How to set up a (Post-Award) PEPPOL Access Point (AP)

This document explains how to apply for and setup a PEPPOL Access Point (AP), which is the technical service for sending and receiving PEPPOL business documents.

Please find below the steps that an organization must follow to become a Certified PEPPOL Access Point (AP) provider:

1. Become an OpenPEPPOL member (submit the signed scanned membership form to info@peppol.eu and await an approval email).

2. Identify the PEPPOL Authority you wish to sign the Transport Infrastructure Agreements (TIA) with and request the TIA Agreement package. You can request to sign with any PEPPOL Authority, however we recommend signing with your national PEPPOL Authority. Alternatively, if no national Authority exists, you can sign with OpenPEPPOL as your Authority temporarily until such time as a national PEPPOL Authority becomes operational. Please see the link below to the list of PEPPOL Authorities:

   https://peppol.eu/who-is-who/peppol-authorities/

3. Scan the signed Agreement and all Annexes into one single pdf document and send it to your PEPPOL Authority along with a scanned copy of your company registration document (legal registration).

4. Your PEPPOL Authority will then review and approve the submitted documentation and advise you to proceed with your PKI test certificate request through the PEPPOL Service Desk at: https://openpeppol.atlassian.net/servicedesk/customer/portal/1

5. Ensure that you read and understand the PEPPOL Business Interoperability Specifications 'BIS' (document specifications) at: http://peppol.eu/downloads/post-award/

6. Ensure that you read and understand the eDelivery Network specifications including the Policy for Use of Identifiers (important to understand how senders and receivers are identified in the PEPPOL network) and the SMP specification (important to understand how the discovery process works and the roles of the SMP and SML) at: https://peppol.eu/downloads/the-peppol-edelivery-network-specifications/

7. Implement your Access Point. You can use open source AS2 implementation software or purchase a hosted Access Point software solution – links available on our website at: https://peppol.eu/downloads/peppolimplementations/. Alternatively, you may decide to build your own implementation or purchase a hosted Access Point software solution.

8. Execute the self-testing process, verifying that you can send and receive a valid PEPPOL BIS document (you can send to and receive from your own Access Point implementation to test the file exchange, in order to be fully prepared for the final Acceptance Test procedure). Please see the link below for an online validation service where you can ensure your documents comply to the current PEPPOL specifications.

https://vefa.difi.no/validator/

9. When ready, initiate the Acceptance Test with DIFI (information on this test process is provided later in this document). Once successful, the Test Facility will send the documentation of a successful test to your PEPPOL Authority.

10. Upon notification from your PEPPOL Authority, you can request your Production PKI certificate through our Service Desk at:

    https://openpeppol.atlassian.net/servicedesk/customer/portal/1

11. Download your certificate and enter into production mode.

Please find below, detailed information for implementing the above-mentioned steps.

1) OpenPEPPOL Membership

OpenPEPPOL membership is mandatory for Access Point providers. You will find membership and fee details in the 'How to Join' section of our website. The OpenPEPPOL Membership form must be completed, signed, scanned and sent back to: openpeppol@peppol.eu

OpenPEPPOL will review the form for completeness. You will then receive a notification from OpenPEPPOL to confirm receipt and will be informed about membership approval.
Once approved, your organization will be included in the online list of OpenPEPPOL members located here: https://peppol.eu/who-is-who/openpeppol-member-list-2/

We strongly recommend engaging with the OpenPEPPOL Coordinating Communities as soon as you become an OpenPEPPOL member, in order to have access to a wide group of private and public sector members with PEPPOL expertise in multiple countries and industries, sharing experience and best practices. Please note: It is mandatory that all Access Points and Service Metadata Publishers join the Transport Infrastructure Coordinating Community.

2) PEPPOL Transport Infrastructure Agreements (TIA)

An OpenPEPPOL Access Point (AP) provider must sign the PEPPOL Transport Infrastructure Agreements (TIA) for AP providers with the PEPPOL Authority in its country, or select any of the official PEPPOL Authorities. The PEPPOL Authority will provide you with the PEPPOL TIA template for you to complete, sign and return. See here the List of PEPPOL Authorities

For more information about the Governance of the PEPPOL eDelivery Network and its legal framework, please visit PEPPOL Transport Infrastructure – An Overview

3) PEPPOL Technical Specifications

To implement and operate the Access Point services, you must, at all times, comply with the mandatory PEPPOL BIS specifications, published here: https://peppol.eu/downloads/post-award/

3.1) PEPPOL eDelivery Network

Before implementing the specifications, it is important for potential Access Point and SMP providers to have a good understanding of the PEPPOL eDelivery Network, how it is structured, how it is governed, the role of an Access Point and/or SMP provider, and the relationship with the respective PEPPOL Authority.
Please review the technical specifications related to the PEPPOL eDelivery Network (the BusDox specifications) to ensure you have the appropriate infrastructure (hardware/software) and the necessary technical expertise in place.

The technical specifications and other network resources are available at 'The PEPPOL eDelivery Network Specifications'.

Note: Two types of certificates are used by the Access Point. One certificate is used to sign the message and the acknowledgement according to the AS2 profile. This certificate is requested through the PEPPOL service desk once the Access Point provider has signed the PEPPOL Transport Infrastructure Agreement. The other type of certificate is used by the AS2 web server software for enabling https: communication. This certificate is not provided by OpenPEPPOL but must be issued by a well- known provider of server certificates. Self-signed certificates **must not** be used.

Access Point Implementations

Solutions are available as Open-source, or you can use commercial implementations of AS2 that are configured/adapted to the PEPPOL specifications.

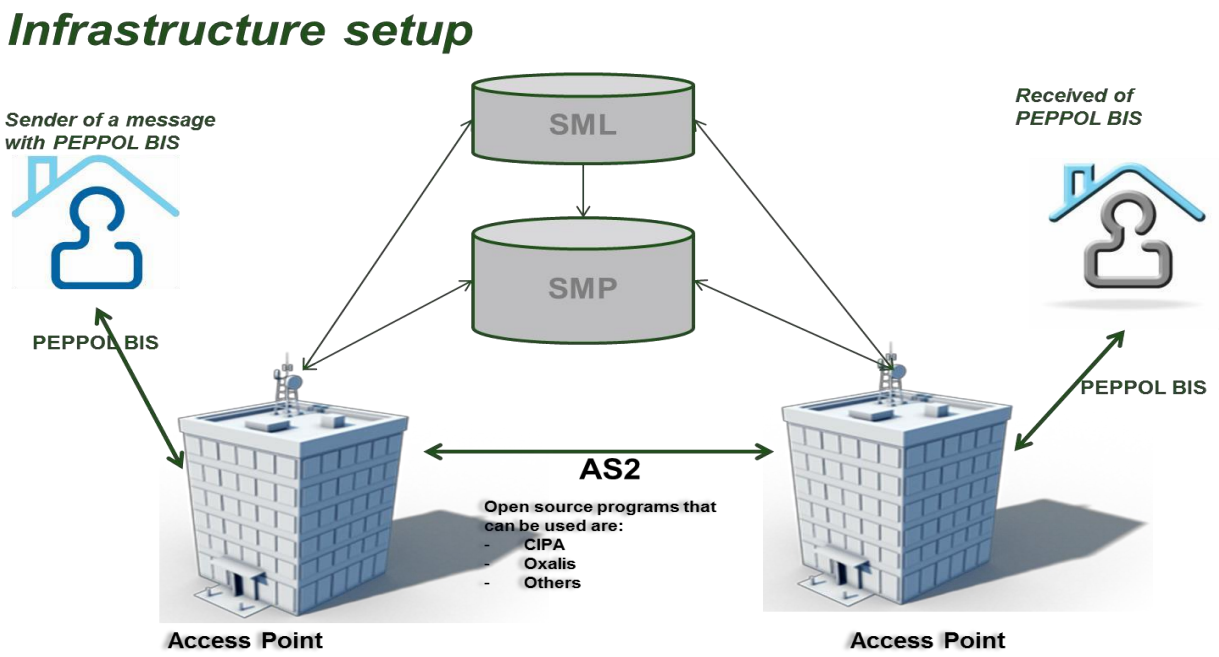
Sample Implementations of the PEPPOL eDelivery Network are provided on our website at 'Links to Software for PEPPOL Implementations'. In particular:

1 - ***Oxalis***: sample Implementation for PEPPOL Access Points, widely used in the PEPPOL community, and maintained by the Norwegian Agency for Public Management and eGovernment (Difi),

https://github.com/difi/oxalis

2 - ***CIPA e-Delivery***: sample Implementation for PEPPOL Access Points, SMP, and SML, maintained by the European Commission.

https://joinup.ec.europa.eu/software/cipaedelivery/home



Note: Access Point service providers can convert a document to the PEPPOL BIS on behalf of the document sender.

3.2) PEPPOL Business Documents

In addition to supporting the appropriate communication protocols, PEPPOL Access Point providers are required to support the PEPPOL Business Interoperability Specifications (BIS) in order to provide PEPPOL-compliant document exchange services to prospective buyers and suppliers.

PEPPOL Business Interoperability Specifications (BIS) v2 is the current mandatory BIS version all receivers must support. This version will be replaced by PEPPOL BIS v3 which will be mandatory from **2019-04-18**

(See: http://docs.peppol.eu/poacc/billing/3.0/migration/ for a full migration overview of the BIS specifications. You can implement one or more PEPPOL BIS in your IT system, following a modular approach, based on your needs and requirements. The current mandatory PEPPOL BIS are:

PEPPOL BIS 1A Catalogue Only

PEPPOL BIS 3A Order Only

PEPPOL BIS 4A Invoice

PEPPOL BIS 5A Billing

PEPPOL BIS 18A Punch Out

PEPPOL BIS Punch Out Login

Transmission Specification

PEPPOL BIS 28A Ordering

PEPPOL BIS 30A Despatch Advice

PEPPOL BIS 36A Message Level Response

PEPPOL BIS 42A Order Agreement

4) Testing

The Norwegian Agency for Public Management and eGovernment (Difi), as a PEPPOL Authority, provides useful tools for testing and self-conformance to PEPPOL specifications (PEPPOL BIS) for Access Point providers.

Test overview with DIFI

Pre-requisites

1) Request your Test PKI certificate through the PEPPOL Service Desk.
2) Before contacting Difi to initiate the Acceptance Test, it is important that you perform self-testing, making sure that you can send and receive PEPPOL BIS documents through the PEPPOL eDelivery Network. To carry out self-testing, you can use the following tools provided by Difi at: https://vefa.difi.no/peppol/tools/ap-test/ . Please note, for testing purposes, Difi will be the receiving organization to which your Access Point will send PEPPOL BIS v2 documents.
3) Once you are ready to perform Acceptance Testing, you need to send an email to AP@Difi.no with a request to begin the test

Details:

- Difi provides their own test SMP for the Acceptance test.
- Difi's PEPPOL Identifier: 9908:810418052 is used as the receiving party in the test
- Check your results at: https://test-aksesspunkt.difi.no/inbound/
- You will be testing against the latest version of the Oxalis Access Point software
- Supported documents you can use in the test: http://test.vefa.difi.no/smp/9908/810418052

4) The test will include:
    a. Verification of certificates (both the PEPPOL and your HTTPS certificate).
    b. Sending of a document from your AP to Difi's Test AP.
    c. Receiving of a document from Difi Test to your AP.
    d. Acknowledgment of the documents sent.
    e. Completion of the Testing Results Template which will be reviewed as part of the test procedure to ensure all the concepts are understood.

Once you have successfully completed the testing activities, your results will be sent by Difi to your PEPPOL Authority who will prompt you to request your production PKI certificate through the PEPPOL Service Desk.

5) OpenPEPPOL Accreditation

Once in production, your company name will be added to the list of Certified Access Points www.peppol.eu and you can contact OpenPEPPOL to receive an “OpenPEPPOL Certified Access Point” logo, for use on your website and in your marketing materials.

Validation Requirements for Access Points in Production

As a sending Access Point provider, you **must** ensure that the business documents sent from your *customers* are confirmed as valid instances, according to the applicable rules, before accepting them for transport through your Access Point services, either by providing validation services on behalf of your customers, or by ensuring that your customers have performed such validation on their PEPPOL BIS documents.