Peppol

The future is open

OpenPeppol AISBL Internal Regulations

Use of the Peppol Network

Status: Gold – Version: 0.2
Last updated: 03.05.2021

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

info@peppol.eu
www.peppol.eu
Last updated: 03.05.2021

Table of Contents

Version control

Version	Date	Comments
Gold 0.2	03.05.2021	Draft produced by the Agreements Task Force for member review

List of Terms and Abbreviations

Term	Definition
API	Application Programming Interface
APP CMB	Agreements, Policies and Procedures Change Management Board
BIS	Peppol Business Interoperability Specifications
CC	OpenPeppol Coordinating Committee
CMB	Change Management Board
EN	European Norm
IPR	Intellectual Property Rights
MC	OpenPeppol Managing Committee
OO	OpenPeppol Operating Office
PA	Peppol Authority
PCA	Peppol Coordinating Authority (OpenPeppol AISBL)
PKI	Public Key Infrastructure
RFC	Request for Change
SBDH	Standard Business Document Header
SML	Service Metadata Locator
SMP	Service Metadata Publisher
SP	Peppol Service Provider
XML	Extensible Markup Language

1 Introduction

1.1 Scope and Structure

The OpenPeppol AISBL Internal Regulations on the Use of the Peppol Network contains a set of Policies that include rules and provisions about the ways to operate in the Peppol Network. The content of these Policies is essential for the proper understanding of the legal obligations assumed through the Peppol Agreements, by further elaborating on the clauses of those Agreements.

The OpenPeppol AISBL Internal Regulations on the Use of the Peppol Network include Policies on the following subjects:

1. Change Management
2. Entity Identification
3. Data Usage and Reporting
4. Service Provider Accreditation
5. Information Security
6. Peppol Authority Specific Requirements
7. Extended Use of Peppol
8. Compliance

1.2 Definitions and Conventions

Whereas:

1. OpenPeppol AISBL has established the Peppol Network as the main means of achieving the Association's purposes. It is defined as: "A logical network enabling secure and reliable exchange of Peppol Dataset Types between End Users via Peppol Service Providers. It is a component in the Peppol Architectural Framework and is based on a set of Peppol specifications which are governed according to the Peppol Governance Framework".
2. OpenPeppol AISBL has developed the Peppol Interoperability Framework in order to regulate the use of the Peppol Network. The Peppol Interoperability Framework is defined as: "The set of agreements, policies and procedures and technical specifications which, taken together, are needed to ensure interoperability. It consists of the Peppol Architectural Framework and the Peppol Governance Framework and is governed by the Peppol Coordinating Authority." The composition of the Peppol Interoperability Framework is included in section 1.3 below.

3. The Peppol Agreements (Peppol Authority Agreement and Peppol Service Provider Agreement) serve as the means of providing legal certainty on the use of the Peppol Network to the contracting parties (The Peppol Coordinating Authority, the Peppol Authorities, and the Peppol Service Providers).
4. The Policies included in the OpenPeppol AISBL Internal Regulations on the Use of the Peppol Network contain rules and provisions that expand in more detail the legal obligations assumed through the Peppol Agreements.
5. Operational details regarding the implementation of the Peppol Agreements and the Policies contained in the OpenPeppol AISBL Internal Regulations on the Use of the Peppol Network are laid out in Operational Procedures.
6. In case of any doubt or the appearance of conflict, the Peppol Agreements shall take precedence over the Policies contained in the OpenPeppol Internal Regulations on the Use of the Peppol Network and these will take precedence over the OpenPeppol Operational Procedures.

1.3 The Peppol Interoperability Framework

1. The Peppol Interoperability Framework includes the following sections:
    a. The Peppol Governance Framework
    b. The Peppol Architectural Framework
2. The Peppol Governance Framework includes the following components:
    a. The Peppol Agreements
        i. Peppol Authority Agreement
        ii. Peppol Service Provider Agreement
    b. Policies for the Use of the Peppol Network (part of the OpenPeppol AISBL Internal Regulations)
    c. Operational Procedures for the Use of the Peppol Network
    d. Peppol Service Domain requirements
        i. List of Applicable Specifications
        ii. Service Level Requirements
    e. Peppol Authority Specific Requirements
3. The Peppol Architectural Framework includes the following components:
    a. Peppol Message Specifications
        i. Peppol Business Interoperability Specifications (Peppol BIS, used globally)

ii. Peppol Authority-governed Specifications

b. Peppol Network Specifications

i. Packaging and Security Specifications

ii. Messaging Specifications

iii. Capability Lookup and Addressing Specifications

Back to Table of Contents

2 Change Management Policy

2.1 Introduction

This Policy defines the overarching provisions, or rules, that must be respected by all actors who take part in activities related to the lifecycle stages concerning artefacts that are subject to this policy.

2.1.1 Artefacts under this Policy

The following artefact categories are in scope of this Policy:

1. Technical Artefacts: Technical specifications and other technology and architecture-related artefacts published as part of the Peppol Architectural Framework, such as the Peppol BIS (Business Interoperability Specifications), and associated validation artefacts and code lists defining compliance criteria for Peppol Services offered to the market.
2. Internal Regulations and Operational Procedures which are necessary to regulate use of the Peppol Network, hereinafter collectively referred to as “governance policies and/or procedures” or simply “policies and/or procedures.
3. Agreements between the main actors responsible for the use of the Peppol Network: the Peppol Authority Agreement and the Service Provider Agreement.

2.2 Provisions for Technical Artefacts

2.2.1 Overarching governance provisions

1. All technical artefacts in the Peppol Architectural Framework must be subject to a controlled lifecycle management process respecting the provisions outlined in this Policy. The artefact lifecycle includes the following stages, all of which are subject

to provisions in this Policy and which may be collectively referred to by using the term “change and release management” or simply “change management”.

a. Introduction of a new artefact
b. Changing an existing artefact
c. Releasing a new version of an existing artefact
d. Migration from an old to a new artefact version
e. Removal of an artefact

2. Each technical artefact shall be allocated to the responsibility of a Domain Community. The Change Management Board (CMB) of that Domain Community shall be considered as being responsible for all stages of lifecycle management related to this artefact.
3. The typical lifecycle management of technical artefacts is set out in the OpenPeppol Operational Procedures. Lifecycle management of technical artefacts should not deviate from these, except for good and specific reasons related to the nature of an artefact or a particular occasion.
4. The common lifecycle management procedure must allow for adequate involvement and participation of OpenPeppol Members affected by the implementation and use of the artefact.

2.2.2 Changing an Existing Technical Artefact

2.2.2.1 Raising an RFC

1. Any OpenPeppol Member may at any point in time raise a Request For Change (RFC) related to any technical artefact in the Peppol Architectural Framework.
2. Upon successful submission of an RFC to an RFC Register, the RFC must be allocated to the relevant CMB, which will be responsible for the next steps in the process.
3. A mechanism enabling members of the Domain and Stakeholder Communities affected by the RFC to monitor its status shall be made available by OpenPeppol.
4. For each step in the process OpenPeppol shall ensure that the status of the RFC is updated in the RFC Register and that the submitter of the RFC is informed accordingly.
5. An RFC may also be raised by the relevant CMB or by the Peppol Coordinating Authority.

2.2.2.2 Processing an RFC

1. Each RFC must be processed in a timely manner according to the severity of the issue raised (e.g. clarification needed, error correction, blocking intended use, etc.).
2. For each RFC the responsible CMB must provide:
   a. a proposed resolution to the issue raised (or a justified rejection), and
   b. an impact assessment on the implementation of the proposed resolution (or its rejection).
3. For each RFC the responsible CMB must consult with the Domain Community to which it belongs, as well as with other relevant Stakeholder and/or Domain Communities as may be relevant. The CMB will determine whether such consultations may be initiated for individual RFCs, or collectively for all RFCs in the review of a new release.
4. In case an RFC, or its proposed resolution, has cross-Community relevance or strategic implications, the topic will be referred to the Coordinating Committee for consultation. The Coordinating Committee shall seek consensus among Community Leaders, whereupon the agreed resolution will be referred back to the responsible CMB. In case of non-consensus or when the matter is deemed strategic, the Coordinating Committee will escalate further for a decision to be made by the Managing Committee.
5. An RFC or its proposed resolution can be suggested to have cross-Community relevance or strategic implications either by the responsible CMB, or by another Community Leader, or by the Operating Office, either directly or after requests from OpenPeppol Members during a review or consultation. In all such cases, the matter shall be referred to the Coordinating Committee for consideration according to the provisions of point 4 above.

2.2.2.3 Deciding on an RFC

1. The decision on acceptance/rejection of an RFC is made by the responsible CMB.
2. In case the RFC is rejected, the responsible CMB must provide a justification outlining the reasons for its rejection.
3. Any disagreement on the RFC acceptance, resolution, or rejection may be escalated to the OpenPeppol Coordinating Committee. The Coordinating Committee shall seek consensus among Community Leaders, whereupon the agreed resolution will be referred back to the responsible CMB. In case of non-consensus or when the matter is deemed strategic, the Coordinating Committee

will escalate further for a decision to be made by the Managing Committee. Such escalations must be adequately substantiated and will be handled according to the operational procedures on this topic.

2.2.3 Introduction of new artefacts

The following provisions concern the introduction of new technical artefacts in an existing, global Peppol Service Domain. For cases that fall under the provisions of Extended Use (chapter 8), the provisions and processes included in that chapter shall be followed.

1. A proposal to introduce a new artefact must be submitted through an RFC, except when it is initiated by the Managing Committee by issuing a mandate for a work group or task force to be formed with that purpose or a decision to use OpenPeppol's own resources.
2. A new artefact may be developed through in-kind contributions of members or own resources provided by OpenPeppol or a combination of the two. Under any circumstances, the availability of sufficient resources to develop a new artefact must be secured before a decision to proceed is taken.
3. A proposal to introduce a new technical artefact in Peppol must be based on a positive assessment of the following elements:
    a. Outline of purpose and main benefits,
    b. impact on operations for OpenPeppol to support and maintain the artefact, and
    c. impact on operations for members and other parties that implement, use, or are otherwise affected by the artefact.
4. If a new artefact is based on contributions that have been developed outside OpenPeppol, such external contributions must be licensed to OpenPeppol by the IPR holders under an open license, in line with provisions in article 9 of the OpenPeppol Statutes. Furthermore, the content and presentation of such external contributions must be aligned with Peppol design principles and architecture through a process that includes consultation with the relevant Domain Communities.
5. Introduction of new Peppol Dataset Types are subject to further conditions, as outlined in the Peppol Authority Agreement clause 12.4.

2.2.4 Releasing a New Version of an Existing Technical Artefact

1. A new release of an artefact in the Peppol Interoperability Framework must be constructed by applying approved RFCs to the current version, and be classified

according to the provisions of Annex 1 on Semantic Versioning of technical Artefacts, as either:

a. A major release, which may contain significant and/or non-backward compatible changes (e.g. removing or adding mandatory functionality),

b. A minor release, which will usually contain backward compatible changes (e.g. adding optional functionality), or

c. A revision, which must be limited to error correction, bug fixing and clarifications.

2. Decision to publish a new release of a technical artefact is taken by the relevant CMB, after conclusion of any escalations to the Coordinating Committee and/or the Managing Committee, if appropriate. Such escalations will follow the process foreseen for deciding on an RFC.

3. Publication of a new release of a technical artefact is made by the Operating Office, following standard notification procedures and publication tools, as described in the OpenPeppol Operational Procedures.

2.2.5 Migration to a new release of a Technical Artefact or Infrastructure

1. Every new release of a technical artefact must be supported by a migration plan, which in itself must respect the migration requirements of the changes contained in the release and define how older versions of the artefact are to be phased out.

2. A migration plan must contain the following steps:

a. Phase-in: The new version is introduced in the Peppol Network as optional and relevant parties start to implement it in their systems.

b. Switch-over: The new version becomes mandatory, and the old version becomes optional in the Peppol Network.

c. Phase-out: The old version is no longer supported and will be removed from the Peppol Network.

3. The migration plan must contain the above steps as a minimum, clearly identifying what is expected of implementers at the beginning and end of each step and what are the time periods between milestones that delineate the beginning and end of each phase. Migration plans may contain more steps if relevant and appropriate.

4. Migrations to new versions or instances of essential infrastructure, such as the Service Metadata Locator (SML) may not follow the steps stipulated in this section and may be done in a synchronised manner, provided that there are compelling reasons to do so.

2.2.6 Removing a Technical Artefact

1. A technical artefact may be removed from the Peppol Architectural Framework and its use may be discontinued in the Peppol Network.
2. Removal is decided on the basis of an RFC submitted by a member and approved by the relevant CMB, after consultation with the Coordinating Committee.
3. An RFC to remove a technical artefact from the Peppol Architectural Framework shall be processed and decided upon according to the provisions set out in this Policy and will be subject to the same rules for escalation.
4. If the artefact is considered irrelevant and no longer valid for use the responsible CMB must issue a plan for how and when the component will be removed from the Peppol Architectural Framework which shall include provisions allowing existing users, if any, to terminate their use of the component.
5. An artefact defined as mandatory for use in a Peppol Service Domain may not be removed for use.
6. Upon completion of the plan for removal, the artefact shall no longer appear within the Peppol Architectural Framework and its further use shall be prevented by suitable means.

2.2.7 Minimum time for consultation and implementation

The table below defines the minimum time that must be allocated for:

1. consultation with relevant communities on proposals for changes to an existing technical artefact as outlined in section 2.3.4 above, and
2. implicated actors to implement (migrate to) a new release of an existing technical artefact as outlined in section 2.2.5 above.

Type of technical artefact	Minimum time that must be allowed for consultation	Minimum time that must be allowed for implementation (migration)
New mandatory technical artefact	4 weeks	6 months
New optional technical artefact	4 weeks	On publication
Network specification, major release	4 weeks	6 months
Network specification, minor release	2 weeks	6 months

Network specification, revision release	2 weeks	On publication
Adding or changing codes in a code list used in a network specification	Na	3 months
Deprecating or removing code values in a code list used in a network specification	Na	On publication
Peppol BIS and associated validation artefacts, major release	2 months	6 months
Peppol BIS and associated validation artefacts, minor release	2 weeks	2 weeks
Peppol BIS and associated validation artefacts, revision release	2 weeks	2 weeks
Changes to code lists used in a Peppol BIS	Na	On publication
Removing an existing technical artefact	4 weeks	On publication

2.3 Provisions for Internal Regulations and Operating Procedures

2.3.1 Overarching governance provisions

1. All policies and procedures in the Peppol Governance Framework must be subject to a controlled lifecycle management process respecting the provisions outlined in this Policy. The lifecycle includes the following stages, all of which are subject to provisions in this Policy and which may be collectively referred to by using the term “change and release management” or simply “change management”:
    a. Introduction of a new policy or procedure
    b. Changing an existing policy or procedure
    c. Releasing a new version of an existing policy or procedure
    d. Migration from an old to a new policy or procedure version
    e. Removal of a policy or procedure
2. All governance policies and procedures shall be allocated to the responsibility of the Agreements, Policies and Procedures Change Management Board (APP CMB). The APP CMB shall be considered as being responsible for all stages of lifecycle management related to governance policies and procedures.

3. The lifecycle management of governance policies and procedures must allow for adequate involvement and participation of OpenPeppol Members affected by putting into effect the governance policies and procedures in question.

2.3.2 Changing an Existing Policy or Procedure

2.3.2.1 Raising an RFC

1. Any OpenPeppol Member may at any point in time raise a Request For Change (RFC) related to any policy or procedure in the Peppol Governance Framework.
2. Upon successful submission of an RFC to an RFC Register, the RFC must be allocated to the APP CMB, which will be responsible for the next steps in the process.
3. A mechanism enabling members of the Domain and Stakeholder Communities affected by the RFC to monitor its status shall be made available by OpenPeppol.
4. For each step in the process OpenPeppol shall ensure that the status of the RFC is updated in the RFC Register and that the submitter of the RFC is informed accordingly.
5. An RFC may also be raised by the APP CMB or the Peppol Coordinating Authority.

2.3.2.2 Processing an RFC

1. Each RFC must be processed in a timely manner according to the severity of the issue.
2. For each RFC the APP CMB must provide:
   a. a proposed resolution to the issue raised (or a justified rejection), and
   b. an impact assessment on the implementation of the proposed resolution (or its rejection).
3. For each RFC the APP CMB must consult with the relevant Communities through the Coordinating Committee and, where either the APP CMB or the CC deems necessary, a wider member consultation may be initiated within one or more Communities as may be relevant. The APP CMB will determine whether such consultations may be initiated for individual RFCs, or collectively for all RFCs in the review of a new release.
4. For reasons of stability and practicality, RFCs may be processed but the implementation of their resolution may be left for a later point in time, when critical mass may develop that will warrant a change in policies or procedures.

OpenPeppol shall avoid too frequent changes in governance policies and procedures unless there are urgent needs to remedy a situation or to mitigate acute or previously unforeseen risk.

5. Batch implementation of RFC resolutions may not result in undue delay in the implementation of agreed changes to policies and procedures. Implementation of agreed changes should not be delayed more than 6 months and must not be delayed more than a year.

2.3.2.3 Deciding on an RFC

1. The initial decision on acceptance/rejection of an RFC is made by the APP CMB.
2. In case the RFC is rejected, the APP CMB must provide a justification outlining the reasons for its rejection.
3. Any disagreement on the RFC acceptance, resolution or rejection may be escalated to the OpenPeppol Coordinating Committee. The Coordinating committee shall seek consensus among Community Leaders, whereupon the agreed resolution will be referred back to the responsible CMB. In case of non-consensus or when the matter is deemed strategic, the Coordinating Committee will escalate further for a decision to be made by the Managing Committee. Such escalations must be adequately substantiated and will be handled according to the operational procedures on this topic.

2.3.3 Introduction of new policies or procedures

1. The provisions in this section concern the introduction of new policies or procedures related to the use of the Peppol Network that shall be added to the Internal Regulations on the Use of the Peppol Network or to the Operational Procedures.
2. A proposal to introduce a new policy or procedure must be submitted through an RFC, except when it is initiated by the Managing Committee by issuing a mandate for a work group or task force to be formed with that purpose. The provisions about raising, processing, and deciding on an RFC shall apply, as stated in section 2.3.2.
3. A proposal to introduce a new policy or procedure in the Peppol Governance Framework must be based on a positive assessment of the following elements:
   a. Outline of purpose and main benefits,
   b. Impact on operations for OpenPeppol to support and maintain the implementation of the policy or procedure,

c. Impact on operations for members and other parties that are affected by the introduction and implementation of the policy or procedure.

4. The OpenPeppol Managing Committee shall decide on the introduction of a new policy or procedure upon recommendation of the APP CMB, after careful consideration of each proposal.
5. After Managing Committee acceptance, the new policy or procedure shall be developed and approved by the APP CMB after being reviewed by members.
6. The final decision to put into effect the new policy or procedure shall be taken by the OpenPeppol Managing Committee.
7. A new policy or procedure may be developed through in-kind contributions of members or own resources provided by OpenPeppol or a combination of the two. Under any circumstances, the availability of sufficient resources to develop a new policy or procedure, together with any tools that may be necessary to implement such policies or procedures, must be secured before a decision to proceed is taken.

2.3.4 Releasing a New Version of an Existing Policy or Procedure

1. A new release of a policy or procedure in the Peppol Governance Framework must be constructed by applying approved RFCs to the current version, and be classified as follows:
   a. A major release, which contains new or removes existing rules or obligations, or substantially alters existing provisions.
   b. A minor release, which only elaborates on a rule, without altering the substance and principles of the policy or procedure.
   c. An amendment, which must be limited to error correction and clarifications of ambiguous language.
2. A major new release must be reviewed by members and the results of such review must be considered by the APP CMB in the production of the final version. All comments shall be processed, and responses will be provided.
3. A decision to publish a new release of a policy or procedure that is part of the Peppol Governance Framework, resulting in a new version of Internal Regulations or Operational Procedures, is taken by the Managing Committee after recommendation of the APP CMB, after conclusion of any escalations to the Coordinating Committee and/or the Managing Committee, if appropriate. Such escalations will follow the process foreseen for deciding on an RFC.

4. Publication of a new release of Internal Regulations or Operational Procedures is made by the Operating Office, following standard notification procedures and publication tools, as described in the OpenPeppol Operational Procedures.

2.3.5 Migration to a new release of a policy or procedure

1. Every new release of a policy or procedure that is part of the Peppol Governance Framework must be supported by a migration plan, which in itself must respect the phase-in requirements of the changes contained in the release.
2. A migration plan must contain the following steps:
   a. Phase-in: The new version is introduced in the Peppol Governance Framework as an upcoming rule set and relevant parties start preparing for its implementation, adjusting their internal processes and systems if necessary.
   b. Switch-over: The new policy or procedure comes into effect, and the old version becomes obsolete.
3. The migration plan must contain the above steps as a minimum, clearly identifying what is expected of implementing parties at the beginning and end of each step and what are the time periods between milestones that delineate the beginning and end of each step. Migration plans may contain more steps if relevant and appropriate.

2.3.6 Removing a policy or procedure

1. A governance policy or procedure may be removed from the Peppol Governance Framework and its effect may be discontinued in the Peppol Network.
2. Removal is decided on the basis of an RFC submitted by a member or by the Managing Committee and approved by the APP CMB, after consultation with the Coordinating Committee and the relevant Communities.
3. An RFC to remove a policy or procedure from the Peppol Governance Framework shall be processed and decided upon according to the provisions set out in this Policy and will be subject to the same rules for escalation.
4. Sufficient lead time for the removal of a Policy must be foreseen.
5. Upon completion of the plan for removal, the policy or procedure shall no longer appear within the Peppol Governance Framework and its further use shall be prevented by suitable means, if needed.

2.3.7 Timeline for consultation and implementation

The table below defines the time that must be allocated for:

1. consultation with members on proposals for changes to an existing policy or procedure as outlined in section 2.3.4 above, and
2. Implementation of resolutions to RFCs into (a new release of an existing policy or procedure as outlined in section 2.3.2 above.

	Minimum time that must be allowed for consultation	Desired maximum time for implementation	Mandatory maximum time for implementation
New policy or procedures	4 weeks	6 months	1 year
Major release of an existing policy or procedure	4 weeks	6 months	1 year
Minor release of an existing policy or procedure	4 weeks	6 months	1 year
Revision release of an existing policy or procedure	4 weeks	On availability	
New policy or procedures	4 weeks	6 months	1 year

2.4 Provisions for Peppol Agreements

2.4.1 Overarching governance provisions

1. The Peppol Authority Agreement and the Peppol Service Provider Agreement, together referred to as Peppol Agreements, shall be subject to a controlled lifecycle management process respecting the provisions outlined in this Policy. The lifecycle includes the following stages, all of which are subject to provisions in this Policy, and which may be collectively referred to by using the term “change and release management” or simply “change management”:
   a. Introduction of a new Agreement
   b. Changing an existing Agreement
   c. Releasing a new version of an Agreement
   d. Migration from an old to a new Agreement version
   e. Removal of an Agreement
2. The Peppol Agreements shall be allocated to the responsibility of the Agreements, Policies and Procedures Change Management Board (APP CMB).

The APP CMB shall be considered as being responsible for all stages of lifecycle management related to Peppol Agreements.

3. The lifecycle management of Peppol Agreements must allow for adequate involvement and participation of Peppol Authorities and Service Providers.
4. Provisions contained in this Policy about lifecycle management of the Peppol Agreement must not contradict relevant provisions contained in the Peppol Agreements themselves. In the event of conflict or doubt, provisions contained in the Peppol Agreements shall prevail.

2.4.2 Changing an Existing Agreement

2.4.2.1 Raising an RFC

1. Any Peppol Authority or Service Provider, as well as the Peppol Coordinating Authority, may at any point in time raise a Request For Change (RFC) related to any Peppol Agreement.
2. Upon successful submission of an RFC to an RFC Register, the RFC must be forwarded to the APP CMB, which will be responsible for the next steps in the process.
3. A mechanism enabling Peppol Authorities and Service Providers to monitor its status shall be made available by OpenPeppol.
4. For each step in the process OpenPeppol shall ensure that the status of the RFC is updated in the RFC Register and that the submitter of the RFC is informed accordingly.

2.4.2.2 Processing an RFC

1. Each RFC must be processed in a timely manner according to the severity of the issue raised.
2. For each RFC the APP CMB must provide:
   a. a proposed resolution to the issue raised (or a justified rejection), and
   b. an assessment of impact incurred by the implementation of the proposed resolution (or its rejection).
3. For each RFC the APP CMB must consult with the Peppol Authority and Service Provider Communities. When either the APP CMB or the Communities concerned deem necessary, a wider member consultation may be initiated including a wider circle of stakeholders if needed. The APP CMB will determine whether such consultations may be initiated for individual RFCs, or collectively for

all RFCs in the review of a new release. The MC is responsible for ensuring the consultation process is fair and open, and the duration of the consultation period is proportional to the importance of the RFC.

4. For reasons of stability and practicality, RFCs may be processed but their resolution may be left for a later point in time, when critical mass may develop that will warrant a change of Agreements. OpenPeppol shall avoid frequent changes in Peppol Agreements unless there are urgent needs to remedy a situation or to mitigate acute or previously unforeseen risk.

2.4.2.3 Deciding on an RFC

1. The initial decision on acceptance/rejection of an RFC is made by the APP CMB.
2. In case the RFC is rejected, the APP CMB must provide a justification outlining the reasons for its rejection.
3. Any disagreement on the RFC acceptance, resolution or rejection may be escalated to the Managing Committee for a final decision. Such escalations must be adequately substantiated.

2.4.3 Introduction of new Agreement

1. The introduction of a new type of Peppol Agreement is not foreseen under this Policy.
2. Any consideration for the introduction of a new Peppol Agreement would need to be instigated by changes in stakeholder requirements and would necessitate major changes to the Peppol Interoperability Framework and the OpenPeppol Internal Regulations, including (but not limited to) this Policy.

2.4.4 Releasing a New Version of an Existing Agreement

1. A new release of a Peppol Agreement shall be constructed by applying approved RFC resolutions to the current version. Editorial support for consolidation shall be provided by the Operating Office.
2. A new release of a Peppol Agreement may be classified as follows:
   a. A major release, which contains new or removes existing rules or obligations, or substantially alters existing provisions.
   b. An editorial revision, which must be limited to changes that do not require the contracting parties to sign a new version of Agreements, such as changes to Annexes.

3. Every new release must be reviewed by members and the results of such review must be considered by the APP CMB in the production of the final version. All comments shall be processed, and responses will be provided. A member review cannot be shorter than 8 weeks.
4. Decision to publish a new version of Peppol Agreements is taken by the Peppol Authorities, following the voting procedures specified in the Peppol Agreements. The Peppol Authorities shall vote on a final version that is submitted to them by the OpenPeppol Managing Committee, following a proposal by the APP CMB, which includes all the agreed changes.
5. Publication of a new release of Peppol Agreements is made by the Operating Office, following standard notification procedures and publication tools, as described in the OpenPeppol Operational Procedures.

2.4.5 Migration to new Peppol Agreements

1. Every new release of the Peppol Agreements must be accompanied by a migration plan, which shall be constructed and approved following the same procedures as the new Agreement release as described in 2.4.4.
2. The contracting parties will implement approved new versions of the agreements according to the migration plan. The migration plan will stipulate whether the Agreements will need to be re-signed.
3. In case re-signing of a new Agreement version is not required;
    a. The new versions will automatically replace superseded versions. Clause 13.3 of the Agreements provides that a new signing process is not required for new versions of the Agreements to take effect.
    b. Notification of the revised versions, and acknowledgement of receipt of notification by the contracting parties is deemed to be acceptance of the revised versions by the contracting parties.
    c. If any of the contracting parties consider the revised versions of the agreements to be unacceptable for whatever reason, the only remedy available will be to terminate the Agreement in accordance with the provisions set out in clause 22 of the Service Provider Agreement and clause 24 of the Peppol Authority Agreement.
    d. A certified master copy of the Agreements text will be hosted on the OpenPeppol Website. This will ensure clarity and consistency is maintained and the contracting parties can easily access the “in force” versions of the Agreement documents. Previous versions and notifications of changes will be archived as well.

4. In case re-signing of a new Agreement version is required; the migration plan must contain the following steps:
    a. PA sign period: The time needed for OpenPeppol to sign new Agreements with Peppol Authorities.
    b. New SP Agreement Phase-in: The new SP Agreement version starts to be signed with Service Providers in each PA jurisdiction.
    c. Old SP Agreement Termination: When Peppol Authorities are confident that signing of the new SP Agreement proceeds smoothly, a termination notice shall be given for the old SP Agreements remaining in effect.
    d. Old SP Agreement Phase-out: Remaining Service Provides must sign the new SP Agreement, otherwise they are out of the Peppol Network at the end of the termination notice.
    e. The migration plan must contain the above steps as a minimum, clearly identifying what is expected of implementing parties at the beginning and end of each step and what are the time periods between milestones that delineate the beginning and end of each step. Migration plans may contain more steps if relevant and appropriate.

2.4.6 Removing an Agreement

1. The removal of a Peppol Agreement is not foreseen under this Policy.
2. Any consideration for the removal of a Peppol Agreement would necessitate major changes to the Peppol Interoperability Framework and the OpenPeppol Internal Regulations, including (but not limited to) this Policy.

2.4.7 Minimum time for consultation and implementation

The table below defines the minimum time that must be allocated for

1. consultation with members on proposals for changes to an existing Agreement as outlined in section 2.4.4 above, and
2. implicated actors to implement (migrate to) a new release of an existing Agreement as outlined in section 2.4.5 above.

	Minimum time that must be allowed for consultation	Minimum time that must be allowed for implementation (migration)
New Agreement	N/A	N/A

Major release	8 weeks	6 months
Editorial release	8 weeks	20 business days
Removal of an existing Agreement	N/A	N/A

Back to Table of Contents

3 Entity Identification Policy

3.1 Policy Overview

This policy contains the following parts:

1. Overview
2. Requirements from the Peppol Agreements
3. End User identification and Reporting Requirements
4. Service Provider Identification Requirements

3.2 Requirements from the Peppol Agreements

The legal obligation to ensure proper Entity Identification follows from

- the Peppol Authority Agreement clause 9.2.4 with respect to the PAs responsibility to verify the entity of the SP, and
- the Peppol Service Provider Agreement clause 9.2 with respect to the SPs responsibility to verify the entity of the End User.

3.3 End User Identification

3.3.1 Information to be Collected

Peppol Service Providers shall ensure that the following information is known for all End Users (senders and receivers) to which they provide Peppol services:

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.

Service Providers must verify the above information concerning End Users to which they provide Peppol Services, except in cases when this is not feasible with reasonable efforts. Such cases may include, but are not limited to, the lack of automated means to retrieve or verify End User information through lookup or API connection to authoritative sources of information in specific jurisdictions.

If and when it comes to the attention of a Service Provider that one of their End Users is trading under names different from its legal name, these must be documented and reported as well. In particular, when the Service Provider becomes aware that different trade names, business units, etc. are associated with different endpoints, this must be adequately documented.

The Service Providers remain responsible for the correctness of End User information at all times. End User information shall be collected and verified at the time of enrolment in the Peppol Network and must be periodically checked at least on an annual basis, provided that mechanisms to that effect are available, e.g. through lookup or API connection to authoritative sources of information in specific jurisdictions.

3.3.2 Requirements for the Peppol Authorities

Peppol Authorities shall provide, to the best of their ability, guidance to Service Providers on how to reliably obtain or verify End User information such as the legal identifier, type, and alternate trade names for businesses or persons resident in their jurisdiction, as well as what constitutes proof of ownership, through authoritative services such as national business registers that offer automated (e.g. through an API) and free of charge services. Where such services exist, Service Providers must use them.

In the absence of such a description (e.g. because there is no Peppol Authority for the End User's jurisdiction, or because the process for accessing the information is costly or otherwise onerous), the Service Provider must exercise all reasonable effort to obtain and validate information required for End Users to which they provide services, as well as proof of ownership of that information.

3.4 Peppol Service Provider Identification

As part of the process to establish the Peppol Service Provider Agreement the Peppol Authority must secure the following minimum data about the Peppol Service Provider:

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.

Peppol Authorities must verify the above information concerning Service Providers with which they are contracted, except in cases when this is not feasible with reasonable efforts. Such cases may include, but are not limited to, the lack of automated means to retrieve or verify Service Provider information through lookup or API connection to authoritative sources of information in specific jurisdictions.

Service Provider information shall be collected and verified at the time of signing a Service Provider Agreement and must be periodically checked, at least before each renewal of production certificate, provided that mechanisms to that effect are available, e.g. through lookup or API connection to authoritative sources of information in specific jurisdictions.

A Peppol Authority shall not enter into any Peppol Service Provider Agreement with an entity which, in the good faith judgment of the Peppol Authority, cannot bear the legal responsibilities of a Peppol Service Provider.

The Peppol Authority may make signing with a prospective Service Provider contingent on the Peppol Authority completing a satisfactory audit of the financial and technical capabilities of the prospective Service Provider. The Peppol Authority shall bear the cost of performing the audit, which must be conducted in the minimally invasive manner feasible. However, the prospective Service Provider shall make reasonable accommodations for facilitating the audit and shall carry any costs they themselves incur in making such accommodations.

Back to Table of Contents

4 Data Usage and Reporting Policy

4.1 Policy Overview

This policy contains the following parts:

1. Overview
2. Requirements from the Peppol Agreements
3. Service Provider Reporting about End Users
4. Service Provider Reporting on Transaction Statistics
5. Data Collection Purposes
6. Data Usage

4.2 Requirements from the Peppol Agreements

The legal obligations related to data usage and reporting follows from

- the Peppol Authority Agreement clause 8.1.8 with respect to the Peppol Coordinating Authority responsibility for collecting data and making aggregated statistics available, and

- the Peppol Service Provider Agreement clause 9.5.8 with respect to the responsibility of the SP to make such data available related to the use of their Peppol Services.

4.3 Service Provider Reporting about End Users

Peppol Service Providers must ensure that information about End Users, as specified in the Entity Identification Policy, shall be acquired and shall be regularly reported to the Peppol Coordinating Authority, which shall make it available, in whole or in part to the Peppol Authorities which have territorial jurisdiction over the country or territory where the End Users are based.

The information thus reported shall be at a sufficient level of detail that it is possible for the Peppol Coordinating Authority to reconstruct the topology of the network from Service Provider to End User – i.e. which End User is served by which Service Provider and for which Peppol services, either directly or through an Intermediary party.

Reporting shall be made on a monthly basis. The reporting mechanism to be used by Service Providers and the Peppol Coordinating Authority is described in the OpenPeppol Operational Procedures

4.4 Service Provider Reporting on Transaction Statistics

To monitor the evolving use of the Peppol Network, OpenPeppol needs to collect information about the Peppol Dataset Types actually being exchanged over the Peppol Network, considering each such exchange as a transaction between End Users. This information must be reported by Service Providers according to the provisions of this Policy.

Only statistical information based on metadata from the SBDH will be collected and reported to OpenPeppol under this Policy. No information from the actual business content of individual datasets will be reported.

The Peppol Service Providers are responsible for ensuring that the relevant data can be collected in an accurate and reliable manner, using whatever methods the Peppol Service Provider deems most efficient in its own infrastructure and operational environment.

The data reported must be entirely anonymous and thus not linkable to any natural persons, including any (contact persons of) End Users.

Information related to actual datasets exchanged over the Peppol Network for both sent and received datasets must be collected and reported based on the following parameters:

1. Date of the exchange

2. Direction of the exchange (incoming or outgoing)
3. Sending Peppol Service Provider
4. Receiving Peppol Service Provider
5. Peppol Dataset Type (Document Type ID)
6. Transport protocol used
7. Country of sender
8. Country of receiver

4.5 Data Collection Purposes

4.5.1 Operational purposes

Under this policy, OpenPeppol may collect and use the information contained herein, for the following operational purposes:

1. Capacity planning, assessing stress capabilities and load management of the Peppol Network and all its components, including identification of trends in volume changes, peak usage areas and peak usage times.
2. To ensure the security and proper operation of the Peppol Network and all its components, notably through risk analysis, threat detection, and other measures to prevent fraud.
3. To ensure compliance to the requirements expressed through the Peppol Interoperability Framework.

4.5.2 Compliance purposes and usage

Data collected may also be used for the following monitoring and compliance control purposes:

1. To enable accurate identification of all End Users of Peppol Services.
2. To monitor the evolution of key metrics for the Network such as, but not limited to:
    a. End User count over time, by Dataset type and by country.
    b. Number of Datasets exchanged per Peppol Dataset Type over time per country and between countries.
3. To support and enable technical troubleshooting.
4. To trace non-compliance cases to the entity ultimately responsible, in order to facilitate speedy and fair resolution.

4.5.3 Strategic purposes

Additionally, the data may be used for the following strategic purposes:

1. To improve internal organization and processes in order to:
   a. Improve service quality to End Users.
   b. Improve the experience of actors involved in the use, operations, and governance of the Peppol Network.
2. Identify potential future use cases and Service Domains for the Peppol Network.
3. To conduct market segmentation analysis of current or potential users.
4. To carry out similar analysis for the purpose of improving the Peppol service offering and promoting increased usage and membership.

4.6 Data Usage

4.6.1 Data usage by OpenPeppol

OpenPeppol may choose to publish or disclose aggregate statistical information based on the data collected, provided that these do not permit the linking of any published or disclosed information to the identity or business practices of individual Peppol Service Providers or End Users without their explicit consent.

In this data collection and processing, each Peppol Authority, Service Provider and End User in the Peppol Network must be treated in the same manner as its comparable peers.

OpenPeppol will regularly analyse information from its Service Metadata Locator (SML) in order to verify compliance to the rules of the Peppol Network including, but not limited to, the following:

1. That End Users have registered capabilities for authorised Peppol Datasets only.
2. That End Users have been registered with authorised identifier schemes only.
3. That Peppol Service Providers are using the agreed transport protocols; and
4. That obsolete Peppol BIS releases are actually removed from the Peppol Network.

OpenPeppol may establish a mechanism for the automatic retrieval of information from Service Metadata Publishers and the processing of such information for the purposes of data collection stated in this Policy.

OpenPeppol may not combine or link data from different reporting data streams except for the purposes included in this Policy.

For the avoidance of doubt, nothing in this Policy shall be construed as mandating any Entity to take any action that would place it in breach of any applicable law, including, but not limited to, applicable data protection regulation. Nor shall this Policy be construed as restricting any otherwise lawful data analysis by the Service Provider.

4.6.2 Data usage by Peppol Authorities

OpenPeppol shall provide on a regular basis to Peppol Authorities all relevant information collected or derived according to the provisions of this Policy, related to the End Users and Service Providers based within their jurisdiction.

Peppol Authorities may request from OpenPeppol particular data aggregation views to enhance their understanding of the information available, provided that these do not permit the linking of any published or disclosed information to the identity or business practices of individual Peppol Service Providers or End Users without their explicit consent. Peppol Authorities may publish or disclose such information.

4.6.3 Data Usage by Service Providers

The Service Provider shall submit current and correct metadata to the SMP(s) in which their End Users' endpoints are listed. This metadata is to cover both the relevant technical capabilities of the Service Provider and the services provided to End Users.

A Service Provider that displays some or all End Users in the Peppol Directory shall be responsible for maintaining the information displayed there. A provider of Peppol Addressing and Lookup Services who relays data about the End Users listed in the SMP to the Peppol Directory shall be responsible for ensuring that the information is accurately relayed. The Peppol Addressing and Lookup Services shall be likewise responsible for following up with the Service Provider who has the primary relationship with the End User, should the provider of Peppol Addressing and Lookup Services at any point become aware of discrepancies or possible errors in the data provided to the Peppol Directory.

4.6.4 Rights of Peppol Service Providers in relation to the data

All Peppol Service Providers shall be permitted to request OpenPeppol to provide a copy of any aggregate statistical information that OpenPeppol has created based on and derived from the collected data, even if such information has not been published or otherwise publicly disclosed by OpenPeppol.

This right only applies to any information which OpenPeppol has already created; it cannot be used to compel OpenPeppol to create new information.

Disclosure under this provision shall be limited only to information that cannot be used to identify End Users or Service Providers.

Back to Table of Contents

5 Service Provider Accreditation Policy

5.1 Policy Purpose and Overview

This Policy contains provisions that describe the requirements for allowing Peppol Service Providers to obtain and maintain access to the Peppol Network. These provisions must be followed by all actors involved, i.e. Service Providers, Peppol Authorities, and the Peppol Coordinating Authority.

The purpose of this Policy is to increase confidence that the services offered across the Peppol Network respect the relevant technical specifications and thus provide the level of interoperability expected.

This Policy consists of the following parts:

1. Purpose and Overview
2. Requirements from the Peppol Agreements
3. Entering the Peppol Network
4. Remaining in the Peppol Network
5. Leaving the Peppol Network

This Policy relates only to accreditation procedures that are performed across the entire Peppol Network in all jurisdictions and does not include any local accreditation procedures that are administered by Peppol Authorities as part of their PA specific requirements.

5.2 Requirements from the Peppol Agreements

The legal obligation to undertake such testing and certification is expressed in the Peppol Service Provider Agreement clause 9.5.1.

5.3 Entering the Peppol Network

5.3.1 Preconditions

Before a Service Provider obtains access to the Peppol Network, the following preconditions must be met:

1. The Service Provider must have passed the onboarding test foreseen for the type of Peppol Services intended to be offered on the Peppol Network.

2. The Service Provider must have signed a Peppol Service Provider Agreement with the relevant Peppol Authority.
    a. A Peppol Authority is relevant to a Service Provider when its jurisdiction includes both dimensions below:
        i. The country or territory where the Service Provider is legally based.
        ii. The Peppol Service Domain(s) in which the Service Provider plans to offer Peppol Services.
    b. Where no Peppol Authority can be considered as relevant, according to the conditions of point 7.a.i-ii above, the Service Provider Agreement shall be signed directly with the Peppol Coordinating Authority, which assumes the role and responsibilities of a Peppol Authority according to the provisions of the Peppol Authority Agreement (clause 8.1.7).
    c. As an exception, the Peppol Coordinating Authority may grant to a Peppol Authority the right to sign a Service Provider Agreement with a Service Provider legally based outside its territorial jurisdiction, provided that:
        i. No other Peppol Authority has territorial jurisdiction in the country or territory where the Service Provider is legally based.
        ii. The Service Domain in which the Service Provider intends to provide Peppol Services is within the jurisdiction of the Peppol Authority in question.
3. The Service Provider must be a member of OpenPeppol AISBL, in the category appropriate for the type of Peppol Services intended to be offered on the Peppol Network.
4. The Service Provider's membership must be in good standing, including (but not limited to) payment of applicable fees, otherwise the Peppol Coordinating Authority retains the right to deny access to the Peppol Network.
5. For the avoidance of doubt, the Service Provider Agreement may be signed at any time between the time of accession of a Service Provider as a member of OpenPeppol AISBL and the time when the Service Provider gains access to the Peppol Network.

5.3.2 Accreditation process

The accreditation process will start after the Service Provider has been admitted as an OpenPeppol Member in the category appropriate to the type of Peppol Services they want to offer.

To gain access to the Peppol Network, a Service Provider must follow the necessary steps as described below:

1. Determine the relevant Peppol Authority to relate with.
    a. The Service Provider should contact the Peppol Authority, the jurisdiction of which meets the requirements of section 5.3.1. If none of the existing Peppol Authorities meets those requirements, OpenPeppol will assume the role of Peppol Authority for that Service Provider.
    b. Initiating a relationship with the relevant Peppol Authority is a prerequisite for the successful execution of the accreditation process. The Peppol Authority will indicate whether it accepts the relationship before it is initiated.
2. Request and obtain a test PKI certificate.
    a. The Service Provider shall request and obtain a test PKI certificate from OpenPeppol, so that they can begin testing.
    b. The request for a test PKI certificate must be approved by the relevant Peppol Authority and the Peppol Coordinating Authority.
    c. If no Service Provider Agreement has been signed, a basic entity identification process must take place as a minimum, usually by the Service Provider submitting the information contained in Annex 3 of the Peppol Authority Agreement and a copy of their business register statutes or equivalent. A more comprehensive identification procedure according to the provisions of the Entity Identification Policy may be undertaken if the Peppol Authority so chooses but is not mandatory at this point in time.
    d. As an exception, OpenPeppol may issue test certificates to interested parties that are not Service Providers or even OpenPeppol Members, provided that their enablement to test Peppol Services is to the interest of OpenPeppol. No production certificates shall be issued to such parties.
3. Pass the onboarding test.
    a. The Service Provider shall perform, and must successfully pass, the required onboarding test as appropriate for the Service Domain in which they intend to offer Peppol Services.
    b. Proof of successful test completion will be the test report generated by the OpenPeppol Testbed.
4. In case the relevant Peppol Authority has additional requirements for local accreditation that have been accepted as PA specific requirements, a local accreditation process must be followed and successfully completed before the Service Provider signs the Service Provider Agreement and before production certificate(s) are issued.
5. Sign the Service Provider Agreement.

a. The Service Provider shall sign the Peppol Service Provider Agreement with the relevant Peppol Authority, to be determined according to the provisions of section 5.3.1.

b. The Service Provider Agreement can be already signed before testing is completed or before testing even starts.

6. Request and obtain production PKI certificate(s).

a. After passing the required onboarding tests and signed a Peppol Service Provider Agreement, the Service Provider can request a production PKI certificate from the Peppol Coordinating Authority.

b. The request must be approved by the Peppol Authority with which the Service Provider has signed an Agreement, as well as by the Peppol Coordinating Authority.

c. Once the request is approved, the Service Provider will be issued production PKI certificate(s) for the Peppol Service Domain(s) in which they intend to offer Peppol Services.

Once the Service Provider has obtained production certificate(s) for the Service Domain(s) in which it intends to offer Peppol Services, the accreditation process is complete, and the Service Provider can start operations.

5.4 Remaining in the Peppol Network

To retain access to the Peppol Network, the following conditions must always be met:

1. All Service Providers must be compliant with all requirements for the use of the Peppol Network as stated in the Service Provider Agreement, the Internal Regulations and Operating Procedures.
2. All Service Providers must pass the relevant tests, as appropriate for the Service Domain(s) in which they offer Peppol Services, at least once, and no earlier than 2 months before their production certificate(s) need to be renewed.
3. Production PKI certificate(s) must be re-issued at least every two years, following the provisions specified in the Operational Procedures.
4. A Service Provider Agreement must be in effect with the relevant Peppol Authority.
5. OpenPeppol membership in the category appropriate to the Peppol Service offered must remain valid.

5.5 Leaving the Peppol Network

A Service Provider may leave the Peppol Network under the following circumstances:

1. Voluntarily, when the Service Provider no longer wishes to provide Peppol Services.
2. When the Service Provider is subject to the penalty of removal from the Peppol Network under the provisions of the Compliance Policy (chapter 9).
3. When the Service Provider Agreement is terminated for whatever reason that is compliant to the provisions of that Agreement, resulting in a situation where no valid Service Provider Agreement is in effect.
4. When, for any valid reason, the membership of the Service Provider to OpenPeppol is terminated.

In all such circumstances, the production certificate(s) issued to the Service Provider shall be revoked.

Back to Table of Contents

6 Information Security Policy

6.1 Policy Overview

This policy contains the following parts:

1. Overview
2. Requirements from the Peppol Agreements
3. Purpose
4. Security provisions

6.2 Requirements from the Peppol Agreements

The legal obligation to have security measures in place is expressed in the Peppol Service Provider Agreement clause 17.1. The provisions based on this clause are stated in chapter 6.4. Furthermore, there are other obligations on security measures stated in the Peppol Service Provider Agreement clauses 9.5 and its sub-clauses, 10.3, 10.4, 10.5, 17.2, 17.3, 17.4, 17.5, 17.6, 17.7, 17.8, 17.9 and 17.10.

6.3 Policy purpose

This policy describes the minimum security provisions Service Providers must have in place. The reasons for having these security provisions are:

1. To Protect the Peppol Network.

2. To Protect End Users.
3. To Protect Service Providers.
4. To increase confidence and trust in the governance of the Peppol Network.

6.4 Security provisions

Service Providers must have technical and organizational measures in place to secure the integrity and continuous operation of the Peppol Interoperability Framework and all data exchanged across the Peppol Network. These measures have to protect against:

1. Accidental or unlawful destruction.
2. Accidental loss.
3. Alteration.
4. Unauthorized disclosure or access.
5. All other forms of processing contrary to obligations as stated in the Peppol Governance framework.

The measures in place shall ensure a level of security appropriate to the risks represented by the data exchange and the nature of the data to be protected.

Back to Table of Contents

7 Peppol Authority specific requirements

7.1 Policy Purpose and Overview

The purpose of this Policy is to define the rules and provisions that must be respected by all actors participating in the definition, approval and enforcement of specific requirements for the use of the Peppol Network, which are applicable within the jurisdiction of a given Peppol Authority (PA), and which will be hereinafter referred to as “PA Specific Requirements”.

This Policy contains the following parts:

1. Purpose and Overview
2. Requirements from the Peppol Agreements
3. General Provisions on the:
    a. Definition of PA Specific Requirements
    b. Applicability of PA Specific requirements

4. Categories of PA Specific Requirements
5. Approval of PA Specific Requirements
6. Availability of PA Specific Requirements

7.2 Requirements from the Peppol Agreements

In accordance with clause 11 of the Peppol Authority Agreement and the Peppol Service Provider Agreement, the Peppol Coordinating Authority has the ability to approve PA Specific Requirements applicable for a given jurisdiction (clause 11.1).

Both the Peppol Authority Agreement and Peppol Service Provider Agreement impose a strong obligation on PAs to ensure that PA Specific Requirements do not hamper interoperability for Service Providers (SPs) and End Users operating actively in more than one jurisdiction or engaged in message exchange across jurisdictions (clause 11.2).

7.3 General Provisions

7.3.1 Definition of PA Specific Requirements

1. Peppol Authorities must define PA specific requirements applicable to the use of the Peppol Network within their jurisdiction only when:
   a. either they need to ensure compliance with legislation, regulation, or market conditions particular to that jurisdiction, or
   b. they need to manage issues and risks as legitimately perceived by regulating authorities within the particular jurisdiction, and
   c. in all cases, such requirements cannot be met by those specifications or other provisions that are universally enforced through the Peppol Interoperability Framework.
2. When defining and enforcing PA specific requirements, Peppol Authorities should strive to minimize the additional compliance costs and increased regulatory burden that such requirements will place on Service Providers.
3. PA specific requirements cannot be used to impose changes to any component of the Peppol Interoperability Framework but **may** be used to constrain their use, such as making an optional Peppol Dataset Type mandatory.
4. PA specific requirements **must not** be defined in a way that creates obstacles for global interoperability in the market of message exchange across jurisdictions by preventing Service Providers from offering services within a given jurisdiction, by measures such as requiring the use of specific tools or procedures that cannot be accessed by Service Providers located outside that jurisdiction.

7.3.2 Applicability of PA Specific Requirements

1. PA specific requirements apply to Peppol Services offered to End Users (senders or receivers) which are legally based within the territorial jurisdiction of a Peppol Authority.
2. PA specific requirements must be respected by all Service Providers who provide Peppol Services to End Users (senders or receivers) which are legally based within the territorial jurisdiction of a Peppol Authority, irrespectively of the location of the Service Provider and independently of whether a Service Provider has signed a Peppol Service Provider Agreement with that Peppol Authority.
3. For the avoidance of doubt, PA specific requirements apply to all Service Providers who provide Peppol Services to End Users (senders or receivers) within the PA's jurisdiction, and not only to the Service Providers who have signed an agreement with that Peppol Authority.

7.4 Categories of PA Specific Requirements

PA Specific Requirements may be defined along the following categories:

1. Applicable or allowed identifier or identification schemes
2. Information security
3. Information Sharing
4. Mandatory use of centralised services and global specifications
5. Service Level Requirements
6. Use of local interoperability specifications
7. Service Provider Accreditation

7.4.1 Applicable or allowed identifier or identification schemes

1. A Peppol Authority may need to express specific requirements related to the actual use of one or more specific identifier schemes for End Users legally based in its jurisdiction, such as a VAT number (or other unique and official identifier).
2. Only identification schemes allowed according to the Peppol Policy for Identifiers may be mandated as PA specific requirements.
3. Further to the provisions included in the Entity Identification Policy as set out in chapter 5, a Peppol Authority may however see a need to define and enforce further requirements, such as the use of a specific authoritative source for verification of Entity identification within the Jurisdiction for tax purposes.

4. If a Peppol Authority defines and enforce PA Specific Requirements under this category, it must provide sufficient information, guidance and access to any tools and resources necessary to enforce identification and verification obligations as stated in the Entity Identification Policy (chapter 5).

7.4.2 Information security

1. Any requirements on Information Security above and beyond what is stated in the Peppol Architectural Framework, which a Peppol Authority wants to enforce, must be defined, or incorporated by reference as part of the PA Specific Requirements.

7.4.3 Information sharing

1. Clause 9.2.8 of the Peppol Authority Agreement sets out the requirement for the PA to provide a forum for communication, coordination and collaboration amongst Peppol Service Providers with whom they have a signed agreement. This requirement ensures that Service Providers are informed of activities and developments related to the Peppol Interoperability Framework relevant for their service offerings, including any upcoming changes to the Peppol Interoperability Framework. It also aims to ensure that Service Providers have an opportunity to contribute to any relevant review processes.
2. A Peppol Authority may, as part of its PA specific requirements, further specify or offer additional fora as well as require participation by Service Providers as a condition of their accreditation to such fora.

7.4.4 Mandatory use of centralised services and global specifications

1. A Peppol Authority **may** require, as part of its PA specific requirements, the use of centralised Peppol Addressing and Capability Look-up services for all or specific type of End Users legally based within its territorial jurisdiction. In such an event, the Peppol Authority must provide sufficient information/guidance for Service Providers, as well as access to all relevant tools or procedures.
2. A Peppol Authority may make the use of the Peppol Directory mandatory for End Users which are legally based within its territorial jurisdiction.
3. A Peppol Authority may make the use of optional global specifications (e.g. Invoice Response) mandatory for End Users which are legally based within its territorial jurisdiction.

7.4.5 Service Level Requirements

1. A Peppol Authority **may** apply, within its jurisdiction, stricter Service Level Requirements than those foreseen in the Peppol Interoperability Framework.

7.4.6 Use of local interoperability specifications

1. A Peppol Authority may request the use of local datasets or other interoperability specifications within its jurisdiction.
2. PA specific requirements under this category must comply with the requirements for Extended Use of Peppol as set out in Chapter 8 and, more particularly, to the general provisions for Extended Use and specific provisions relevant to Local Extension.
3. The Peppol Coordinating Authority may grant an exception to the obligation for End Users to support the relevant Peppol BIS, subject to the provisions outlined in clause 12.3 of the Peppol Authority Agreement and Peppol Service Provider Agreement.

7.4.7 Service Provider Accreditation

1. Clause 11.3 of the Peppol Authority Agreement and Service Provider Agreement provides the PA with the authority to define and enforce its own specific accreditation scheme to ensure compliance to their PA Specific Requirements.
2. The use of any such accreditation scheme to be enforced by the Peppol Authority must be defined or incorporated by reference as part of the PA Specific Requirements.

7.5 Approval of PA Specific Requirements

1. Before coming into effect, any newly developed or modified PA Specific Requirements:
   a. must undergo a compliance review by the Operating Office, in order to ensure that they respect the rules and provisions included in this Policy,
   b. must be made available to other Peppol Authorities and the Service Providers for review, and
   c. must be approved by the OpenPeppol Managing Committee.
2. The Peppol Authority responsible for the PA Specific Requirements should, to the extent possible, address the feed-back and comments provided through the

review by other PAs and SPs before submitting the final version of its proposed PA Specific requirements for approval by the OpenPeppol Managing Committee.

3. The Compliance Report and recommendation from the Operating Office must be made available to the Managing Committee as part of the basis for decision together with the final version of the proposed PA Specific Requirements.
4. For PA specific requirements on the use of local interoperability standards, the provision of Extended Use (chapter 8) applies to the approval process.
5. In case PA specific requirements that fall into the category of “Mandatory use of centralised services and global specifications” (section 7.4.4) and a similar precedent has already been established, these will be approved automatically without involving the OpenPeppol Managing Committee. They will be directly published as part of PA specific requirements within the Peppol Interoperability Framework by the Operating Office, which will be acting in a delegated role to facilitate the process.

7.6 Availability of PA Specific Requirements

In accordance with clause 11.1 of the Peppol Authority Agreement and the Peppol Service Provider Agreement, PA Specific Requirements will be documented as part of the Peppol Interoperability Framework.

OpenPeppol shall be responsible for publishing all PA specific requirements on the Peppol website as part of the Peppol Interoperability Framework description.

Back to Table of Contents

8 Extended Use of Peppol

8.1 Policy Statement

In addition to the global Peppol Service Domains, which cover all jurisdictions within the Peppol Network, individual Peppol Authorities may develop and implement additional services, or extend the use of the Peppol Network.

OpenPeppol shall encourage and facilitate such initiatives, with a view to the gradual integration of Extended Use cases as global Peppol Service Domains, subject to sufficient interest and uptake from Peppol Authorities, Service Providers and End Users.

In all cases, any proposed additional Peppol Services or extension(s) of the Peppol Network must be able to integrate fully with the existing governance, operations and policies applying to the Peppol Network.

8.2 General Provisions

8.2.1 Types of Extended Use

Global Service Domains in OpenPeppol are the ones that are in use across the entire Peppol Network and are governed by OpenPeppol.

Extended use of Peppol can occur beyond the global Service Domains, built around use cases that can be categorized into one of three groups:

1. **Local Extensions to global Service Domains** which are already established across all jurisdictions within the Peppol Network:
    a. They are unique to the territorial jurisdiction of a specific Peppol Authority, as defined by that Peppol Authority.
    b. They do not involve changes to the Peppol technical specifications which are applicable within the existing global Service Domain in question.
    c. Such cases may include localized customisations of globally applicable technical specifications or bespoke local Datasets required for End Users to comply with local laws, regulations, or standards.
2. **Local Service Domains** newly established within the jurisdiction of a Peppol Authority:
    d. Their business process scope falls outside existing Peppol Service Domains.
    e. They do not require support outside a given local jurisdiction or cross-border capabilities.
    f. Such cases may include national usage scenarios relevant to local stakeholders and processes, not relevant to stakeholders outside a specific geographical jurisdiction, which can be defined to include a country or a multi-country region.
3. **Incubations** of new global Service Domains:
    g. Aim to establish an entirely new Peppol Service Domain with potential to be relevant across the entire Peppol Network.
    h. Incubation will take place under the responsibility of a Peppol Authority when the prospect is deemed beneficial and preferable for OpenPeppol or if OpenPeppol lacks the capacity to develop a new Service Domain centrally and scale it to a global level.

8.2.2 Basic principles and requirements

1. All cases of Peppol Extended Use must be approved by the OpenPeppol Managing Committee.
2. They can be initiated either by OpenPeppol itself or by a Peppol Authority that wishes to embark on such a prospect.
3. Approval of Extended Use will be based on the fulfilment of required criteria, as stated below.
    a. To be approved, Extended Use must:
        i. Cause no foreseeable conflict with:
            - any global Service Domains already existing,
            - any Peppol Services already approved for Extended Use,
            - any promising prospects for new such Service Domains already considered by OpenPeppol for global or local use.
        ii. Describe the impact of the proposed Extended Use on the use of technical specifications that are applicable and mandatory in existing Peppol Service Domains, so that it can be determined that no negative impact is caused on interoperability across the Peppol Network.
        iii. Be feasible within the organizational and financial capacity and capability of the proposing Peppol Authority and/or OpenPeppol as may be relevant.
    b. To be approved, Extended Use should:
        i. Extend the coverage and usage of the Peppol Network in terms of users, transaction types, Service Providers, new stakeholder constituencies, application areas and technology fields, increasing the value of the Peppol Network.
        ii. Increase the potential of Peppol to play the role of a robust interoperability environment that can be dependably considered as essential IT infrastructure within and among national jurisdictions.
        iii. Enhance the reputation of OpenPeppol and build trust in internal and external stakeholders, strengthening the Peppol brand.
4. A proposal for approval of Extended Use must meet the criteria stated above and include, inter alia:
    a. Use case description.

b. Stakeholder analysis – who are the end users, the potential Service Providers, the Peppol Authority (if different than the proposing one).

c. Growth potential for the Peppol Network – high-level indications pointing to the addition of new users, transactions, service providers.

d. Technical specifications to be used, including terms of availability and IPR status. Differences with existing, globally applicable specifications must be highlighted and justified.

e. Change management responsibilities for the proposed Extended Use, intended to be assumed either by a Peppol Authority or by another relevant body within the jurisdiction concerned, if applicable.

f. Peppol Authority responsibilities related to the proposed Extended Use.

5. The OpenPeppol Managing Committee shall decide on all submitted proposals for Extended Use, based on the criteria included under point 2 above.

6. OpenPeppol shall maintain a public list of approved Extended Use cases, and the Peppol Authorities that are responsible for each.

8.3 Particular Provisions and Governance

8.3.1 Local Extensions and Service Domains

Local Extensions to existing global Service Domains are adopted by Peppol Authorities through their PA Specific Requirements.

Local Service Domains are adopted through inclusion to the Domain jurisdiction of Peppol Authorities by listing them in Annex 2 of the Peppol Authority Agreement. Onboarding Service Providers to a Local Service Domain can be done through Annex 2 of the Peppol Service Provider Agreement.

Subject to the general rules set out above, individual Peppol Authorities may construct their Local Extensions and Domains, subject to the principles outlined in clause 11.2 and 11.4 as well as 12.4 of the PA Agreement.

In case other Peppol Authorities may wish to adopt any approved Local Extension or Local Service Domain, the Peppol Authorities concerned and OpenPeppol shall first consider the possibility of moving to a global specification or Service Domain before the Managing Committee takes a final decision on further Extended Use at a local level.

8.3.2 Incubation

8.3.2.1 Function and goal

A successful incubation process leads to the establishment of a new global Service Domain in Peppol, conforming to all the relevant governance structures and processes of existing Service Domains that are applicable across the entire Peppol Network. Unlike local types of Extended Use, an incubation is therefore an inherently and explicitly temporary construct.

8.3.2.2 Incubation Charter

An Incubation is founded upon a project charter, which shall be called the Incubation Charter.

The structure of the Incubation Charter and the requirements it must fulfil are laid out in the OpenPeppol Operational Procedures. They must include at least such tangible deliverables as to demonstrate that the Incubated Service Domain is ready to graduate into full global Service Domain status.

The Incubation Charter may be developed after an initial, in principle approval of the incubation prospect by the Managing Committee. It must be submitted to and approved by the Managing Committee prior to the start of the undertaking. Such approval shall not be withheld except for specific and compelling reasons.

8.3.2.3 Incubation Monitoring Committee

An incubation is overseen by a Monitoring Committee, which is established for the purposes of a particular incubation project and is therefore transient in nature. Its function is to monitor on a regular basis the progress of an incubation, according to stated objectives and deliverables laid out in the Incubation Charter.

The Incubation Monitoring Committee is composed of:

- A representative of the proposing Peppol Authority.
- A representative of the Managing Committee or, in case no MC member is available, a representative of the Operating Office.
- Depending on relevance and availability, representatives of other Peppol Authorities, Service Providers or Domain Communities. External subject matter experts may also be included.

The Incubation Monitoring Committee composition will be decided as part of the Incubation Charter at the time of incubation approval. Communities will be consulted during this process.

The Incubation Monitoring Committee is a consulting body and does not make formal decisions. The final decision about the incubation results will be made by the Managing Committee based on achievement of goals stated in the Incubation Charter. Full adoption shall not be denied to any incubation which has fulfilled the requirements laid out in its charter, unless conditions have materially changed since the approval of the charter, in a manner that could not have reasonably been foreseen at the time of approval. The Management Committee shall without delay notify the Incubation Monitoring Committee of such developments as may come to its attention.

The Incubation Monitoring Committee may submit deliverables foreseen in the Incubation Charter to a peer review by Peppol Authorities and Service Providers, or all OpenPeppol Members.

Back to Table of Contents

9 Compliance Policy

9.1 Policy purpose and overview

This policy is focused on the responsibilities of the Peppol Authorities and the Peppol Service Providers with a view to ensure interoperability across the full Peppol Network and to improve the communication and convergence between all parties.

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 parties involved.

It contains the following parts:

1. Purpose and overview
2. Requirements from the Peppol Agreements
3. Compliance supervision and enforcement
4. Claim escalation and dispute resolution
5. Authority delegation

9.2 Requirements from Peppol Agreements

The legal obligation on SPs to ensure that Peppol Services offered to the market comply to the relevant components of the Peppol Interoperability Framework follows from the Peppol Service Provider Agreement clause 9.5.

Furthermore, clause 7.1.2 of the Peppol Service Provider Agreement mandates the PA to ensure that Peppol Services offered within their jurisdiction are in compliance with the components of the Peppol Interoperability Framework.

Reactions to cases of non-compliance are defined in clause 18 of the Peppol Service Provider Agreement.

9.3 Compliance supervision and enforcement

Compliance of a Peppol Authority is measured against the Peppol Authority Agreement and the Internal Regulations on the Use of the Peppol Network.

Compliance of a Service Provider is measured against the Service Provider Agreement and the Internal Regulations on the Use of the Peppol Network.

9.3.1 Peppol Network supervisory bodies

The compliance supervisory bodies are:

1. Peppol Coordinating Authority: It is the main governing body in the Peppol Network. The Peppol Coordinating Authority is responsible for the supervision and enforcement of the policies and procedures for the Peppol Authorities and for the issue resolution of claims that may affect more than one Peppol Authority.
2. Peppol Authorities: As defined in the Peppol Authority Agreement, the Peppol Authorities are responsible for the supervision of Service Providers within their jurisdiction. They are the entities that shall enforce the OpenPeppol policies and procedures on their Service Providers. They shall also enforce on their Service Providers, the Peppol Authority Specific Requirements of all Peppol Authorities.

9.3.2 Types of supervisory procedures

There is a proactive and a reactive type of supervision and respective ways to enforce compliance.

1. Reactive supervision and enforcement are initiated as a result of a non-compliance complaint raised to a Peppol Authority or the Peppol Coordinating Authority, subject to provisions described in section 9.3.4. Such complaints may be related to:
    a. an alleged breach of any rules stated in the Peppol Agreements or Internal Regulations for the use of the Peppol Network,
    b. any actors or bodies allegedly not following due process in the execution of their duties and responsibilities as described in the Peppol Interoperability Framework.
2. Proactive supervision and enforcement are continuous, and relevant actions are executed by the supervisory body analysing the Peppol Network infrastructure and the data obtained from the Service Providers. Specific provisions are

described in section 9.3.3 related to actions taken by the Peppol Coordinating Authority, but this does not preclude similar or other proactive supervision procedures to be established and executed by Peppol Authorities within their jurisdiction.

9.3.3 Continuous and proactive supervision

9.3.3.1 Monitoring Compliance

Continuous supervision and monitoring of compliance is done by the Peppol Coordinating Authority and Peppol Authorities through the use of the data gathered from the Peppol Network and the data reported by Service Providers according to the provisions of the Data Usage and Reporting Policy.

Checks on available data will be done regularly by the OpenPeppol Operating Office, which acts on behalf of the Peppol Coordinating Authority. Results will be made available to Peppol Authorities in relation to the Service Providers and End Users within their jurisdiction. Specific controls on behalf of Peppol Authorities can be performed by the Operating Office through the tools available to and by the Peppol Coordinating Authority.

The goal of the monitoring process is to determine whether the rules for the use of the Peppol Network are followed, focusing on (but not limited to) the following:

a. Applicable Specifications, as determined by the Peppol Architectural Framework.
b. End User Identification, as foreseen by the Entity Identification Policy.

When a migration process is in progress, the Operating Office shall take into account the deadlines for the phase-in of the new specification and phase-out of the deprecated one.

9.3.3.2 Managing non-compliance

Derived from the above monitoring process, the supervisory body shall describe the non-compliance issues with the list of End Users and Service Providers in breach.

Each Peppol Authority shall act on issues concerning its Service Providers and/or End Users derived both from the proactive monitoring of the Peppol Coordinating Authority or from its own proactive monitoring processes.

To manage non-compliance, the supervisory bodies shall follow the provisions below:

1. When the Peppol Coordinating Authority discovers an incident of non-compliance, it shall open a non-compliance issue in the Peppol Service Desk reporting the breach. The ticket shall explain the breach of compliance and identify the Service Providers and End users with whom the issue has occurred. The ticket shall be assigned to the Peppol Authority responsible for the Service Provider.

2. When a Peppol Authority discovers an incident of non-compliance or receives notification of such an incident from the Peppol Coordinating Authority, it shall contact the Service Provider or Service Providers and address the non-compliance, proceeding to its resolution. The Peppol Authority shall set the non-compliance issue resolution deadline as may be appropriate.
3. Once resolved, the supervisory body shall process to closing the issue.
4. Any party affected can escalate the issue to the Peppol Coordinating Authority as defined in section 9.4.2 if the party considers the problem of non-compliance is not resolved in a satisfactory manner.

9.3.4 Supervisory procedure based on a complaint

1. When a non-compliance incident occurs, a direct discussion among the involved parties should take place in an attempt to resolve the issue.
2. In case no agreement can be reached on a resolution, any affected party has the right to raise the non-compliance to its Peppol Authority or to the Peppol Authority/Authorities of the other party/parties involved in the incident.
3. The Peppol Authority shall mediate between the parties trying to find a resolution to close the issue according to the Peppol Agreements, internal regulations and operational procedures.
4. Once resolved, the Peppol Authority shall close the issue.
5. Should the issue not be resolved because it affects more than one Peppol Authority, due to its complexity or by any other reason, the Peppol Authority shall escalate the issue as described in section 9.4.2.
6. Any party affected by the complaint can also escalate the issue to the Peppol Coordinating Authority as defined in section 9.4.2 if the party considers the problem of non-compliance is not resolved in a satisfactory manner.

9.4 Enforcement of policies and procedures

9.4.1 General Provisions

A supervisory body has the power to enforce the procedures and policies on the set of entities it is responsible for, as defined in this policy.

Procedures and policies can be enforced through the penalties specified in section 9.4.3.

As a result of penalty enforcement, End Users may be removed from the Peppol Network and added to a blacklist of End Users so that they will not be allowed to become a Peppol End User again.

For Service Providers, the final penalty is to remove them from the Peppol Network by revoking their technical capability to exchange datasets.

9.4.2 Escalation process in case of dispute

In case of dispute, the issue, the resolution, and the dispute arguments from the party raising the dispute shall be filed in the Peppol Service Desk.

The Peppol Coordinating Authority, through the Operating Office shall try to resolve the issue, and in case the issue cannot be resolved, they shall escalate it to the Managing Committee with a pre-analysis and a suggested resolution.

The Managing Committee shall assess the case and provide a final decision. The Operating Office shall communicate the final decision to the parties through the Peppol Service Desk.

The resolution from the Managing Committee shall be considered final, and there is no other body to appeal.

9.4.3 Penalties

Penalties are the means to support the enforcement of the policies and procedures. The penalties that may be enforced by the supervisory body are defined in the Peppol Agreement clause18 as follows:

1. Blacklisting on the OpenPeppol Member website, i.e. publication of the fact that the Service Provider or the End User is in a non-compliance situation on the closed member site of OpenPeppol.
2. Public blacklisting, i.e. publication of the fact that the Service Provider or the End User is in a non-compliance situation on the public website of OpenPeppol (www.peppol.eu) and on the website used by the relevant PA for market communication.
3. Suspension of access to the Peppol Network for a limited period of time. This requires the revocation of the certificate and re-issuance of a new one after the established period of suspension.
4. Expulsion from the Peppol Network, i.e. permanent revocation of the Peppol certificate.

The Peppol Authority may extend an initially limited suspension, depending on conditions set up by the Peppol Authority or ultimately exclude the Service Provider from the Peppol Network by revoking their Peppol Certificate. Any extension in suspension shall be documented by a warning note.

If the Service Provider fails to respond within the set time-limit the Peppol Authority may without further notice escalate the case and ultimately revoke the certificate.

9.5 Authority delegation

Every Peppol supervisory body can delegate the role of supervision to an entity or team within their internal organization.

The Peppol Coordinating Authority delegates the compliance processing to the Operating Office and its authority to the Managing Committee.

Back to Table of Contents

1 ANNEX – Semantic Versioning Guidelines

1.1 Introduction

This guideline provides Peppol's versioning policy of technical artefacts. The policy takes inspiration and builds upon the semantic versioning policy[1] by keeping the semantic versioning core aspect of "Major.Minor.Patch" versioning pattern while defining the sets of rules of increment based on the perceived overall implementation impact.

1.2 Peppol Semantic Versioning Baseline

The semantic version follows the MAJOR.MINOR.PATCH pattern for the versioning string. The principal, high-level rules are as follows:

Given a version number MAJOR.MINOR.PATCH, increment the:

MAJOR version when you make incompatible changes,

MINOR version when you add functionality in a backwards-compatible manner,

PATCH version when you make backwards-compatible bug fixes.

Additional labels for pre-release and build metadata are available as extensions to the MAJOR.MINOR. PATCH format.

The incremental rule is straightforward, but incompatible change and backwards-compatible change is domain and context-specific.

Peppol creates and versions **Business Interoperability Specifications (BIS) as a versioned atomic bundle** that combines the following types of technical artefacts:

- Syntax Binding
- Code Lists
- Schematron Rules
- Specifications
- Software artefacts

To version them, Peppol builds on semantic versioning baseline of having normative rules for Major, Minor and Patch version increment, depending on the perceived implementation impact change applied.

[1] Semantic versioning - https://semver.org/

In the following sections, we define what “major version increment change”, “minor version increment change”, and “patch version increment change” are for each artefact type.

1.3 Patch Version increment changes in Peppol

1.3.1 Changes in Syntax Bindings

The following changes must increase the patch version in Syntax Binding

- Changes in Syntax Binding documentation
- Changes that are considered bugfixes, i.e. when there is a misalignment between a specification and its Syntax Binding

1.3.2 Changes in Code Lists

The following changes must increase the patch version in Code Lists, assuming that specification changes that lead to code list changes are analysed per the specification.

- Deprecation of an element in a code list, except the “Transport Profile Code List”
- Modification of an element in a code list, as long as it is not a key column
- Update of Inherited codelists, which are part of a contractual or legal obligation

1.3.3 Changes in Schematron Rules

The following changes must increase the patch version in Schematron Rules

- Changes in rule descriptions (Editorial Changes)
- Changes in rule names
- Bug fixing of business rules
- Update of Inherited artefacts, which are part of a contractual or legal obligation
    - EN Business Rules
    - National Rules

1.3.4 Changes in Specifications

The following changes must increase the patch version in Specifications:

- Editorial changes that don’t affect the implementation

1.3.5 Changes for Software Artefacts

The following changes must increase the patch version in Software Artefacts:

- Fix editorial errors
- Bug fixing that does not affect the overall functionality
- Improve the performance of existing functionality

1.4 Minor Version increment changes in Peppol

Any minor version increment automatically sets the “patch version” to 0 (zero).

1.4.1 Changes in Syntax Bindings

The following changes are backwards compatible and must increase the minor version in Syntax bindings

- Addition of an optional element
- Decreasing minimum cardinality of an element (e.g. from “1..1” to “0..1”)
- Augmenting maximum cardinality of an element (e.g. from “0..1” to “0..n”)
- Generalisation / change the element data type (e.g. from “number” to “string”)

1.4.2 Changes in Code lists

The following changes must increase the minor version in Code Lists, assuming that specification changes that lead to code list changes are analysed per the specification.

- Addition of an element in a code list, except the “Transport Profile Code List”
- Deprecation of an element in the “Transport Profile Code List”

1.4.3 Changes in Schematron Rules

The following changes must increase the minor version in Schematron Rules

- Removal of a business rule
- Generalising a business rule (making it only less strict)
- Addition of a business rule to a new optional element

1.4.4 Changes in Specifications

The following changes must increase the minor version in Specifications:

- Add new glossary item

1.4.5 Changes for Software Artefacts

The following changes must increase the minor version in Software Artefacts:

- Provide new functionality without modifying the existing one
- Define new APIs or interfaces

1.5 Major Version increment Changes in Peppol

Any major version increment automatically sets the “minor version” and the “patch version” to 0 (zero).

1.5.1 Changes in XML profiles

The following changes must increase the major version in XML Profiles

- Addition of a mandatory element
- Augmenting minimum cardinality of an element (e.g. from “0..1” to “1..1”)
- Decreasing maximum cardinality of an element (e.g. from “0..n” to “0..1”)
- Removal of an element
- Restriction / change the element data type (e.g. from “string” to “number”)

1.5.2 Changes in Code lists

The following changes must increase the major version in code lists

- Addition of a new element in the “Transport Profile Code List”
- Removal of an element in a code list

1.5.3 Changes in Schematron Rules

The following changes must increase the major version in Schematron Rules

- Addition of a business rule to an existing element, except for new National Rules
- Further restricting an existing business rule

1.5.4 Changes in Specifications

The following changes must increase the major version in Specifications:

- Create new rules
- Change existing algorithms

1.5.5 Changes for Software Artefacts

The following changes must increase the major version for Software Artefacts:

- Change existing APIs so that clients need to change.

1.6 Manual assessment needed

Sometimes it is necessary to manually assess if a change is considered backwards compatible or incompatible. Especially in the area of Specification changes, there is no simple set of rules that makes it easy to assess a change.

In situations where although a change is considered minor, its implementation impact is severe, the change must be considered as a candidate for a major version increment, i.e. addition of a new section in a business document with many new complex rules and processes.

E.g. the following topics need manual assessment:

- Adding a new normative reference
- Updating an existing reference
- Updating of third-party artefacts, we depend on

Back to Table of Contents