



Welcome to the World of Standards



ETSI Electronic Signatures and Infrastructures (ESI) TC

Presented by Andrea Caccia, ETSI/ESI liaison to ISO SC27 (a.caccia @ kworks.it)

ETSI TC ESI - Electronic Signatures and Infrastructures

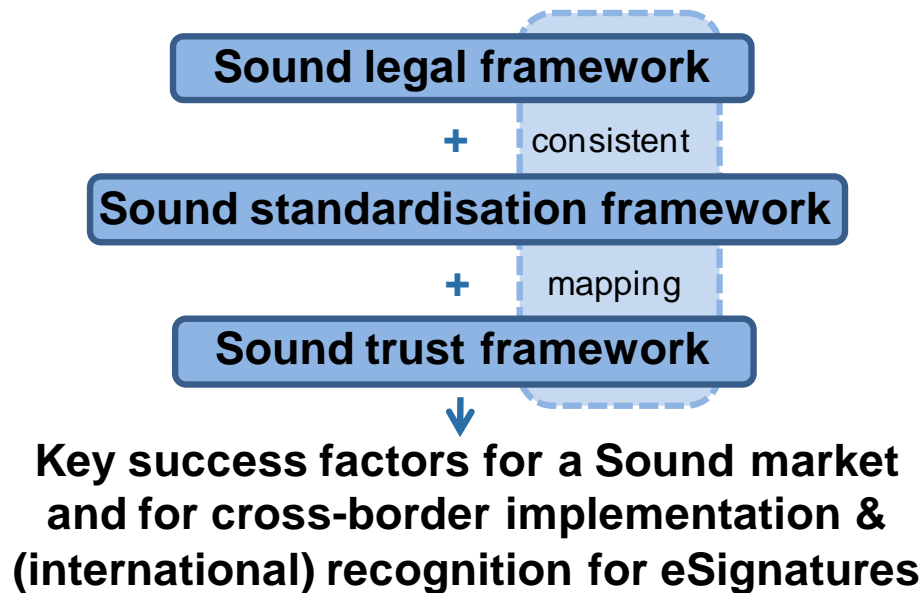


- TC ESI is responsible for Electronic Signatures and Infrastructures standardization within ETSI
- ETSI (with CEN, European Committee for Standardization) are collaborating to execute the European Commission mandate M/460 on Electronic Signature Standardisation ("Rationalised Framework")
- Collaborates with ETSI Centre for Testing and Interoperability (CTI) to organize Plugtests™ for conformance and interoperability testing events
<http://www.etsi.org/services/plugtests>
- General information on TC ESI activities available at:
http://portal.etsi.org/esi/esi_activities.asp

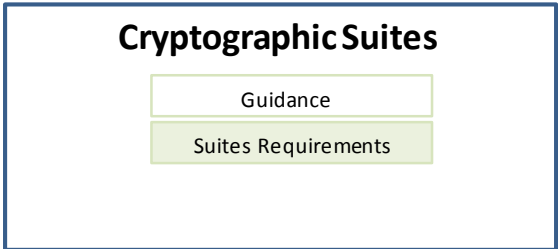
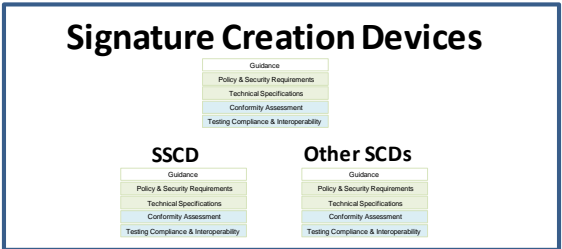
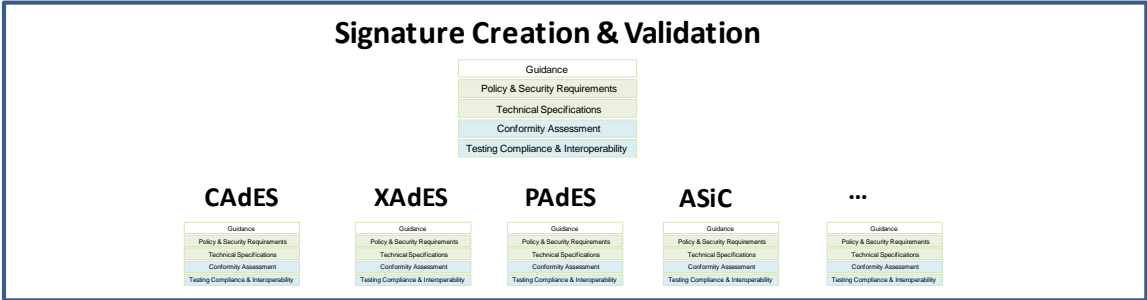
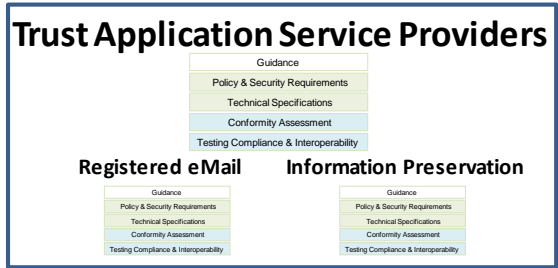
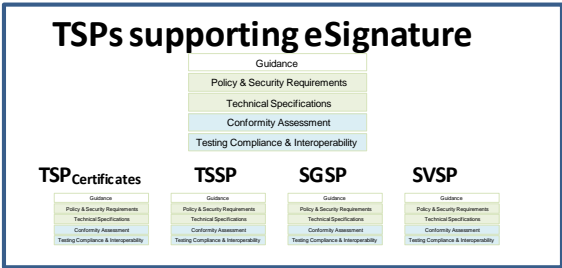


➤ **More sound eSignature Market through the rationalization of:**

- the legal framework
- the standardisation framework
- the trust framework



The new rationalized framework (CEN-ETSI)

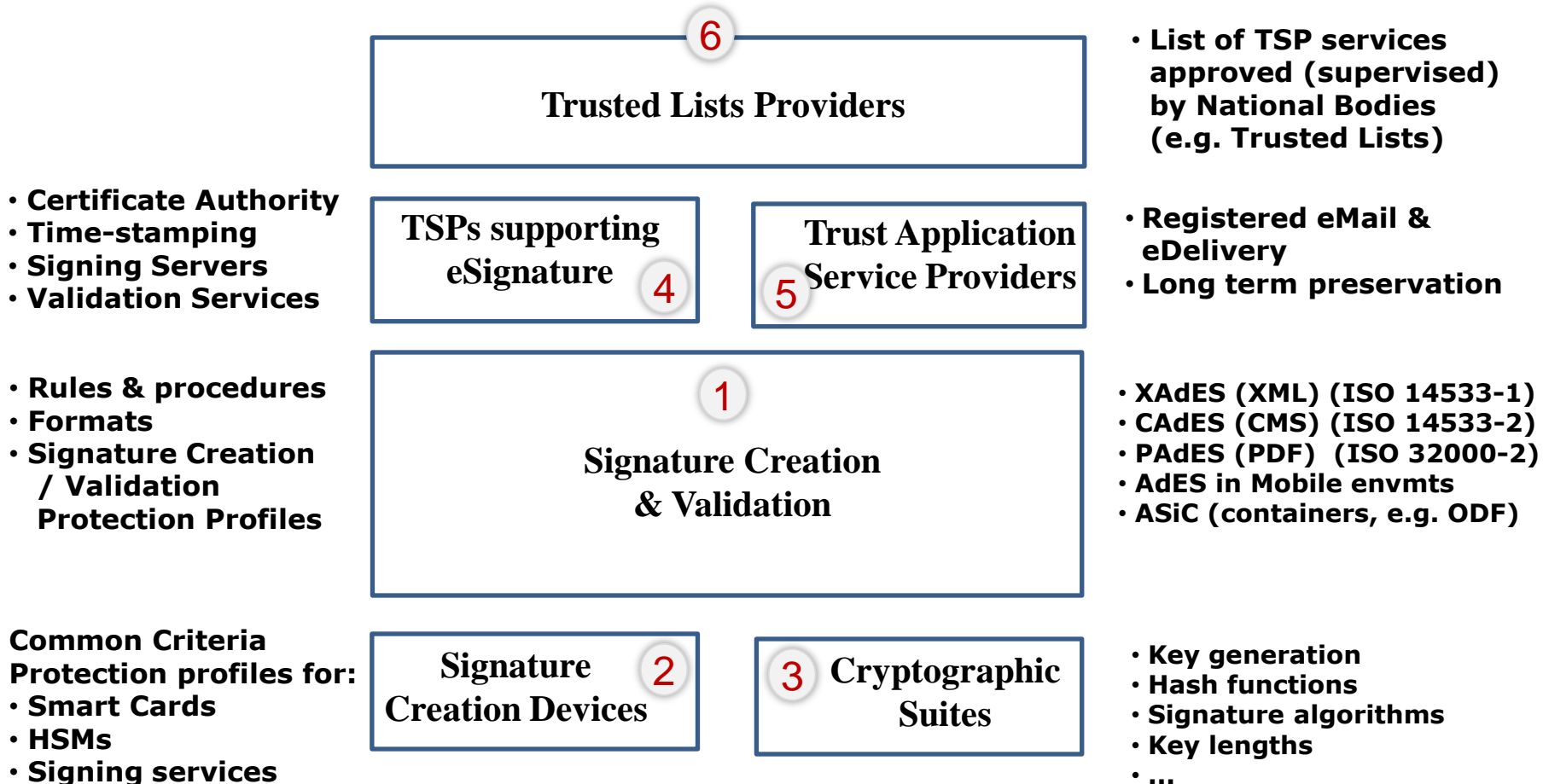


Standards classified by:

- 6 Functional Areas (& Sub-Areas)
- 5 Document types:
 - Guidance
 - Policy & Security requirements
 - Technical specifications
 - Conformity assessment
 - Testing compliance and interoperability
- Consistent numbering scheme (19XXX series)

**Documented in:
ETSI SR 001 604**

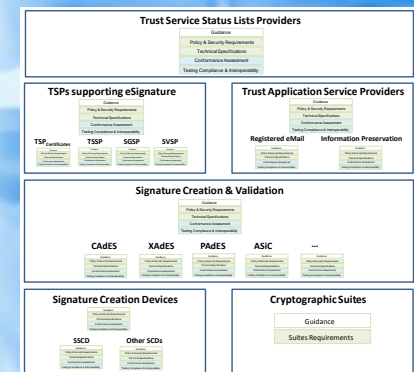
6 Functional Areas (& Sub-Areas)



Scope & objectives of the framework



- Business oriented/driven
- Simple & easy to use and tuned to business needs
 - Business guidelines (as for “dummies” as possible)
 - Clear specifications & requirements (baseline profiles with less options as possible)
 - Conformity Assessment Guidance
 - Testing specifications and facilities
- Mapped to legal requirements
- Target clear EN status whenever applicable
- Easy to find



Framework specification & Quick Fixes

- Rationalised Framework definition ([STF 425](#))
 - Inventory of eSignature Standards (worldwide)
 - Rationalised Framework Definition
 - Gap Analysis & Work Plan
- Quick Fixes
 - [STF 427](#) (CSP Conformity Assessment, QC profile, Sig. Validation Procedures, eSig algorithms maintenance)
 - [STF 426](#) (X/C/PAdES & ASiC baseline profiles)
 - [STF 428](#) (XAdES conformance testing, PAdES & ASiC interoperability tests)
 - [CEN](#) (Update CWA 14169 & CWA 14167 towards EN's)

Stakeholders involvement:

- Website: www.e-signatures-standards.eu
- Workshop on Nov 21st, 2011 Paris (FR)
- Mailing list available



- STF 457 Framework and Coordination Activities
 - fulfilment of the Rationalised Framework across all areas as defined in Phase 1
http://portal.etsi.org/stfs/STF_HomePages/STF457/STF457.asp
- STF 458 Activities related to Signature Creation and Validation and Trusted Service Providers (TSP) supporting eSignatures
 - align specifications for procedures and formats for signature creation and verification with the framework and progression to EN
 - align specifications for TSP supporting electronic signatures with the framework and progression to EN
http://portal.etsi.org/stfs/STF_HomePages/STF458/STF458.asp
- STF 459 Testing Compliance & Interoperability and Trust Applications Service Providers
 - study standardisation requirements for Electronic Delivery applying electronic signatures
 - develop a set of technical specifications and tools that act as catalysers for implementing essential standards of the framework
http://portal.etsi.org/stfs/STF_HomePages/STF459/STF459.asp

- Stakeholders level: Business driven guidance
- Policy level: Policy and security requirements, including protection profiles
- Technical specification Level:
 - Formats and packaging of signatures
 - Procedures for creation and validation
 - Signature Policies
- Assessment level: conformance assessment of applications and procedures
- Testing compliance and interoperability



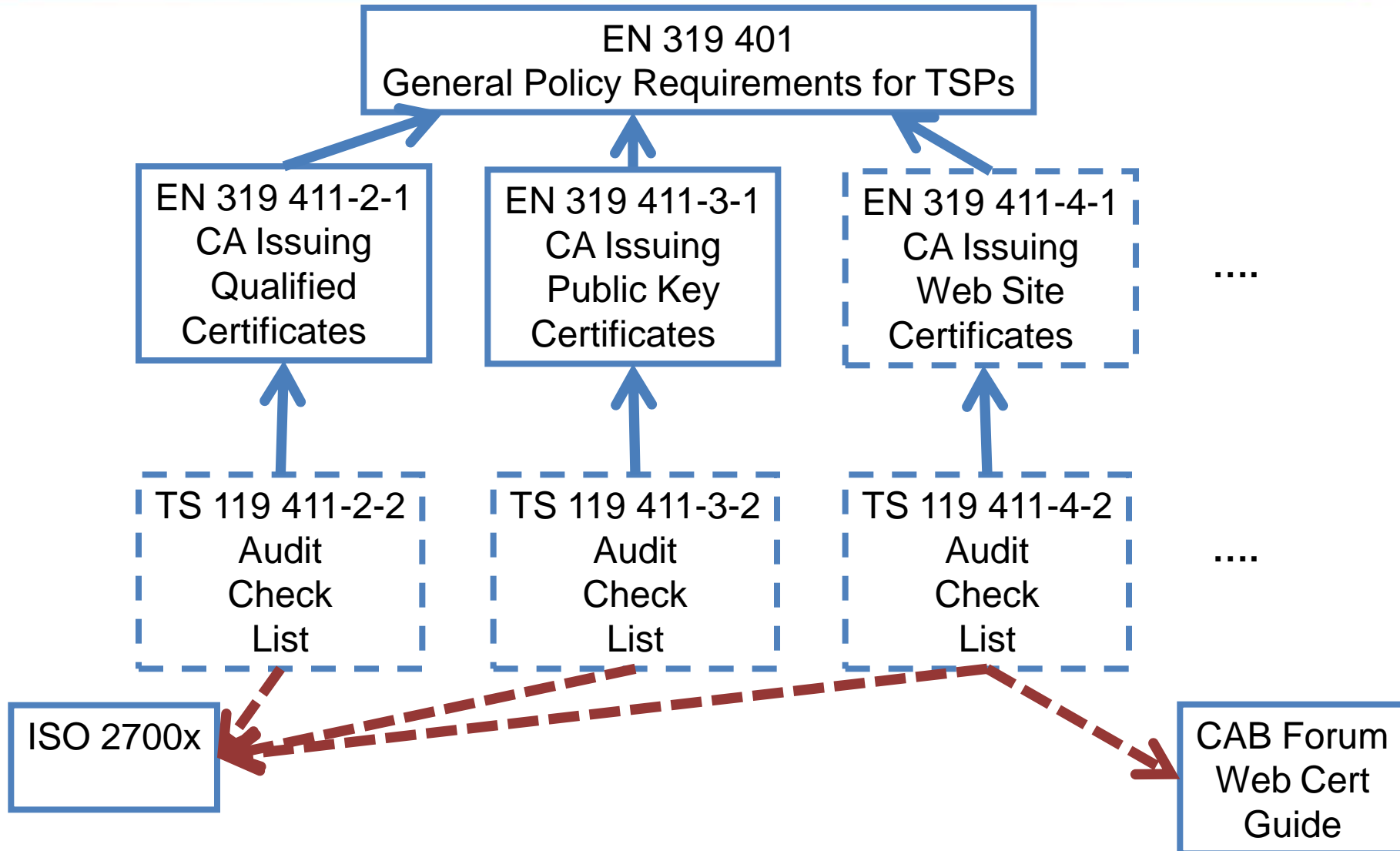
- Secure Signature Creation Device (SSCD)
 - Smart card
 - HSM for Server signing (massive/remote)
- > "Signature in the Cloud" workshop, Mar 14, 2013
[http://docbox.etsi.org/Workshop/2013/201303 SIGNATURES IN CLOUD](http://docbox.etsi.org/Workshop/2013/201303_SIGNATURES_IN_CLOUD)
- Other Signature Creation Devices
 - Cryptographic devices used by Trust Service Providers for signing services or for key generation
 - Electronic seals (legal persons)
- Conformity Assessment based on Common Criteria



- TSP issuing certificates
 - Qualified
 - SSL Certificates
 - Other PKC
- TSP Providing Time-Stamping Services
- TSP Providing Signature Generation Services
- TSP Providing Signature Verification Services



Policy Requirements Document Structure Planned (Provisional)



- Registered Electronic Mail
 - delivery evidences for mail based services
- Registered Electronic Delivery (to be specified)
 - delivery evidences for messaging services (such as ISO 15000-2 ebXML Messaging Service Specification) -> ISO TC 154
- Data Preservation Systems Security
 - specifies security and reliability measures for Electronic Data Preservation Service Providers consistent with ISO 27001 and 27002



- Need for guidance for interoperability
- Maintain existing TS 102 176
- Further take into account (inter)national rules
 - France: ANSSI RGS
 - Germany: BSI
 - ...
 - NIST, etc.
- Further take into account recognised experts recommendations
- look after crypto algorithm guidance in long term



- Policy requirements for Trust List Providers
- Trust Status List Formats
- Conformity assessment
- Testing conformance and interoperability



Thank You – Any Questions



Subscribe to the E-SIGNATURES_NEWS mailing list
see www.e-signatures-standards.eu

Documents available from

<http://pda.etsi.org/pda/queryform.asp>

Other questions:

a.caccia @ kworks.it