PEPPOL Compliance Policy

Version 1.0

Last updated 19. November 2018

OpenPEPPOL AISBL
Rond-point Schuman 6, box 5
1040 Brussels Belgium

Revision History

Date of this revision: 21-02-2019		Date of next revision:	
Version	Date	Summary of Changes	Changes marked
1.0	19-11-2018	First version Approved	(N)
1.0_PUBLISHED	21-02-2019	Editorial revisions – for publication	

Approvals

This document is approved by: OpenPEPPOL Managing Committee

Owner, Editor and Contributors

This document is provided by:

Unit	OpenPEPPOL AISBL
Owner	OpenPEPPOL Operating Office (OO)
Editor	Jostein Frømyr, Compliance Project Lead
Contributors	Oriol Bausà, co-editor, OO Compliance Expert Mairi Hayworth, OO Business Lead Jesper Larsen, OO Technical Lead

Table of Content

1. Introduction

1.1. Context

OpenPEPPOL is founded on a recognition "that national and/or regional infrastructures do exist and will continue to exist in the foreseeable future"[1]. Based on this recognition the aim of OpenPEPPOL is to "*provide a means by which users connected to one infrastructure are able to exchange business documents with users connected to another infrastructure*"[1]. To achieve this objective OpenPEPPOL has adopted two levels of governance where *"… the PEPPOL Coordinating Authority will have authority over all central components of the PEPPOL Transport Infrastructure. The PEPPOL Coordinating Authority will delegate the authority over the implementation and use of the PEPPOL Transport Infrastructure within a defined domain to a PEPPOL Authority*"[2].

As PEPPOL is being adopted in more and more countries, the proliferation of PEPPOL Authorities, Access Points and Service Metadata Publishers and the need to enlarge the scope to domestic transactions implies that PEPPOL Authorities use the Annex 5 on the PEPPOL Authority Agreement to define the specificities applicable within their geographical or industrial jurisdiction.

This document is prepared by a task force established under a mandate given by the OpenPEPPOL Management Committee on May 30, 2018 to establish a set of guiding principles and rules that can serve to clarify:

the degree of freedom given to PEPPOL Authorities when defining requirements in Annex 5;

the operational aspects, such as sending documents without validation, using test certificates in production, mandatory BIS compliance, adherence to SLA terms, etc.;

ways of cooperation between PEPPOL Authorities in resolution of problems related to Service Providers with different PEPPOL Authorities as their contractual party.

Compliance of the different organizational and administrative entities of OpenPEPPOL AISBL is not addressed in this document.

The key words "must", "must not", "required", "shall", "shall not", "should", "should not", "recommended", "may", and "optional" in this document are to be interpreted as described in RFC 2119[3].

[1] PEPPOL Authority Agreement clause 2.1.

[2] PEPPOL Authority Agreement clause 2.2.

[3] Key words for use in RFCs to indicate Requirement Levels

1.2. Purpose of the document

This Compliance Policy is focused on the contractual responsibilities of the PEPPOL Authorities, the PEPPOL AP and SMP providers with a view to ensure interoperability across the full PEPPOL network and to improve the communication and convergence between all actors. This can only be achieved if the OpenPEPPOL community maintains a common rule set, i.e. principles and compliance criteria, as a baseline for all actors involved.

This does however, not negate or diminish the value and role of the PEPPOL Authorities as a main driver for digital procurement and invoicing in their jurisdiction. The role of OpenPEPPOL is to provide the tools, including the agreement and the governance framework, to ensure interoperability (cross border/cross system), and to make this happen in a cost effective and standardised way.

1.3. Intended audience

The document is specifically aimed at PEPPOL Authorities and PEPPOL AP and SMP providers. It is intended as a supplement to the PEPPOL agreement and governance framework to provide clarifications on compliance issues that has been discussed and resolved.

1.4. Current status of the document

Version 1.0 of this document was approved by the OpenPEPPOL Management Committee for implementation and use in December 2018.

2. Glossary of terms

Compliance is the adherence to agreed rules and policies.

The **PEPPOL Secretary General**, supported by the **PEPPOL Operating Office**, fills the role of **PEPPOL Coordinating Authority** as described in the PEPPOL eDelivery Agreement[4], and therefore has the authority over all the central components of the PEPPOL eDelivery Network.

PEPPOL Coordinating Communities (CC) are member communities within the OpenPEPPOL AISBL targeting a specific business or functional domain. A key function of the PEPPOL Coordinating Communities is to define and sustain technical specifications, standards and policies relevant for their domain, such as PEPPOL BIS Specifications.

The **PEPPOL eDelivery Network** is comprised of the technical standards and service specifications, the Service Metadata Locator and the eDelivery Agreements Framework and its annexes. The network is created by Access Points and its participants are registered in the Service Metadata Publishers[5].

A **PEPPOL Authority** (PA) is an organisation or body to whom the PEPPOL Coordinating Authority has delegated authority for the implementation of the PEPPOL eDelivery Network within a defined geographical or Industrial jurisdiction[6]. It is responsible for implementing the PEPPOL agreement framework by signing the Transport Infrastructure Agreement with organisations deploying the role of PEPPOL Access Points and/or PEPPOL Service Metadata Publisher providers. It is also responsible for implementing the local PEPPOL Authority governance structure ensuring that these services are provided in conformance to the PEPPOL technical standards and service specifications.

A **PEPPOL Access Point** (AP) is an entry point to the PEPPOL eDelivery Network[7]. An AP implements the PEPPOL eDelivery Network transport protocols and connects a PEPPOL Participant to the network. APs are maintained by organisations that have signed an AP Provider Agreement with a PEPPOL Authority.

A **PEPPOL Service Metadata Publisher** (SMP) is an address book or business registry containing receiving capabilities for PEPPOL Participants. An SMP is a distributed element of the PEPPOL eDelivery Network that allows the discovery of the endpoint of any PEPPOL Participant. SMPs are maintained by organisations that have signed an SMP Provider Agreement with a PEPPOL Authority.

A **PEPPOL Participant** (participant) is an end user of the PEPPOL eDelivery Network using the network for the exchange of messages with other participants. It is also known as C1 (Corner 1) or C4 (Corner 4).

A **sender** is a participant sending a message through the PEPPOL eDelivery Network. The sender must be known to the AP that is providing him access. It is also known as C1 (Corner 1) and does not have to be registered in any SMP.

A **receiver** is a participant receiving a message over the PEPPOL eDelivery Network. It is also known as C4 (Corner 4) and must be registered in an SMP.

[4] PEPPOL Authority Agreement clause 4.2.

[5] https://peppol.eu/what-is-peppol/peppol-transport-infrastructure/

[6] https://peppol.eu/who-is-who/peppol-authorities/

[7] https://peppol.eu/who-is-who/peppol-certified-aps/

A **PEPPOL Business Interoperability Specification** (PEPPOL BIS) is technical standard defining a standard document model and its validation rules defined by a PEPPOL Community. PEPPOL BIS are developed for common business processes to standardise electronic documents exchanged and validated through the PEPPOL eDelivery network[8].

A **Domain** in PEPPOL is a business area where different business processes are described and standardized through one or more PEPPOL BIS.

[8] https://peppol.eu/what-is-peppol/peppol-profiles-specifications/

3. Overarching Principles

OpenPEPPOL is governed by a set of overarching principles that must be preserved and respected by all actors and roles involved in the governance and operation of the network. The overarching principles are:

1. **No actor can sign an agreement with itself**

   OpenPEPPOL allows a given actor to fill several roles[9], e.g. a PEPPOL Authority may itself offer PEPPOL AP or SMP services to the market. In such case the relevant actor shall sign the AP/SMP Provider Agreement with the PEPPOL Coordinating Authority.

2. **Connect once – serve all**

   A service provider who has signed a PEPPOL AP/SMP Agreement shall be allowed to offer its services to any PEPPOL Participant[10]. Likewise, a PEPPOL Participant connected to the network shall be allowed to send business documents to any other participant registered in an SMP in the PEPPOL eDelivery Network, in any country, through one single Access Point connection.

3. **PEPPOL technical standards and service specifications are baseline for interoperability**

   Technical standards and service specifications issued or recognised by OpenPEPPOL shall be considered as the common baseline for interoperability in the PEPPOL eDelivery Network that all actors shall support and respect[11].

4. **Different domains may have different service level requirements**

   Each PEPPOL domain specific community may define and enforce specific service level requirements for their domain as documented in Annex 3 and approved by the relevant PEPPOL Change Management Bodies.

5. **Mandatory support for PEPPOL BIS**

   PEPPOL Communities define PEPPOL BIS to promote global interoperability. Nevertheless, new document types and customizations may be defined and supported if they are defined and registered according to PEPPOL registration procedures. Receivers with a registered receive capability for a business function for which a PEPPOL BIS is available shall have receive capabilities for the PEPPOL BIS registered in an SMP, as a minimum.

6. **Only valid documents are to be exchanged over the network**.

   The sender is accountable for the technical correctness and quality of the submitted business documents and shall ensure that submitted business documents are valid according to the relevant specification (e.g. PEPPOL BIS). Available tools, such as validation artefacts, may be used by the participant, or service provider acting on his behalf, to ensure that only technically valid document instances are submitted through the PEPPOL eDelivery Network.

7. **Service provider freedom to choose a PEPPOL Authority**

   A service provider who wants to offer PEPPOL AP or SMP services in any market is free to sign one single PEPPOL AP Provider or PEPPOL SMP Provider Agreement with any PEPPOL Authority.

   A service provider may however choose to sign more than one Annex 5 to indicate that he fulfils the requirements of different PEPPOL Authorities but cannot be compelled to do so.

[9] PEPPOL Authority Agreement clause 4.4.

[10] PEPPOL Authority Agreement clause 4.5.

[11] PEPPOL Authority Agreement clauses 5.1 and 5.2, and PEPPOL AP Provider Agreement clause 4.4

8. Know your customer (KYC)

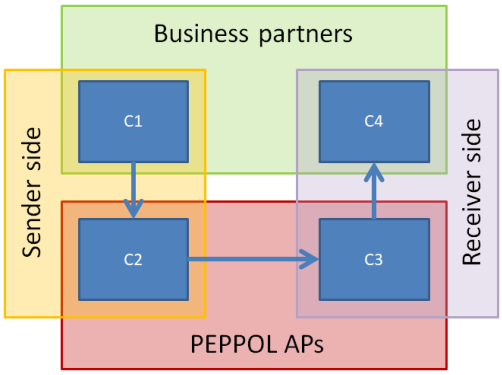
Each AP service provider must have a written service contract with its customers carrying forward the minimum requirements defined by OpenPEPPOL. Furthermore, the identity of PEPPOL participants acting in the role as sender or receiver of documents exchanged over the PEPPOL eDelivery Network shall be identified in the message exchange between APs.

9. Implementing the four-corner model

The PEPPOL eDelivery Network is built on the 4-corner model. This model requires the exchange of business documents to be performed through four corners:

- Corner 1 is the sender of the electronic document. He issues a document intended to the final recipient (corner 4)
- Corner 2 is the entry point to the network. In PEPPOL, the Access Point that acts on behalf of the sender and submits the document to the receiving Access Point.
- Corner 3 is the recipients' network endpoint. In PEPPOL, the Access Point that acts on behalf of the receiver (corner 4) of the document.
- Corner 4 is the receiver of the business document. The party that will process the business document and provide a business response as needed.

A main feature of the four-corner model is that the sender and receiver (C1 and C4) may choose the service provider completely independent of each other. Furthermore, In the PEPPOL eDelivery Network, no roaming agreements or charges are allowed between C2 and C3.



4. Addressed issues and recommendations

Any organisation offering services within OpenPEPPOL shall ensure that the services they offer comply to:

- the overarching principles defined above;
- the agreement they have signed with a PEPPOL Authority or with the PEPPOL Coordinating Authority in case there is not PEPPOL Authority established in their domain/country/region;
- the technical standards and service specifications relevant for their service offering.

Common use cases and issues relevant to the different roles in the PEPPOL are discussed in the following sections.

4.1. PEPPOL Authority compliance – use of annex 5

PEPPOL Authorities are usually created by Governments that are implementing PEPPOL as their domestic document exchange infrastructure as a driver for digital procurement and invoicing in their jurisdiction.

When new PEPPOL Authorities sign a PEPPOL Authority Agreement with the PEPPOL Coordinating Authority, they can define an Annex 5 including specific requirements that will be part of the agreement for the SMPs and APs under their jurisdiction.

A template for the content of Annex 5 is provided as an annex to this document. Commonly addressed topics are discussed in the following sub-sections.

4.1.1. Purpose and approval of Annex 5

The purpose of Annex 5 is to allow a PEPPOL Authority to express and enforce any "…additional restrictions and criteria, beyond those enforced by the PEPPOL Coordinating Authority… on PEPPOL AP Providers and PEPPOL SMP Providers they contract with"[12]. The content on any Annex 5 shall however "… not hamper the interoperability with PEPPOL Participants using other PEPPOL AP Providers and PEPPOL SMP Providers".

PEPPOL authorities thus shall take due note to ensure that their additional restrictions and criteria do not violate the overarching principles of OpenPEPPOL defined above and places an unnecessary burden on the service providers.

To ensure that the overarching principles of OpenPEPPOL are respected and properly reflected, all new or amended Annex 5 shall be approved by the PEPPOL Coordinating Authority based on the following process:

1. A draft of the proposed Annex 5 shall be prepared by the PEPPOL Authority.

[12] PEPPOL Authority Agreement clause 5.1

2. A review of the draft Annex 5 shall be performed by the PEPPOL Agreement Coordinator and the PEPPOL Compliance & QA Lead to ensure that:
    a. all overarching principles are respected;
    b. the requirements and criteria do not represent an unnecessary burden on service providers.
3. Comments to the draft resulting from the review process shall be resolved by the PA.
4. Following the comment resolution and in consultation with the PEPPOL Authority, the PEPPOL Compliance & QA Lead shall make a recommendation to accept or reject the draft Annex 5, supported by a summary of the process including issues addressed during comment resolution and any outstanding issues not yet resolved.
5. Based on the recommendation from the PEPPOL Compliance & QA Lead, the PEPPOL Coordinating Authority shall approve or reject the draft Annex 5 for implementation.

4.1.2. National Boundaries (scope of Annex 5)

The initial clause of Annex 5 refers to its scope. The meaning of the scope defined within Annex 5 is to identify the geographical or industrial jurisdiction within which the PA will enforce its additional requirements.

Respecting the overarching principles of "freedom to sign agreement" (principle 7) and "connect once – serve all" (principle 2) it follows that a service provider shall not be required to sign more than one PEPPOL AP or SMP Provider Agreement.

There are several indications that the use of PEPPOL is becoming increasingly domestic. Countries are starting to use PEPPOL as the backbone infrastructure to support their national document exchange in addition to the cross-border use case. In national scenarios, national legal rules shall of course apply. Such national legal rules are typically related to the business content of exchanged documents. Should the national legal rules not be supported by the PEPPOL BIS, a PEPPOL Authority can create a PEPPOL BIS Customization that will be supported by the PEPPOL eDelivery Network for domestic trade in that specific national legal framework (see also section **Fejl! Henvisningskilde ikke fundet.** below). Any PEPPOL Customization may be supported in OpenPEPPOL.

Domestic traffic may be covered by domestic rules set forth in Annex 5. An AP or SMP provider who wants to be recognised to offer their services for domestic use in a jurisdiction covered by a PEPPOL Authority may choose to sign and comply with the Annex 5 requirements of that PEPPOL Authority. This does not require them to sign a completely new AP/SMP Provider Agreement, only to sign the appropriate Annex 5[13].

Senders that have not signed with a domestic service provider in the country of the recipient does not – per se – need to comply with the domestic rules in the country of the recipient. However, senders might have a business agreement with the recipients that require them to comply with domestic rules on a bilateral basis.

[13] PEPPOL Authority Agreement clause 5.4.

Besides, even if using AP service providers from different countries, these senders might want to send documents to a recipient in their own country, and therefore, the exchange would be considered domestic, and the use of domestic rules in that country would apply.

4.1.3. National testing

To support the overarching principle of "*PEPPOL technical standards and service specifications are baseline for interoperability*" (principle 3), OpenPEPPOL will provide a central testbed to verify that the services provided by certified AP and SMP providers comply to PEPPOL technical standards and service specifications[14]. The aim is to ensure a common interpretation and implementation to guarantee consistency across the entire PEPPOL eDelivery Network.

It is recognised that PEPPOL Authorities frequently wants to define extended or new national testing mechanisms to verify and ensure compliance to their additional rules defined in Annex 5. There are different types of national testing frameworks which, under the right conditions, can take place without breaking compliance, but mandatory national testing as a general practice to test PEPPOL BIS or eDelivery interoperability should be avoided.

- AP-to-AP interoperability testing

  Ensuring that APs can exchange documents using the protocols of the PEPPOL eDelivery Network is sometimes requested or imposed. Such practice can create risks of non-compliance with overarching PEPPOL principles and specifications and shall not be requested once the centralized OpenPEPPOL testbed is available.

- End-to-end and/or AP-to-Government testing

  OpenPEPPOL has deliberately defined the relationship between service providers (AP and SMP providers) and the end users (PEPPOL Participants) as out of scope for its governance. Consequently, it is up to the service provider to establish a service contract with the participants giving the participant access to the PEPPOL eDelivery Network. The existence of such a service contract is required[15], but only limited requirements are stated for its content.

  As the PEPPOL Authority does not have a direct relationship to the end users nor a mandate to require specific behaviour, other than as expressed in a PEPPOL BIS, requirements for end-to-end and/or AP-to-Government testing shall not be stated in Annex 5.

  To the extent that a government entity also operates a centralised document processing service, this is not done in their role as PEPPOL Authority and any testing of such processing services shall not be part to Annex 5.

On the other hand, a PEPPOL Authority is free to define testing requirements towards AP and SMP providers with whom they have a contractual relationship, including a signed Annex 5, to verify that the service provider complies to their additional requirements defined in Annex 5[16].

[14] https://peppol.eu/downloads/

[15] PEPPOL AP Provider Agreement clause 6.9 and 6.10.

[16] PEPPOL Authority Agreement clause 5.5

4.1.4. Additional or Customized BIS

Only PEPPOL Communities can develop and approve PEPPOL BIS for use in the PEPPOL eDelivery Network. A PEPPOL Authority can however create derivative versions of the BIS, but these customisations need to be identified with a new Document Identifier.

Furthermore, a PEPPOL Authority may also develop or approve new documents types for business functions where a PEPPOL BIS does not exist. The possibility to create derivative versions (or national rulesets within v3) of PEPPOL BIS and BIS for a new document types, lies exclusively with the PEPPOL Authorities.

- Create additional customizations

  When new customizations of existing PEPPOL BIS are defined by a PEPPOL Authority, they need to provide full documentation and establish support mechanisms that can be used by the sender to verify the content of such documents according to the following process:

- Perform a gap analysis identifying the requirements derived from national legal rules or common practices in the PEPPOL Authority scope.
- Submit to the relevant PEPPOL Community the list of new requirements for assessment. The PEPPOL Community shall review the requirements and decide whether they can be considered for a new revision of the PEPPOL BIS or whether a new customization must be created.
- If a new customization must be created, and according to the comments received from the PEPPOL Community, the PEPPOL Authority shall implement the customization documentation following the PEPPOL templates for a customization.
- The PEPPOL Authority shall also provide validation artefacts to support the new customization.
- Both the customization documentation and the validation artefacts shall be submitted to the relevant PEPPOL Community for review and publication on the PEPPOL website.

Create variations of "BIS 3.0"

In "BIS 3.0", i.e. a BIS following the principles laid down for PEPPOL BIS Billing 3.0, national rules should be included in the PEPPOL BIS and national variants should be avoided. The way to deal with National CIUS within OpenPEPPOL shall be as follows:

- PEPPOL Authorities identifies national variants to the PEPPOL BIS 3.0 according to national requirements.
- These differences shall be submitted to the relevant PEPPOL Community Change Management Board for consideration.
- The PEPPOL Community Change Management Board shall review the PEPPOL BIS 3.0 to accommodate specific national CIUS requirements.
- To the extent possible national CIUS requirements shall be added to the PEPPOL BIS as national rules rather than developing a customisation.

- Should the needed changes be too specific for a CIUS, the PEPPOL Community Change Management Board may decide not to implement these specific requirements in the PEPPOL BIS 3.0 and the PEPPOL Authority may consider developing a customization.

Create new document types

A PEPPOL Authority may create or approve new document types for use in any of the existing or new functional domains in PEPPOL following the process as outlined below:

- The process of creating a new document type starts with gathering the requirements
- Based on the requirements, the PEPPOL Authority shall draft the new document type according to the PEPPOL BIS template.
- The draft PEPPOL BIS shall be submitted to the relevant PEPPOL Community for review. For new document types for which no PEPPOL Community exists, the role as PEPPOL Community is allocated to the PEPPOL Coordinating Authority.
- The PEPPOL Community shall assess the new BIS and provide comments to the PEPPOL Authority.
- Consensus shall be achieved between the PEPPOL Authority and the PEPPOL Community to resolve the issues and comments provided by the PEPPOL Community on the new document type.
- Once the new document type is agreed, the PEPPOL Authority shall develop the validation artefacts to support the new document type and its business rules.
- The Community shall publish the new document type on the PEPPOL website.

Compliance to the overarching principle of "*mandatory support for standard PEPPOL BIS*" shall always be preserved, taking appropriate measures such as making sure that any national variants of a BIS is differently named and identified, and cannot be confused as an acceptable alternative to the PEPPOL BIS.

4.1.5. Additional eDelivery and Security requirements

New eDelivery mechanisms or security features can be required due to specific requirements, especially if the PEPPOL Authority engages in new functional business domains. In general, Domains in PEPPOL shall have a PEPPOL Community established once its development process has been proven, finalized and approved by the PEPPOL Management Committee. A PEPPOL Authority may be nominated by the PEPPOL Management Committee as the lead for the development of a new domain and regulate domain specific requirements within its jurisdiction.

The channel to define new eDelivery and security mechanisms for use in the PEPPOL eDelivery Network is vested to the OpenPEPPOL organization and specifically the rules and policies agreed by the eDelivery Community.

A two-layer PEPPOL agreement structure is being defined, and in such a structure, use of the PEPPOL eDelivery Network will be the common denominator for all functional domains covering all acceptable variants of security settings and requirements.

All eDelivery and security mechanisms allowed for use in the PEPPOL eDelivery Network shall be defined as part of the PEPPOL technical standards[17]. Any changes to existing or additional eDelivery and security mechanisms required to support specific requirements shall be agreed by the PEPPOL eDelivery Community as this has a potential consequence on AP providers offering services in several domains. A PEPPOL Authority may however request the use of a specific eDelivery or security mechanism or set of security mechanisms as part of its Annex 5 for new domains subject to approval by the OpenPEPPOL Managing Committee. Any such additional eDelivery or security mechanisms shall respect the PEPPOL Transport Security Policy[18].

PEPPOL Participants and AP Providers involved in the exchange of documents within a given functional domain shall implement the security features or settings relevant for that domain.

4.1.6. Additional Service level requirement

Service Level Requirements for a given PEPPOL Domain (SLA requirements) shall be the same for all actors taking a specific role in the PEPPOL eDelivery Network. It is however also recognised that there may be a need to define specific SLA requirements within specific functional domains. A PEPPOL Authority nominated by the PEPPOL Managing Committee may start the definition of a new PEPPOL Domain, where its service level requirements will be described.

Before entering the process of defining additional, and stricter, SLA requirements the PEPPOL Authority should take due consideration of the consequence on the service providers and shall consult with the PEPPOL Service Provider Community on the feasibility of its requirements.

4.1.7. Centralized SMP

The general principle in OpenPEPPOL is that SMP services may be freely offered to the market by any certified PEPPOL SMP Provider. To support national policy objectives and requirements, some PEPPOL Authorities may however restrict the establishment of SMP services to a single and centralized SMP provider within their jurisdiction. This typically implies that legal entities (receivers) must have their receive capabilities registered in one centrally maintained SMP.

OpenPEPPOL does however not encourage PEPPOL Authorities to enforce the use of centralised SMP services since it disrupts an open market for service providers and end users. Centralised SMPs also introduce complexity for service providers since they are likely to have receivers registered in many SMPs instead of one.

[17] https://peppol.eu/downloads/the-peppol-edelivery-network-specifications/

[18] https://peppol.eu/downloads/the-peppol-edelivery-network-specifications/

4.2. AP compliance

4.2.1. Signing the PEPPOL AP Provider Agreement

A PEPPOL Access Points provider shall sign the PEPPOL AP Provider Agreement with a PEPPOL Authority. Following the overarching principle on "*Service provider freedom to sign agreements*" (principle 7) and "*Connect once – serve all*" (principle 2) a PEPPOL AP provider may sign the agreement with any PEPPOL Authority and offer its services to all participants in the PEPPOL eDelivery network.

OpenPEPPOL does however recommend that the AP provider signs the agreement with the PEPPOL Authority in the country they are registered in or where they have a majority of their business.

4.2.2. Additional testing against specific AP rules

It is noted that some AP providers are imposing additional tests on behalf of their customers (the PEPPOL Participants) to other AP providers, imposing additional business rules to the ones described in the PEPOL BIS.

To the extent that such requirements are aimed at other AP providers they are considered to be in violation of the overarching principle on "*Connect once – serve all*" (principle 2) and shall not be allowed.

To the extent that such requirements are aimed at PEPPOL participants connected to other APs this is a question of end-to-end testing between PEPPOL participants and thus out of scope for OpenPEPPOL. Such requirements shall not be presented as part of the AP service and should, as a rule, be avoided.

4.2.3. Non-validation of issued documents

The lack of validation of documents before sending is an unfortunately a fact. Such practise is against the overarching principle that states that only valid business documents are exchanged over the PEPPOL eDelivery Network (principle 6). The issued business documents shall be a valid instance according to the rules stated in the governing BIS and should be validated using available validation artefacts before being sent into the PEPPOL eDelivery Network.

As per the overarching principle on "*Only valid documents are to be exchanged*" (principle 6), it is the sender of the document that is accountable for the technical correctness and quality of the submitted business documents. To the extent that a provider of PEPPOL AP services also offers validation services to its senders this validation shall be considered a separate service that is performed on behalf of the sender.

When acting as a sending Access Point, the PEPPOL AP Provider shall however monitor the behaviour and performance of the sender to ensure that business documents are confirmed as valid instances according to the applicable rules and technical specifications.

As a general rule, in cases where non-compliance is detected by a receiving PEPPOL Participant or AP this should be addressed with the sending AP (with the help of the OO), that will need to approach the sender(s) they have as customer(s) to resolve the issue.

If the sending PEPPOL Participant continues to send non-compliant BIS documents, the receiving AP shall report this to the PEPPOL Authority they have signed the AP Provider Agreement with. The PEPPOL

Authority will then follow up with the sending AP directly or through the PEPPOL Authority the sending AP has signed their AP Provider Agreement with. Non-compliance, and failing to respond to PEPPOL Authority intervention may eventually lead to revocation of the sending APs PEPPOL certificate.

Non-compliance reports for non-validation shall contain the following information:

a) Message type
b) Timestamp
c) Sending AP
d) Participant ID of sender/receiver
e) Description of validation error detected

4.2.4. Rejection to receive

The basic role of a PEPPOL AP is to act as a "delivery man" in the exchange of messages between PEPPOL participants. It is not the role of an AP provider to process the actual content of business documents.

In this role, the AP provider is expected to ensure that the transport is done according to the relevant eDelivery specifications. This includes a responsibility to ensure that the transmission has the correct metadata, including the appropriate identity of the sender and receiver of messages. On the other hand, it is not acceptable for a receiving AP to reject a transmission from other APs in the PEPPOL eDelivery Network due to policy or business reasons.

The legal entity operating in the role as AP provider may however also offer additional services to its customers, such as validation services.

4.2.5. Acceptance of standard BIS

It is the responsibility of the PEPPOL AP provider to ensure proper registration of receive capabilities of its customers in an PEPPOL SMP[19]. This includes a responsibility to ensure that the receiver has receive capabilities registered for the PEPPOL BIS.

4.3. e-Delivery compliance

The PEPPOL eDelivery Network defines a set of protocols and agreements that shall be adhered to in order to ensure efficiency and consistency when exchanging messages through the PEPPOL eDelivery Network.

[19] PEPPOL AP Provider Agreement clause 4.5.

4.3.1. Transparent gateway

To the extent that a PEPPOL AP provider acts as a gateway to other infrastructures/networks the complexity of these other networks shall not be exposed to other PEPPOL AP providers. This implies that specific requirements on formats, security, and addressing, that are often implemented by means of different mechanisms and protocols, shall not be imposed on other AP providers. Nor shall the PEPPOL participants have to specify addresses or take security measures in a special way due to the need for the message to be delivered to a non-PEPPOL infrastructure.

4.4. SMP compliance

4.4.1. Signing the PEPPOL SMP Provider Agreement

A PEPPOL SMP provider shall sign the PEPPOL SMP Provider Agreement with a PEPPOL Authority. Following the overarching principle on "*Service provider freedom to sign agreements*" (principle 7) and "*Connect once – serve all*" (principle 2) an SMP provider may sign the agreement with any PEPPOL Authority and offer its services to all participants in the PEPPOL eDelivery Network.

OpenPEPPOL does however recommend that the SMP provider signs the agreement with the PEPPOL Authority in the country they are registered in or where they have a majority of their business.

4.4.2. Identification of all the receiving participants

It is noted that some SMPs hide the actual receivers of business documents in the SMP entries, adding only a proxy participant and using other types of elements for internal routing. This is a practice usually found in some countries with proprietary delivery infrastructures and national gateways, where a PEPPOL AP is the single point of entry.

Such practice is not compliant to the overarching principle of "*Know your customer*" (principle 8). A PEPPOL SMP provider shall ensure that only actual receivers are registered in the SMP.

4.4.3. Register the minimum receiving capabilities for receivers

It is noted that some participants register a customized version of a PEPPOL BIS, but do not register receive capabilities for the mandatory PEPPOL BIS.

To respect the overarching principle of "*Mandatory BIS*" (principle 5) an SMP provider shall have procedures in place to ensure that receivers with a registered receive capability for a business function for which a PEPPOL BIS is available, also have receive capabilities for the PEPPOL BIS registered in its SMP.

There is usually a migration path defined for the introduction of a PEPPOL BIS in the market. This also contains provisions for when an old version of a PEPPOL BIS shall no longer be used.

The SMP provider shall have procedures in place to ensure that receive capabilities for old and deprecated PEPPOL BIS are removed from their SMP.

5. Compliance issue detection and resolution process

Actors involved in PEPPOL are encouraged to report incidents of non-compliance to the PEPPOL Authority with whom they have a contract or directly to the OpenPEPPOL OO who will forward such reports to the PEPPOL Compliance Team for further investigation.

The tool to report issues in OpenPEPPOL is JIRA/Confluence. PEPPOL Authorities are free to use the tool of their choice for non-compliance reporting.

5.1. Resolution process on PEPPOL Authorities

Compliance of a PEPPOL Authority will be established by the PEPPOL Management Committee based on the assessment of the Compliance Team on the basis of an approved Annex 5.

If a new issue on compliance for a PEPPOL Authority is recognised, the following process will apply:

1. Report the issue to the service desk by means of the JIRA/Confluence ticketing system.
2. The OpenPEPPOL OO will assign an issue manager to assess the new issue.
3. The issue manager shall investigate, evaluate and provide a recommendation on the way to deal with the new issue. This task may involve consultation or even establishing a task team of involved or affected stakeholders.
4. The suggestion for resolution shall be submitted to the PEPPOL Authorities and the PEPPOL Coordinating Authority for review.
5. The final decision on the resolution shall be made by the PEPPOL Coordinating Authority.
6. According to the final resolution, the OO will amend the Compliance Policy or other appropriate documents

5.2. Non-compliance process for PEPPOL AP and SMP Providers

Non-compliance reports received by the OpenPEPPOL OO will be assessed by the PEPPOL Compliance Team before being forwarded to the PEPPOL Authority with whom the AP or SMP has signed the PEPPOL AP/SMP Agreement.

As soon as the PEPPOL Authority is made aware of a possible situation of non-compliance, it shall initiate an investigation to confirm the cause of the situation as well as the consequence on the PEPPOL eDelivery Network as a whole.

Once a situation of non-compliance is confirmed, the PEPPOL Authority shall inform the AP/SMP provider on the observed situation by sending a Warning Note, with copy to the PEPPOL Compliance Team. The Warning Note shall:

- clearly identify the reason for the non-compliance;
- give the AP/SMP provider the possibility to correct the situation by inviting him to come up with a realistic plan for correcting the non-compliance within 5 working days; and

- clearly identify the type of penalties that will be enforced if the non-compliance situation is not corrected.
- The escalation process and type of penalties that may be enforced by the PEPPOL Authority are:
- Blacklisting on the OpenPEPPOL member site, i.e. publication of the fact that the AP/SMP provider is in a non-compliance situation on the closed member site of OpenPEPPOL;
- Public blacklisting, i.e. publication of the fact that the AP/SMP provider is in a non-compliance situation on the public web site of OpenPEPPOL (www.peppol.eu) and on the web site used by the relevant PA for market communication;
- Suspension of certificate, i.e. suspension of the PEPPOL certificate for a limited period of time;
- Revocation of certificates, i.e. permanent revocation of the PEPPOL certificate.

If the situation of non-compliance continues over time, the PA may initiate the next step in the escalation process as described above. For each step in the escalation process the PEPPOL Authority shall send a Warning Note with a defined timeline for correction.

The PEPPOL Authority may extend the suspension, depending on conditions set up by the PEPPOL Authority or ultimately exclude the AP/SMP provider from the PEPPOL eDelivery Network by revoking their PEPPOL Certificate. Any extension in suspension shall be documented by a Warning Note.

If the AP/SMP provider fails to respond within the set time-limit the PA may without further notice escalade the process and ultimately suspend or revoke the certificates.

6. Further work

Further work is needed by the OpenPEPPOL compliance team to prepare an Annex 5 template, and to establish a customisation registration procedure.