Security is the cornerstone of TC ESI standardisation activities from the beginning

- Born as WG of the former TC SEC, it became a TC in Fall 2002 to develop industrial standards to support the Directive 1999/93/EC on the electronic signatures
  - Activity partially funded by the EC within the framework of EESSI initiative, joint work with CEN/ISSS e-Sign workshop
- The activity has then been carried on partially on the industrial needs basis and partially on requests/funding from the European Commission
  - E.g. Mandate M/460 for a joint work with selected CEN TC-224 WGs to establish a Rationalised European eSignature standardisation Framework
  - From the electronic signatures as a means to guarantee the electronic transactions to eIDAS: electronic Identity, Authentication and Signature/Seal
Current standardisation work is bound to the **Rationalised** European eSignature standardisation **Framework**

- EU-funded (M/460)
- Foreseen completion by end of 2015

Six functional areas covered by ETSI TC ESI and CEN TC 224 selected WGs

For each standardisation area, the following specification types (i.e. documents) are foreseen (not all types for all areas)

- Guidance
- Policy & Security Requirement
- Technical Specification
- Conformance Assessment
- Testing Compliance & Interoperability
Area 1: Signature Creation & Validation (AdES digital signature supporting EU Advanced and Qualified Electronic Signatures)

- Signature creation and validation
- Signature and other formats
  - CAdES based on IETF Cryptographic Message Syntax (CMS)
  - XAdES based on W3C XML Signature (XMLDISG)
  - PAdES based on Adobe/ISO PDF document format
  - Associated Signature Containers (ASiC) based on OASIS Open Document Format (ODF)
  - Signature Policy to specify constraints for signature creation and validation

Area 3: Cryptographic Suites

- Guidance on selection of cryptographic suites to apply for digital signatures with particular emphasis on security
- Based on recommendations given by other standardization bodies, security agencies and supervisory authorities of the Member States
Area 4: TSPs supporting eSignature

• Trust Service Provider types (non Qualified / Qualified according to the Directive of the new Regulation)
  • Certification Authorities
  • Time Stamping Authorities

• Specification types
  • Policy and Security Requirements for TSPs
  • Profiles for X.509 certificates and time-stamping protocol

Area 5: Trust Application Service Providers

• Registered Electronic Mail (REM)
  • existing pre-RF specification of protocols and formats based on S/MIME

Area 6: Trust Service Status Lists Providers

• List of TSP services approved (supervised) by National Bodies (e.g. Trusted Lists)
  • Format (XML and ASN.1/DER)
Current work is for execution of M/460 through three EU-funded Specialist Task Forces (STFs)

- One STF with collaborative work with CEN: coordinating the fulfillment of the Rationalised Framework
- For many of the mentioned standardisation areas, Testing Compliance and Interoperability specifications have been produced
- 61 documents to be progressed and fulfil the Rationalised Framework
  - About 20 deliverables approved for TS publication and EN approval by end of May 2015
- Increase of the international applicability of TC ESI’s European Standards (ENs)
  - Deep review of the drafts approved / being approved
  - Liaisons with some ISO/IEC Technical Committees or Working Groups
  - Informal cooperation with Japan Network Security Association (JNSA)
  - Joint effort with ENISA for maintenance of “algo paper” on cryptographic suites
With respect to the EU Directive, the new Regulation

- Introduces the electronic identities (eID)
- Introduces the electronic seals
- Explicitly defines a number of trust services, in addition to the certification, and the requirements for the Qualified ones (few of them already covered by the ongoing standardisation activity)
  - Issuing certificates for ESignatures / ESeals / Web site authentication
  - Validation/preservation of ESignatures / ESeals, time stamping, E-R-delivery

TC ESI will submit new proposals for EC/EFTA funding on

- (new) Additional TSP requirements and specifications, e.g.
  - Policy requirements for TSP issuing certificates for code signing
  - Profiles for certificate revocation information
- (new) Mobile signatures, remote signature creation and validation
- Registered (new) Delivery and (revision) E-mail
- (new) Long term preservation
Riccardo Genghini
ETSI TC ESI & CEN-ETSI e-SIGN coordination group Chairman
Professor for Comparative Commercial Law

Thank you!
ANNEX: LIST OF TC ESI SPECIFICATIONS

Latest published, approved, under approval and drafts
under Rationalised Framework umbrella
List of TC ESI deliverables per RF area
Rationalized framework (Area 0)

- TR 119 000 Rationalised structure for electronic signature standardisation
- TR 119 001 The framework for standardisation of signatures
  Definitions and abbreviations [approved, to be published]
- SR 019 020 Rationalised Framework of Standards for
  Advanced Electronic Signatures in Mobile Environment [under
  approval]
- SR 019 050 Rationalized framework of Standards for
  Electronic Registered Delivery Services Applying Electronic
  Signatures [approved, to be published]
TR 119 100 Business driven guidance for Signature Creation and Validation

TS 119 101 Policy and security requirements for Signature Creation and Validation [under approval]

EN 319 102 Procedures for Creation and Validation of AdES digital signatures [Started EN approval process; approved as TS 119 102, to be published]
  • Part 1: Creation and validation

EN 319 122 CAdES digital signatures [Started EN approval process; approved as TS 119 122, to be published]
  • Part 1: Building blocks and CAdES baseline signatures
  • Part 2: Extended CAdES signatures
List of TC ESI deliverables per RF area
Signature Creation and Validation (Area 1)

EN 319 132 XAdES digital signatures [Started EN approval process; approved as TS 119 132, to be published]
• Part 1: Building blocks and XAdES baseline signatures
• Part 2: Extended XAdES signatures

TS 119 134 XAdES testing conformance & interoperability
• Part 5: Conformance Testing for XAdES Baseline Profile

EN 319 142 PAdES digital signatures [Started EN approval process; approved as TS 119 142, to be published]
• Part 1: Building blocks and PAdES baseline signatures
• Part 2: Extended PAdES signatures

TS 119 144 PAdES testing conformance & interoperability
List of TC ESI deliverables per RF area
Signature Creation and Validation (Area 1)

EN 319 162 ASiC - Associated Signature Containers [under approval for starting EN process and for publication as TS 119 162]
- Part 1: Building blocks and ASiC baseline signatures
- Part 2: Other ASiC containers

TS 119 164 ASiC testing conformance & interoperability
- Part 2: Test Suite for testing interoperability of ASiC

TS 119 172 Signature policies [approved, to be published]
- Part 1: Framework
List of current TC ESI deliverables per RF area
Cryptographic Suites (Area 3)

- TR 119 300 Business driven guidance for cryptographic suites [published]
- TS 119 312 Cryptographic suites for secure electronic signatures [published]
List of current TC ESI deliverables per RF area
TSP supporting Electronic Signatures (Area 4)

- TR 119 400 Business Driven Guidance for TSPs Supporting Electronic Signatures
- EN 319 401 General policy requirements for TSPs supporting electronic signatures [Started EN approval process; approved as TS 119 401, to be published]
- EN 319 403 Requirements for conformity assessment bodies assessing Trust Service Providers [Started EN approval process; approved as TS 119 403, to be published]
- EN 319 411 Policy and security requirements for Trust Service Providers issuing certificates [Started EN approval process; approved as TS 119 411, to be published]
  - Part 1: General requirements
  - Part 2: Requirements for TSP issuing EU qualified certificates

© ETSI 2011. All rights reserved
EN 319 412 Certificates Profiles

[Started EN approval process; approved as TS 119 412, to be published]

- Part 1: Overview and common data structures
- Part 2: Certificate profile for certificates issued to natural persons
- Part 3: Certificate profile for certificates issued to legal persons
- Part 4: Certificate profile for web site certificates issued to organisations
- Part 5: QCStatements
EN 319 421 Policy and security requirements for TSPs issuing electronic time-stamps [Started EN approval process; approved as TS 119 421, to be published]

EN 319 422 Time-stamping protocol and electronic time-stamps profiles [Started EN approval process; approved as TS 119 422, to be published]
List of current TC ESI deliverables per RF area

Trust Service Status Lists Providers (Area 6)

- TR 119 600 Business driven guidance for trust service status lists providers profiles [approved, to be published]
- EN 319 612 Trusted lists format [approved, to be published]