Trust Services Forum

Global Recognition of EU Trust Services – what are the challenges?

COL Peter Rybár
Member of ISO, CEN and ETSI
National eIDAS expert
Regulation and Supervision Department
National Security Authority
Bratislava | Slovak Republic
peter.rybar@nbu.gov.sk | www.nbu.gov.sk

Free QES application qes.webnode.sk/en/

Smart national solutions accessible in global standards - ISO

German – positive statement - ***CertHash*** OCSP *SingleResponse*

ISO 14533-4:2019, Annex B - Definition of the *CertHash* OCSP *SingleResponse*

Estonia – OCSP time-stamp based on fields *producedAt* and *Nonce*.

The time at which the OCSP responder signed this response is included in the ***producedAt*** field and the hash (OID, value) of the time-stamped digital signature is included in the ***nonce*** field.

ISO 14533-4:**2019**, Annex C - Signature timestamp as a timestamp through OCSP

IETF RFC 8954 **November 2020**, Updates: IETF RFC 6960

Online Certificate Status Protocol (OCSP) *Nonce* Extension

IETF RFC 6960 - Nonce ::= OCTET STRING

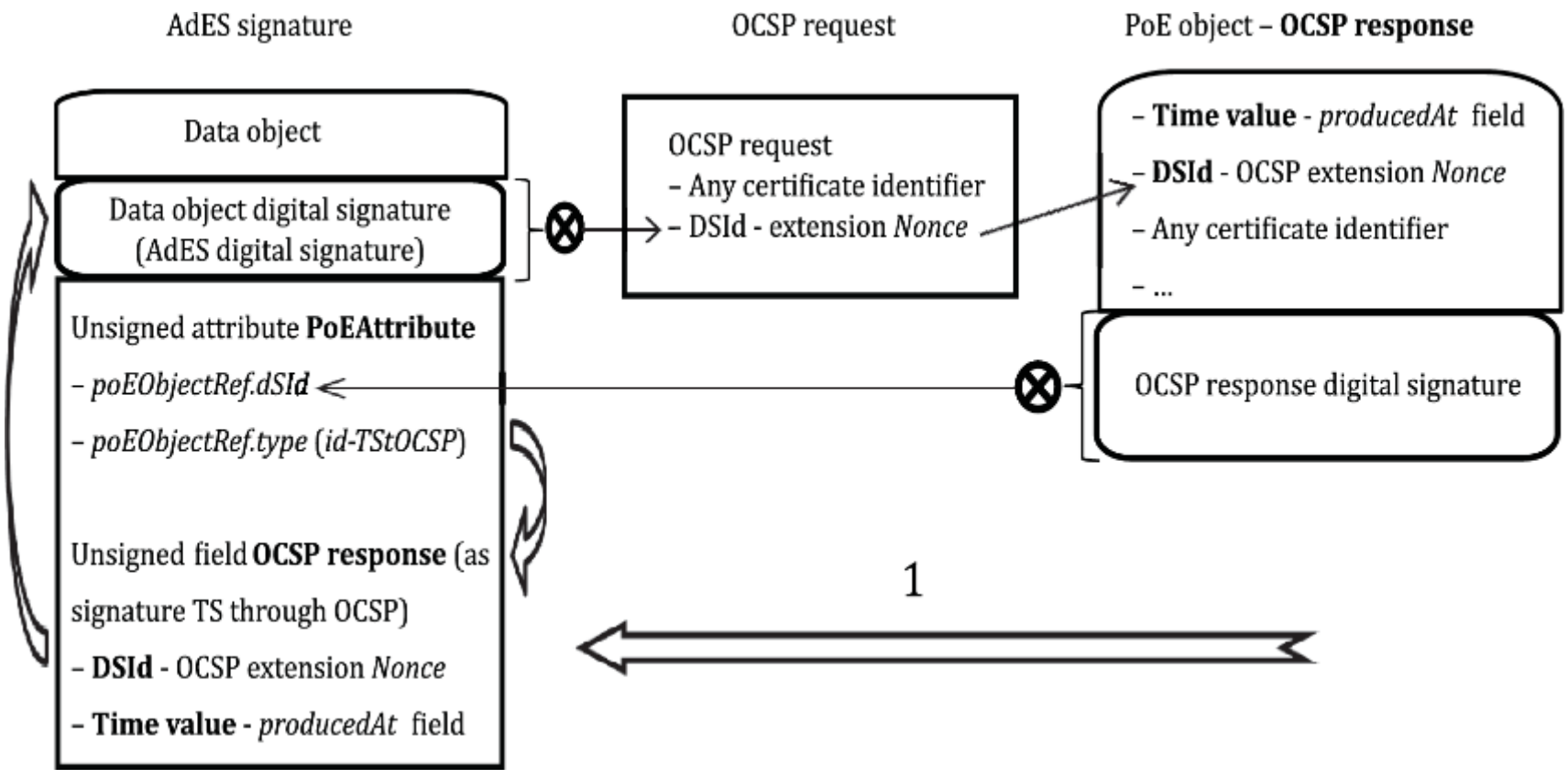
IETF RFC 8954 - Nonce ::= OCTET STRING(SIZE(1..**32**))

A server MUST reject any OCSP request that has a nonce in the Nonce extension with a length of either 0 octets or more than **32** octets with the *malformedRequest OCSPResponseStatus*, as described in Section 4.2.1 of [RFC6960].

IETF RFC xyz, update with a compromise - Nonce ::= OCTET STRING(SIZE(1..**98**))

A server MUST reject any OCSP request that has a nonce in the Nonce extension with a length of either 0 octets or more than **98** octets with the *malformedRequest OCSPResponseStatus*, as described in Section 4.2.1 of [RFC6960], where the **nonce with a length of more than 32 octets SHALL be permitted after the authentication of the client requesting OCSP response**.

OCSP response as the Signature Timestamp ISO 14533-4:2019



1 **External PoE object is included in the signature.**
NOTE **OCSP extension Nonce contains the hash value of the signature.**

ISO 14533-4:2019, Annex C - Signature timestamp as a timestamp through OCSP

Remote QSCD service is also a qualified time-stamping service

Clause 3.3 of ISO 14533-4:2019, defines document signature identifier **DSId** as an indirect identifier of signature of a document for machine processing in the form of DER encoded ASN.1 type *MessageImprint* defined in IETF RFC 3161 covering the DER encoded result of the asymmetric signature algorithm.

The service of the remote qualified electronic signature/seal creation devices (QSCD)

- creates the digital signature value, using the signer private key after the signer authorization (the knowledge authentication factor), and
- can create also the signature time-stamp token of this value, and publish it on the service web https://www.example.eu/qts/dsid/[**DSId** "base64url"].tst for downloading by the signature creation application.

See examples:

The signature time-stamp for CMS AdES and PDF AdES formats (ASN.1 LTV):
https://www.example.eu/qts/**cms**/MDEwDQYJYIZIAWUDBAIBBQAEIO5VatzJpwUTWk1JyWHks1MHRldJ8Pk2CMnBI5sNifVw.tst

The signature time-stamp for XML AdES format (from the XML element):
https://www.example.eu/qts/**xml**/MDEwDQYJYIZIAWUDBAIBBQAEIO5VatzJpwUTWk1JyWHks1MHRldJ8Pk2CMnBI5sNifVw.tst

The signature time-stamp for CMS/PDF/XML/… AdES in a new attribute:
https://www.example.eu/qts/**der**/MDEwDQYJYIZIAWUDBAIBBQAEIO5VatzJpwUTWk1JyWHks1MHRldJ8Pk2CMnBI5sNifVw.tst

Trust infrastructure of the supervisory body

Article 17(5) of Regulation (EU) No 910/2014 - Member States may require the supervisory body to establish, maintain and update a trust infrastructure in accordance with the conditions under national law.

§ 11(g) of Act No. 272/2016 Coll. on Trust Services – the supervisory body provides information from the trusted infrastructure, in particular information after the expiry of a qualified certificate, in the form of a positive statement (ISO 14533-4:2019, Annex B) on the validity or revocation status of qualified certificates (OCSP response). See the web Trusted List - NBU (gov.sk):

Trusted List

TL and QES Applications

Qualified Certificates

Standards

e-forms

information related to the qualified trust services provided by them, in accordance with the relevant provisions laid down in Regulation (EU) No 910/2014 of the European Parliament and of the Council of 23 July 2014 on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC.

Trusted list according to Commission Implementing Decision (EU) 2015/1505

In machine processable form	http://ep.nbu.gov.sk/kca/tsl/tsl.xml http://tl.nbu.gov.sk/kca/tsl/tsl.xml https://tl.nbu.gov.sk/kca/tsl/tsl.xml
In the form of seal from "tsl.xml" form in the format of CMS advanced electronic seal	http://ep.nbu.gov.sk/kca/tsl/tsl.xml.p7s http://tl.nbu.gov.sk/kca/tsl/tsl.xml.p7s https://tl.nbu.gov.sk/kca/tsl/tsl.xml.p7s

Documentation of the Trusted List XML Extensions

Documentation of TL X.509 XML Scheme for Trusted List (pdf, 497kB)

Authorized service - Trusted List service Identifier (TLI)

The "AuthorizedService" element specifies the other service authorized for providing services on behalf of this service. The other service is identified by "TLIxx-y" or "TLIxx-" included in "TLServiceIdentifier", where "xx" is a Country Code from 'Scheme territory' (TS 119 612 v2.1.1,5.3.10) and "y" is a positive number (service name index) in TL "Name" of "ServiceName" as "(y) z", where the "z" is a service name or when "(y) " is not included in "Name" of "ServiceName" then the other service is identified by "TLIxx-" and by one or more "TrustAnchor" elements containing, e.g. certificates in "TLServiceX509Certificate" element. The elements "notBefore" and "notAfter" determine the time interval, in which the other service provider is authorized for providing the service on behalf of this service provider.

```
</ServiceSupplyPoints>
- <ServiceInformationExtensions>
  - <Extension Critical="false">
      <ExpiredCertsRevocationInfo>2009-12-08T12:47:30Z</ExpiredCertsRevocationInfo>
    </Extension>
  - <Extension Critical="false">
    - <tlx509:URLContentTypeAndAuthorizedServiceList
      xmlns:tlx509="http://ep.nbu.gov.sk/kca/tsl/x509types#">
      - <tlx509:URLContentTypeAndAuthorizedService>
          <tlx509:URL>http://ocsp.nbu.gov.sk/ocsp/pqc</tlx509:URL>
          <tlx509:ContentType>application/ocsp-request</tlx509:ContentType>
        - <tlx509:AuthorizedService>
            <tlx509:TLServiceIdentifier>TLISK-99</tlx509:TLServiceIdentifier>
            <tlx509:notBefore>2019-12-08T12:46:26Z</tlx509:notBefore>
          </tlx509:AuthorizedService>
        </tlx509:URLContentTypeAndAuthorizedService>
      </tlx509:URLContentTypeAndAuthorizedServiceList>
    </Extension>
  - <Extension Critical="true">
    - <AdditionalServiceInformation>
        <URI
          xml:lang="en">http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/ForeSignatur
      </AdditionalServiceInformation>
    </Extension>
  - <Extension Critical="true">
```

Supervisory body as authorized service - national trusted list extension

Trusted List XML Extensions

Documentation of TL X.509 XML Scheme for Trusted List (pdf, 497kB)

National rules, identified by OIDs of the Certificate Policy (CP), must be fulfilled by qualified trust service providers. Such rules are delegated by Regulation (EU) No 910/2014 to the national law, e.g. the suspension laid down in Article 28(5) or the creation of the trust infrastructure laid down in Article 17(5).

The certificate policy, OID 1.3.158.36061701.0.0.0.1.2.2, for certificates issued by the qualified trust service provider requires at least:

1. the usage of suspension is forbidden,
2. when the trust infrastructure implements the OCSP then the OCSP response must contain *CertHash* OID 1.3.36.8.3.13 (ISO 14533-4:2019, Annex B a positive statement is an extension defined for the *SingleResponse* type in *singleExtensions*), and
3. the Member State supervisory body's database must be an additional repository (the repository is actualized at least once a month) which contains all qualified certificates (at least the certificates once they reach their expiration date) issued by supervised qualified trust service providers together with their validity status.

This repository guarantees the qualified certificate usage and the qualified certificate verification after the certificate expiration and also after the date when the qualified status of the provider issuing the certificate of the affected service has been withdrawn. It means, the supervisory body's database is used in the situation when the trust service provider is not able to remedy any failure to fulfil requirements under Regulation (EU) No 910/2014 and where that provider does not act accordingly.

Trusted List Identifier - TLI

The TL Service Identifier shall be used as "TLIxx-y" or "TLIxx-", where "xx" is a Country Code from 'Scheme territory' (TS 119 612 v2.1.1,5.3.10) and "y" is a positive number (service name index) in TL "Name" of "ServiceName" as "(y) z", where the "z" is a service name.

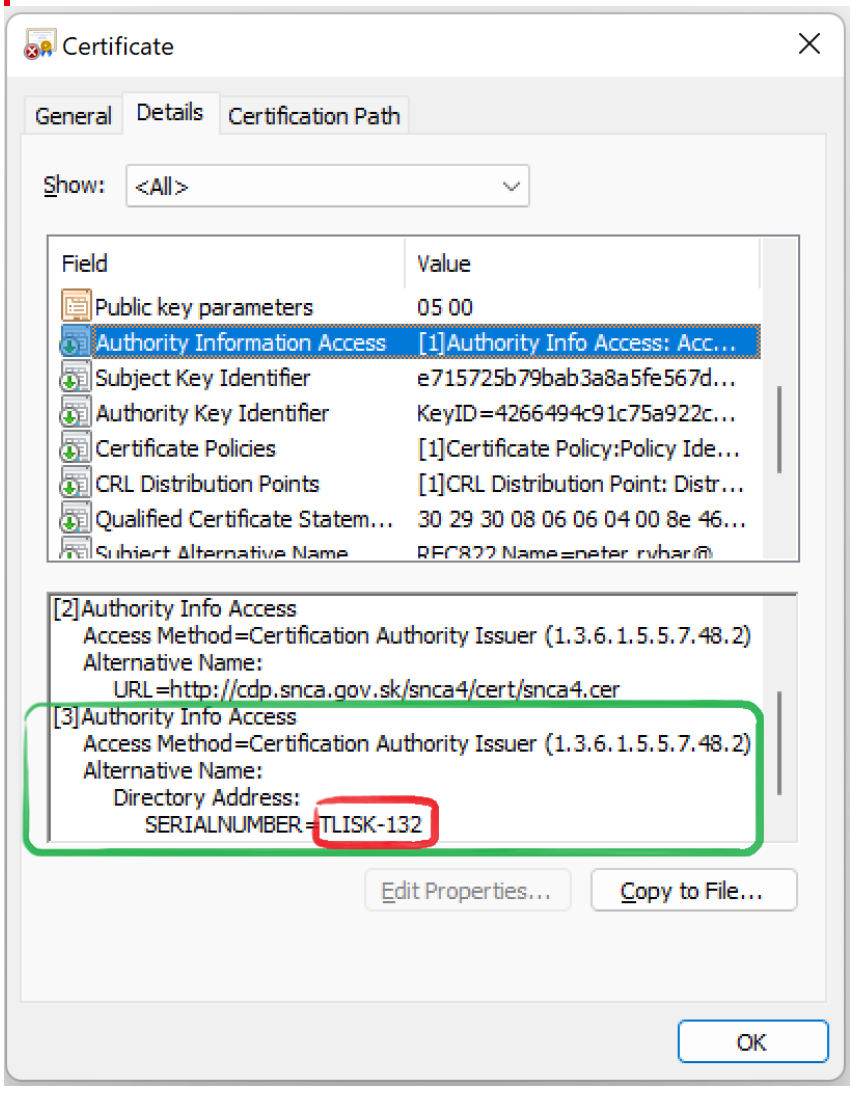
NOTE 1: When this service is a qualified trust service, the value "TLIxx-y" of TL "Name" of "ServiceName" as "(y) z" can be associated with graphical elements defined for the EU trust mark in Annexes I and II of the Commission Implementing Regulation (EU) 2015/806 of 22 May 2015 laying down specifications relating to the form of the EU trust mark for qualified trust services.

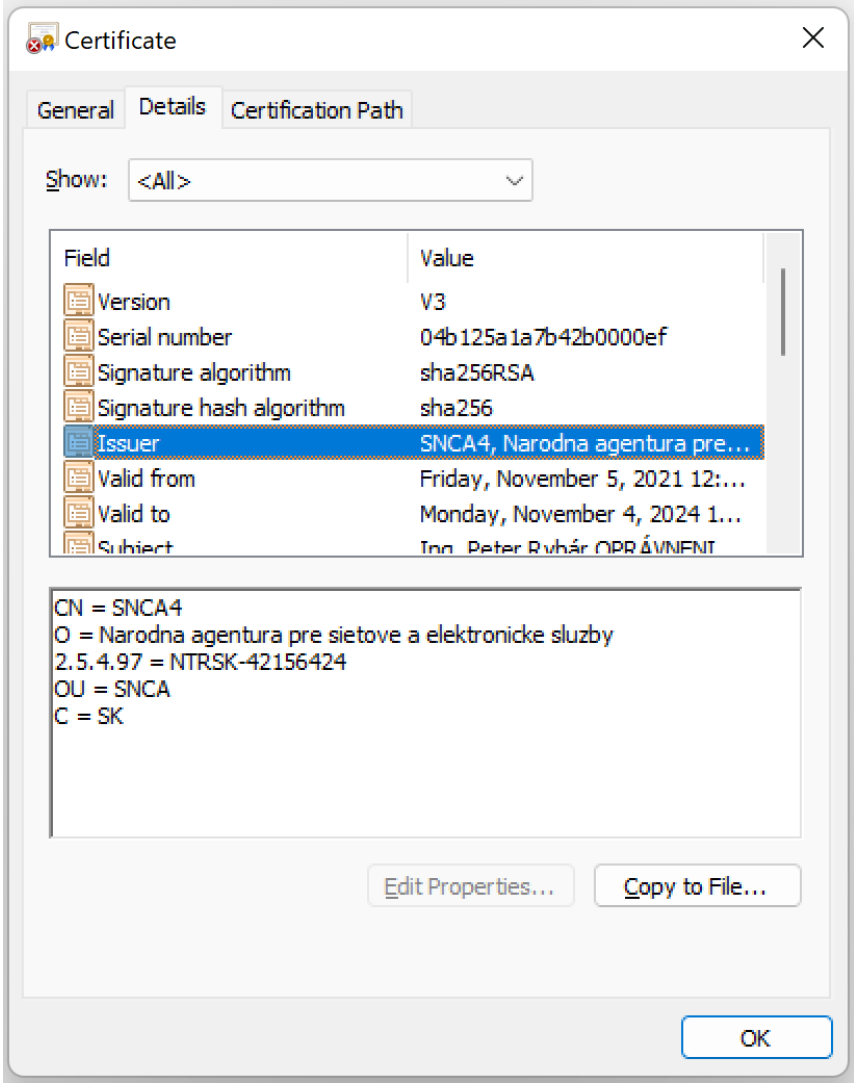
NOTE 2: When this service is an issuer of the certificate, then issued certificate can contain the value "TLIxx-y" of TL "Name" of "ServiceName" as "(y) z" as a reference to this service, in the certificate extension Authority Information Access. In this case the *accessMethod* field contains *id-ad-caIssuers* (see RFC5280 Section 4.2.2.1). The trusted list service identifier of the issuer service is included in the ***accessLocation*** field of *GeneralName* type as *directoryName* as a component of *X520SerialNumber* type.

Issuer of the qualified certificate **TLISK-132**
https://tl.nbu.gov.sk/kca/tsl/tsl.xml

Example: X520SerialNumber = "TLISK-132"

Example: X520SerialNumber = "TLISK-132"





NATIONAL SECURITY AUTHORITY

TLI in the validation report of the qualified electronic signature

The validation report of the qualified electronic signature according to Article (32)1 of the Regulation (EU) No 910/2014:

(a) the certificate that supports the signature was, at the time of signing [claimed time 23. 9. 2022 22:48:02, given time 23. 9. 2022 22:48:22] a qualified certificate for electronic signature complying with Annex I [Yes];

(b) the qualified certificate was issued [5. 11. 2021 11:15:59] by a qualified trust service provider

[TSL Sequence Number: 95
TSP name: National Agency for Network and Electronic Services
Service identifier: **TLISK-132**
] and was valid at the time of signing [given time 23. 9. 2022 22:48:22];

(c) the signature validation data corresponds to the data provided to the relying party [Yes];

(d) the unique set of data representing the signatory in the certificate is correctly provided to the relying party [Subject:

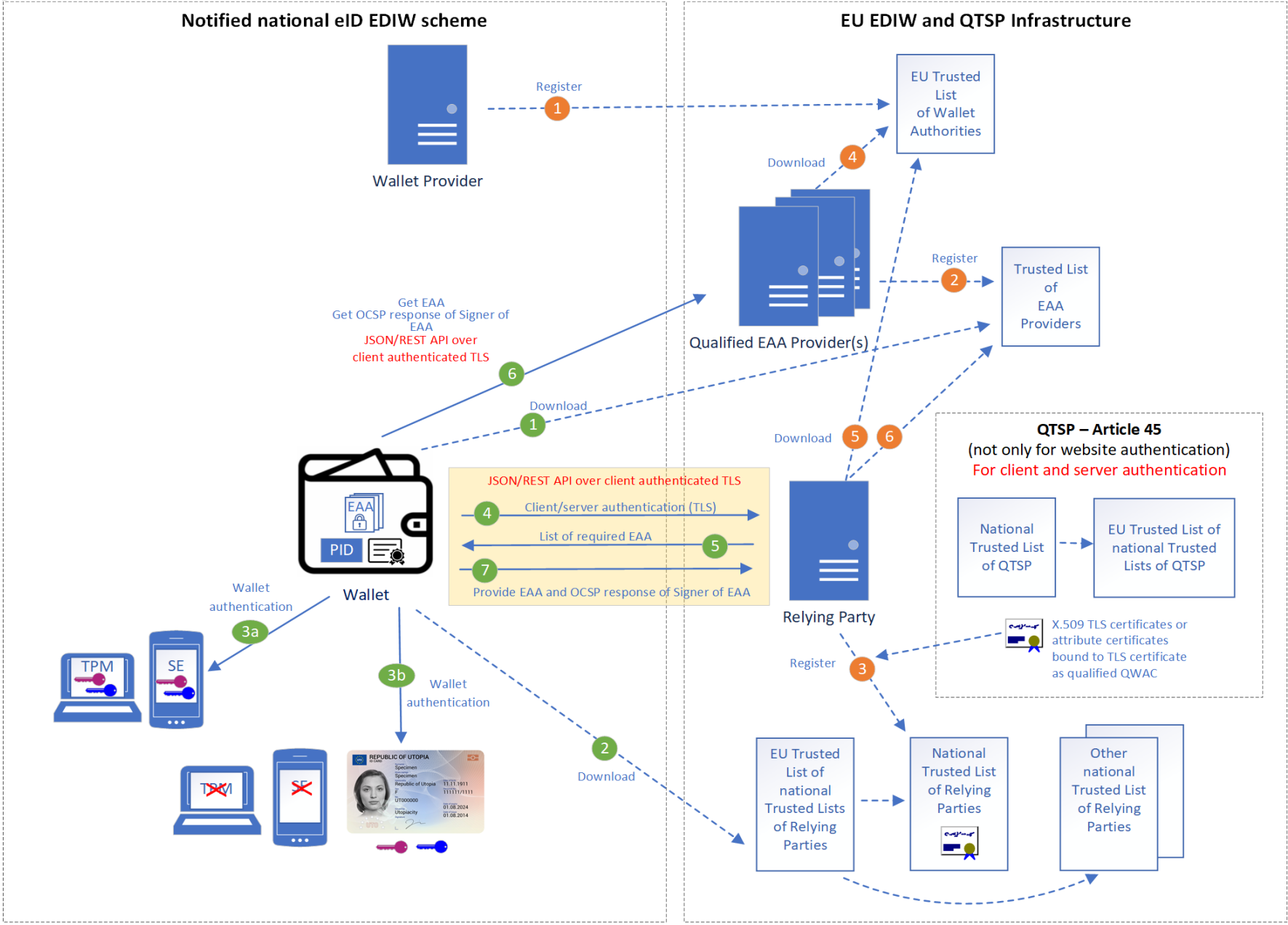
SK	countryName(2.5.4.6)
Bratislava	localityName(2.5.4.7)
Peter	givenName(2.5.4.42)
Rybár	surname(2.5.4.4)
PNOSK-NSA-1443	serialNumber(2.5.4.5)
Ing. Peter Rybár	commonName(2.5.4.3)
peter.rybar@nbu.gov.sk	RFC822Name]

(e) the use of any pseudonym is clearly indicated to the relying party if a pseudonym was used at the time of signing [Yes];

(f) the electronic signature was created by a qualified electronic signature creation device [Yes];

(g) the integrity of the signed data has not been compromised [Yes];

(h) the requirements provided for in Article 26 were met at the time of signing [Yes].



SE Secure Element

TPM Trusted Platform Module

Authentication Certificate

PID Person Idenitification Data

Encryption keypair

Authentication keypair

Encrypted Electronic Attestation of Attributes (EAA)

Unencrypted Electronic Attestation of Attributes (EAA)

Qualified Website authentication certificate (QWAC)

THANKS FOR YOUR ATTENTION