World Class Standards

ETSI ESI

Standardisation activity

Riccardo Genghini
ESI Chairperson

Origins of EESSI Standards (EESSI)

1. ETSI ESI was established in 1999 within ETSI Sec, in order to share the work with Cen-ISSS e-Sign WS for establishing an European set of standards for the implementation of the EU Directive on Electronic Signatures (1999/93/EC)
2. Until 2003 ETSI ESI and Cen-ISSS eSign WS worked under the umbrella of the EESSI (European Electronic Signature Standardisation Initiative) Steering Group, that is dormant since 2004
3. Today NISSG of ICT Standard Board, is the only coordination entity

Origins of EESSI Standards (Cen-ISSS eSign)

1. Cen-ISSS eSign published several standards for security of SSCDs, signature creation and verification, for security assessment of Certification Authorities, for smartcard interoperability
2. In 2003 Cen-ISSS eSign was disbanded: all standards had been realized according to plan. Some CWAs have been referenced in the OJ of the EU:

- 14167-1: (March 2002) security requirements for trustworthy systems managing certificates for electronic signatures
- 14167-2: (March 2002) cryptographic module for CSP signing operations — Protection Profile (MCSO-PP)
- 14169 (March 2002): secure signature-creation devices

Origins of EESSI Standards (ETSI ESI)

1. ETSI ESI has focused ist activity on the format of signature, of qualified X509 certificates, on the format and technical features of digitally signed documents and on security policies
2. ETSI's TSs have been referenced/adopted worldwide: in USA by US Fed.CA, in Asia by Asia PKI Forum, in Japan by ECOM and Japan PKI Forum, in Korea by KISA, in Africa by Africa PKI Forum. Some of them have been submitted to and adopted by IETF

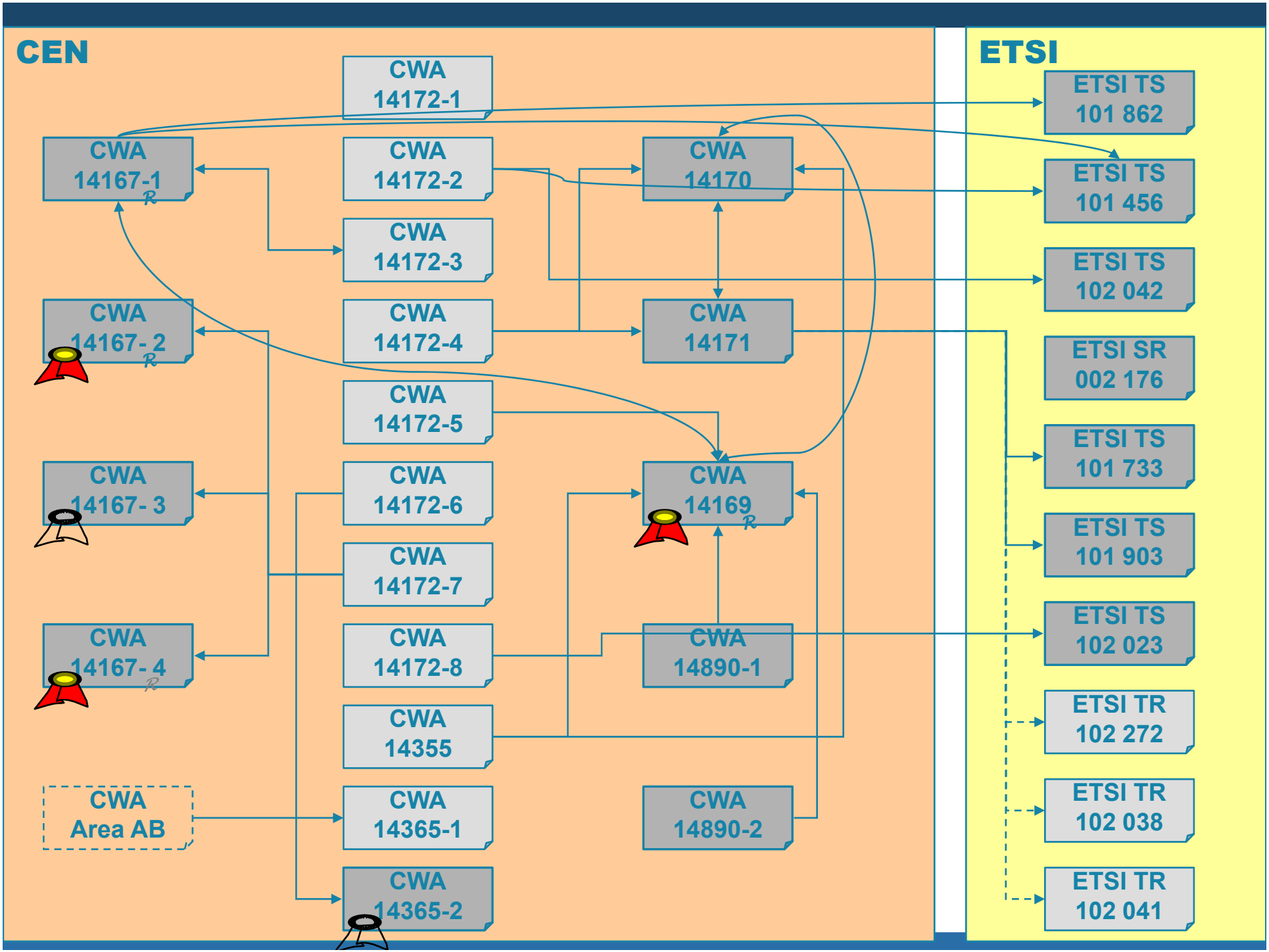
- 101733: Qualified Signature Format
- 101903: XML Signature Format
- 101862: Qualified Certificate Profile
- 101456: Policy requirements for CA issuing QC
- 102023: Policy requirements for TSA
- 102042: Policy requirements for CA issuing PKC
- 102231: Provision of harmonized Trust-service status information

ETSI ESI 2007-2008

1. ETSI ESI is also closely co-operating with OASIS and the CA Browser Forum
2. ETSI ESI has started standardisation activity on Registered Emails (REM), that has attracted interest and active participation worldwide. The TS will be divided in three deliverables: Architecture, Formats and Policies
3. ETSI ESI has initiated closed co-operation with ISO 32000, in order to integrate QAdES and XAdES into the PDF format, whose IPRs now belong to ISO (and not anymore to Adobe)
4. The vision of such co-operation is to establish a single technical environment for displaying securely a digital document and “see” and verify securely the digital signatures on it

Great Complexity of Standard ... Patchwork

1. Technically speaking, we have a complete framework.
2. It looks like a patchwork
3. Integration and co-ordination requires a document management coordination effort
4. Outside of Europe, still the CWAs and ETSI TSs are referred to as EESSI Standards
5. EESSI is ... dorment !


CEN
ETSI
CWA 14172-1
CWA 14167-1
CWA 14172-2
CWA 14170
CWA 14172-3
CWA 14167- 2
CWA 14172-4
CWA 14171
CWA 14172-5
CWA 14167- 3
CWA 14172-6
CWA 14169
CWA 14172-7
CWA 14167- 4
CWA 14172-8
CWA 14890-1
CWA 14355
CWA Area AB
CWA 14365-1
CWA 14890-2
CWA 14365-2
ETSI TS 101 862
ETSI TS 101 456
ETSI TS 102 042
ETSI SR 002 176
ETSI TS 101 733
ETSI TS 101 903
ETSI TS 102 023
ETSI TR 102 272
ETSI TR 102 038
ETSI TR 102 041

Opportunities or adoption of QES

1. ISO ETSI co-operation on PDF and “PDF Signatures”: impact on the market in 2 or 3 years from now
2. Registered Email: impact on the market in 1 or 2 years from now
3. Long Term Archival using QAdES and XAdES
4. Electronic Invoicing: in the EU regulation there is not already the right balance between security and usability

FACIT:

Electronic Signatures still require professional skills in order to be successfully used. Regulation, Administrative action and EU funded projects shall support business models and technologies that trigger the use of QES by professionals (lawyers, notaries, architects, accountants, auditors, doctors, engineers, etc.)

Actions recommended to the EU Commission

1. W3.org on XML signatures: formal co-operation never was started for two main reasons
   - 1.a IPR issues
   - 1.b ETSI STF funding rules (no dissemination!)

   recommendation:
   - support to the solution of IPR issues between ETSI and W3.org
   - support dissemination activities of European Standard Organisations
2. Insufficient budget for explanatory work and dissemination. There is greatest interest towards ETSI TSs (and also for CWA 14170, CWA 14171 and CWA 14890):
   - 2.a More regular participation to Asia PKI Forum

   recommendation:
   - support dissemination: The Economist 20.9.2007 “Brussels Rules OK”

Thank you for your attention.

Questions, comments?

Riccardo Genghini
riccardo.genghini@sng.it

STUDIO NOTARILE GENGHINI

2witness technology

2euro notaries

notarize the digital world