Security in the PEPPOL infrastructure

Presentation for OASIS BUSDOX TC, March 2011

Thomas Gundel, IT Crew
Agenda

PART I
• Security goals in PEPPOL
• Scope and requirements
• Security overview

PART II
• Trust models
• Authentication assurance
• Secure communication
• Operational security requirements

PART III
• Attacks and mitigations
Security Goals

- Enable confidence and faith in the infrastructure by setting high security standards
- Establish a common minimum-level of security in the PEPPOL infrastructure across organizations and countries
- Prevent fraud and security incidents
Scope of infrastructure security

Infrastructure security scope:
- Communication to/from AP / SMP / SML
  i.e. (not end-to-end)
- Independent of payload
- Sender authentication

Outside of scope:
Document or Business level security:
- Between sender and receiver (end-to-end)
- Requirements for payload (e.g. signed and/or encrypted documents)
Infrastructure Security Overview

Security rests on five pillars:

- Trust via a Public Key Infrastructure
- Ensuring service providers sign an agreement before they join the infrastructure
  - Agreement regulate responsibilities, requirements, liability
  - Checks for compliance may be performed
- Using secure communication protocols
  - Employs encryption, signing, certificates, security tokens
- Operational security requirements for service providers
  - Firewalls, intrusion detection, patching, logging, penetration test
- Sender authentication
  - Sender Access Point vouches for sender identity
Trust

• How do service providers know whether communicating peers are valid members of PEPPOL?
  – For example, if a received message is from a valid PEPPOL Access Point?
  – Is metadata signed by a PEPPOL Service Metadata Publisher?
• Different trust mechanisms have been considered:
  a) Establish a PEPPOL PKI
  b) Publish Trusted Parties Lists
  c) Establish a service where trusted service providers can be looked up
Trust via PEPPOL PKI

- A public key infrastructure can be established by:
  - A Certificate Authority issuing digital certificates under a central PEPPOL root certificate
  - Anyone with a PEPPOL certificate is considered a valid member of the infrastructure (closed user group PKI)
  - The PEPPOL Governing Board acts as Registration Authority
Trust via PEPPOL PKI

Advantages:

- The CA service can be acquired as a standard offering by PKI vendors
- Service providers can validate peers just by installing the PEPPOL root certificate (does not need to invoke services)
- Validation of certificates is offered out-of-the-box by most middleware
- Scales well
- Proven technology
- Easy to revoke members
- Reasonable cost (centralized)
Service Providers can only join the infrastructure (and receive a PEPPOL certificate) once they have signed the relevant agreements with the PEPPOL Governing Board.

When entering the agreement, service providers commit to fulfill the stated quality and security requirements.

The PEPPOL Governing Board may perform checks on new Service Providers including review of documentation, review of auditor statements on compliance etc.
Secure Communication

We want to achieve the following properties for secure communication in the infrastructure:

- **Authentication**
  - Who sent a document?

- **Integrity**
  - Has the contents been altered? Is it correct?

- **Confidentiality**
  - Can outsiders learn the content?
Secure Communication (2)

Secure communication is achieved by:

- Signing SOAP messages (WS-Security)
  - Authentication of service providers
  - Message integrity
- Using transport-layer security (SSL/TLS)
  - Confidentiality & integrity
- Including SAML tokens vouching for sender identity (WS-Security)
  - Sender authentication
- Similar to OIO Identity-Based Web Services
Sender authentication

- Sender Access Point is required to authenticate sender of document and vouch for the identity to the recipient
  - Recipient is relieved from the complexity of handling many different types of credentials
  - Recipient needs only to know sender identity – not details of their credential
  - Sender Access Points have business relationships with their customers and should know how to authenticate them (may e.g. have issued their credential)
Sender authentication (2)

Access Point (sending) -> Access Point (receiving)
authenticate (PEPPOL cert)
Vouch for sender identity (SAML 2.0 token)

Authenticate (any credential)

Sender -> Sender identity
Recipient
Sender authentication (3)

- Sender Access Point issues SAML 2.0 token stating:
  - Sender Identity (result of authentication)
  - Level of identity assurance (1-4)
  - Issuer of token (signed with PEPPOL certificate)
- Level of identity assurance:
  - 1 => low confidence in claimed in identity
  - 4 => very high confidence in claimed identity
  - Technology Agnostic
- Assurance level classified according to Liberty Alliance Identity Assurance Framework
  - Takes into account:
    - The technical quality of the credential
    - The credential issuing process
    - Organizational factors
- Discussion with STORK project to align (eID focused)
Operational security req.

- Goal: ensure that service providers operate their IT-systems in a secure and controlled manner
- Security requirements are an annex to the agreement service providers sign with the PEPPOL Governing Board
- Example requirements:
  - Requirement for information security programme
  - Use of digital certificates (PEPPOL PKI), revocation checks
  - Allowed cryptographic algorithms and key lengths
  - Incident reporting
  - Penetration testing
  - Firewalls and network segmentation
  - Logging
  - Patching and vulnerability scanning
  - Surveillance and intrusion detection
Attacks and mitigations

- **DNS poisoning**
  - DNSSEC can be used
  - Registering signed top-level response

- **Denial of service attacks**
  - Hard to guard against (needs cooperation from ISPs)
  - Robustness and scalability of DNS helps with SML
  - Individual Access Points and SMP must work with their ISPs

- **Rogue PEPPOL certificates: impersonate AP or SMP**
  - Liability for mis-use of *your* private key
  - Operational security requirements (e.g. document key management procedures)
  - Certificate revocation