PEPPOL
Pan-European Public Procurement Online

Specifications for eSignature Interoperability across Europe

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

PEPPOL
Pan-European Public Procurement Online

PEPPOL
http://www.peppol.eu

The Project

PEPPOL Starting Point

Overall, governments are the largest buyer in the European Union, but they are lagging behind major industries in electronic data exchange with suppliers.

- Government purchases in the European Union account for around 16 % of GDP, which is equal to 1,500 Billion Euro.
- Overall capabilities of governments to handle key processes with their suppliers such as tenders, orders, delivery notes, catalogues, invoices, or payments is lagging behind other major industries.
- The lack of common standards for electronic data exchange is considered an obstacle for companies to participate without barriers in public procurement processes.

Change Ahead

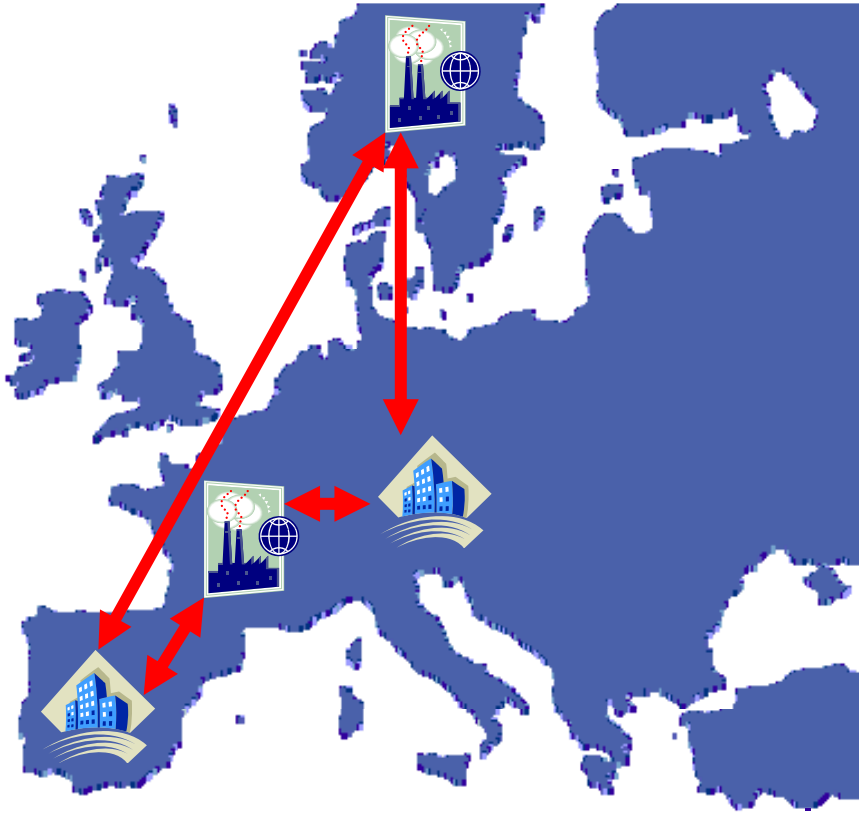
EU member states have expressed a political will to change public procurement significantly.

The Manchester ministerial declaration of 24 November 2005 defines the target:

> "By 2010 all public administrations across Europe will have the capability of carrying out 100 % of their procurement electronically and at least 50 % of public procurement above the EU public procurement threshold will be carried out electronically."

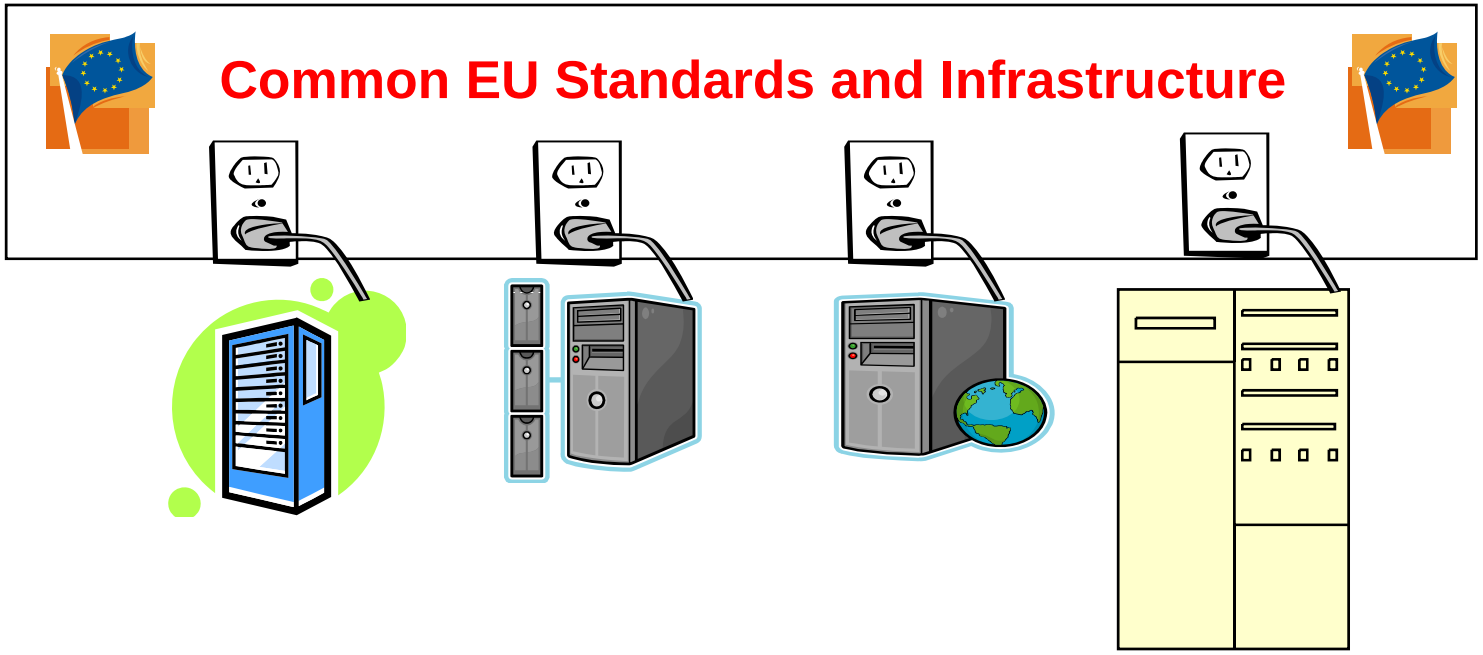
Vision

The broader vision is that any company (incl. SMEs) in the EU can communicate electronically with any EU governmental institution for all procurement processes.

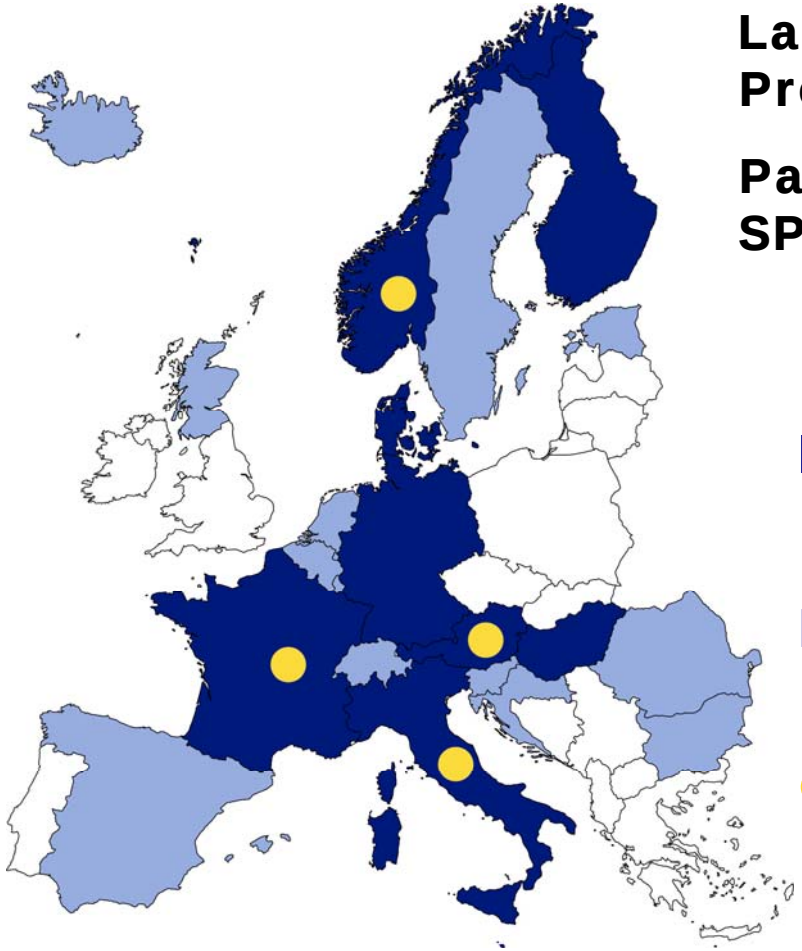


Strategy

National solutions will not be replaced, instead they will be aligned with common European standards and then linked through a common interoperability layer



The Project

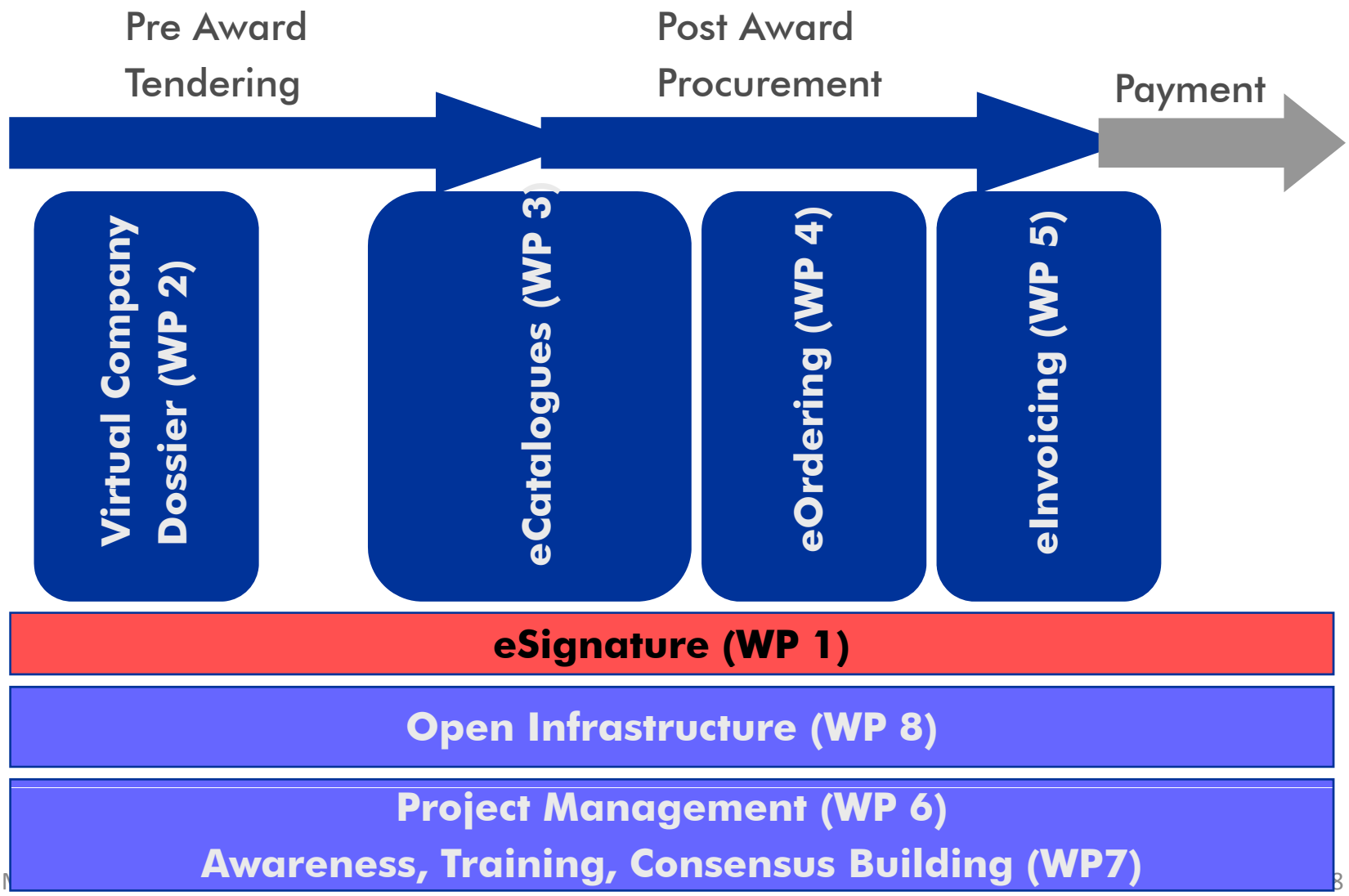


Large-scale pilot under the CIP Programme

Parallel to STORK, epSOS, SPOCKS

- Present consortium (ongoing enlargement process)
- Present reference group (some will become partners)
- Regional Nodes

Framework


Pre Award
Tendering
Post Award
Procurement
Payment
Virtual Company Dossier (WP 2)
eCatalogues (WP 3)
eOrdering (WP 4)
eInvoicing (WP 5)
eSignature (WP 1)
Open Infrastructure (WP 8)
Project Management (WP 6)
Awareness, Training, Consensus Building (WP7)

High level project plan

- May 2008 – April 2009: Requirements and design
- May 2009 – April 2010: Implementation
- May 2010 – April 2011: Pilots running

PEPPOL

eSignature Interoperability

The Public Procurement Directives
Note: Cover tendering only

COMMISSION OF THE EUROPEAN COMMUNITIES

Brussels, 13.12.2004

COMMUNICATION FROM THE COMMISSION TO THE COUNCIL, THE EUROPEAN PARLIAMENT, THE EUROPEAN ECONOMIC AND SOCIAL COMMITTEE AND THE COMMITTEE OF THE REGIONS

Action plan for the implementation of the legal framework for electronic public procurement

Qualified signatures not available in all member states and use limited in many member states.

Use of non-qualified signatures must be considered also for other reasons.

- *"Directives oblige any public purchaser in the EU to effectively recognize, receive and process tenders submitted, if required, with a qualified signature and their accompanying certificates,* ***regardless of their origin within the EU or their technical characteristics****"*
- *"The existing* ***significant differences between qualified signatures*** *…. should therefore be reason for great concern. The* ***interoperability problems*** *detected despite the existence of standards …. pose* ***a real and possibly persistent obstacle*** *to cross-border e-procurement."*

Other Directives - Requirements

PEPPOL
Pan-European Public Procurement Online

- Public Procurement Directives cover tendering only

- Service Directive requires e-signatures
- E-invoicing – e-signature primary mechanism
  - Can be avoided ("EDI Clause" of Directive) if other mechanisms are guaranteed to provide authenticity and integrity end to end
  - Can e-signatures be avoided in the PEPPOL case?
  - (Note: Directive has been revised.)

- Order process, catalogue etc. not covered by legal requirements for e-signature

Paper-Based E-signature Paradigm

PEPPOL
Pan-European Public Procurement Online

- Qualified eID must be issued to a natural person
  - Only a person can produce a qualified signature
- But e-invoices are usually not signed in a user interface
  - Personal signature is a problem
- An e-signature binds to the name in the eID
  - Why does that name have to be a person name?
  - E.g. corporate signatures on e-invoices (person is not relevant)
  - What about automated orders/invoices between systems with no person involved?

- But we are largely stuck with personal signatures in Europe
  - Possible compromise: Inner, personal signature, outer corporate signature (e.g. invoice issuer)

eID / eSignature Interoperability

1. "Front-end" interoperability
   - U **Out of scope of PEPPOL – actors sign inside their** ept "any" card
     o **own infrastructure. Leave this to STORK.**
2. "Back-end" interoperability
   - Receiver (relying party) shall be able to validate and accept signatures and eIDs from all relevant counterparts, no matter the eID issuer of the counterpart. Not "on-line", rather asynchronous, message passing protocols.
3. Other parties: Verification of signed documents may (later) be required by parties not involved in the signing process

PEPPOL Deliverable D1.1

- **Requirements for Use of Signatures in Public Procurement Processes – 7 parts:**

1. Background and Scope
2. E-tendering Pilot Specifications
3. Signature Policies
4. Architecture and Trust Models
5. XKMS v2 Interface Specification
6. OASIS DSS Interface Specification
7. eID and e-Signature Quality Classification

http://www.peppol.eu/deliverables/wp-1

PEPPOL Pilots

- E-procurement Processes:
  - Can be a single transaction
    - Like an invoice
  - Or a "long transaction"
    - Exchange of sets of messages according to some business protocol
  - Frequently asynchronous (message passing) protocols

1. Automated, system to system
   - Information and protocol must be well-defined and executable
   - Typically XML documents (or EDIFACT, or …)

2. Humanly controlled
   - Information intended for human inspection
   - Protocol (at least partly) controlled by human
   - Typically PDF documents (or Word/Excel, or ….)

- PEPPOL main scope
- CEN/BII Workshop

- Tendering today (mostly)
- PEPPOL must test eSignatures even in this case due to Public Proc. Directives

Signature Policies (1)

PEPPOL
Pan-European Public Procurement Online

- Commitment rules – binding of person names to, enterprises, roles and authorizations
  - Alternative 1: Accept signed documents (optimistic approach)
  - Alternative 2: Registration procedure to establish links
  - Alternative 3: Virtual Company Dossier (VCD) and attestations
  - Alternative 4: Employee eID (not available in general)
  - Alternative 5: Corporate eID (not acceptable in many countries)
  - Alternative 6: Inner personal + outer corporate signatures (requires solutions for issuing of corporate eIDs)

- VCD in PEPPOL is a structured set of certificates and attestations for the status of an enterprise, issued from existing registers

Signature Policies (2)

PEPPOL
Pan-European Public Procurement Online

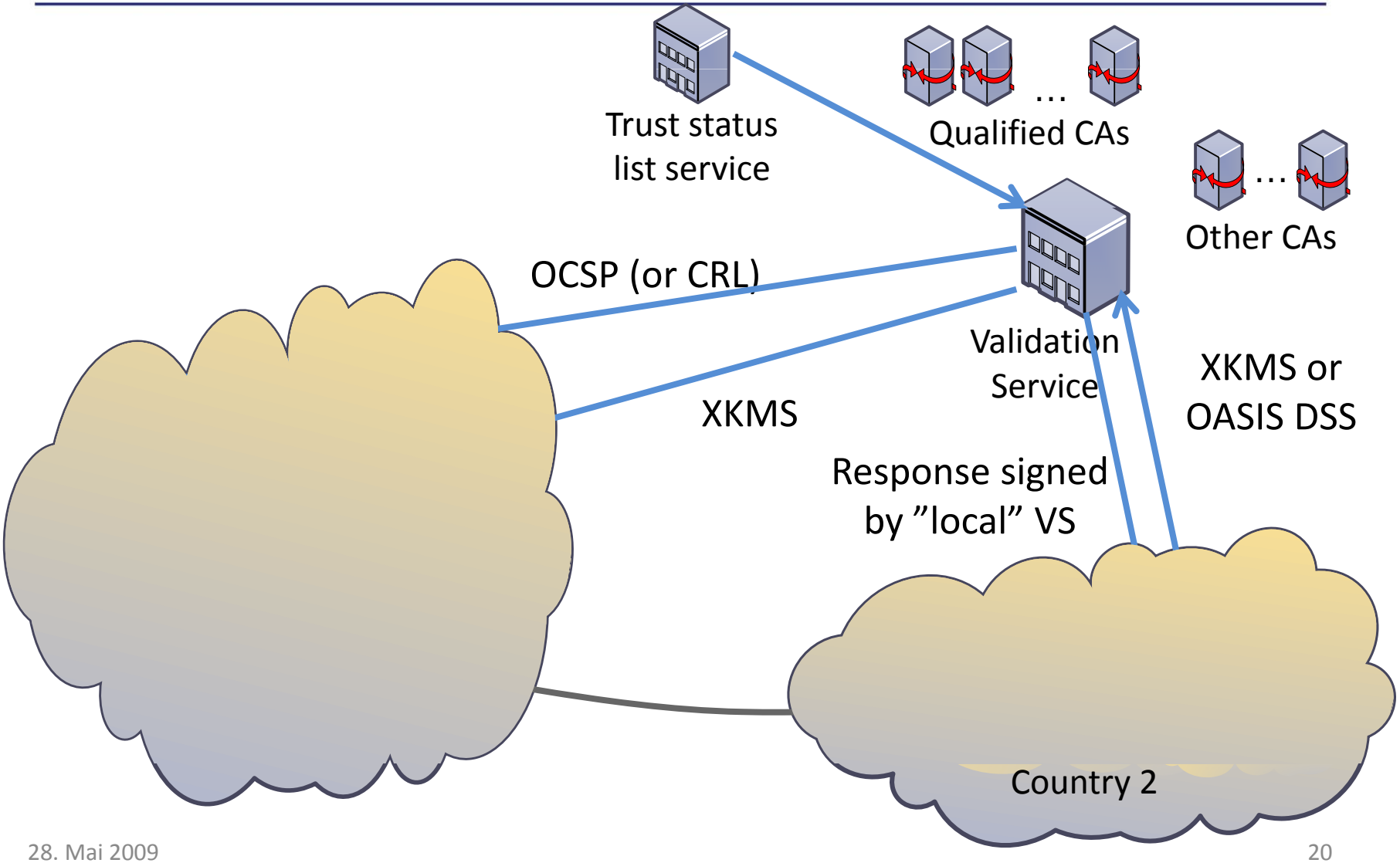
- Business protocols – what shall/should/can be signed in an eCommerce protocol?
  - Adding signatures to protocol specifications
  - Signing is (hardly) ever mandatory
    - Requirements may be determined by national legislation
    - Protocol specifications must support alternatives
  - Transparent, non-discriminatory selection of alternatives
    - If asked for, this document shall be signed at this stage of the protocol
    - Signature requirements that can be fulfilled by any actor
  - Technical specification of how to sign
    - Documents signed individually
    - Cover letter signed, attachments unsigned
    - Sign group of documents (e.g. a zip-file)
    - One + multiple signatures (sequential, parallel, countersignature)

Signature Policies (3)

PEPPOL
Pan-European Public Procurement Online

- Signature validation policy
  - Signature formats
    - Decision: Few requirements on sender, receiver must cope
    - Basic XML DSIG, XAdES BES (PDF, PKCS#7, CMS also allowed)
    - “Advanced XAdES/CAdES” lack software support at present – not required from sender at this stage
  - Requirements for signature verification process
    - Requirements for certificate validation process (path validation etc.)
    - Quality requirements and approval status of eID (see part 7)
  - Interfaces and protocols: XKMS v2, OASIS DSS (see parts 5 and 6)
    - “Rich validation interfaces” to provide all information needed for signature acceptance (as opposed to merely verification)
  - Time stamps and TSAs (Time Stamp Authority)
    - No TSA requirement on sending side! Receiver may use TSA.
  - Logging, archival, records creation
    - Local matter to receiver – information must be available

Federated Validation Services



Validation Service vs Authority

PEPPOL
Pan-European Public Procurement Online

- Service: Process eIDs (and signatures), issue assertion, responsible only for its own actions
  - Assertions are validation responses
  - Refer to CAs (their policies and national laws) for liability
- Authority: Independent liability for validation assertion.
  - Assertions are authority statements
  - One trust anchor for the relying party
  - Uniform liability for all eIDs of same quality
  - From national law (of the CAs) to contract law

XKMS v2 Interface

PEPPOL
Pan-European Public Procurement Online

- Profile of XKISS part of XKMS v2
  - Based on German profile
- eID validation interface
- Rich interface (more information) needed for validation
  - Merely validity (OCSP, CRL) is not enough to determine signature policy adherence

- Responses signed by <u>“local” XKMS responder</u>
  - If chained, responses are re-signed
  - CA signatures on OCSP/CRL but XKMS part signed separately

OASIS DSS Interface

PEPPOL
Pan-European Public Procurement Online

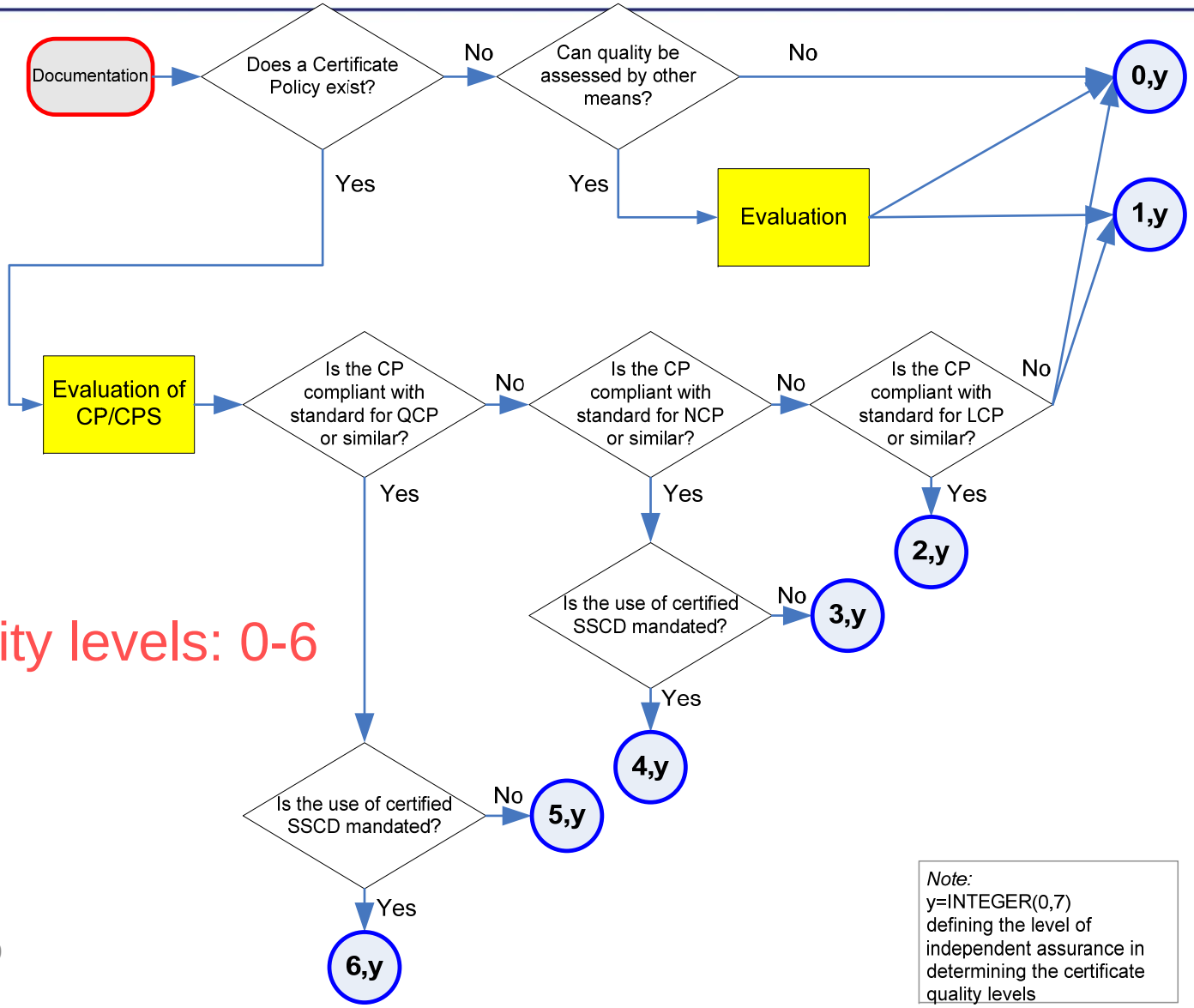
- Profile of OASIS Digital Signature Services validation part
  - Based on DNV VA work (http://va.dnv.com)
- Signature verification interface
  - Whole signed document or pairs of signatures and hash values
  - Returns overall assertion on document and individual assertions on each signature and eID
  - Responses shall be signed by responder
- XKMS v2 interface used for chaining
  - Signatures processed locally, chaining of eID validation
- Gateway solution to remove content if needed
  - Install in customer network
  - Remove content, forward only signatures and hashes

Part 7: Quality Classification (1)

PEPPOL
Pan-European Public Procurement Online

- Qualified e-signature
  - Particular legal status according to EU e-Signature Directive
  - European term – what about e-signatures from outside of Europe?
  - Available in only (about) half of EU Member States
  - 6 states require this level today for public tendering (IDABC *Preliminary Study on Mutual Recognition of eSignatures for eGovernment Applications*)
- Advanced e-signature
  - May have additional requirement for qualified eID
  - How can quality be assessed?
  - 7 states require this level today
- Simple e-signature
  - Authenticate and submit
  - Logs ensure link between authentication, action, and documents
  - 2 states require this level today
- PEPPOL: Policies defined as general rules
  - Today: Lists of accepted eID issuers – national only, few exceptions
  - Future: General quality requirements to eIDs and e-signatures
  - Requirements for (national) approval status

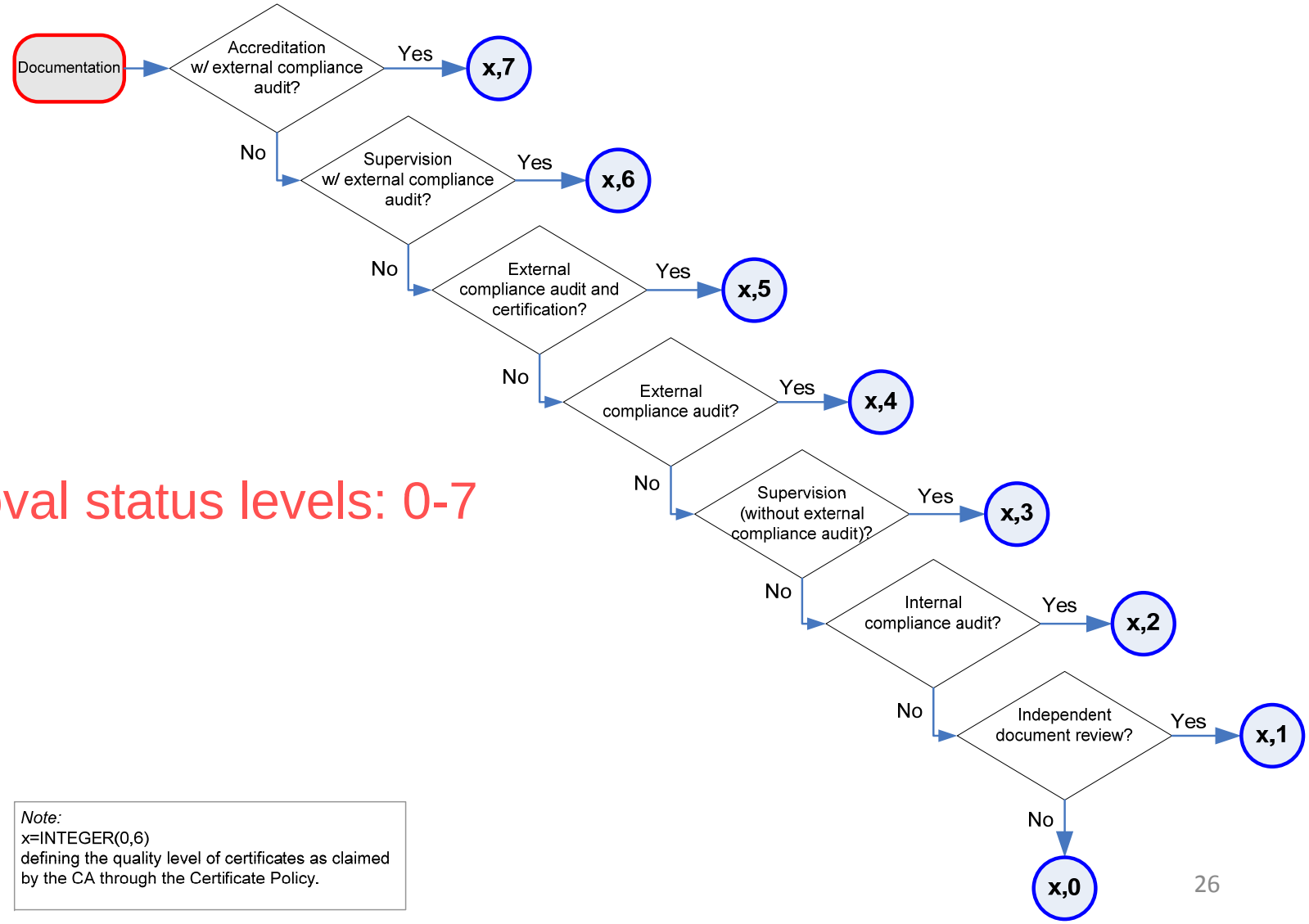
Part 7: Quality Classification (2)



eID quality levels: 0-6

Note:
y=INTEGER(0,7)
defining the level of independent assurance in determining the certificate quality levels

Part 7: Quality Classification (3)



Approval status levels: 0-7

Note:
x=INTEGER(0,6)
defining the quality level of certificates as claimed by the CA through the Certificate Policy.

Part 7: Quality Classification (4)

PEPPOL
Pan-European Public Procurement Online

- Cryptographic Quality
  - Hash quality for signatures (note: controlled by signing software)
  - Public key algorithm and key length quality
  - **Quality 0:** Inadequate – should not be trusted
    - E.g. MD5 hash
  - **Quality 1:** Reasonably secure for 3 years
    - E.g. SHA-1 hash, RSA-1024
  - **Quality 2:** Regarded as trustworthy for 5-10 years
    - E.g. SHA-224, RSA-2048
  - **Quality 3-5:** Increasing levels of security
- Signature quality:
  - [{eID quality, approval status}, hash quality, public key quality]

Validation Service vs Local

- VS used to handle all eID issuers that are not handled locally
  - Tune this as desired from 100 % locally to 100 % by VS
- Pure add-on to existing solutions
  - Add a VS interface to handle all not handled locally
- VS may issue independent assertion (kind of notary service)
  - An advantage in some cases even for “local” eID issuers

Conclusions

PEPPOL
Pan-European Public Procurement Online

- Public procurement is really B2B scenario
  - With public agency in “B” role
- Signatures required – validation <u>and acceptance</u> needed
  - Cryptographic validity
  - Signature policy adherence
    - Names -> organization, roles, authorizations
    - What must be signed?
    - Signature formats and verification rules
    - Quality and approval status requirements
  - Trust models for validation “proofs”
- Standardized interfaces
- Standardized scheme for quality classification

Contact

Further information can be obtained from the regional contact points below and at http://www.peppol.eu

Denmark, Estonia,
Finland, Ireland, Iceland, Ireland
Lithuania, Latvia, Norway, Sweden,
UK/Scotland
please contact:
Mr. André HODDEVIK
(Project Director)
Email: andre.hoddevik@peppol.no

Austria, Czech Republic, France,
Hungary, Poland, Slovakia, Slovenia,
Switzerland and Western Balkan
please contact:
Mr. Peter SONNTAGBAUER
(Public Relation Director)
Email: peter.sonntagbauer@brz.gv.at

Bulgaria, Cyprus, Italy, Greece, Malta,
Portugal, Spain, Romania
please contact:
Mr. Giancarlo DE STEFANO
Email: giancarlo.destefano@tesoro.it

Belgium, Germany,
Luxembourg, Netherlands
please contact:
Ms. Maria A. WIMMER
Email: wimmer@uni-koblenz.de