The Standards People

Standards for TSPs issuing certificates ETSI EN 319 401/411/412

Presented by: **Sylvie Lacroix**

For: **Training on ETSI Standards for trust services**

01.06.2021

Trust service issuing certificates: Policy and security requirements

- ETSI EN 319 401 General Policy Requirements for Trust Service Providers
  - TSP documentation
  - TSP management & operation (HR, physical security, network security, business continuity & incident management, termination of service)
- ETSI EN 319 411-1: Policy and security requirements for Trust Service Providers issuing certificates; Part 1: General requirements
  - Basically two levels: LCP (good practices) – NCP (best practices. E.g. supports Advanced eSignature)

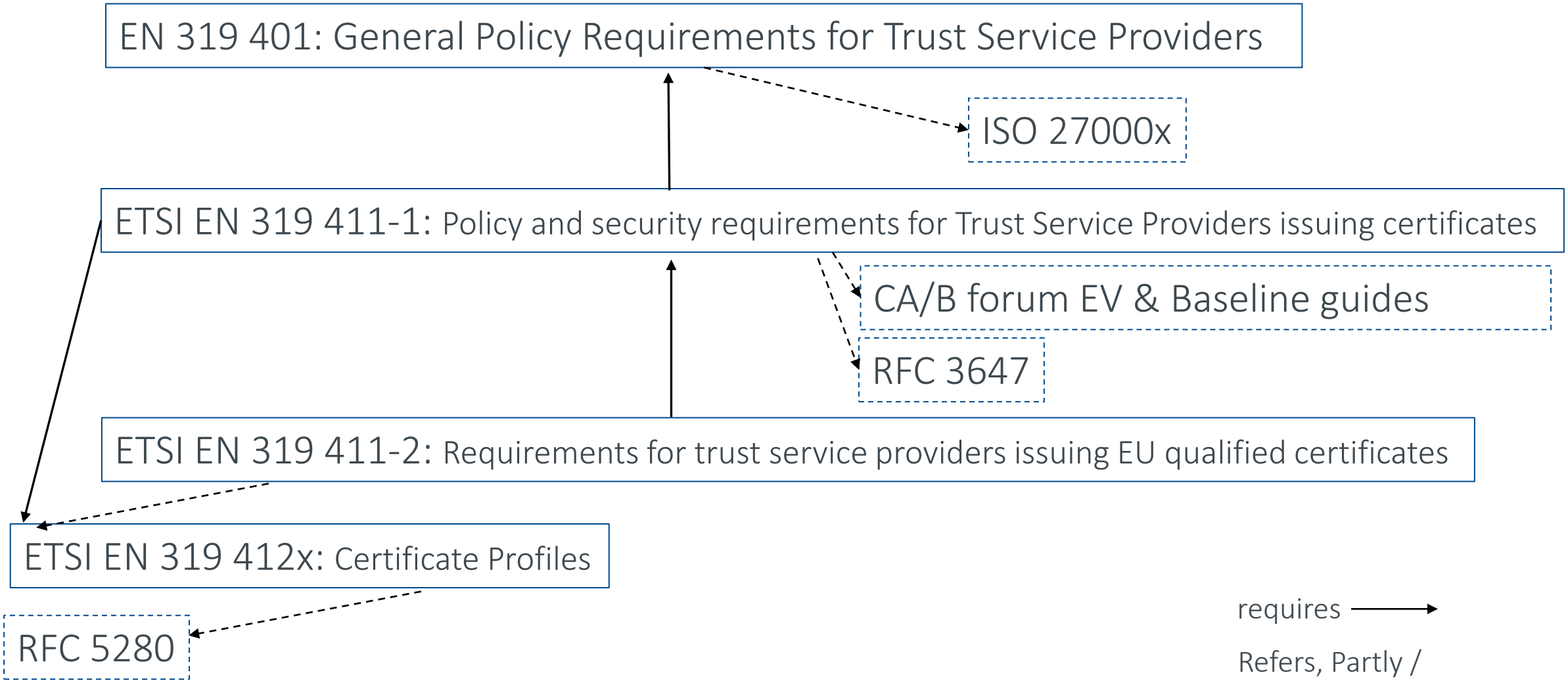
Trust service issuing certificates: Policy and security requirements

- ETSI EN 319 411-2: Policy and security requirements for Trust Service Providers issuing certificates; Part 2: Requirements for trust service providers issuing EU qualified certificates
  - Reference CPs: QCP-l, QCP- n, QCP-l-qscd, QCP-n-qscd, QCP-w, for the issuance, maintenance and life-cycle management of qualified certificates issued to natural persons (including natural persons associated with a legal person), to legal persons and websites
  - Level aligned on NCP and additional requirements for EU qualified certificates. E.g. information on revocation status kept beyond certificate expiry, qCstatement as per EN 319 412-5
- Other countries may build their own “part2” on the basis of EN 319-411-1 similarly to EN 319 412-2 for EU certificates (see clause 7)
- ETSI TR 119 411-4: Checklist for TSPs issuing certificates (with filters to sort per CP, e.g.)

Trust service issuing certificates: Certificate Profiles

- EN 319 412-1: Part 1: Overview and common data structures
  - Based on RFC 5280
- EN 319 412-2: Part 2: Certificate profile for certificates issued to natural persons
  - DN, KU combination, etc.
- EN 319 412-3: Part 3: Certificate profile for certificates issued to legal persons
  - Refers to part 2 + indications for identifiers for organization e.g.
- EN 319 412-4: Part 4: Certificate profile for web site certificates
  - Reference to CA/B forum
- EN 319 412-5: Part 5: QCStatements
  - E.g. to advertise a certificate is EU-qualified or issued under another legal context, stored on a QSCD, for eSeal, etc.

Trust service issuing certificates



Trust service issuing certificates

- Update on EN 319 401 and EN 319 411-1 & -2 in October 2021
  - Mostly for clarifications, improvement of wording, small corrections
- The above EN provides technical criteria for TSP issuing certificates. Specification for audit(or) are provided in other EN (presented by M. Fiedler)
- Important to note:
  - Open to other than European context
  - Support for short-term certificate, i.e. “certificate whose validity period, i.e. the period of time from notBefore through notAfter, inclusive, is shorter than the maximum time to process a revocation request as specified in the certificate practice statement”
    - No obligation for a ‘revocation service’ (i.e. call desk), no obligation for both OCSP and CRL
    - the relying party can decide not to check the certificate revocation status, for example, when validating a digital signature

Certification Policy and Certificate Profiles for Open Banking.

Arno Fiedler,
Nimbus Technologieberatung GmbH

Motivation for TS 119 495

Article 34

Revised Payment Services Directive (PSD2, Directive (EU) 2015/2366)

Certificates

1. For the purpose of identification, as referred to in Article 30(1)(a), payment service providers shall rely on qualified certificates for electronic seals as referred to in Article 3(30) of Regulation (EU) No 910/2014 or for website authentication as referred to in Article 3(39) of that Regulation.

- The Technical Specification defines the branch specific requirements for Trust Service Provider issuing qualified seals and website certificates to payment service provider.
- The purpose is to prove origin and authenticity of transactions.

Meeting Open Banking / Finance requirements in TS 119 495

Applicable Open Banking / Open Finance Certificate Policy Requirements

TS 119 495

EN 319 411-1 TSP issuing Certs

or

EN 319 411-2 TSP issuing EU Qualified Certs

\+

EN 319 412-4 Website Authentication

and / or

EN 319 412--3 Legal Person (Seal)

Applicable Open Banking / Open Finance Certificate Content Requirements

Authorisation Number:
PSD<country code> <Competent Authority ID> <Assigned identifier>

Roles: PSP_AS, PSP_PI, PSP_AI, PSP_IC
or other competent authority defined role of Unspecified

Competent Authority Name and Identifier 2-8 upper case alpha)

New in 2021: JAdES digital signature specification supports implementation (see ETSI TS 119 182-1)

Many thanks!

Sylvie Lacroix

Arno Fiedler