The early days of validation services – the PEPPOL project and lessons learned

ETSI eSignature and eSeal validation workshop
Sophia Antipolis, France, 10th January 2018

Jon Ølnes, Unibridge AS, https://unibridge.no, jon.olnes@unibridge.no

Starting 1st February 2018: Signicat AS, Norway, https://signicat.com, jon.olnes@signicat.com
Jon's timeline for validation services

**Startup exploring validation services**
- Mid-2001: Validsign

**Validsign bought by IBM Norway**
- 2003

**DNV Validation Authority**
Close to launch when DNV mgmt. end 2008 made strategic decision to not focus on services for IT related trust services.
- End-2008

**eIDAS draft 2012 with regulation 2014 – validation service as identified trust service**
- 2012

**Qualified validation services offered**
- 2014

**First papers:**
- 2006
  - PKI interoperability by an independent, trusted validation authority (NIST PKI R&D workshop)
  - Use of a validation authority to provide risk management for the PKI relying party (EuroPKI workshop)

**PEPPOL Large-Scale Pilot**
Successful use of validation services for real tenders in public procurement.
- 2012

**PEPPOL validation service identified as building block but not used in pilots**
- 2014

--- and more
The DNV VA vision: *Revising the trust model for the relying party*

From *the relying party trusting 100s of CAs*
A trust model that does not scale
To the **VA as trust anchor for the relying party**

A 4-corner model for PKI. The relying party gets one single trusted party:
- One point of trust
- One agreement
- One bill
- One liable actor
- One point of complaining

(Ultimately, you may even avoid path processing)
Trust framework in place for qualified level within the EU – but interoperability cannot be limited to «EU qualified only»; global interoperability must be possible

eIDAS Article 14: Acceptance of a trust services from a country outside of the EU requires an agreement between the EU and this country at government level with associated unrealistic(?) requirements for harmonisation of national laws

Current situation on liability of a CA:
- Stated in policy, which may be in a foreign language to the relying party
- Referring to the CA’s national legislation
- Requiring a court case in the CA’s country of registration

A contract with a validation authority may provide:
- Liability and other conditions stated in contract between relying party and VA
- Level out and possibly extend CA’s liabilities (the VA «providing insurance»)
- Referring to contract law and legislation of chosen country
- One point of complaining if anything goes wrong – not «200 different CAs»

Enables transfer from national law to contract law
The PEPPOL specifications

PEPPOL found that the following was needed:

• **Architecture and trust model**
  • The trusted VA, and possibilities to forward requests to another VA

• **Signature policy framework**
  • To specify what (which steps and documents) to sign in a business process, why (semantics of signatures), by whom (authorisations), and how (technical specifications and quality level)

• **OASIS DSS SOAP profile for signature validation**
  • «Same style as» the draft ETSI TS 119 442, which also adds JSON

• **W3C XKMS (XML Key Management Service) profile for certificate validation**
  • The relying party validates signatures, only certificate validation by VA
  • Plus can support validation of certificates used for other purposes
  • Should this be part of ETSI work?

• **Quality classification system for signatures and certificates**
  • This is missing from the ETSI scope
PEPPOL pilots and experience

- Several PEPPOL eSignature Pilots from mid-2010 to 2013
- **Main conclusion: It works!!**
- **Example:** Pilot until 2013 by EU-supply – Sweden-based tendering/sourcing service provider
  - Service provisioning in > 10 European countries
  - PEPPOL validation service for all signature processing in selected countries
  - **Example Lithuania:** > 1000 transactions per month – daily operation for real tenders
  - “Test your certificate early” to avoid rejected tenders
  - Less than 2 % of tenders were cross-border (more than 98 % domestic)

- Some reuse of solution by other LSPs and nationally

- **PEPPOL demonstrated international interoperability**
  - Russia, Ukraine, Belarus, Kazakhstan and more covered (important trade partners for the EU)
  - Studied how to add CAs cross-certified with US Federal Bridge
The PEPPOL goals for VA specifications (1)

- Architecture shall be agnostic to legal environment and business model
  - Validation service provisioning on commercial basis, national or domain specific solutions, in-house or other
- **Shall be add-on to other solutions at relying party**
  - Use other (local) validation as far as desired, validation service for the rest – tune from 0 – 100 % via validation service
- Shall be based on the EU TL system as far as this system reaches
  - Official source for information on supervised (at least qualified) CAs
- **Should support both system-system validation and user interfaces**
  - System integration (web services or other) most important
  - But there may be a human receiver doing manual validation
- Shall support interoperability beyond qualified level
  - Restriction to qualified signature/certificate is a risk/policy decision
  - Interoperability at “lower” levels than qualified may be needed even in the EU (at least Denmark, Sweden, France, the Netherlands)
  - Add global interoperability, where “EU qualified” does not apply
The PEPPOL goals for VA specifications (2)

- **Should support different trust models** for certificate validation
  - E.g. selection of trust anchors by the relying party
  - Validation process according to ETSI EN 319 102-1 and eIDAS requirements
- **Shall enable verification against signature policy**
  - Verify acceptance (good enough for the purpose at hand)
- **Should supply information needed to build long-term signature formats**
  - The receiver may be required to do this based on the information returned
  - Optionally the validation service may return an augmented signature format?
- **Should be able to support “historical validation” at time in the past**
- **Should be able to provide a validation report that can be used as a POE (proof of existence) for validation**
  - Alternative to long-term signature formats
  - Requires a standardised validation report (refer draft ETSI TS 119 102-2)
  - And a signed validation report with trusted time
Feedback on the draft standards

• Overall comment: keep up the good work!
• First question: Is a quality classification (framework) standard needed (this is only a placeholder in draft ETSI TS 119 102-2)?
• Second question: Should a certificate validation interface be in scope in addition to the signature validation interface?
• A few other comments (disclaimer; from brief reading only):
  – A validation service should state its coverage – which CAs are supported
  – A validation service may need to state its support for multiple signatures and modes
    • This can be made arbitrarily complex, e.g. mixing enveloped/enveloping/detached, mixing parallel/enveloping/countersignatures, mixing formats (CAdES/XAdES/PAdES/etc.), mixing signature levels (from B-B to long-term)....
    • Perhaps a best effort statement is most appropriate
  – Is there a need for an overall status for a signed document (all signatures combined) or is per signature only OK?
  – Standards should recommend processing to continue with other signatures even if one signature fails

• Final comment: (To me) difficult to see how a relying party can «trust the world» unless a validation service is used in a four corner model – the DNV VA vision is still relevant
Jon Ølnes, senior advisor
https://unibridge.no
jon.olnes@unibridge.no / mobile (+47) 478 46 094

From 1st February 2018: Jon Ølnes, product manager
https://signicat.com
jon.olnes@signicat.com / mobile (+47) 478 46 094