Solutions for e-signature Interoperability

Riccardo Genghini
ETSI ESI Chairman

5th ETSI Security Workshop - 20/22 January 2010
Why is E-Signature interoperability so hard?

- Technical overkill
- Legal processes reproduced as understood by engineers
- Poor understanding of E-Signatures by lawyers
- BUT FIRST AND FOREMOST ...
- The unwillingness to accept that a digital document is something very different from a paper document, and has a different meaning and purpose (…and lifecycle, and context and effect, and…)

5th ETSI Security Workshop - 20/22 January 2010
EU Mandate, following COM 798 - 2008

- Formal restructuring and re-organization of EU signature standards: technical content quite stabilized
- Update and adjournment of expired CEN CWAs
- Better integration of the TSs
- Greater simplicity to understand and use TSs
- Common presentation framework (Portal, dynamically updated)
- Defined lifecycle: generation as TSs and evolution into ENs or ISO standards
- Action Plan with 4 years lifespan
- Possibility of a permanent budget for maintenance of the TSs dissemination and of the presentation infrastructure
A new approach in the EU Mandate

- European Commission budget covers an intense activity of dissemination besides the usual maintenance of the TSs.

- ETSI TSs form part of ISO 32000 and ETSI plays a key role in the development of ISO 32000.

- Worldwide interest: next week ESI Chairman Riccardo Genghini has been invited to present four years plan at AICTO (Arab Information and Communication Technologies Organization) PKI event.
TSL – Trusted Service List
ETSI TS 102 231

Definition: “Supervision/Accreditation Status List of certification services from Certification Service Providers which are supervised/accredited by the referenced Member State (or participating EEA country) for compliance with the relevant provisions laid down in the eSignatures Directive 1999/93/EC

Such a Trusted List shall cover:

- all Certification Service Providers, those latter being defined as per Article 2.11 of the eSignatures Directive i.e. “entity or a legal or natural person who issues certificates or provides other services related to electronic signatures”;
- that are supervised/accredited for compliance with the relevant provisions laid down in the eSignatures Directive 1999/93/EC.
TSL – Trusted Service List

- **Characteristics:**
  - Structure defined in XML and ASN.1.
  - **Contents:**
    - Preface with details of the assessment scheme and the TSL itself
    - Details on each entity providing the service(s).
    - Current details on each service provided by a certain entity.
    - Historical details on each service provided by a certain entity reporting status changes.
TSL – Trusted Service List

- Profile for Qualified Certificates Services Providers.
  - IDABC produced a profile of ETSI TS 102 231 TSLs for reporting on Certification Services Providers issuing Qualified Certificates.
  - The set of 27 TSLs, each one issued by one EU Member State shall constitute a core piece in the European framework for mutual recognition of electronic signatures.
  - ETSI has finalized the review of ETSI TS 102 231 for incorporating the requirements identified by IDABC.
  - ETSI has built up an infrastructure (a remote accessible portal) for conducting interoperability.
ETSI and IDABC have worked together in setting up and conducting interoperability tests on the TSLs profiled by IDABC, where EU Member States have checked (before the end of 2009) the interoperability of their TSLs implementations using ETSI CTI infrastructure for supporting remote and face to face interoperability tests.
TSL – Trusted Service List

- ETSI has deployed a portal and supported an interoperability event on the TSL profile specified by IDABC.
  - Up to 20 EU Member States (EUMS) have participated, as well as representatives of the European Commission.
  - The portal specified and allowed to conduct Life cycle tests of TSLs to EUMS.
  - The portal incorporated means for allowing EUMS to test interoperability of XAdES signatures supported with qualified certificates and TSLs.
- The portal included the following tools:
  - Checker of Life cycle tests. For testing Life cycle TSL tests
TSL – Trusted Service List

- Tool that checks a qualified certificate against the TSL listing its provider.
- Conformance checker. To check conformance against ETSI TS and Profile by IDABC
- Pretty print tool, which provides a good human readable version of the TL.
STF 364 – PAdES:
PDF Advanced Electronic Signatures

TS 102 778: set of profiles to integrate the support of advanced
Electronic Signatures with PDF (ISO 32000).

Part 1: PAdES Overview
  Provides roadmap for all the profiles

Part 2: PAdES Basic - Profile based on ISO 32000-1
  Basic variant of advanced Electronic Signatures in PDF using the
  existing features of PDF signatures (ISO 32000-1)

Part 3: PAdES Enhanced - BES and EPES Profiles
  Incorporates basic features of in CAdES in PDF Signatures

Part 4: PAdES Long Term - PAdES-LTV Profile
  Extends CAdES features to support Long Term Validation of PDF
  Signatures

Part 5: PAdES for XML Content
  Applies basic and long term features to XML Content using XAdES
TS 102 778: PAdES LTV Structure

- Certification Authority Certificate(s)
- Certificate Revocation Status (OSCP / CRL)
- RFC 3161 TSA Signed Time-stamp over document + Validation data
- Validation Data \{Sig\}
- Time-stamp TS1 \{2009\}
STF 364: PAdES Ongoing Activities

- FAQ for PAdES Users and Implementers
  see: http://www.padesfaq.net/
  Also to be published as Guidelines

- Profile for Visible Signatures
  - Includes:
    - Visible representation of electronic signature when verified
    - Visible form of signature added by signatory when creating signed document
    - Printable encoding of signature in PDF (e.g. Bar code)
  - Aims to aid untrained user in understanding signature in its visible forms
Associated Signatures
(New work item under development)

- Package Format for Associating Advanced Electronic Signature with one or more files to which the signature applies

- Based on ZIP structure

- Supports Signatures / Timestamps
  - CAdES
  - XAdES
  - RFC 3161 secure time-stamp

- Aim to align with existing package formats
  - OCF (e-Book)
  - ODP (Open Office documents)
  - UCF (PDF documents)

- Signature preserved outside ZIP structure (e.g. in archive storage)
STF-318 Registered Electronic Mail Concept

- **Summary of STF-318 activities:**
  - PHASE 1: Carried survey existing and purported REM systems
  - PHASE 2: Developed multipart ETSI TS 102 640: “Registered Electronic Mail (REM): Architecture, Format for signed evidences and Policies for REM TSPs”. Three parts:
    - Part 2: Data requirements and formats for signed evidences
    - Part 2: Information Security Policy Requirements for REM Management Domains
  - PHASE 3: Developed two new parts of the TS:
    - Part 4: Assessment profile. Compliance requirements for systems providing REM services.
    - Part 5: Interoperability profile. Minimum set of requirements allowing interoperability among different REM services
  - PHASE 3: Specification of conformance and interoperability profile. Review of Parts 1, 2 and 3 in the view of comments received so far.
STF 318 – REM

- Phase 1: analysis of the market needs and expectations
- Phase 2: specification development
- Phase 3: investigation in, and confrontation with, the “real world”, specification of conformance and interoperability profile.
STF 318 – REM

- Phase 1:
  - September 2006 - July 2007
  - Survey receiving feedback from 39 stakeholders that provided information on REM-like implementations, already existing, planned or simply envisaged or wished.
  - ETSI TR 102 605
  - Available for free download (as any ETSI deliverable) from the address: http://pda.etsi.org/pda/queryform.asp.
STF 318 – REM

- **Phase 2:**
  - September 2007 – August 2008

- “REM Managed Domain” – REM-MD:
  - Part 2: Data Requirements and Formats for Signed Evidences for REM.

- ETSI TS 102 640
STF 318 – REM – Phase 2

- **SEM Management Domain Classic MIA**
- **REM Management Domain**
- **S-MSI: Sender Message Submission Interface**
- **S-MSRI: Sender Message Store Retrieval Interface**
- **R-MSRI: Recipient Message Store Retrieval Interface**
- **RSRI: Reference Store Retrieval Interface**
- **TP-ERI: Third Party Evidence Retrieval Interface**
- **MD-RI: REM-MD Message and Evidence Relay Interface**
- **MUA**
- **Recipient**
- **Third Party**
- **Recipient**

Annotation interface in the model.
Phase 3:

- Investigating with a number of market actors, among which: Swiss IncaMail, German Bürgerportale, Italian CNIPA (Authority supervising the Italian PEC), Italian Postecom, Belgian CERTIPOST, European Notary eWitness, Spanish Correos, etc.

- Issuing a new Part 4 of the ETSI TS 102 640 profiling two sets of conformance requirements, one basic and one advanced, ensuring one e-mail services provider is actually a REM-MD.

- Issuing a new Part 5 of the ETSI TS 102 640 profiling a common set of requirements suitable to ensure interoperability among REM-MDs that implement them.
Future activities

- Most of the external entities contacted by the STF have implemented or are implementing SMTP-based REM systems.
- Nevertheless, UPU and the European Pilot Project PEPPOL, on electronic tendering, are addressing SOAP as transport protocol.
- That is why the ESI TC is supporting to carry out the following activities concerning REM:
  - Specification of one or more mechanisms that would allow to interoperate SMTP-based REM systems with REM based on other transport protocols (mainly SOAP).
  - Preparation, definition and conduction of Plugtest™ Events on REM, for conducting interoperability tests among different service providers.
Riccardo Genghini
ETSI ESI Chairman
riccardo.genghini@sng.it