PEPPOL: Electronic Signature Interoperability Using Public Procurement as a Case Study

Jon Ølnes
Difi – Agency for Public Management and eGovernment (Norway)

EU-US Electronic Signature Workshop:
McLean, Virginia, 9th February 2012
The PEPPOL Project

**PEPPOL is a large scale pilot project 50 % funded by the European Competitiveness and Innovation Programme (CIP) ICT Policy Support Programme (ICT PSP)**

Sister projects are STORK (eID interoperability), SPOCS, epSOS (health care information across Europe), e-CODEX

- **Objective: Enabling EU-wide public eProcurement**
  - 17 partners from 11 countries
  - Project start up: 1 May 2008, duration **48 months** (until end April 2012)
  - Now in piloting phase

- **Pre-award phase**: Tendering – until contract is entered
  - Largely **manual process** using electronic documents to be read by humans (PDF etc.)

- **Post-award phase**: Buying – e-order, e-catalogue, e-invoice
  - In PEPPOL **system-system** by structured information (XML)
The PEPPOL Vision

Any supplier (incl. SMEs) in the EU can communicate electronically with any European contracting authority for all procurement processes.

Building blocks:

• Business process standardisation
• Standardised message formats (e.g. order, invoice, catalogue)
• Reliable and secure message transport
• eSignature interoperability (validation and acceptance)
• Document container for qualification documentation, mapping of document requirements cross-border (Virtual Company Dossier)
Pre-Award: The Public Procurement Directive and the Utilities Directive – e-Signatures in Tendering

• These Directives point at use of electronic signature for tenders
  ▶ At least qualified signatures must be accepted cross-border

• Pre PEPPOL: IDABC study 2007 – e-tendering for public procurement in 15 European countries
  ▶ 6 required qualified signatures, 7 required advanced signatures (sometimes with additional requirement for a qualified eID), 2 required only authentication (“simple” electronic signature)
  ▶ Services either listed one or a few eID issuers or were able to accept all domestic issuers and perhaps a few foreign issuers

• PEPPOL: Pre-award public procurement (tendering) cross-border is only possible if e-signature interoperability is solved!

• Interoperability of only qualified signatures is not sufficient. In particular, interoperability cannot be only European-wide plus interoperability of corporate signatures (seals) will be needed
Post-Award: VAT Directive – e-Signatures for Invoicing

- e-Signature primary mechanism of VAT Directive for e-invoice authenticity and integrity – two strategies:
  - **Avoid** – “EDI Clause” of VAT Directive: e-signature may be skipped if authenticity and integrity are otherwise guaranteed end to end. In practice, e-signature not much used for e-invoicing today.
  - **Make it work** – including cross-border e-signatures

- CIDX (Chemical Industry Data Exchange) survey 2008:
  - 11 European countries require (formally) qualified signatures for e-invoices
  - Other countries: Other signatures accepted or no requirement

- Order process, catalogue etc. not covered by EU requirements for signature
  - May be legal requirements at national levels

- **PEPPOL**: No pilot on signed invoices – but the e-signature interoperability solutions can be used for e-invoices (catalogues, orders) as well

- **Corporate signature (seal) is the right mechanism for signing invoices**
PEPPOL Focuses on the Receiver (the Relying Party)

• Assumes all actors are capable of signing, using their preferred eID, in their own, internal systems
  ▶ Signing is independent from verification
  ▶ Different tools have different capabilities!

• The receiver faces the complexity of accepting whatever is produced by the signer
  • Signature policies may be used to specify requirements
  • PEPPOL specifies relevant elements of signature policies
  • Reference to standards is a great advantage
  • Flexibility preferred if possible – what is available at signing side?
  • Do not (at this stage) require more than short-term formats – tools are not yet up to speed on more advanced formats
  • Build long-term formats on the receiving side if needed
Example: e-Signatures in Tendering

- What needs to be signed?
  - Tender letter, usually not attachments (at least not mandatory)
  - Signature may be required in a registration process (intention to submit a tender)
  - Contract signed if electronic documents used

- What happens if requirements are not fulfilled? Non-signed tenders or signatures not according to requirements?
  - May be mandatory (national regulation) to reject tender
  - Or there may be a right to reject but not mandatory

Recommendation: Test eID and e-signature early in process – require signed test document to be submitted to detect non-compliance early

PEPPOL piloting: Regular use for tendering on some tendering service platforms – works as anticipated!
PEPPOL eSignature Contributions

- Validation service interface: XKMS v2 profile for certificate validation
  - One interface to call for validation of any certificate
  - Validation options, e.g. path validation if needed
  - Returns validity plus quality and assurance level of certificate

- OASIS DSS profile for signature verification (not implemented)
  - Assessment of all signatures individually and put together
  - Send entire document to validation service
  - Gateway approach: Send signature fields and computed hashes

- Quality classification system for eID and e-signature
  - Assess: Claimed quality and assurance level (not only qualified)
  - Based on ETSI certificate policy frameworks
  - Supports mapping of certificates originating outside of Europe

- Signature policy framework

- Validation service architecture
Validation Service Architecture

Official EU TSL system

Trust list download

Qualified CAs

Other CAs, e.g. non-QCA, non-European

Validation Service

Response signed by "local" VS

XKMS Web Service, eID validation

OCSP (or CRL)

XKMS

Process signature

Signer's CA

Validation Service

Country 1

Sig

Receiver

Country 2

Signer

Validation Service Architecture
Quality: Separate (Claimed) Quality and Legal/Approval Status

Qualified is a European term – what about rest of the world?
Non-qualified interoperability is desired, e.g. corporate signature (seal)
Usage: Signature policies, in Trusted Lists, in validation service assessments

6: QCP+ – qualified signature level
5: QCP – qualified certificate but not qualified signature
4: NCP+ – highest available for authentication and legal persons
3: NCP
2: LCP
1: Low but policy exists or other assessment possible
0: Very low or not assessable (e.g. no policy)

All policy indications are “or similar” to cover non-European policies (e.g. FBCA)

6-7: Qualified certificates – but may be applied to other certificates as well

7: Accredited – external compliance audit
6: Supervised – external compliance audit
5: External compliance audit and certification
4: External compliance audit
3: Supervision without compliance audit
2: Internal compliance audit at CA
1: Independent document review
0: Self-assessment only
The Main Gaps for Cross-Border eSignature in PEPPOL

1. No cross-border, standardised naming (including identifier) of persons – persistent, unique identification is needed

2. No cross-border, standardised naming (identifier) for enterprises – this should be simpler than naming of persons

3. No standardised mapping of persons to roles and authorisations, e.g. business register interoperability (PEPPOL VCD may help)

4. Still a risk of incompatible requirements across countries, e.g. technical requirements that are difficult to fulfil from other countries

5. Still a risk of legal incompatibilities between countries. What is required in one country is not possible in another. E.g. more roles (TSA, validation and more) may need to be recognised.

6. Interoperability needs for non-qualified levels, e.g. corporate signature (seal) (PEPPOL suggests quality classification system)
Conclusions

- Signatures required for public tendering
  - Actors sign inside their own systems and submit signed documents
- Signatures must be proved valid and according to acceptance criteria regardless of origin in Europe (and over time from outside of Europe)
  - PEPPOL validation services can assess validity and quality
  - Signature policies can be defined to express criteria
- PEPPOL solves e-signature validation for tendering!
- Web Service interface for system integration
- Web GUI interface for manual side step in process
- Can we solve the e-tendering scenario, we are near a general solution for e-signature interoperability in Europe!
eProcurement without borders in Europe

www.peppol.eu
Backup slides
Business Driven Standards Development

• Real world interoperability happens if there is a business case
  ▶ A technical solution in a pilot is not enough

• Deploy solutions targeting the business case
  ▶ Public procurement is a good business case
  ▶ PEPPOL as a pilot fuels the business case

• Make the solution applicable across other areas
  • “Long tail” market etc.

The real world challenge:
ALL TRUSTED ROLES MUST HAVE A SOUND BUSINESS MODEL
Government funding is one possible model
Commercial viability is the only alternative
Signatures in Context

Electronic signatures are building blocks of electronic processes

Description of processes and requirements for (signed) documents

PEPPOL e-signature interoperability:
1. Transparency to signers – signature policy framework
2. Enable receiver to assess requirements fulfilment – validation services

The quick wins:
1. Qualified signature
2. Advanced signature using qualified eID
Signatures in Context

Electronic signatures are building blocks of electronic processes

Description of processes and requirements for (signed) documents

PEPPOL e-signature interoperability:
1. Transparency to signers – signature policy framework
2. Enable receiver to assess requirements fulfilment – validation services

The quick wins:
1. Qualified signature
2. Advanced signature using qualified eID
The TL System, Experiences

Very useful but has limitations today:

1. Lots of manual effort to configure if path validation is needed (which most often is the case)

2. As a rule only qualified eID issuers – TLs listing non-qualified issuers with a national approval status are emerging

3. Procedures at TL issuer are still too shaky – issuing is not always timely

4. Security and quality – in particular if used as trust anchor for “path”?

5. CAs get away with limitations in their services – e.g. “closed” OCSP but open CRL, but infeasible to use large CRLs (e.g. include them in long-term signature objects)