>
         <ns4:Identifier Qualifier="OIDAsURN">urn:oid:1.2.804.2.1.1.1.2.4</ns4:Identifier>
       </ns5:PolicyIdentifier>
     </ns5:PolicySet>
    -<ns5:Description>
       The policy identifier with OID "1.2.804.2.1.1.1.2.4", present in the Certificate Policies extension, is used to indicate that the electronic seal creation data related to the electronic seal validation data is
       located in a UA qualified electronic seal creation device.
     </ns5:Description>
   </mra:CertificateContentDeclarationPointedParty>
 </mra:CertificateContentReferenceEquivalence>
```

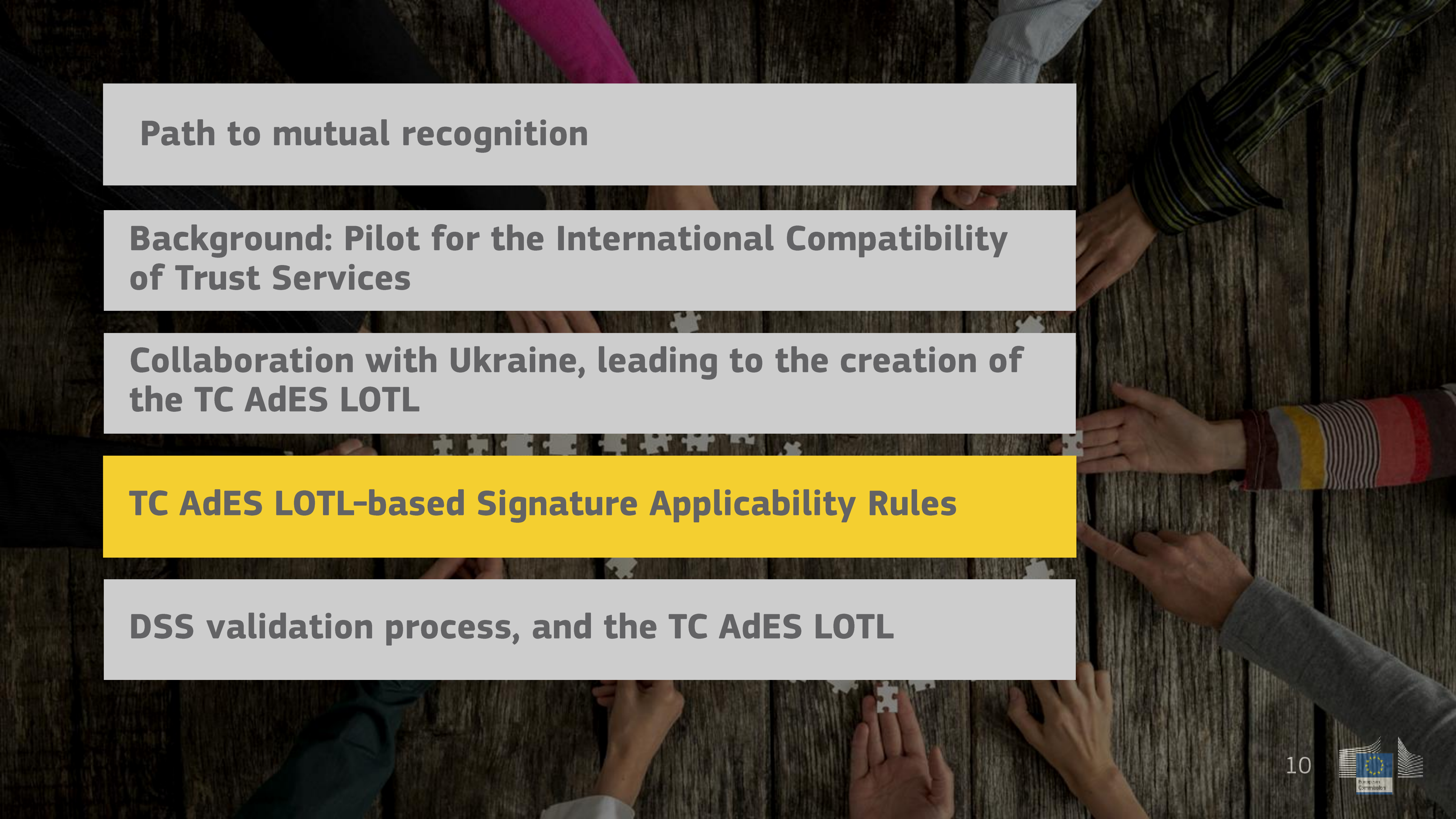
TC AdES LOTL

MRA element content – Exceptions

MRA element makes **equivalence** between the UA framework (PointedParty) and the eIDAS framework (PointingParty)



```
−<mra:CertificateContentReferenceEquivalence>
   <mra:CertificateContentReferenceEquivalenceContext>http://ec.europa.eu/tools/lotl/mra/QcType</mra:CertificateContentReferenceEquivalenceContext>
  −<mra:CertificateContentDeclarationPointingParty assert="all">
    −<ns5:Description>
       Under eIDAS, the QcStatement "QcType" (id-etsi-qcs-QcType OID "0.4.0.1862.1.6") with value id-etsi-qct-esign (OID "0.4.0.1862.1.6.1") is the reference machine processable statement included in a
       certificate to declare (as a statement made by the issuing TSP) that it has been issued as a certificate for electronic signature.
     </ns5:Description>
    −<ns5:otherCriteriaList>
      −<mra:QcStatementSet>
        −<mra:QcStatement>
          −<mra:QcStatementId>
             <ns4:Identifier Qualifier="OIDAsURN">urn:oid:0.4.0.1862.1.6</ns4:Identifier>
           </mra:QcStatementId>
          −<mra:QcStatementInfo>
            −<mra:QcType>
               <ns4:Identifier Qualifier="OIDAsURN">urn:oid:0.4.0.1862.1.6.1</ns4:Identifier>
             </mra:QcType>
           </mra:QcStatementInfo>
         </mra:QcStatement>
       </mra:QcStatementSet>
     </ns5:otherCriteriaList>
   </mra:CertificateContentDeclarationPointingParty>
  −<mra:CertificateContentDeclarationPointedParty assert="all">
    −<ns5:Description>
       For UA qualified certificates, similar to eIDAS qualified certificates, the QcStatement "QcType" (id-etsi-qcs-QcType OID "0.4.0.1862.1.6") with value id-etsi-qct-esign (OID "0.4.0.1862.1.6.1") is the
       reference machine processable statement included in a UA qualified certificate to declare (as a statement made by the issuing TSP) and to confirm (as a benchmark for establishing the content of the
       corresponding UA TL trust service entry) that it has been issued as a UA qualified certificate for electronic signature.
     </ns5:Description>
    −<ns5:otherCriteriaList>
      −<mra:QcStatementSet>
        −<mra:QcStatement>
          −<mra:QcStatementId>
             <ns4:Identifier Qualifier="OIDAsURN">urn:oid:0.4.0.1862.1.6</ns4:Identifier>
           </mra:QcStatementId>
          −<mra:QcStatementInfo>
            −<mra:QcType>
               <ns4:Identifier Qualifier="OIDAsURN">urn:oid:0.4.0.1862.1.6.1</ns4:Identifier>
             </mra:QcType>
           </mra:QcStatementInfo>
         </mra:QcStatement>
       </mra:QcStatementSet>
     </ns5:otherCriteriaList>
   </mra:CertificateContentDeclarationPointedParty>
 </mra:CertificateContentReferenceEquivalence>
```



Path to mutual recognition

Background: Pilot for the International Compatibility of Trust Services

Collaboration with Ukraine, leading to the creation of the TC AdES LOTL

TC AdES LOTL-based Signature Applicability Rules

DSS validation process, and the TC AdES LOTL

How to perform a TC AdES LOTL-based signature validation

Validation policy (Signature Applicability Rules)

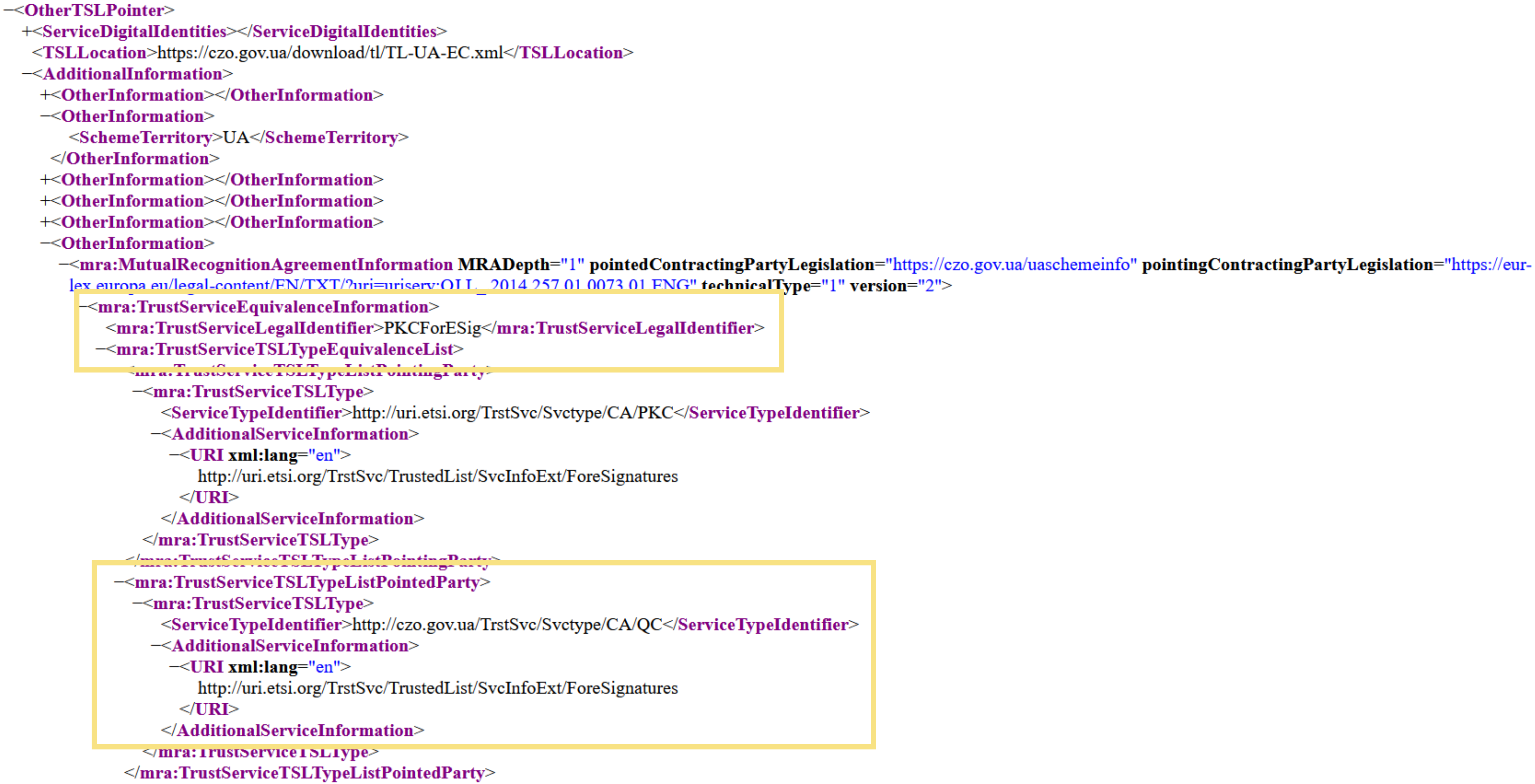
Rules for the technical validation of digital signatures originating from 3rd countries and the determination of their **applicability to the specific context** of **Article 27** (and consequently Article 26) of the eIDAS Regulation, i.e. to determine whether they can be (technically) considered as EU advanced electronic signatures using the **TC AdES LOTL** and the corresponding TC TLs in the sense of eIDAS.

Based on **ETSI TS 119 172-4**, relying on ETSI TS 119 615 and ETSI EN 319 102-1, parameterized with:

- How to rely on the **TC AdES LOTL**
- How to identify the TC QTS issuing QCs (for eSig / for eSeal) in the TL: “**TC_CA/QC**”
- How to identify in the TC QC:
    - **“TC_QcCompliance”**
    - **“TC_QcType”**
    - **“TC_QcQSCD”**

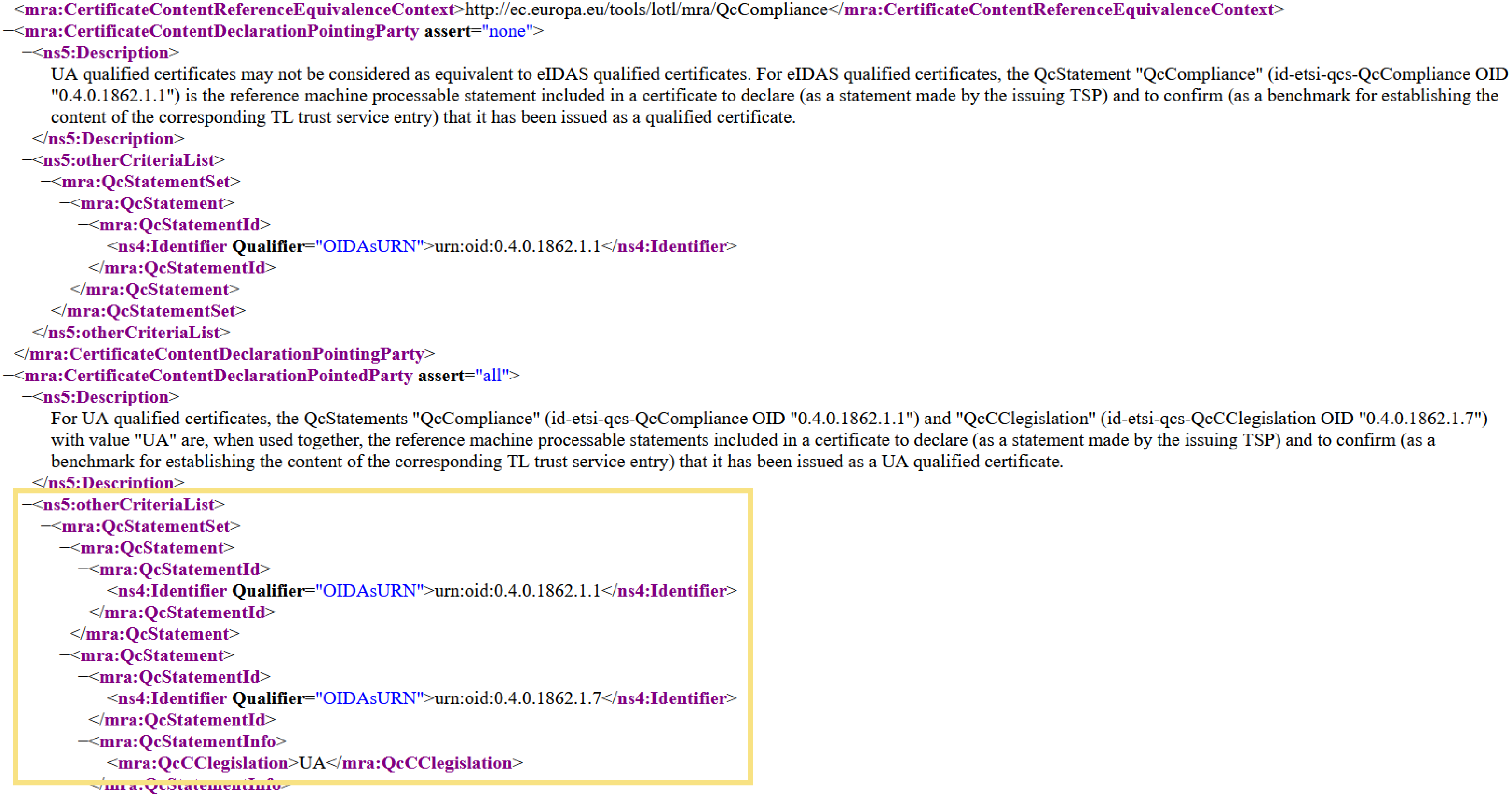
The SAR document is available at: https://eidas.ec.europa.eu/efda/tl-browser/#/screen/tc-tl or in the MRA Bundle on the pilot page https://eidas.ec.europa.eu/efda/intl-pilot/#/screen/home/demo

How to identify the TC QTS issuing QCs in the TL: “TC_CA/QC”

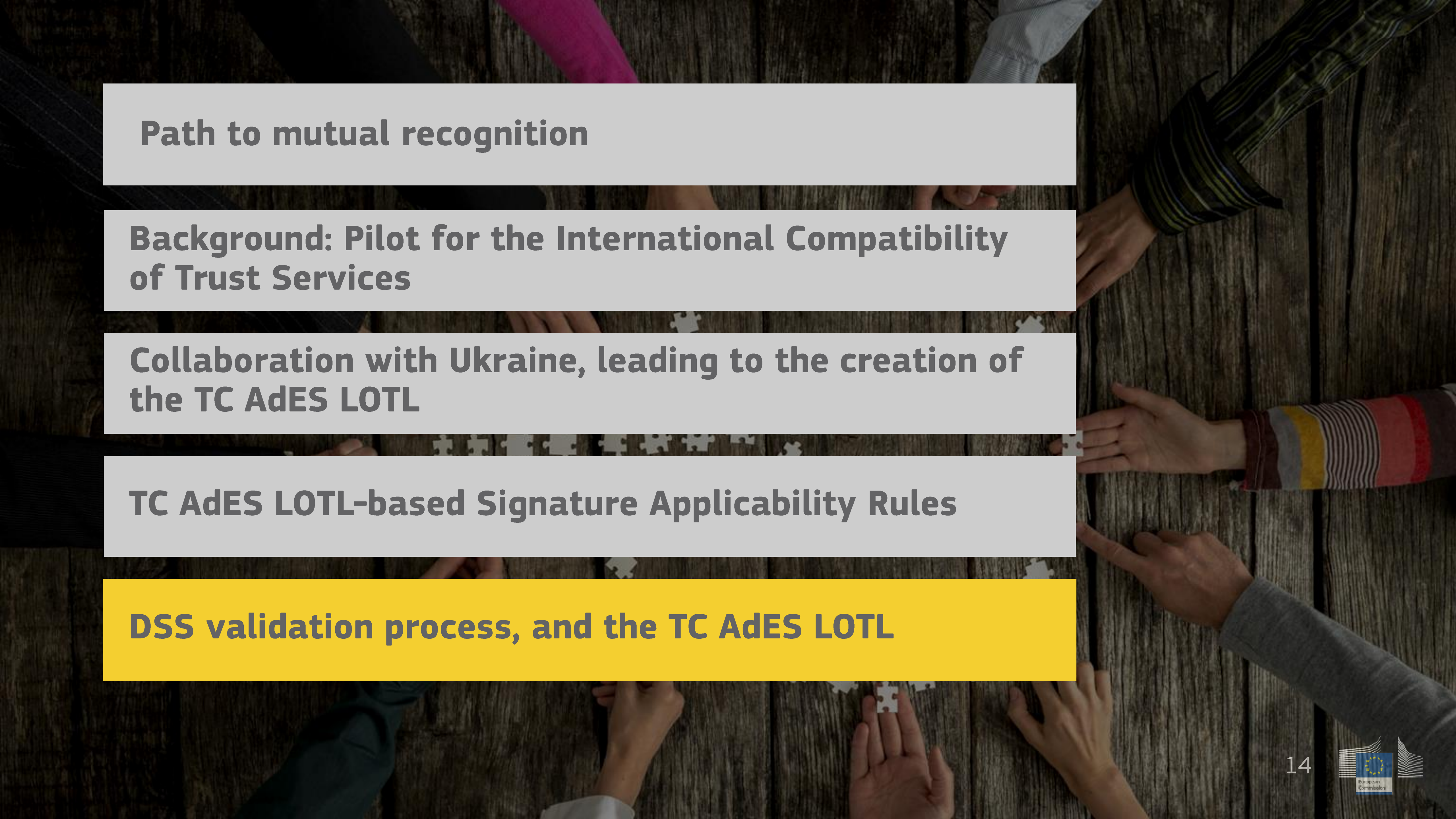


```
−<OtherTSLPointer>
  +<ServiceDigitalIdentities></ServiceDigitalIdentities>
   <TSLLocation>https://czo.gov.ua/download/tl/TL-UA-EC.xml</TSLLocation>
  −<AdditionalInformation>
    +<OtherInformation></OtherInformation>
    −<OtherInformation>
        <SchemeTerritory>UA</SchemeTerritory>
     </OtherInformation>
    +<OtherInformation></OtherInformation>
    +<OtherInformation></OtherInformation>
    +<OtherInformation></OtherInformation>
    −<OtherInformation>
      −<mra:MutualRecognitionAgreementInformation MRADepth="1" pointedContractingPartyLegislation="https://czo.gov.ua/uaschemeinfo" pointingContractingPartyLegislation="https://eur-
       lex.europa.eu/legal-content/EN/TXT/?uri=uriserv:OJ.L_.2014.257.01.0073.01.ENG" technicalType="1" version="2">
        −<mra:TrustServiceEquivalenceInformation>
           <mra:TrustServiceLegalIdentifier>PKCForESig</mra:TrustServiceLegalIdentifier>
         −<mra:TrustServiceTSLTypeEquivalenceList>
            <mra:TrustServiceTSLTypeListPointingParty>
             −<mra:TrustServiceTSLType>
                <ServiceTypeIdentifier>http://uri.etsi.org/TrstSvc/Svctype/CA/PKC</ServiceTypeIdentifier>
              −<AdditionalServiceInformation>
                −<URI xml:lang="en">
                   http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/ForeSignatures
                 </URI>
                </AdditionalServiceInformation>
              </mra:TrustServiceTSLType>
            </mra:TrustServiceTSLTypeListPointingParty>
           −<mra:TrustServiceTSLTypeListPointedParty>
             −<mra:TrustServiceTSLType>
                <ServiceTypeIdentifier>http://czo.gov.ua/TrstSvc/Svctype/CA/QC</ServiceTypeIdentifier>
              −<AdditionalServiceInformation>
                −<URI xml:lang="en">
                   http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/ForeSignatures
                 </URI>
                </AdditionalServiceInformation>
              </mra:TrustServiceTSLType>
            </mra:TrustServiceTSLTypeListPointedParty>
```

How to identify the TC QC certificate profile: e.g. “TC_QcCompliance”



```
 <mra:CertificateContentReferenceEquivalenceContext>http://ec.europa.eu/tools/lotl/mra/QcCompliance</mra:CertificateContentReferenceEquivalenceContext>
-<mra:CertificateContentDeclarationPointingParty assert="none">
  -<ns5:Description>
     UA qualified certificates may not be considered as equivalent to eIDAS qualified certificates. For eIDAS qualified certificates, the QcStatement "QcCompliance" (id-etsi-qcs-QcCompliance OID
     "0.4.0.1862.1.1") is the reference machine processable statement included in a certificate to declare (as a statement made by the issuing TSP) and to confirm (as a benchmark for establishing the
     content of the corresponding TL trust service entry) that it has been issued as a qualified certificate.
   </ns5:Description>
  -<ns5:otherCriteriaList>
    -<mra:QcStatementSet>
      -<mra:QcStatement>
        -<mra:QcStatementId>
           <ns4:Identifier Qualifier="OIDAsURN">urn:oid:0.4.0.1862.1.1</ns4:Identifier>
         </mra:QcStatementId>
       </mra:QcStatement>
     </mra:QcStatementSet>
   </ns5:otherCriteriaList>
 </mra:CertificateContentDeclarationPointingParty>
-<mra:CertificateContentDeclarationPointedParty assert="all">
  -<ns5:Description>
     For UA qualified certificates, the QcStatements "QcCompliance" (id-etsi-qcs-QcCompliance OID "0.4.0.1862.1.1") and "QcCClegislation" (id-etsi-qcs-QcCClegislation OID "0.4.0.1862.1.7")
     with value "UA" are, when used together, the reference machine processable statements included in a certificate to declare (as a statement made by the issuing TSP) and to confirm (as a
     benchmark for establishing the content of the corresponding TL trust service entry) that it has been issued as a UA qualified certificate.
   </ns5:Description>
  -<ns5:otherCriteriaList>
    -<mra:QcStatementSet>
      -<mra:QcStatement>
        -<mra:QcStatementId>
           <ns4:Identifier Qualifier="OIDAsURN">urn:oid:0.4.0.1862.1.1</ns4:Identifier>
         </mra:QcStatementId>
       </mra:QcStatement>
      -<mra:QcStatement>
        -<mra:QcStatementId>
           <ns4:Identifier Qualifier="OIDAsURN">urn:oid:0.4.0.1862.1.7</ns4:Identifier>
         </mra:QcStatementId>
        -<mra:QcStatementInfo>
           <mra:QcCClegislation>UA</mra:QcCClegislation>
         </mra:QcStatementInfo>
```



Path to mutual recognition

Background: Pilot for the International Compatibility of Trust Services

Collaboration with Ukraine, leading to the creation of the TC AdES LOTL

TC AdES LOTL-based Signature Applicability Rules

DSS validation process, and the TC AdES LOTL

Introduction to DSS

The DSS (Digital Signature Service) project is an open-source software library for electronic signature creation, augmentation and validation in line with the eIDAS Regulation and related standards.

This project is available in **Java** language.

https://ec.europa.eu/digital-building-blocks/wikis/display/DIGITAL/Digital+Signature+Service+-++DSS

DSS consists of:

- DSS core: https://github.com/esig/dss - the main repository containing code of the framework;
- DSS demonstrations: https://github.com/esig/dss-demonstrations - repository containing integration examples of the framework.
  It includes Spring Web Application, JavaFX standalone application, etc.

Validation process using MRA element in DSS

DSS is a signature **library**, not a signature service / application (i.e. an "SVA").

DSS is designed to:

- validate **QESig** mainly (i.e. "Is it a QESig: Yes or No ?", used as baseline for information messages)
- perform a "**signature diagnosis**", i.e. answers "What is it? QESig / AdESig-QC / AdESig / QESeal / AdeSeal-QC / AdESeal / …" together with **diagnostic data** (DD)
- produce a **validation report**, available for post-processing.

Signature Applicability Rules are meant for **SVA / DA**. DSS provides elements for an application to implement them as **post-processing**.

Objective of the approach: Recognize electronic signatures that are not qualified in the EU, but that meet similar requirements in third countries regulatory framework, as being fit for purpose **in contexts requiring an advanced electronic signature**.

Conclusion should be "Applicable: Y/N ?" and not "AdESig: Y/N?"

Validation process using MRA element in DSS

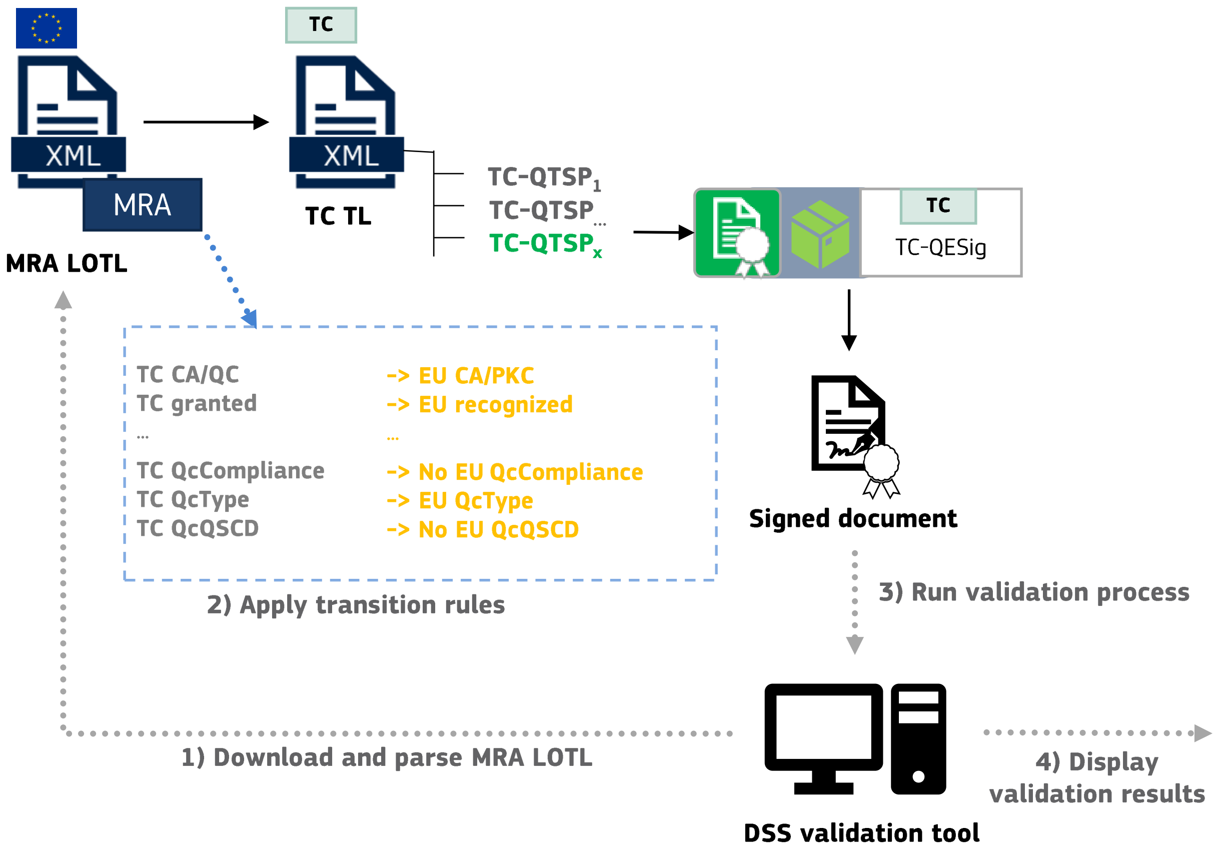
1. Parsing the LOTL and MRA element;

2. Applying MRA transition rules;

3. Running signature/certificate validation;

4. Producing the results.

Validation process using MRA element in DSS



XML

MRA

MRA LOTL

TC

XML

TC TL

TC-QTSP$_1$

TC-QTSP$_{...}$

TC-QTSP$_x$

TC

TC-QESig

TC CA/QC -> EU CA/PKC

TC granted -> EU recognized

… …

TC QcCompliance -> No EU QcCompliance

TC QcType -> EU QcType

TC QcQSCD -> No EU QcQSCD

2) Apply transition rules

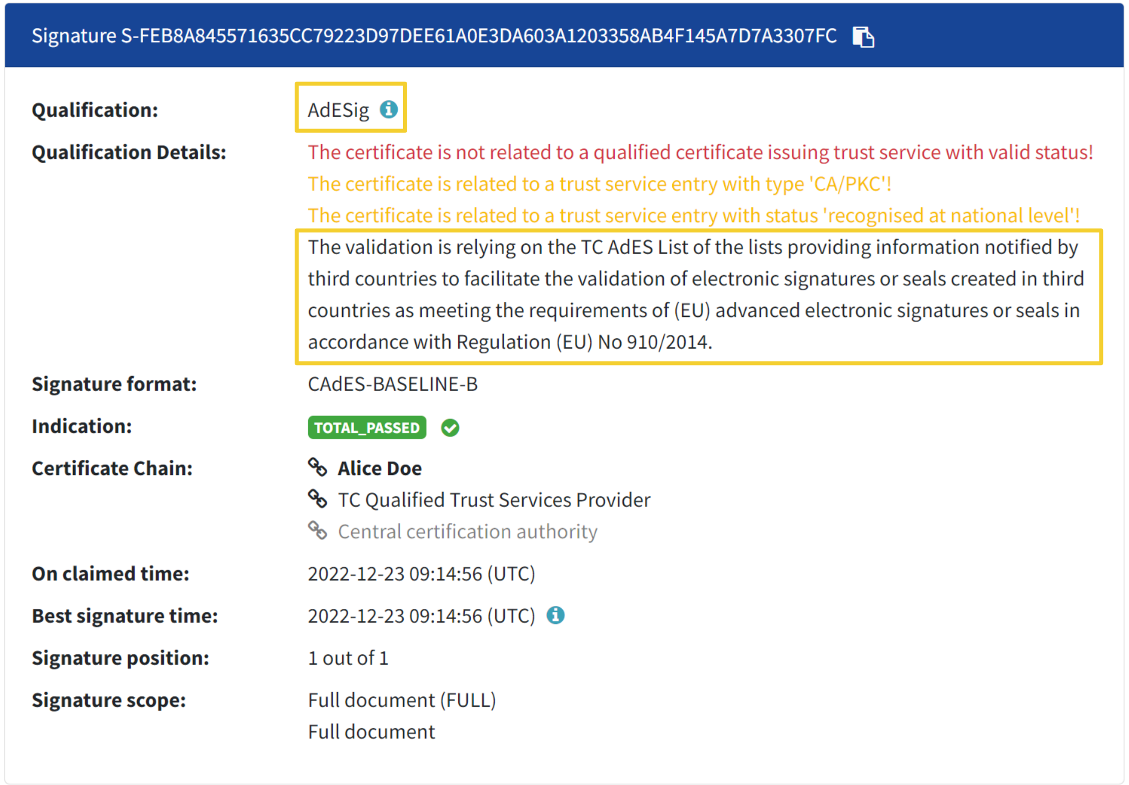
Signed document

3) Run validation process

1) Download and parse MRA LOTL

DSS validation tool

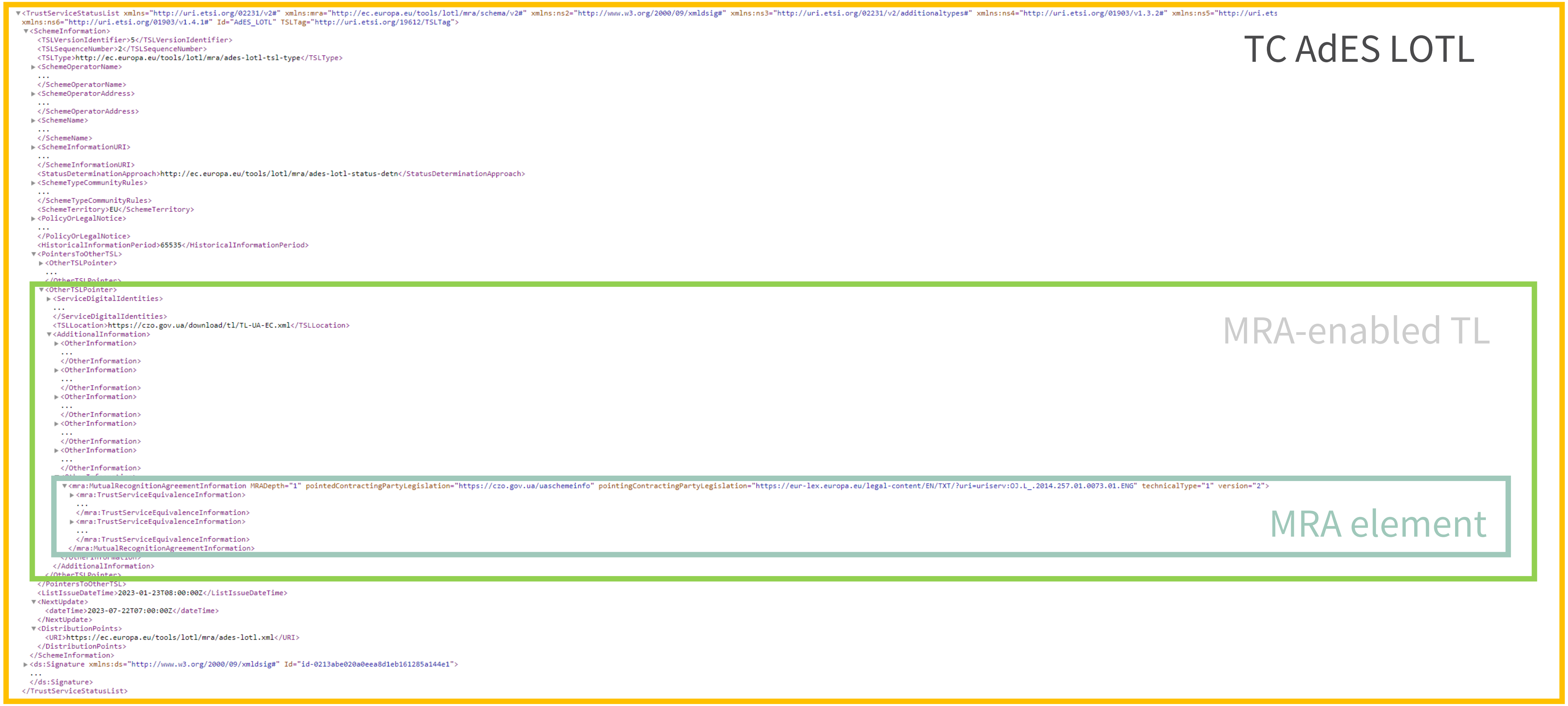
4) Display validation results



Signature S-FEB8A845571635CC79223D97DEE61A0E3DA603A1203358AB4F145A7D7A3307FC

Qualification:	AdESig
Qualification Details:	The certificate is not related to a qualified certificate issuing trust service with valid status! The certificate is related to a trust service entry with type 'CA/PKC'! The certificate is related to a trust service entry with status 'recognised at national level'! The validation is relying on the TC AdES List of the lists providing information notified by third countries to facilitate the validation of electronic signatures or seals created in third countries as meeting the requirements of (EU) advanced electronic signatures or seals in accordance with Regulation (EU) No 910/2014.
Signature format:	CAdES-BASELINE-B
Indication:	TOTAL_PASSED ✓
Certificate Chain:	**Alice Doe** TC Qualified Trust Services Provider Central certification authority
On claimed time:	2022-12-23 09:14:56 (UTC)
Best signature time:	2022-12-23 09:14:56 (UTC)
Signature position:	1 out of 1
Signature scope:	Full document (FULL) Full document

1. Parsing the LOTL and MRA element



```
▼<TrustServiceStatusList xmlns="http://uri.etsi.org/02231/v2#" xmlns:mra="http://ec.europa.eu/tools/lotl/mra/schema/v2#" xmlns:ns2="http://www.w3.org/2000/09/xmldsig#" xmlns:ns3="http://uri.etsi.org/02231/v2/additionaltypes#" xmlns:ns4="http://uri.etsi.org/01903/v1.3.2#" xmlns:ns5="http://uri.ets
 xmlns:ns6="http://uri.etsi.org/01903/v1.4.1#" Id="AdES_LOTL" TSLTag="http://uri.etsi.org/19612/TSLTag">
  ▼<SchemeInformation>
     <TSLVersionIdentifier>5</TSLVersionIdentifier>
     <TSLSequenceNumber>2</TSLSequenceNumber>
     <TSLType>http://ec.europa.eu/tools/lotl/mra/ades-lotl-tsl-type</TSLType>
    ▶<SchemeOperatorName>
     ...
     </SchemeOperatorName>
    ▶<SchemeOperatorAddress>
     ...
     </SchemeOperatorAddress>
    ▶<SchemeName>
     ...
     </SchemeName>
    ▶<SchemeInformationURI>
     ...
     </SchemeInformationURI>
     <StatusDeterminationApproach>http://ec.europa.eu/tools/lotl/mra/ades-lotl-status-detn</StatusDeterminationApproach>
    ▶<SchemeTypeCommunityRules>
     ...
     </SchemeTypeCommunityRules>
     <SchemeTerritory>EU</SchemeTerritory>
    ▶<PolicyOrLegalNotice>
     ...
     </PolicyOrLegalNotice>
     <HistoricalInformationPeriod>65535</HistoricalInformationPeriod>
    ▼<PointersToOtherTSL>
      ▶<OtherTSLPointer>
       ...
       </OtherTSLPointer>
      ▼<OtherTSLPointer>
        ▶<ServiceDigitalIdentities>
         ...
         </ServiceDigitalIdentities>
         <TSLLocation>https://czo.gov.ua/download/tl/TL-UA-EC.xml</TSLLocation>
        ▼<AdditionalInformation>
          ▶<OtherInformation>
           ...
           </OtherInformation>
          ▶<OtherInformation>
           ...
           </OtherInformation>
          ▶<OtherInformation>
           ...
           </OtherInformation>
          ▶<OtherInformation>
           ...
           </OtherInformation>
          ▶<OtherInformation>
           ...
           </OtherInformation>
          ▼<OtherInformation>
            ▼<mra:MutualRecognitionAgreementInformation MRADepth="1" pointedContractingPartyLegislation="https://czo.gov.ua/uaschemeinfo" pointingContractingPartyLegislation="https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=uriserv:OJ.L_.2014.257.01.0073.01.ENG" technicalType="1" version="2">
              ▶<mra:TrustServiceEquivalenceInformation>
               ...
               </mra:TrustServiceEquivalenceInformation>
              ▶<mra:TrustServiceEquivalenceInformation>
               ...
               </mra:TrustServiceEquivalenceInformation>
             </mra:MutualRecognitionAgreementInformation>
           </OtherInformation>
         </AdditionalInformation>
       </OtherTSLPointer>
     </PointersToOtherTSL>
     <ListIssueDateTime>2023-01-23T08:00:00Z</ListIssueDateTime>
    ▼<NextUpdate>
       <dateTime>2023-07-22T07:00:00Z</dateTime>
     </NextUpdate>
    ▼<DistributionPoints>
       <URI>https://ec.europa.eu/tools/lotl/mra/ades-lotl.xml</URI>
     </DistributionPoints>
   </SchemeInformation>
  ▶<ds:Signature xmlns:ds="http://www.w3.org/2000/09/xmldsig#" Id="id-0213abe020a0eea8d1eb161285a144e1">
   ...
   </ds:Signature>
 </TrustServiceStatusList>
```

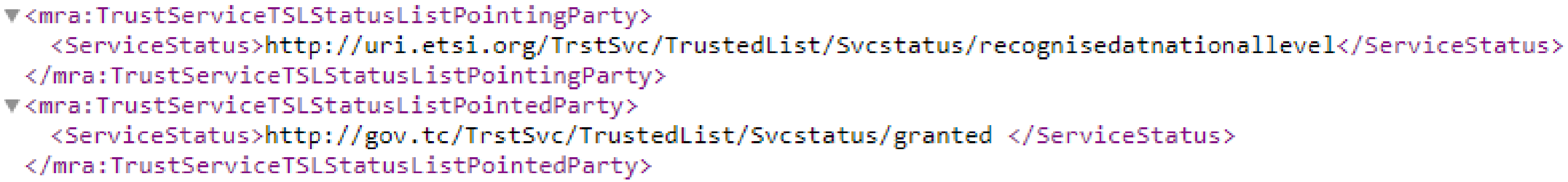
TC AdES LOTL

MRA-enabled TL

MRA element

2. Applying MRA transition rules : Trust service information from MRA

For a Trust Service:



```
▼<mra:TrustServiceTSLStatusListPointingParty>
   <ServiceStatus>http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/recognisedatnationallevel</ServiceStatus>
 </mra:TrustServiceTSLStatusListPointingParty>
▼<mra:TrustServiceTSLStatusListPointedParty>
   <ServiceStatus>http://gov.tc/TrstSvc/TrustedList/Svcstatus/granted </ServiceStatus>
 </mra:TrustServiceTSLStatusListPointedParty>
```

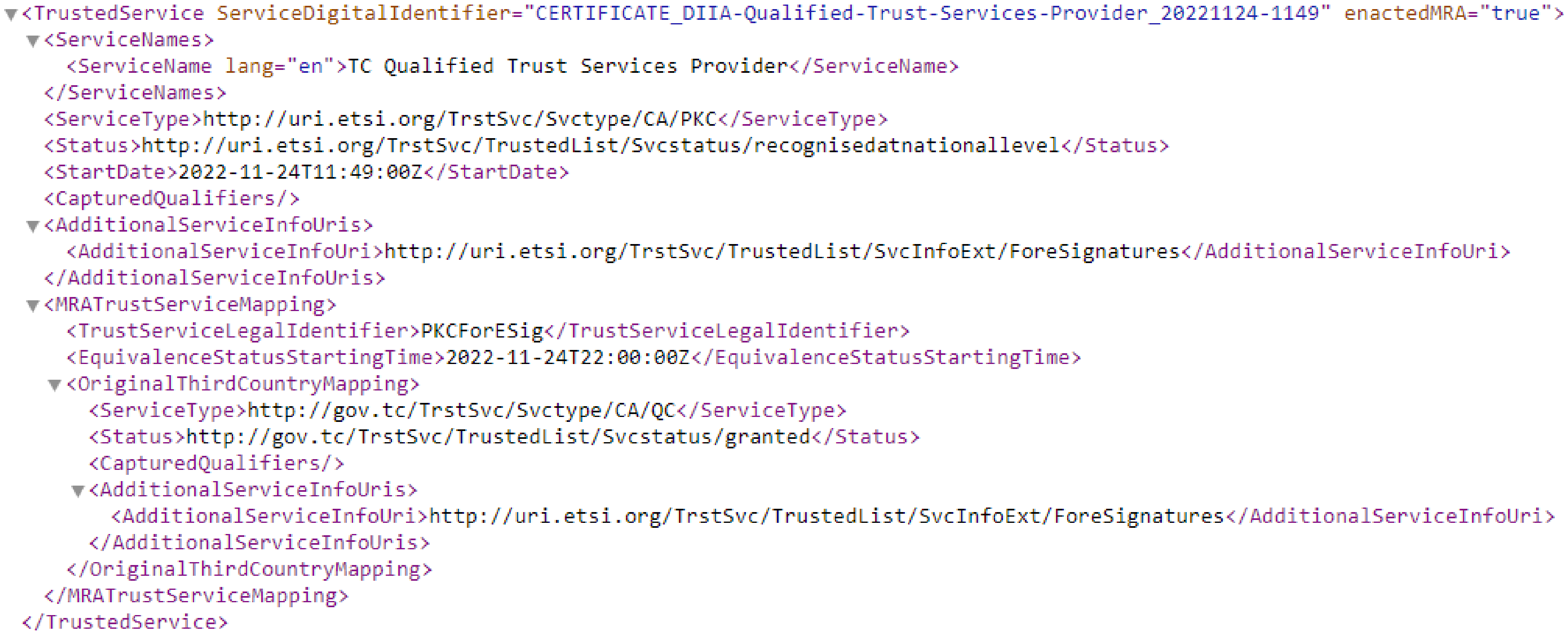
`http://gov.tc/TrstSvc/TrustedList/Svcstatus/granted` defined in Third Country TL

should be understood as:

`http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/recognisedatnationallevel` in EU scope

2. Applying MRA transition rules: Resulting Diagnostic Data (DD)

For each matching Trust Service, DSS performs transition of rules according to the mapping:



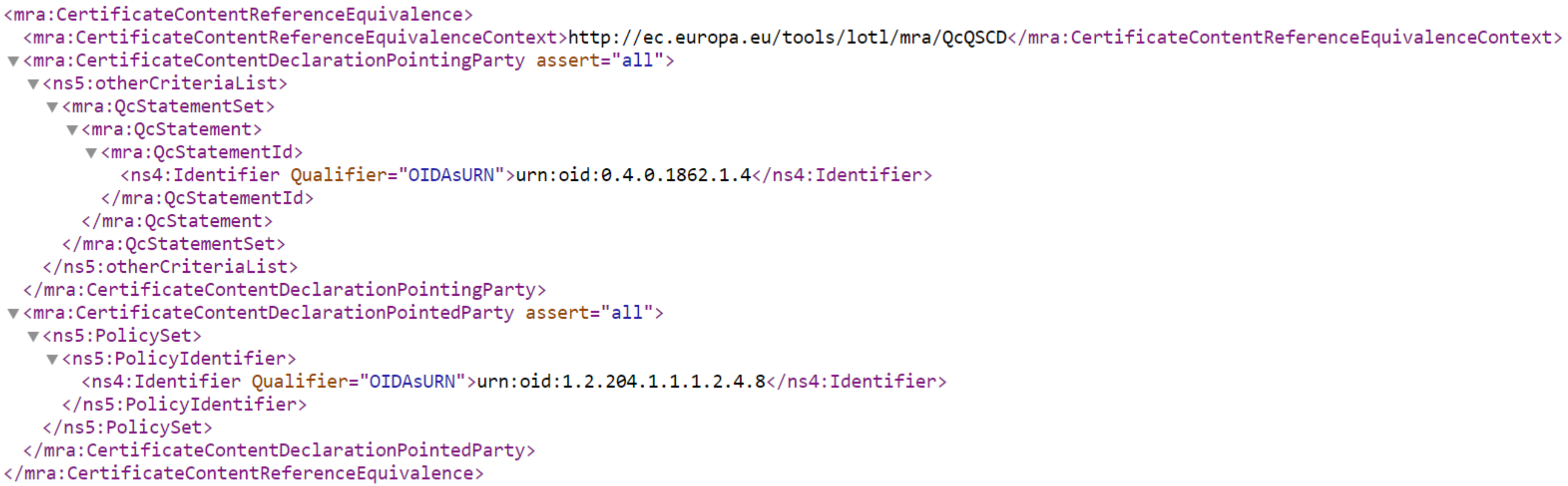
```
▼<TrustedService ServiceDigitalIdentifier="CERTIFICATE_DIIA-Qualified-Trust-Services-Provider_20221124-1149" enactedMRA="true">
  ▼<ServiceNames>
     <ServiceName lang="en">TC Qualified Trust Services Provider</ServiceName>
   </ServiceNames>
   <ServiceType>http://uri.etsi.org/TrstSvc/Svctype/CA/PKC</ServiceType>
   <Status>http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/recognisedatnationallevel</Status>
   <StartDate>2022-11-24T11:49:00Z</StartDate>
   <CapturedQualifiers/>
  ▼<AdditionalServiceInfoUris>
     <AdditionalServiceInfoUri>http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/ForeSignatures</AdditionalServiceInfoUri>
   </AdditionalServiceInfoUris>
  ▼<MRATrustServiceMapping>
     <TrustServiceLegalIdentifier>PKCForESig</TrustServiceLegalIdentifier>
     <EquivalenceStatusStartingTime>2022-11-24T22:00:00Z</EquivalenceStatusStartingTime>
    ▼<OriginalThirdCountryMapping>
       <ServiceType>http://gov.tc/TrstSvc/Svctype/CA/QC</ServiceType>
       <Status>http://gov.tc/TrstSvc/TrustedList/Svcstatus/granted</Status>
       <CapturedQualifiers/>
      ▼<AdditionalServiceInfoUris>
         <AdditionalServiceInfoUri>http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/ForeSignatures</AdditionalServiceInfoUri>
       </AdditionalServiceInfoUris>
     </OriginalThirdCountryMapping>
   </MRATrustServiceMapping>
</TrustedService>
```

transformed info

original content

2. Applying MRA transition rules: Certificate information from MRA

For certificate content:



```
<mra:CertificateContentReferenceEquivalence>
  <mra:CertificateContentReferenceEquivalenceContext>http://ec.europa.eu/tools/lotl/mra/QcQSCD</mra:CertificateContentReferenceEquivalenceContext>
▼<mra:CertificateContentDeclarationPointingParty assert="all">
  ▼<ns5:otherCriteriaList>
    ▼<mra:QcStatementSet>
      ▼<mra:QcStatement>
        ▼<mra:QcStatementId>
            <ns4:Identifier Qualifier="OIDAsURN">urn:oid:0.4.0.1862.1.4</ns4:Identifier>
          </mra:QcStatementId>
        </mra:QcStatement>
      </mra:QcStatementSet>
    </ns5:otherCriteriaList>
  </mra:CertificateContentDeclarationPointingParty>
▼<mra:CertificateContentDeclarationPointedParty assert="all">
  ▼<ns5:PolicySet>
    ▼<ns5:PolicyIdentifier>
        <ns4:Identifier Qualifier="OIDAsURN">urn:oid:1.2.204.1.1.1.2.4.8</ns4:Identifier>
      </ns5:PolicyIdentifier>
    </ns5:PolicySet>
  </mra:CertificateContentDeclarationPointedParty>
</mra:CertificateContentReferenceEquivalence>
```

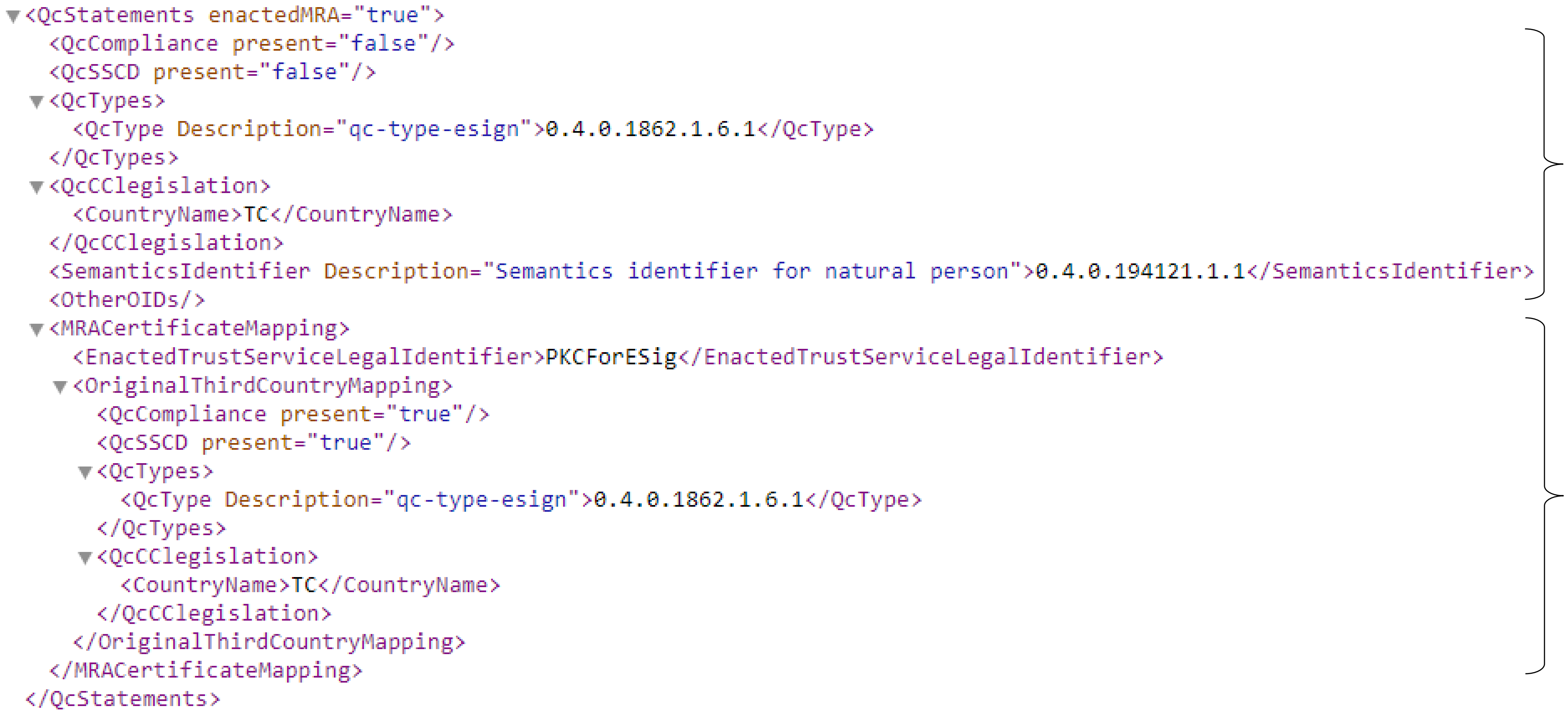
Certificate policy `1.2.204.1.1.1.2.4.8` defined in Third Country TL

corresponds to:

QcStatement `0.4.0.1862.1.4 (qc-sscd)` in EU scope

2. Applying MRA transition rules: Resulting Diagnostic Data (DD)

The same is done for corresponding certificate's content rules:



```
▼<QcStatements enactedMRA="true">
   <QcCompliance present="false"/>
   <QcSSCD present="false"/>
 ▼<QcTypes>
     <QcType Description="qc-type-esign">0.4.0.1862.1.6.1</QcType>
   </QcTypes>
 ▼<QcCClegislation>
     <CountryName>TC</CountryName>
   </QcCClegislation>
   <SemanticsIdentifier Description="Semantics identifier for natural person">0.4.0.194121.1.1</SemanticsIdentifier>
   <OtherOIDs/>
 ▼<MRACertificateMapping>
     <EnactedTrustServiceLegalIdentifier>PKCForESig</EnactedTrustServiceLegalIdentifier>
   ▼<OriginalThirdCountryMapping>
       <QcCompliance present="true"/>
       <QcSSCD present="true"/>
     ▼<QcTypes>
         <QcType Description="qc-type-esign">0.4.0.1862.1.6.1</QcType>
       </QcTypes>
     ▼<QcCClegislation>
         <CountryName>TC</CountryName>
       </QcCClegislation>
     </OriginalThirdCountryMapping>
   </MRACertificateMapping>
 </QcStatements>
```

transformed info

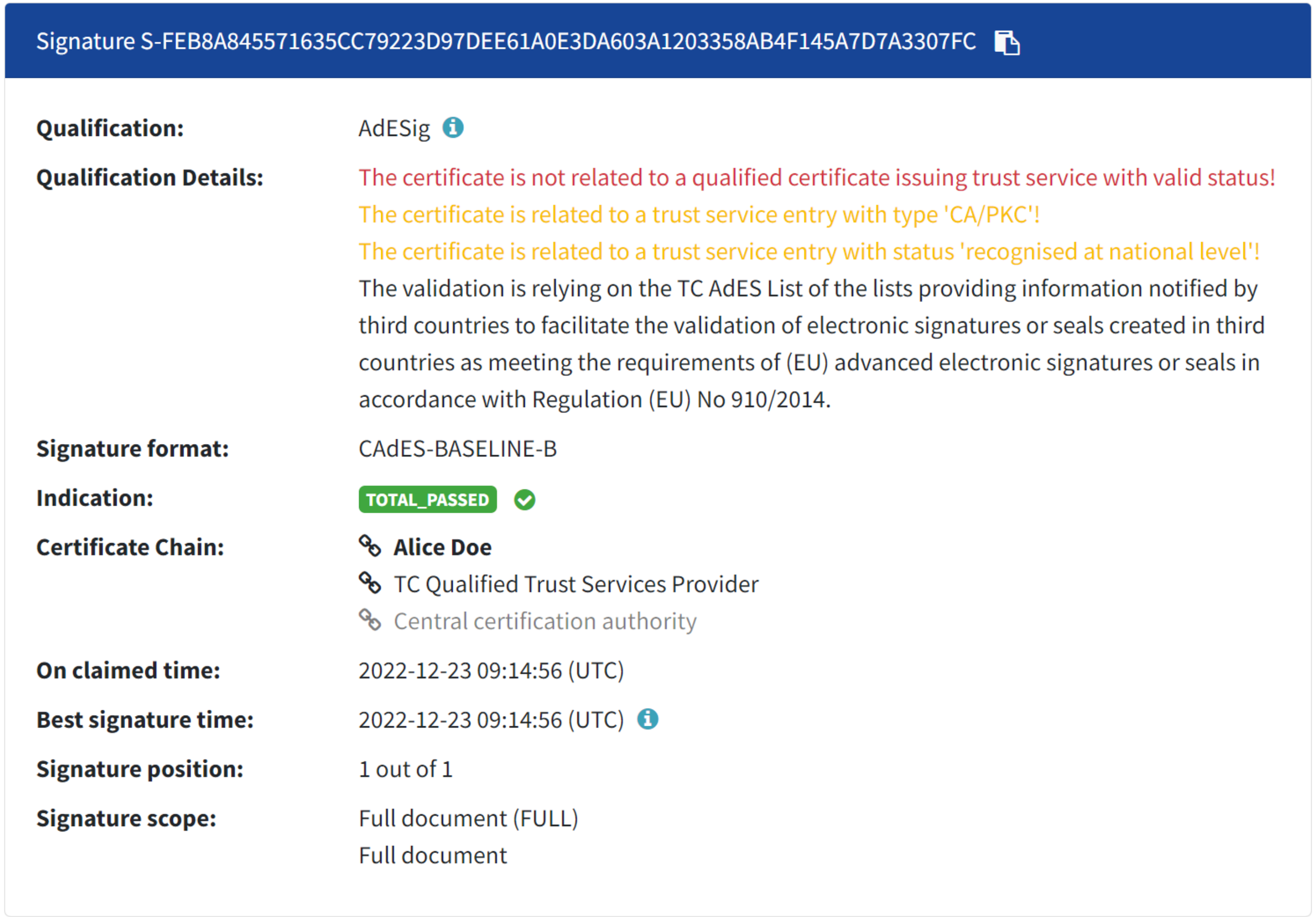
original content

3. Running signature/certificate validation

Run validation process using the transformed data:

- per ETSI EN 319 102-1 (AdES validation);
- per ETSI TS 119 615 (qualification status determination).

4. Producing the results



Signature S-FEB8A845571635CC79223D97DEE61A0E3DA603A1203358AB4F145A7D7A3307FC

Qualification:	AdESig
Qualification Details:	The certificate is not related to a qualified certificate issuing trust service with valid status! The certificate is related to a trust service entry with type 'CA/PKC'! The certificate is related to a trust service entry with status 'recognised at national level'! The validation is relying on the TC AdES List of the lists providing information notified by third countries to facilitate the validation of electronic signatures or seals created in third countries as meeting the requirements of (EU) advanced electronic signatures or seals in accordance with Regulation (EU) No 910/2014.
Signature format:	CAdES-BASELINE-B
Indication:	TOTAL_PASSED ✓
Certificate Chain:	**Alice Doe** TC Qualified Trust Services Provider Central certification authority
On claimed time:	2022-12-23 09:14:56 (UTC)
Best signature time:	2022-12-23 09:14:56 (UTC)
Signature position:	1 out of 1
Signature scope:	Full document (FULL) Full document

final qualification level (in EU scope)

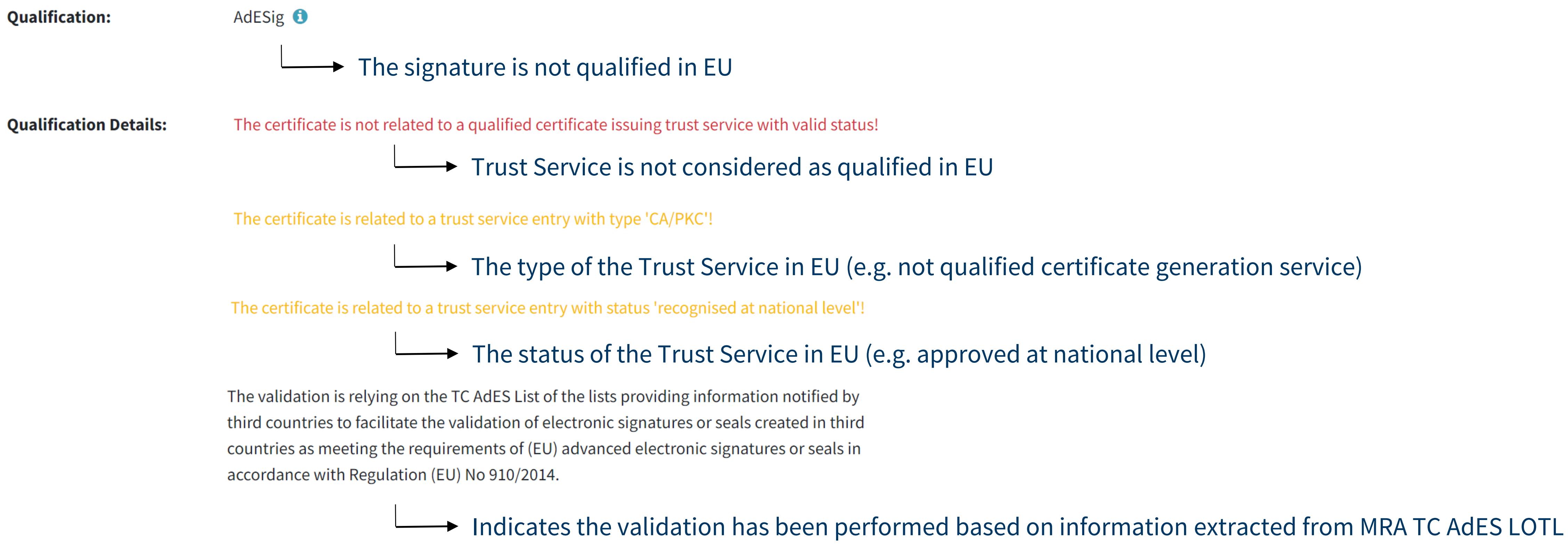
qualification details (in EU scope)

label indicating the MRA applicability

basic signature validation information (ETSI EN 319 102-1)

4. Producing the results

The qualification determination process returns **a qualification status**, but also **a list of messages** helping to identify applicability of a signature in the given context.



Qualification: AdESig ℹ

→ The signature is not qualified in EU

Qualification Details:

The certificate is not related to a qualified certificate issuing trust service with valid status!

→ Trust Service is not considered as qualified in EU

The certificate is related to a trust service entry with type 'CA/PKC'!

→ The type of the Trust Service in EU (e.g. not qualified certificate generation service)

The certificate is related to a trust service entry with status 'recognised at national level'!

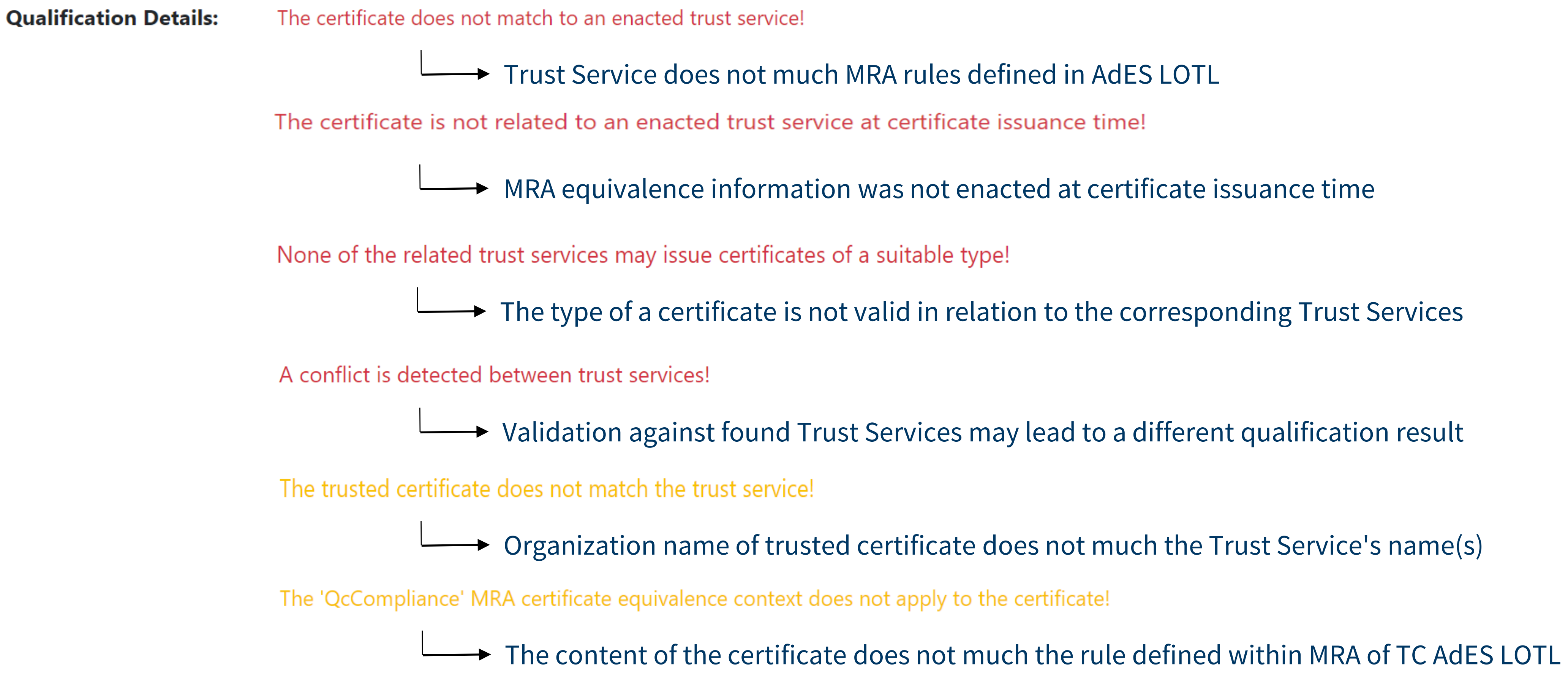
→ The status of the Trust Service in EU (e.g. approved at national level)

The validation is relying on the TC AdES List of the lists providing information notified by third countries to facilitate the validation of electronic signatures or seals created in third countries as meeting the requirements of (EU) advanced electronic signatures or seals in accordance with Regulation (EU) No 910/2014.

→ Indicates the validation has been performed based on information extracted from MRA TC AdES LOTL

4. Producing the results

The messages may also **point to issues** within a Trust Service or a certificate, for instance:



Qualification Details:

The certificate does not match to an enacted trust service!

→ Trust Service does not much MRA rules defined in AdES LOTL

The certificate is not related to an enacted trust service at certificate issuance time!

→ MRA equivalence information was not enacted at certificate issuance time

None of the related trust services may issue certificates of a suitable type!

→ The type of a certificate is not valid in relation to the corresponding Trust Services

A conflict is detected between trust services!

→ Validation against found Trust Services may lead to a different qualification result

The trusted certificate does not match the trust service!

→ Organization name of trusted certificate does not much the Trust Service's name(s)

The 'QcCompliance' MRA certificate equivalence context does not apply to the certificate!

→ The content of the certificate does not much the rule defined within MRA of TC AdES LOTL

Future outlook

- **Trusted lists** are likely to play a crucial role in building trust and interoperability in **cross-border digital transactions** between countries/regions with differing regulatory environments.

- New standardization efforts should be launched to ease and support adoption of **trusted lists by non-EU countries**, in particular re-usable **standardized procedures** should be established to **interpret** non-EU trusted lists.

COFFEE BREAK

15:50 – 16:20

11

Ask your questions in our open discussion

Join at

slido.com

#4172 878

12

Closing remarks

Natalia ARISTIMUÑO PÉREZ

Director Digital Services – DG DIGIT, European Commission

Thank you

Sign up to receive updates about future events