The Peppol Network

Jesper Larsen – Peppol Support Lead

The three pillars of Peppol

- The Peppol Network> **How we exchange**
  - The network architecture OpenPeppol utilize to allow Certified Peppol Service providers to send and receive Peppol BIS documents on behalf of their customers. Also referred to as the 4 corner model
- The Peppol BIS (Business Interoperability specifications) **> What we exchange**
  - The actual document content/format that is exchanged. OpenPeppol maintains, refines and develop these BIS specifications on a running basis to accommodate market requirements.
  - Some countries have their own BIS Extension to accommodate their country legislation (Singapore, Australia, New Zealand and hopefully also Japan!)
- The Peppol Governance framework > **Ensures integrity and compliance**
  - A set of agreements and policies between the different key stakeholders in Peppol defining the rules under which all entities operate and adhere to

The Peppol Network key components

The three central components are:

- **Access Point (AP)**
  - the Service providers sends and receives Peppol messages in a secure and reliable way, on behalf of the participants/End Users (senders and receivers). The AP is a distributed component in the eDelivery Infrastructure, and is usually offered by a Service Provider. All Access Points must support the mandatory AS4 transport protocol with **the dynamic discovery process** as well as the Peppol PKI infrastructure. Access points are provided by certified Peppol Service Providers.
- **Service Metadata Publisher (SMP)**
  - once the sender discovers the address of the receiver's SMP, it is able to retrieve the required information (metadata) about the receiver. With the metadata, a message can be sent. The SMP is a distributed component in the eDelivery Infrastructure, and is usually offered by a Service Provider or a government entity Peppol member (centralized SMP approach). SMPs are provided by certified Peppol Service Providers
- **Service Metadata Locator (SML)**
  - the SML manages the resource records of the the participants and SMPs in the Domain Name System (DNS). The SML is the only centralised component in the

Dynamic discovery (1) – registration of a receiver

The registration processes are:

- **Submit metadata about the receiver**
  - the AP operating on behalf of a receiver, registers the receiver identifier, supported message types, and endpoint identifier in any SMP.
- **Create participant**
  - The SMP creates a record in the SML, which associates the receiver with the SMP.
- **Register participant**
  - the SML updates the Domain Name System (DNS), which creates a DNS record for the receiver, pointing to the SMP

Dynamic discovery (3) – receiver metadata registered in the SMPs

- the identifier of the participant
- supported business message type(s)
- type of transport protocol to use for the message (AS4 is mandatory for all)
- technical endpoint/address where the message is to be sent (technical address of the receiving Access Point / corner 3)

Dynamic discovery (2) – operations when sending

The operations processes are:

- **Submit**
  - the sender (corner 1) issues an eDocument (such as an eInvoice) and transmits it to its selected AP (corner 2). This activity is not governed by Peppol and the creation of the actual Peppol BIS can be done directly by C1 or with help from C2 (mappings etc.)
- **Lookup**
  - the AP (corner 2) makes a lookup to the DNS using HTTP GET. The DNS/SML directs the AP to the SMP of the receiver (corner 4).
- **Retrieval**
  - use of HTTP GET retrieves the service metadata for the endpoint AP (corner 3) from the SMP
- **Send**
  - the sender's AP (corner 2) sends the eDocument to receiver's AP via AS4 (corner 3)

Dynamic discovery (4) – key points and benefits

- enables mass use of the network / mass onboarding
- uses DNS, which is stable and provides high performance
- uses technical specifications based on open and approved standards
- prevents service provider lock-in for end users (senders and receivers)
- security and trust is provided by the public key infrastructure (Peppol PKI certificate infrastructure)
- a legal agreement structure enables strong governance and compliance
- ‘roaming’ fees between service providers are not allowed
- rejection of valid inbound messages is not allowed on the technical level
- Pretesting and whitelisting not necessary. All Peppol Service Providers are equal and can equally reach all of each others end users by default.

Dynamic discovery (5) – summary

- Dynamic Discovery enables sending Access Points to dynamically discover the Address of a receiving Access point as well as the capabilities (supported documents) of a receiver.
- instead of using a static list of IP addresses, the sending Access Point asks a Service Metadata Publisher (SMP) where information about a participant (receiver) in the data exchange network is stored and kept up to date.
- at any point, there can be several SMPs operating in the network
- every participant is given a unique identifier (URL) that is published by the Service Metadata Locator (SML) on the Domain Name System of the network.
- the URL enables the sending Access Point to dynamically locate the correct SMP and then locate the correct receiver by retrieving the receiver identifier

The Peppol network model visualised (e-Invoice scenario)

C1

- Send Invoice data to C2 (method out of scope for Peppol)

C2

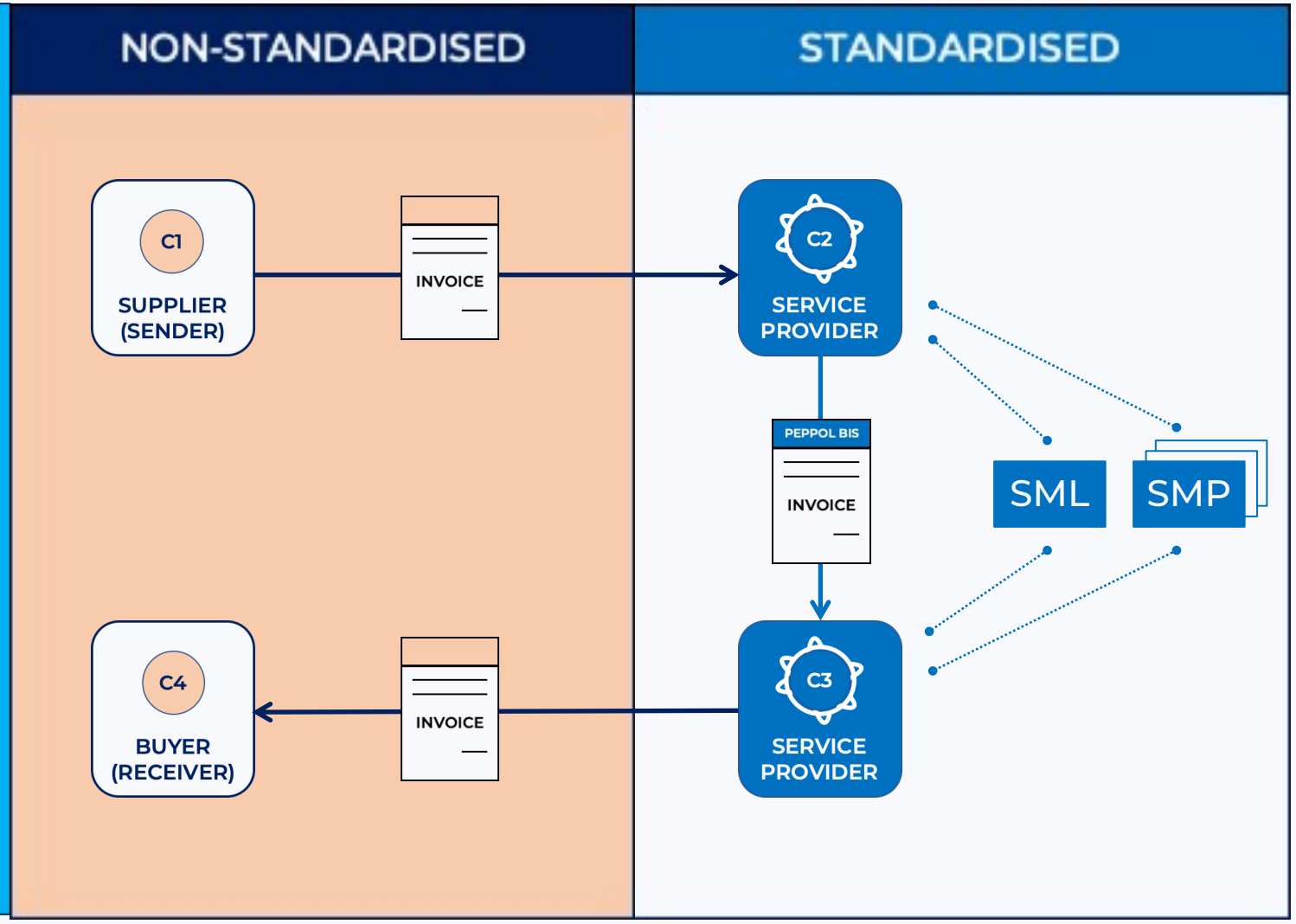
- Connects to the SML to look up the address of the Receiver's SMP
- Connects to the Receiver's SMP to look up the capability of the receiver

C3

- Receive and send receipt to C2 for the document. Then sends it to C4 (method out of scope for Peppol)

C4

- Receive and process the Invoice (accept or reject)



Peppol BIS Specifications (1)

Basic Principles surrounding the Peppol format

- The document Format is XML and based on UBL (Universal Business Language)
- The specifications are developed and maintained by the respective Peppol domain community where they belong and updates to the specifications are released twice a year Fall and Spring
- **Post-Award documents Norway**

  Invoice & CreditNote documents

  Order & OrderResponse

  DespatchAdvice

  Catalogue only with Response

  Punch Out

  Order Agreement

  Message Level Response

  Invoice Response

  Catalogue without response

  Pre-Award documents

  Procurement Procedure subscription

  Procurement document access

  Tender Submission

  ESPD Request

  Pre-award catalogue

  Payment in

  ISO20202 bank standard

Peppol BIS Specifications (2)

Basic Principles surrounding the Peppol format

- All Peppol documents MUST be validated by C2 before sending
  - Validation engines for standard Peppol BIS documents are provided by OpenPeppol and implemented by the Service Providers
  - Ensures: High quality and a very low error rate on exchanged documents. Receiver can trust what he gets is compliant to the Peppol Specifications!

- The mandatory document principle of Peppol
  - All receivers registered in any SMP must be as a minimum support receival of the mandatory Peppol BIS. Current mandatory Peppol BIS version is 3.0.
  - Ensures: Interoperability as all receivers in the network have a minimum of receiving capability that is known and understand by all.
  - Some countries **cant** support standard Peppol BIS 3.0 standard like Singapore, Australia, New Zealand and Japan why these rules do not apply in the same way.

Entity Identification Policy

Jesper Larsen – Peppol Support Lead

Entity Identification Policy - End user information (KYC)

- End user Identification > What information MUST Peppol Service Providers obtain as a minimum of the customers to whom they offer Peppol services (the senders and receivers)

1. Legal identifier of the End User in the jurisdiction within which it is legally based, and legal identifier Type (e.g. VAT number, company registration number).
2. Legal form of the End User.
3. Legal name of the End User, in the jurisdiction within which it is legally based.
4. Legal address, including country and (where applicable) territory information.
5. Name and identifier of the legal representative of the End User, authorised to act on its behalf.
6. End User's capability to receive and/or send Peppol Dataset Types (Document Type ID).
7. All Peppol identifiers used by the End User. If these are associated with different trade names or legal entities within the same organization, associations must likewise be mapped.
8. Name and contact details for End User representative(s) responsible for the Peppol Service, at a minimum email address.
9. Proof of ownership – i.e. that the information has been provided by the entity it concerns.
10. Which intermediaries, if any, intermediate the End User's access to the Peppol Services. The following information must be known about each intermediary:

    a. Legal identifier of the Intermediary in the jurisdiction within which it is legally based, and legal identifier Type (e.g. VAT number, company registration number).

    b. Legal name of the Intermediary, in the jurisdiction within which it is legally based.

    c. Legal address of the Intermediary, including country and (where applicable) territory information.

Entity Identification Policy - End user information

- Core rules and principles
  - Service Providers remain responsible for the correctness of End User information at all times
  - End User Information shall be collected and verified when the End User is enrolled into the Peppol Network by the Service Provider and the information should be verified on an annual basis

Entity Identification Policy - Peppol Service Provider identification

- Peppol Service Provider Identification > What information MUST Peppol Authorities obtain as a minimum of the Peppol Providers with whom they sign Peppol agreements with

1. Legal identifier of the Service Provider in the jurisdiction within which it is legally based, and legal identifier Type (e.g. VAT number, company registration number).
2. Legal form of the Service Provider.
3. Legal name of the Service Provider, in the jurisdiction within which it is legally based.
4. Legal address, including country and (where applicable) territory information.
5. Contact information for formal notices.
6. Any other names the Service Provider trades under.
7. Name and identifier of the legal representative of the Service Provider, authorised to act on its behalf.
8. Name and contact details for Service Provider representative(s) responsible for the Peppol Service, at a minimum both email and telephone number.
9. Proof of ownership – i.e. that the information has been provided by the entity it concerns.

Entity Identification Policy - Peppol Service Provider Identification

- Rules and principles
  - Peppol Authorities remain responsible for the correctness of Service Provider information for the providers they have contracted
  - Service Providers Information shall be collected and verified when the Service Provider is signed.
  - This information needs to be checked and verified at least before each renewal of production PKI certificates
  - Peppol Authorities can require audits of the financial and technical capabilities before chossing to sing
    - The cost of such audits falls on the Peppol Authority and must be minimally invasive as possible

Service Provider Accreditation Policy

Jesper Larsen – Peppol Support Lead

Service Provider Accreditation Policy

- Preconditions for being accredited
  - Any new Provider must have passed the onboarding test for the type of Peppol services they intend to offer (AP, SMP, Post-Award, Pre-Award)
  - Signed the SP agreement with the relevant Peppol Authority. The relevance depends on two things; where the Service Provider is based and where the Service Provider plans to offer Peppol Servives
  - The Provider has to be a member of Peppol in the apprpriate categories (Post-Award, Pre-Award,

Service Provider Accreditation Policy

- Accreditation Process
  - Initiate relations with a Peppol Authority with whom they will sign
  - Request a test PKI Peppol certificate from OpenPeppol (PA will have to approve)
  - Do the central onboarding test with OpenPeppol and any other PA specific accreditation if that is applicable
  - Finally sign the Service Provider agreement with the Peppol Authority
  - Request a test PKI Peppol certificate from OpenPeppol (PA will have to approve)
  - Accredited meaning:
    - Production certificate(s) can be enrolled
    - Appear on the Peppol Website as Certified Peppol Service Providers
    - Allowed to use the official Peppol Provider logo

Reporting policy

Jesper Larsen – Peppol Support Lead

Japan specific questions

- **Who manages and authenticates participants (senders and receivers)**
  - The Service Providers manage and ”activate” the buyers and suppliers in the Peppol Network. All Service Providers are expected to have an agreement the end user and have done the correct KYC (know your customer)
  - When **receiving** Service Providers register the end user in an SMP and the SML (either their own SMP or another SMP)
  - When **sending** Service Providers start sending on behalf of the participants (no registration is needed in the SML)

Japan specific questions - 1

- **Who manages and authenticates Peppol actors (End Users and Service Providers)**
  - **C1 and C4**
    - The Service Providers manage and ”activate” the buyers and suppliers in the Peppol Network. All Service Providers are expected to have an agreement with the end user and have done the correct KYC (know your customer procedure)
    - When **receiving** Service Providers register the end user in an SMP and the SML (either their own SMP or another SMP)
    - When **sending** Service Providers start sending on behalf of the participants (no registration is needed in the SML)
    - As a basis Peppol does not interfere in the relation between C1-C2 and C3-C4
    - Mass adoption through the use of a centralized SMP approach (the Singapore Model)
  - **C2 and C3**
    - The Peppol Authorities authenticate and manage the Peppol Service Providers by agreements
    - OpenPeppol onboard and test their implementations are compliant to the Peppol Specifications (AS4, SMP and BIS). Currently we only test AS4

Japan specific questions - 2

- **The Peppol Network and other domains**
  - Peppol has several domains which all are approved by OpenPeppol and follow the Peppol rules and governance
    - PoAC
    - PrAC
    - eDelivery
  - Peppol has one other business domain approved for Norway
    - Payment Domain (bank specific documents)
    - Approved by OpenPeppol to run on the Peppol Network but exclusively maintained and run by the Norwegian Peppol Authority
    - In the end this domain could be formally adopted as general Peppol business domain

Japan specific questions - 3

- **Different approach to the SMP setup - Centralized vs decentralized**
  - Centralized SMP approach: Norway, Netherlands and Singapore and partially Denmark and Belgium
  - Mandates use of a centralized SMP run and maintained by the governments
    - Norway mandates for entire Public sector but is highly used for Private sector participants aswell. 120k+ users in this SMP
    - Singapore mandates for registering singapore participants. No end user is forced into Peppol but effective encouragement through econcomic benefits are used. When Service Providers add singapore end users to the central SMP they are rewarded.

    Pros

    - High control and transparency to the Peppol evolvement in a country
    - Better control of compliance and control of what the service providers are registering on behalf of their end users and the processes they need to go through when registering end users (like KYC)

    Cons

    - The market of SMP providers and their offerings will most likely not be present

Japan specific questions - 4

- **Different approach to the SMP setup - Centralized vs decentralized**
  - Decentralized SMP approach: Sweden, UK, Ireland, AU, NZ and Germany
  - The market of SMP providers (often the AP providers) run their own SMP and register end users.

    Pros

    - Market mechanism. Competition increase the offerings and the innovation.
    - Easier for the Service Providers to have all their end users in the same SMP.

    Cons

    - Loose control from a political point of view. Hard to monitor the evolvement in terms of new end users being added in a country (the Peppol reporting policy will however deal with this)
    - Excersizing compliance to the processes of Peppol can be become harder. Control of what documents are allowed to be registered and what the actual process a provider has to go through to register a new end user (KYC etc.)

Questions