How to set up a PEPPOL Access Point (AP)

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

Prerequisites

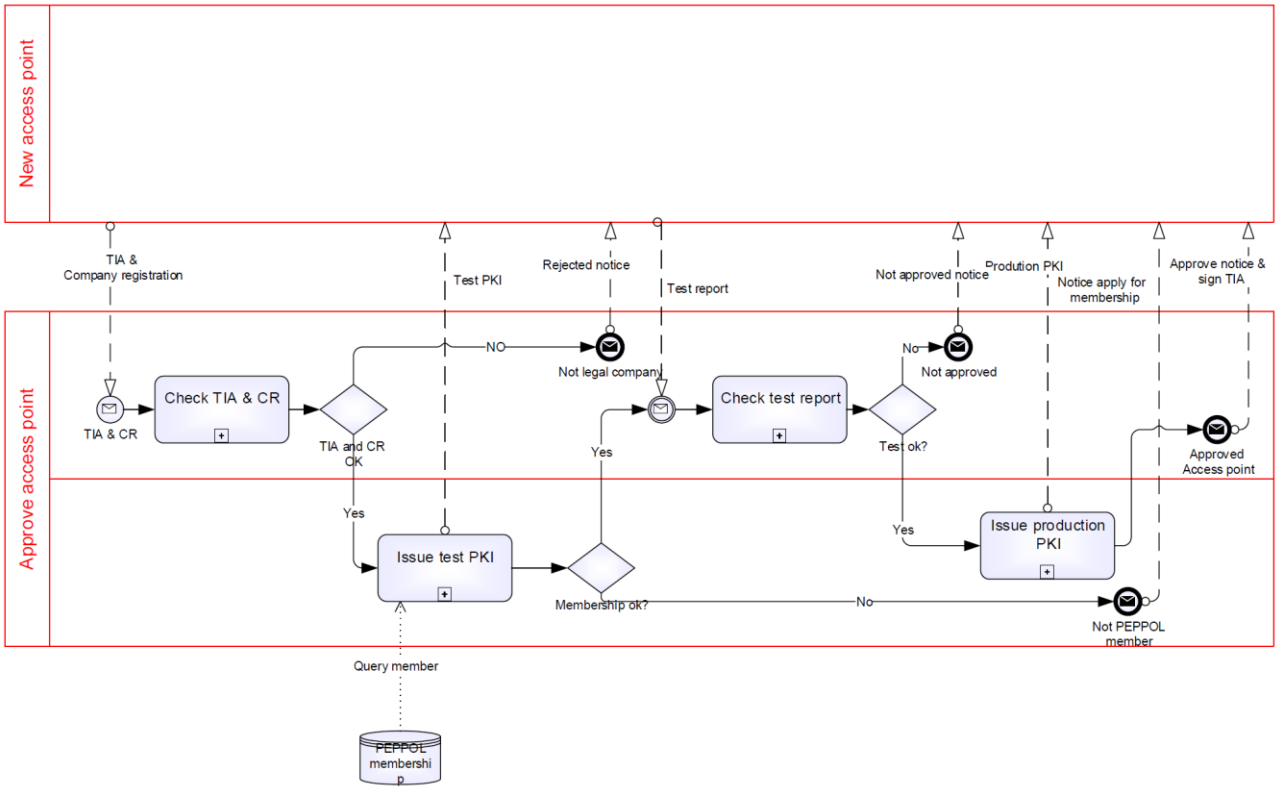
Please find below the steps that an organisation must follow to become a PEPPOL Access Point (AP) provider:

1. Become an OpenPEPPOL member.
2. Sign the PEPPOL Transport Infrastructure Agreements (TIA) for Access Point providers with the PEPPOL Authority of your choice.
3. Send us a copy of your company registration document.

The chosen PEPPOL Authority will then review the submitted documentation and inform you accordingly. Once the membership has been approved by the OpenPEPPOL Managing Committee and the PEPPOL TIA are completed correctly, you will receive access to a site where the Access Point can generate PKI Pilot/test certificate from the PEPPOL Certification Authority.

4. Implement the PEPPOL technical specifications. You can use the sample implementations available on our website, decide to build your own, or purchase a software solution.
5. Carry out testing activities for self-conformance and accreditation, using the available tools.

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 organisation will be included in the online list of OpenPEPPOL members.

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.

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. 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 PEPPOL specifications, based on the OpenPEPPOL Migration Policy.

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.

Since September 1st, 2014, the use of the AS2 transport protocol and the SBDH message wrapper became mandatory.

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 provided by OpenPEPPOL 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.

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

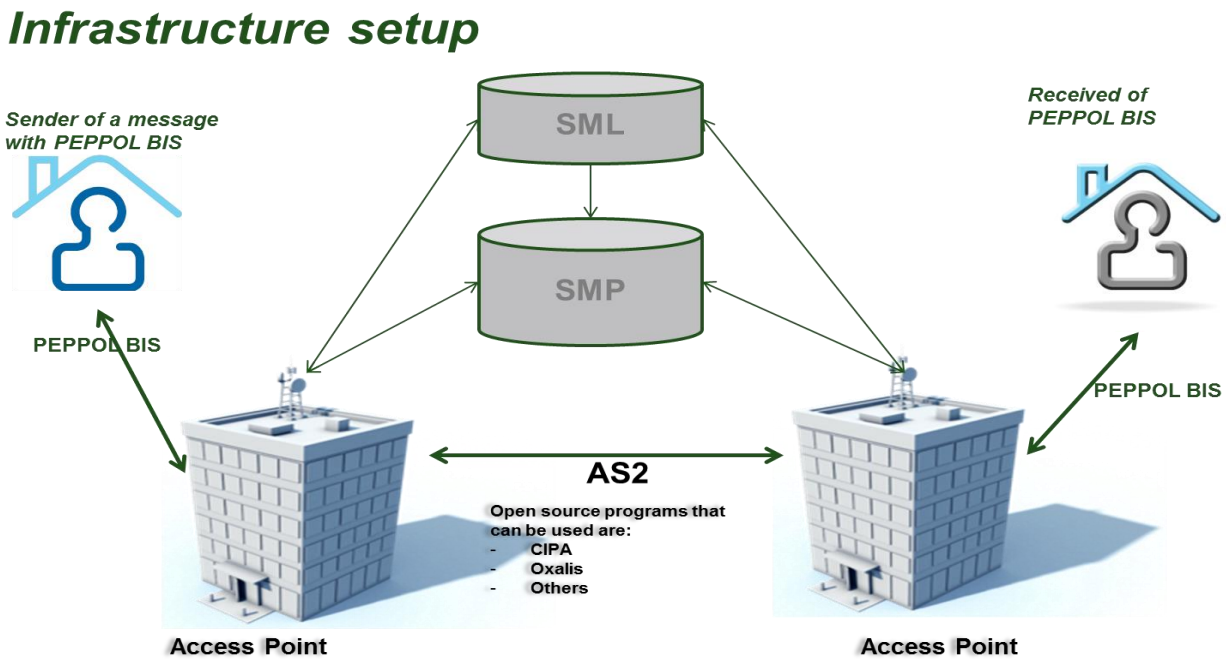
Sample Implementations of the PEPPOL eDelivery Network are provided on our website at '[Links to Software for PEPPOL Implementations]'. In particular:

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 Post-Award 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 became mandatory from September 1st, 2014. You can implement one or more PEPPOL BIS in your IT system, following a modular approach, based on your needs and requirements. The current PEPPOL BIS are:

PEPPOL BIS 1A Catalogue Only
PEPPOL BIS 3A Order Only
PEPPOL BIS 4A Invoice
PEPPOL BIS 5A Billing
PEPPOL BIS 28A Ordering
PEPPOL BIS 30A Despatch Advice
PEPPOL BIS 36A Message Level Response

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.

Pre-requisites

1) Contact your PEPPOL Authority to request a test.
2) Your PEPPOL Authority will contact Difi to initiate test procedures by sending an email to AP@Difi.no .
3) Once you have received and created a TEST Certificate, you can start using the tools provided by Difi, which supports testing of PEPPOL BIS v2 and other document formats used in Norway. Oxalis is the most common Access Point sample implementation used in Norway. For testing purposes, Difi will be the receiving organisation to which your Access Point will send PEPPOL BIS documents.

Details:

- Difi's Identifier: 9908:810418052
- Results: https://test-aksesspunkt.difi.no/inbound/
- Access Point software: Oxalis (latest version)
- Supported documents: http://test.vefa.difi.no/smp/9908/810418052

4) The test will include:
    a. Verification of certificates (both PEPPOL and 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.

5) Once you have completed the testing activities, please fill in the Testing Results template and send it to your PEPPOL Authority for review.

5) Self-Conformance

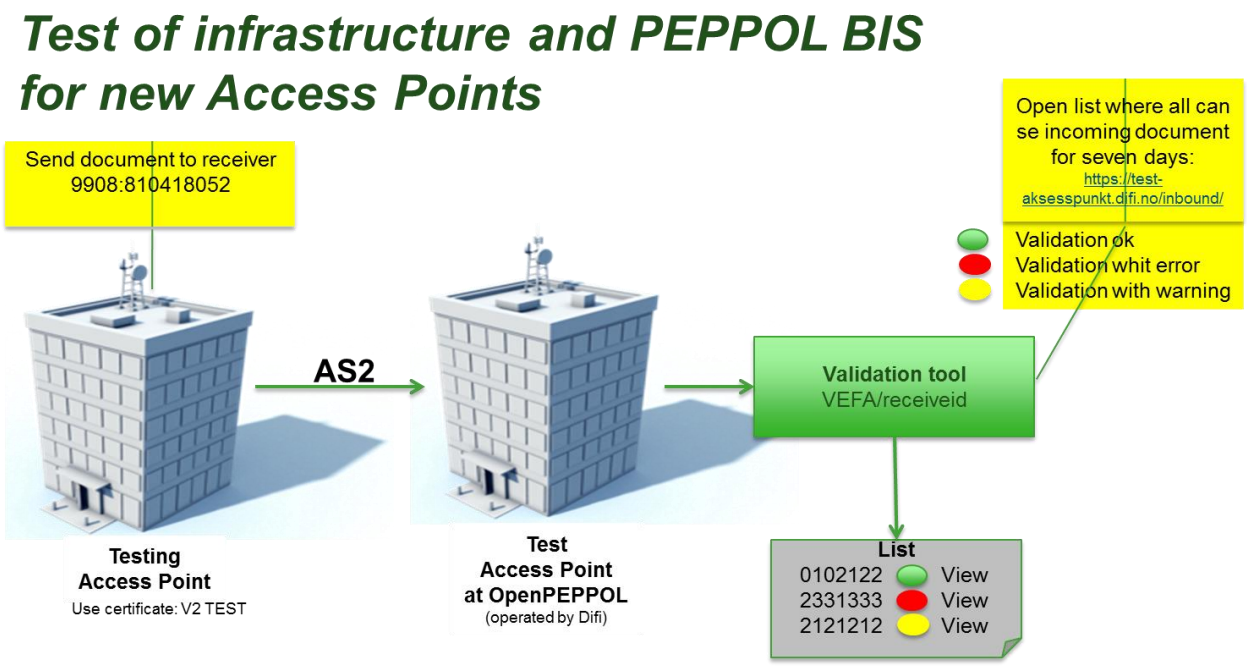
Once your PEPPOL Authority has reviewed the results of your testing activities, if successful, your organisation can move forward with self-conformance activities by:

1) Contacting your PEPPOL Authority to request an OpenPEPPOL Production PKI Certificate
2) Start using the Production PKI Certificate

Difi supports testing activities for Access Point providers using OpenPEPPOL PKI Production certificates, using the lookup functionalities of the PEPPOL SML (Service Metadata Locator). For initial testing purposes, Difi will be the receiving organisation to which your Access Point will send the PEPPOL BIS documents.

Details:

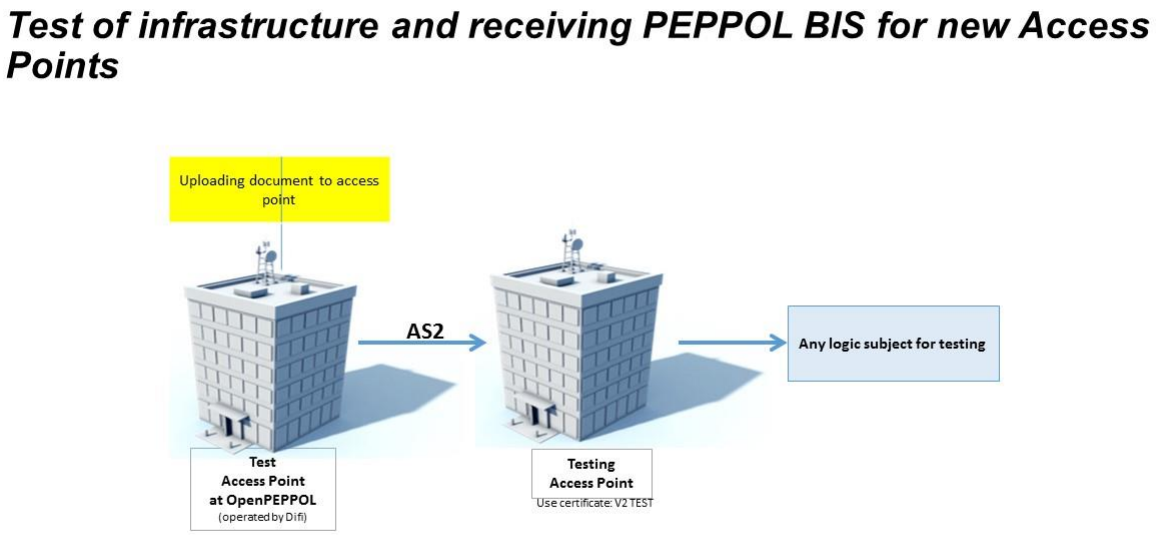
- Difi's Identifier: 9908:810418052
- Results: https://aksesspunkt.difi.no/inbound/
- AP software: Oxalis (latest stable version)
- Supported documents: http://vefa.difi.no/smp/9908/810418052



Validation Requirements

As a sending Access Point provider, you **must** ensure that the business documents received 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 such services on behalf of your customers, or by ensuring that your customers have performed such validation.

Test receiving PEPPOL BIS



As a receiving Access Point provider, you must send an email to ap@difi.no to receive information on how to send documents from the Difi testing access.

When you have received the document, it must be validated so it is a valid instance, according to the applicable rules, before accepting it.

6) OpenPEPPOL Accreditation

Contact OpenPEPPOL to receive an “OpenPEPPOL Certified Access Point” logo, for use on your website and in your marketing documents.