# Operational Procedures

## Onboarding and Accreditation of Peppol Service Providers

Version: 1.0
Approved: 15 February 2022

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

info@peppol.eu
www.peppol.eu

# Table of Contents

# Version control

| Version | Date | Comments |
|---|---|---|
| 1.0 | 15.02.2022 | Approved by the OpenPeppol Managing Committee (MC161 meeting) |

# List of Terms and Abbreviations

| Term | Definition |
|---|---|
| **OO** | OpenPeppol Operating Office |
| **PA** | Peppol Authority |
| **PCA** | Peppol Coordinating Authority (OpenPeppol AISBL) |
| **PKI** | Public Key Infrastructure |
| **SP** | Peppol Service Provider |
| **SP Agreement** | Peppol Service Provider Agreement |

The procedures included in this document expand on the legal obligations assumed through the Peppol Agreements, and the rules and provisions in the OpenPeppol AISBL Internal Regulations for Use of the Peppol Network.

This Operational Procedure provides operational details for the implementation of the Peppol Agreements and the Policies contained in the OpenPeppol AISBL Internal Regulations for Use of the Peppol Network.

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 for Use of the Peppol Network and these will take precedence over the OpenPeppol Operational Procedures.

# 1 Purpose

This document sets out the processes and procedures for onboarding of a Peppol Service Provider to become active in the Peppol Network. This includes:

- **Acquiring a Peppol test certificate** – how the SP can get a Peppol test certificate allowing it to test the compliance of its Peppol Services.
- **Acquiring a Peppol production certificate** – how the SP can test its Peppol Services and upon successful testing be granted a production certificate.
- **Local accreditation** (if applicable**)** – how the SP will be accredited according to the local rules applicable for the PA with whom it will sign the SP agreement.
- **Signing the Peppol SP Agreement** – how the SP will be formally recognised as a Peppol SP by signing the SP Agreement, thus allowing it to offer Peppol Services to the market.
- **Renewal of certificates** – how an SP will obtain a renewed Peppol production certificate.

**Out of scope**

- **Becoming a member of OpenPeppol AISBL** – how to establish a valid membership in OpenPeppol AISBL.
- **Installing, operating and maintaining Peppol Services** – how the SP will install, operate and maintain its Peppol Services, including the technical options available.
- **Onboarding of End Users** – how an SP will promote its Peppol Services to the market and do its onboarding of End Users.
- **Accounting and reconciliation of accounts** – how membership fees are billed and reconciled.
- **Issuing PKI Test certificates to Interested parties** – How these test certificates are issued by OpenPeppol to interested parties.

# 2 Introduction

As the Peppol Network grows in usage, new Peppol Service Providers will join. To ensure compliance and consistency in the global network, a new SP needs to be onboarded according to common procedures independent of the PA with whom it signs the SP Agreement and the Peppol Services to be offered. Also it is stated how SP's can remain in the Peppol network.

The process and procedures set out in this document aim to ensure transparency and consistency of approach to the onboarding of Peppol Service Providers across the full Peppol Network respecting the agreed policies.

The policies on Onboarding and Accreditation of Peppol Service Providers are stated in Internal Regulations for Use of the Peppol Network (chapter 5).

# 3 Process Overview

The below table provides an overview of the key steps in the process. The table is a general representation of the process flow; some steps can be undertaken in parallel and do not need to be completed in strict sequential order.

| | Step | Description | Responsibility |
|---|---|---|---|
| 1 | Obtain PKI test certificate | The SP will need to obtain a PKI test certificate | SP |
| 2 | Test Peppol Services | The SP will complete the required testing of its Peppol Services to ensure compliance to relevant Peppol specifications | SP |
| 3 | Sign Peppol SP Agreement | The SP and PA will sign the SP Agreement | Peppol Authority and SP |
| 4 | Obtain PKI production certificate | Based on successful testing and signing the SP Agreement the SP will be able to obtain its PKI production certificate. | SP |
| 5 | Re-issuing PKI production certificate | The SP will be re-issued a PKI production certificate when conditions are met | SP |

# 4 Procedure

## 4.1 Obtain PKI test certificate

The purpose of this step is to provide the SP with a Peppol test certificate which will subsequently allow the SP to test its Peppol Services.

1. **To initiate the process the SP will establish contact with the PA with whom they will sign the SP Agreement.**

The SP will contact their national PA, i.e., the PA in the country where the SP has its business registered, identifying themselves as an OpenPeppol Member and requesting the SP Agreement package for review.

A list of PAs and their key contacts is maintained on the website of OpenPeppol.

If there is no PA in the country or territory where the SP is legally based or that PA does not have the applicable Peppol Service Domain within its jurisdiction, the SP should contact OpenPeppol and sign the SP Agreement directly with the Peppol Coordinating Authority as stated in clause 5.3.1.2 of Internal Regulations for Use of the Peppol Network.

2. **The SP must file a certificate request with OpenPeppol.**

   OpenPeppol uses software to handle the workflow required to obtain approvals for and to process incoming SP requests, including for PKI certificates.

   A PKI certificate request may be initiated by the SP or by an organisation who hosts and plans to test the relevant Peppol Services. However, PKI certificate requests must be initiated in the Peppol Service Desk and in all cases, the link and passcode details for obtaining PKI certificates are sent only to the cell phone and email address of the SP representative directly.

   Requests for PKI certificates must be accompanied by a signed copy of the SP Agreement annex with contact information and a business registration document, attached in the Peppol Service Desk request.

3. **The OO will confirm that the SP has a valid membership in OpenPeppol.**

   Requests are assigned in the Service Desk to an OO representative for confirmation that the organisation is a valid member and that the required documents are attached. Any overdue invoices are addressed, and requests may be put on hold until the member has confirmed payment. Confirmed requests are then assigned to the appropriate PA using the software workflow.

4. **The PA will approve the certificate request.**

   PAs need to decide who in their organisation will receive and approve day-to-day requests for test and production PKI certificates. This can be a single person's email address or to ensure coverage and timeliness, A PA may create a group mail address specifically for this purpose and provide it to the OO for the set-up in the software to be used.

   The PA receives an auto-email from the Service Desk, with a link to access the PKI case, to review and approve or reject accordingly.

5. **The OO will enrol the PKI test certificate.**

   After PA approval the OO will enrol the certificate for the SP to download.

6. **The SP will download the PKI test certificate.**

Upon successful enrolment the SP will be able to download the PKI test certificate.

## 4.2 Test Peppol Services

The purpose of this step is to allow the SP to test its Peppol Services to ensure compliance to relevant components of the Peppol Interoperability Framework.

As a prerequisite to initiating this step the SP must have

- Obtained a test certificate from OpenPeppol.
- Implemented services based on the relevant components of the Peppol Architectural Framework.

1. **The SP will perform the required testing of its Peppol Services.**

   Once the SP has installed the PKI test certificate in their browser, they can test independently through the centralised testbed as many times as needed to verify the required quality.

   The SP will test all its Peppol Services according to the requirements for the Peppol Service Domains in which it will offer its services.

   The SP shall follow the most recent test documentation very closely.

2. **The SP will review test results.**

   At any time during the testing process the SP may download and review its test results.

## 4.3 Sign Peppol SP Agreement

The purpose of this step is to ensure that the Peppol Service Provider Agreement is signed between the SP and the Peppol Authority.

As a prerequisite to initiating this step, the SP must have a valid membership in OpenPeppol.

1. **The SP will contact the PA with whom they will sign the SP Agreement.**

   The SP will contact their PA, and file a request for signing a SP Agreement with the PA.

2. **The PA will verify the membership status of the SP.**

   The PA can confirm that the SP is an OpenPeppol Member by checking the member list on peppol.eu.

Upon successful confirmation of the membership status of the SP, the PA will send the SP Agreement package to the SP. This will include:

- The latest version of the Peppol Service Provider Agreement and its annexes,
- information about any PA Specific Requirements applicable within the jurisdiction of the PA, and
- information about any specific accreditation that is applicable within its jurisdiction and documentation needed to support the accreditation process.

3. **The PA will perform the required Entity Identity of the SP.**

   In Internal Regulations for Use of the Peppol Network the policies on Entity Identification are stated (chapter 3)

   In clause 3.4 of Internal Regulations for Use of the Peppol Network the requirements on Service Provider Identification are stated. Such assessment must at a minimum comply to these requirements.

4. **The PA will carry out any local accreditation according to its PA Specific Requirements.**

   The SP will provide all documentation needed for local accreditation. This accreditation is based on clause 5.3.2.4 of Internal Regulations for Use of the Peppol Network.

5. **The SP will sign the SP Agreement and return it to the PA.**

   Once the SP has successfully passed the local accreditation, the SP will return a signed version of the agreement with completed version of the agreement annexes.

6. **The PA will sign the Peppol SP Agreement.**

   Having received the signed SP Agreement from the SP and upon successful completion of the verification of identity and local accreditation, the PA will countersign the SP Agreement.

   A copy of the countersigned SP Agreement will be returned to the SP in order to complement their records.

7. **The PA will inform OO about the signed SP Agreement.**

   To complete the process the PA will inform the OO about the signed SP Agreement and file the agreement for its records.

## 4.4 Obtain PKI production certificate

The purpose of this step is to allow the SP to obtain a Peppol PKI production certificate.

As a prerequisite to initiating this step the SP must have

- Signed the SP Agreement with the PA, and
- Passed successful testing of its Peppol Services with OpenPeppol central test facility and have completed any local accreditation.

1. **The SP will request a PKI Production certificate.**

   The SP will request their PKI production certificate through the Service Desk (following the same request and approval process used for obtaining their Test certificate).

   The SP has successfully completed all test requirements for the Peppol Services to be offered. The SP must download their test report from the testbed and attach it for review and approval by OpenPeppol as part of the request for a PKI production certificate

2. **The OO will verify that successful testing is completed.**

   This review will verify that all required testing is completed and that the results of the tests performedmeet the set requirements.

3. **The OO will verify that an SP Agreement has been signed.**

   The OO will do a verification with the PA that the SP has passed any local accreditation requirements and that the SP Agreement has been signed.

4. **OO enrols the PKI production certificate.**

   Once the required verification has been confirmed and the PA has approved the PKI request, the OO will enrol the PKI production certificate for the SP to download.

5. **The SP will download the PKI production certificate.**

   Upon successful enrolment the SP will be able to download the PKI production certificate.

6. **OO will list the accredited SP on the website of OpenPeppol.**

   Upon successful enrolment the accredited SP will be listed on the website of OpenPeppol.

## 4.5 Re-issuing a PKI test certificate

The PKI test certificate expires every two years. To be issued a new PKI test certificate the following procedure must be followed.

The purpose of this step is to provide the SP with a Peppol test certificate which will subsequently allow the SP to test its Peppol Services. This testing is required for obtaining a new PKI production certificate.

1. **To initiate the process the SP must file a certificate request with OpenPeppol.**

   OpenPeppol uses software to handle the workflow required to obtain approvals for and to process incoming SP requests, including for PKI certificates.

   A PKI certificate request may be initiated by the SP or by an organisation who hosts and plans to test the relevant Peppol Services. However, PKI certificate requests must be initiated in the Peppol Service Desk and in all cases, the link and passcode details for obtaining PKI certificates are sent only to the cell phone and email address of the SP representative directly.

   Requests for PKI certificates must be accompanied by a signed copy of the SP Agreement annex with contact information and a business registration document, attached in the Peppol Service Desk request.

2. **The OO will confirm that the SP has a valid membership in OpenPeppol.**

   Requests are assigned in the Service Desk to an OO representative for confirmation that the organisation is a valid member and that the required documents are attached. Any overdue invoices are addressed, and requests may be put on hold until the member has confirmed payment. Confirmed requests are then assigned to the appropriate PA using the software workflow.

3. **The PA will approve the certificate request.**

   PAs need to decide who in their organisation will receive and approve day-to-day requests for test and production PKI certificates. This can be a single person's email address or to ensure coverage and timeliness, A PA may create a group mail address specifically for this purpose and provide it to the OO for the set-up in the software to be used.

   The PA receives an auto-email from the Service Desk, with a link to access the PKI case, to review and approve or reject accordingly.

4. **The OO will enrol the PKI test certificate.**

   After PA approval the OO will enrol the certificate for the SP to download.

5. **The SP will download the PKI test certificate.**

   Upon successful enrolment the SP will be able to download the PKI test certificate.

## 4.6 Re-issuing a PKI production certificate

The PKI production certificate expires every two years. To be issued a new PKI production certificate the conditions expressed in clause 5.4 of Internal Regulations for Use of the Peppol Network must be met.

1. **The SP will perform the required testing of its Peppol Services.**

   The earlier issued PKI test certificate has to be installed by the SP in their browser. After installation the SP can test independently through the centralised testbed as many times as needed in order to verify the required quality.

   The SP will test all of its Peppol Services according to the requirements for the Peppol Service Domains in which it will offer its services.

   Make sure to follow the most recent test documentation very closely.

2. **The SP will review test results.**

   At any time during the testing process the SP may download and review its test results.

3. **The SP will request a PKI production certificate.**

   The SP will request the renewal of their PKI production certificate through the Service Desk (following the same request and approval process used for obtaining their previous PKI production certificate).

   It is assumed that the SP has successfully completed all test requirements for the Peppol Services to be offered. The SP must download their test report from the testbed and attach it for review and approval by OpenPeppol as part of the request for a PKI production certificate. This test report may not be older than two months.

4. **The OO will verify that successful testing is completed.**

   This review will verify that all required testing is completed and that the results of the tests performed meet the set requirements.

5. **The OO will verify that an SP Agreement has been signed.**

   The OO will do a verification with the PA that the SP still has a Service Provider Agreement.

6. **OO enrols the PKI production certificate.**

   Once the required verification has been confirmed and the PA has approved the PKI request, the OO will enrol the PKI production certificate for the SP to download.

7. **The SP will download the PKI production certificate.**

   Upon successful enrolment the SP will be able to download the PKI production certificate.