An introduction to PEPPOL

Steve Graham
OpenPEPPOL Operating Office
The PEPPOL vision

To enable businesses to communicate electronically with any European public sector entities in the procurement process, increasing efficiencies and reducing costs.
Key players

- Buyers and Sellers
- Service Providers
- PEPPOL Authorities
- OpenPEPPOL
Governance arrangements

- Membership organisation
- AISBL under Belgian law
- General Assembly
- Elected Managing Committee
- Elected Coordinating Committee
- Domain communities (eg post-award) with elected leaders
The PEPPOL Interoperability Framework

PEPPOL Authorities and Service Providers work together within the Governance Framework to provide services compliant with the Architecture Framework.
The PEPPOL Governance Framework

- **OpenPEPPOL AISBL** is responsible for the strategic governance, the governance of sustainability and development, as well as the operational governance, all according to the OpenPEPPOL Statutes and Internal Regulations.

- **PEPPOL Authorities** have the delegated responsibility for the governance of the PEPPOL eDelivery Network and PEPPOL Business Interoperability Specifications (BIS) within a defined jurisdiction according to a PEPPOL Authority Agreement.

- **Service Providers** are responsible for delivery of services to PEPPOL End Users based on the PEPPOL Architecture Framework and according to a PEPPOL Service Provider Agreement.
The PEPPOL Architecture Framework

- PEPPOL BIS – Business Interoperability Specifications
  - Based on the Universal Business Language
    - (UBL – ISO/IEC 19845)

- The PEPPOL eDelivery Network
  - Packaging and Security Specifications
    - SBDH, ASIC etc
  - Messaging Specifications
    - AS2/AS4 etc
  - Capability Lookup and Addressing Specifications
    - SML, SMP etc
The PEPPOL Compliance Policy

Main principles

- Connect once – serve all
- Mandatory support for the four-corner model
- Mandatory support for PEPPOL BIS
- Only valid documents are to be exchanged over the PEPPOL eDelivery Network
- PEPPOL technical standards and service specifications are baseline for interoperability
- Different domains may have different service level requirements
- Service provider freedom to choose a PEPPOL Authority
- Know your customer (KYC)
- No actor can sign an agreement with itself
Current use of PEPPOL

348 OpenPEPPOL members and observers from 35 countries

232 Certified Access Points in 28 countries in Europe, North America and Asia

13 PEPPOL Authorities

- Agency for Digital Government (Sweden)
- Agency for Digital Italy (Italy)
- Agency for Public Management and eGovernment (Norway)
- Danish Business Authority (Denmark)
- Department of Health and Social Care (UK)
- Department of Public Expenditure and Reform (Ireland)
- Federal Public Service Policy and Support (Belgium)
- Free Hanseatic City of Bremen – KoSIT (Germany)
- Info-communications Media Development Authority (Singapore)
- Ministry of Business Innovation and Employment (New Zealand)
- Ministry of Economic Development (Poland)
- SimplerInvoicing (Netherlands)
- OpenPEPPOL AISBL

Member Countries where Access Points are not yet certified: Australia, Mexico, New Zealand, Romania, Slovak Republic, and Turkey
PEPPOL going global

- **South-East Asia**
  - Singapore: First meeting February 2018, official launch January 2019
  - The first PEPPOL Authority outside Europe
  - Helping to engage other ASEAN countries
  - Malaysia may be next – hopefully by late 2019

- **Trans-Tasman region**
  - New Zealand already joined, Australia joining soon
  - The two countries coordinate and align their requirements
  - Planning to go live late 2019

- **How do we engage other regions?**
  - Establish understanding of the PEPPOL approach
  - Formulate value proposition on focus (eg market-driven/government-driven)
  - Accommodate regional requirements, maintain compliance with PEPPOL principles
The benefits of the PEPPOL approach

- **Origin** – arose from EU need for cross-border electronic trading
- **Trusted** – supported and driven by public authorities
- **Proven** – adopted in many countries
- **Safe** – standards-based, secure transport mechanism
- **Open** – avoids lock-in to any service provider
- **Easy** – straightforward to trade electronically, using a single connection
- **Resilient** – distributed service providers operating independently
- **Relevant** – not just for B2G but also B2B and potential for G2C and B2C
- **Governance** – not-for-profit, democratically led by members, within legal framework
Technical fundamentals

Jerry Dimitriou
OpenPEPPOL AISBL, Belgium
Technical Overview

- Technical Aspects of the OpenPEPPOL Network
  - **HOW** we do Message Exchange
    - PEPPOL eDelivery Network Topology
    - Dynamic Discovery of Participants
    - eDelivery Specifications
  - **WHAT** messages we exchange
    - The PEPPOL BIS
The PEPPOL 4-corner model

A simple model consisting of 4 primary corners and two central technical components enabling open, reliable and secure exchange of business information between trading partners based on a common standard.
What is the 4-corner model challenging?

- Bilaterally agreed configuration, format, transport protocol, security, error handling
- In-house IT systems
- Every additional connection is a project
- Expensive maintenance

- Central hub does the routing
- Buyer and seller need to be customers of the hub
- Business partners must use the same hub
- Closed circles and incapability to exchange service provider
The four corners of the PEPPOL eDelivery Network

- **C1/Sender**: The sending trading partner.

- **C2/SrcAP**: The PEPPOL Access Point operating on behalf of C1. Primary role is to send messages in a secure and reliable way.

- **C3/DestAP**: The PEPPOL Access Point Operating on behalf of C4. Primary role is receive sent messages in a secure and reliable way.

- **C4/Receiver**: The receiving trading partner.
Technical components of the 4-corner model

- **The SMP (Service Metadata Publisher)**
  - Address library containing metadata about the capabilities of a receiver
    - Participant ID, Supported document formats, Endpoint Address
  - Knowing only the Participant Identifier of a receiver, the sender is able to retrieve the receiver’s needed metadata and send the message.

- **The SML (Service Metadata Locator)**
  - Manage the resource records of the participants and SMPs in the DNS (Domain Name System)
    - Maps Participant Identifiers to SMPs
  - The only centralized component in the PEPPOL eDelivery Network
The exchange process - overview
The exchange process – Initial Registration of Participant/Receiver

- **Step 1:** PEPPOL Receiver ID, Support Document type (like PEPPOL Invoice BIS v3.0), and endpoint is registered in an SMP

- **Step 2:** The SMP creates a record in the SML which associates the participant with the SMP

- **Step 3:** The SML updates the DNS which creates a DNS record for participant/receiver pointing to the SMP
The exchange process – The Dynamic discovery of a receiver

**Step 1:** Seller/C1 issues an Invoice and transmits to C2.

**Step 2:** C2 does a lookup using an HTTP GET. The DNS directs C2 to the SMP of the receiver.

**Step 3:** The HTTP GET results in the service metadata result for the endpoint pointing to C3 (receiver’s Access point)
The exchange process – The Dynamic discovery of a receiver – full exchange

- **Step 1:** Seller/C1 issues an Invoice and transmits to C2
- **Step 2:** C2 does a lookup using an HTTP GET. The DNS directs C2 to the SMP of the receiver
- **Step 3:** The HTTP GET results in the service metadata result for the endpoint pointing to C3 (receiver’s Access point)
- **Step 4:** C2 signs and encrypts the message and it sends to the AP of the receiver(C3)
- **Step 5:** C3 receives, decrypts and verifies the signature of the document, then transmits it to the receiver (C4)
PEPPOL eDelivery Standards

PEPPOL uses Standard Protocols for the communication of the Access Points

- **PEPPOL AS2**
  - A Profile of AS2, Mandating the use of message signatures in the communication and a synchronous signed Delivery Receipt

- **PEPPOL AS4**
  - Based on CEF AS4, Mandating the use of Message Signature, Message Encryption and a synchronous signed Delivery Receipt

Access Points that are in the PEPPOL Network

- MUST implement the PEPPOL AS2 protocol (Mandatory Protocol, becoming Optional in 2020)
- SHOULD implement the PEPPOL AS4 protocol (Optional Protocol, becoming Mandatory in 2020)
- MUST Sign and Encrypt the messages using certificates issued by PEPPOL.
PEPPOL eDelivery AP Governance

- An Access Point Service Provider, becomes part of the PEPPOL network when a PEPPOL AP Certificate is issued to be used by the Service Provider APs
  - There is a specific process, which also includes testing of the capabilities of the service provider’s APs before the Certificate can be issued.
  - Upon issuing of the Certificate by PEPPOL, the APs become trusted PEPPOL APs and can immediately send to the rest of the PEPPOL Network’s APs and/or receive from the rest of the PEPPOL Network.
    - No roaming fees or discrimination of participants are allowed
- If for any reason, a Service Provider’s APs stop following the PEPPOL standards, PEPPOL can ultimately revoke the AP certificate.
Summary of the 4-corner model and dynamic lookup

- Automatic dynamic discovery, necessary for mass use (setup, operations, and to avoid service provider lock-in for end users)
- A single agreement structure, security and trust infrastructure
- The service metadata contains all that is required to dynamically find receiver info, connect and exchange messages
- No roaming fees or discrimination of participants allowed
What is being exchanged?

- PEPPOL BIS (Business Interoperability Specifications)
  - Based on a common electronic business standard (UBL – Universal Business language maintained by OASIS)
  - Thoroughly documented and maintained by OpenPEPPOL communities
    - Pre-award Community
    - Post-award Community
    - eDelivery Community
A PEPPOL BIS, is a complete specification of a process executable through the PEPPOL eDelivery Network. It defines:

- The actors of the process (e.g. Buyer and Seller)
- The main Process Flow (BPMN Diagrams)
- Process Business Requirements
- Semantic Data Types used
- Codelists
- Business Validation Rules
- Validation Artifacts
- Syntax Mapping
PEPPOL BIS Process

- Each PEPPOL BIS Defines a Process Flow.
- The Process Flow consists of steps required to execute the process.
- Steps that communicate information between two actors (e.g. a Buyer and a Seller) are called transactions.
- A Process might have one or more transactions.
- Each Transaction has a semantic information model, consisting of semantic information elements.
- Each semantic element might have business rules, value restriction rules etc.
- Each Transaction is syntactically mapped to an XML Document, containing all the information elements.
Standards used in PEPPOL BIS

- Process definitions are based on standards issued by European Standardization Bodies
  - CEN-BII Workshops
  - CEN TC 434 (Invoicing European Norm)

- Actor and Item Identification Schemes are based on ISO Standards
  - ISO 6523 ICD
    - EAN Location Code
    - GTIN - Global Trade Item Number

- Measurements, Types, Based on United Nations CLs

- Syntax Mapping
  - OASIS UBL v2.1 and v2.2

- Business Validation rules are implemented using XML Validation Artifacts
  - Schematrons
PEPPOL Defines its Business Interoperability Specifications, which are used for creating business documents like Orders, Invoices etc.

A Receiver registers its capability of receiving such documents in an SMP, using a Specific Access Point for secure and reliable communication

A Sender generates a BIS Document following the Standards and the Business Rules defined in the BIS and sends it to a receiver only knowing its Participant Identifier and the Type of Document to be sent, by using a PEPPOL Access Point.
More information

E-mail: info@peppol.eu

Web address: www.peppol.eu