ETSI standards for trust services and digital signatures
- Overview

Presented by: Nick Pope
Security & Standards Associates

For: ETSI Standards Training Webinar

01.06.2021

© ETSI 2021 – All rights reserved
<table>
<thead>
<tr>
<th>Time</th>
<th>Topic</th>
<th>Presented by</th>
</tr>
</thead>
<tbody>
<tr>
<td>11:00</td>
<td>1) Overview of ETSI TSP standards</td>
<td>Nick Pope (Security &amp; Standards Associates)</td>
</tr>
<tr>
<td>11:20</td>
<td>2) Signature formats &amp; verification procedures</td>
<td>Andrea Rock (Universign) &amp; Juan Carlos Cruellas (UPC)</td>
</tr>
<tr>
<td>11:40</td>
<td>3) Standards for TSPs issuing certificates</td>
<td>Sylvie Lacroix (Sealed) &amp; Arno Fiedler (Nimbus)</td>
</tr>
<tr>
<td>12:00</td>
<td>Break</td>
<td></td>
</tr>
<tr>
<td>12:15</td>
<td>4) Other Trust Application standards</td>
<td>Andrea Caccia (Small Business Standards), Andrea Rock (Universign), Juan Carlos (UPC)</td>
</tr>
<tr>
<td>12:35</td>
<td>5) TSP Supervision, Certification and Audit</td>
<td>Arno Fiedler (Nimbus)</td>
</tr>
<tr>
<td>12:55</td>
<td>6) Identity proofing</td>
<td>Sylvie Lacroix (Sealed)</td>
</tr>
<tr>
<td>13:15</td>
<td>Break</td>
<td></td>
</tr>
<tr>
<td>13:30</td>
<td>7) Remote signing</td>
<td>Andrea Rock (Universign)</td>
</tr>
<tr>
<td>13:50</td>
<td>8) Trusted lists</td>
<td>Olivier Delos (Sealed)</td>
</tr>
<tr>
<td>14:10</td>
<td>9) Mutual recognition of non-EU trust service</td>
<td>Olivier Delos (Sealed)</td>
</tr>
<tr>
<td>14:30</td>
<td>10) Future trends, Discussion &amp; Closing remarks</td>
<td>Nick Pope (Security &amp; Standards Associates)</td>
</tr>
<tr>
<td>15:00</td>
<td>Close</td>
<td></td>
</tr>
</tbody>
</table>
ETSI a Global Standardisation Body Based in the EU

➢ More than 900 member organizations worldwide,

➢ Drawn from 65 countries and five continents

➢ Recognised by EU as provider of European Norms
EU Qualified & Globally applicable standards

EU Qualified: EU Regulation 910/2014 defines specific requirements on practices which give legal assumption. These are met by specific options within ETSI standards.

ETSI Standards: Build on globally accepted best practices and can be applied to context.

Global Best Practices + eIDAS Specific Requirements

Global Best Practices (e.g. ISO, CA / Browser Forum)
Framework for ETSI Standardisation for Digital Signatures and Trust Service

Note: ETSI Standards
TR 119 xxx = Technical Report
TS 119 xxx = Technical Specification
EN 319 xxx = European Norm

CEN standards:
TR 419 xxx = Technical Report
TS 419 xxx = Technical Specification
EN 419 xxx = European Norm
Framework - General

119 6xx
Trust service status lists

x19 4xx
TSPs supporting digital signatures

x19 5xx
Trust application service providers

x19 1xx
Signature Creation & Validation

419 2xx
Signing Devices

119 3xx
Cryptographic suites

119 0xx
General Framework

- Standards framework
- Common definitions
- Guides
Framework – Signature Creation & Validation

- **119 6xx**: Trust service status lists
- **x19 4xx**: TSPs supporting digital signatures
- **x19 5xx**: Trust application service providers
- **x19 1xx**: Signature Creation & Validation
  - AdES creation & validation
    - Part 1: procedures
    - Part 2: signature validation report
  - Formats:
    - XAdES (XML)
    - CAdES (CMS)
    - PAdES (PDF)
    - JAdES (JSON)
    - ASIC (containers)
- **419 2xx**: Signing Devices
- **119 3xx**: Cryptographic suites
- **119 0xx**: General Framework
Framework – Signing Devices

General Framework

119 0xx

Cryptographic suites

119 3xx

Signatures Devices

419 2xx

CC Protection Profiles
- QSCD - Smart Cards
- HSM used as QSCD
- HSM used by TSPs
- Remote QSCD

119 6xx

Trust service status lists

19 5xx

Trust application service providers

19 4xx

TSPs supporting digital signatures

19 1xx

Signature Creation & Validation

EU list of Approved Devices:
https://ec.europa.eu/futurium/en/content/compilation-member-states-notification-sscds-and-qscds

© ETSI 2021 – All rights reserved

ETSI Standards Training – 1 Overview

9
# Framework - Cryptographic Suites

## General Framework

### Signatures Creation & Validation

- **TSPs supporting digital signatures**
- **Trust application service providers**

### Signing Devices

- **Cryptographic suites**
  - Signature suites
    - Hash
    - Asymmetric crypto
    - Key generation
    - Lifetime

### Cryptographic suites

- **x19 4xx**
  - TSPs supporting digital signatures
- **x19 5xx**
  - Trust application service providers
- **x19 1xx**
  - Signature Creation & Validation
- **419 2xx**
  - Signing Devices
- **119 0xx**
  - General Framework
- **119 3xx**
  - Cryptographic suites
- **119 6xx**
  - Trust service status lists
Framework for ETSI Standardisation for Digital Signatures and Trust Service

Trust services for:
- Issuing certificates
- Time Stamping
- Signature creation services
- Signature validation services

119 6xx
Trust service status lists

x19 4xx
TSPs supporting digital signatures

x19 5xx
Trust application service providers

x19 1xx
Signature Creation & Validation

419 2xx
Signing Devices

119 3xx
Cryptographic suites

119 0xx
General Framework
Framework for ETSI Standardisation for Digital Signatures and Trust Service

- Trust service status lists
- TSPs supporting digital signatures
- Signature Creation & Validation
- Signing Devices
- Cryptographic suites
- General Framework

Trust services for:
- Registered eDelivery / eMail
- Long term preservation
Framework for ETSI Standardisation for Digital Signatures and Trust Service

- **General Framework**
  - **119 0xx**
  - **119 3xx**
    - Cryptographic suites
  - **119 2xx**
    - Signing Devices

- **Signature Creation & Validation**
  - **x19 1xx**

- **Trust service status lists**
  - **x19 4xx**
    - TSPs supporting digital signatures
  - **x19 5xx**
    - Trust application service providers

- **List of approved QTSPs & services supervised by National Bodies**