



PKI Certificate Migration

Jesper Larsen, Technical Support Lead (Operating Office)
Mike Aksamit, Expert (Operating Office)

OpenPEPPOL AISBL, Belgium

The migration in general

- ▶▶ Migration from PKI Version 2 to PKI version 3
 - ▶▶ Introducing new Root CAs supporting SHA256
 - ▶▶ Moving the signing responsibility from DIGST to OpenPEPPOL AISBL
 - ▶▶ New CN Structure to identify the certificates to ease maintainability of the certificate issuing
(Issue)
 - ▶▶ Currently not possible to match a certificate ID to an Access Point (work in progress)

Migration Plan

- ▶▶ **C1 = 2018-04-16 00:00:00** = Issuing of new v3 certs begins
- ▶▶ **T1 = 2018-09-03 00:00:00** = All must support both PKI versions for sending and receiving
- ▶▶ **C2 = 2018-10-31 23:59:59** = All APs and SMPs should have enrolled for their PKI v3 certificate
- ▶▶ **T2 = 2018-11-30 23:59:59** = All APs and SMPs must ONLY exchange using the v3 certificates

The enrolling process

- ▶▶ Make a ticket in the service desk
- ▶▶ OpenPEPPOL operations will review membership status
- ▶▶ Ticket is moved for PA approval
- ▶▶ PA approves for enrolment and Operations enrol the cert and send SMS Passcode
- ▶▶ 10 days pickup

Status today

- ▶▶ **68 Access Points haven't enrolled their v3 PKI**
- ▶▶ **Actions? (PA involvement and more communication)**
- ▶▶ **By end of November v2 certificates are not supposed to be entrusted anymore!**

Missing PKI v3 requesters

- ▶▶ In doubt if you have requested the PKI v3 certificate contact OpenPEPPOL Operations
- ▶▶ Request here: <https://openpeppol.atlassian.net/servicedesk/customer/portal/1>

Questions

Questions?



OpenPEPPOL Centralized Testbed

Jesper Larsen, Technical Support Lead
Mike Aksamit, PEPPOL expert

OpenPEPPOL AISBL, Belgium

Background, scope and vision

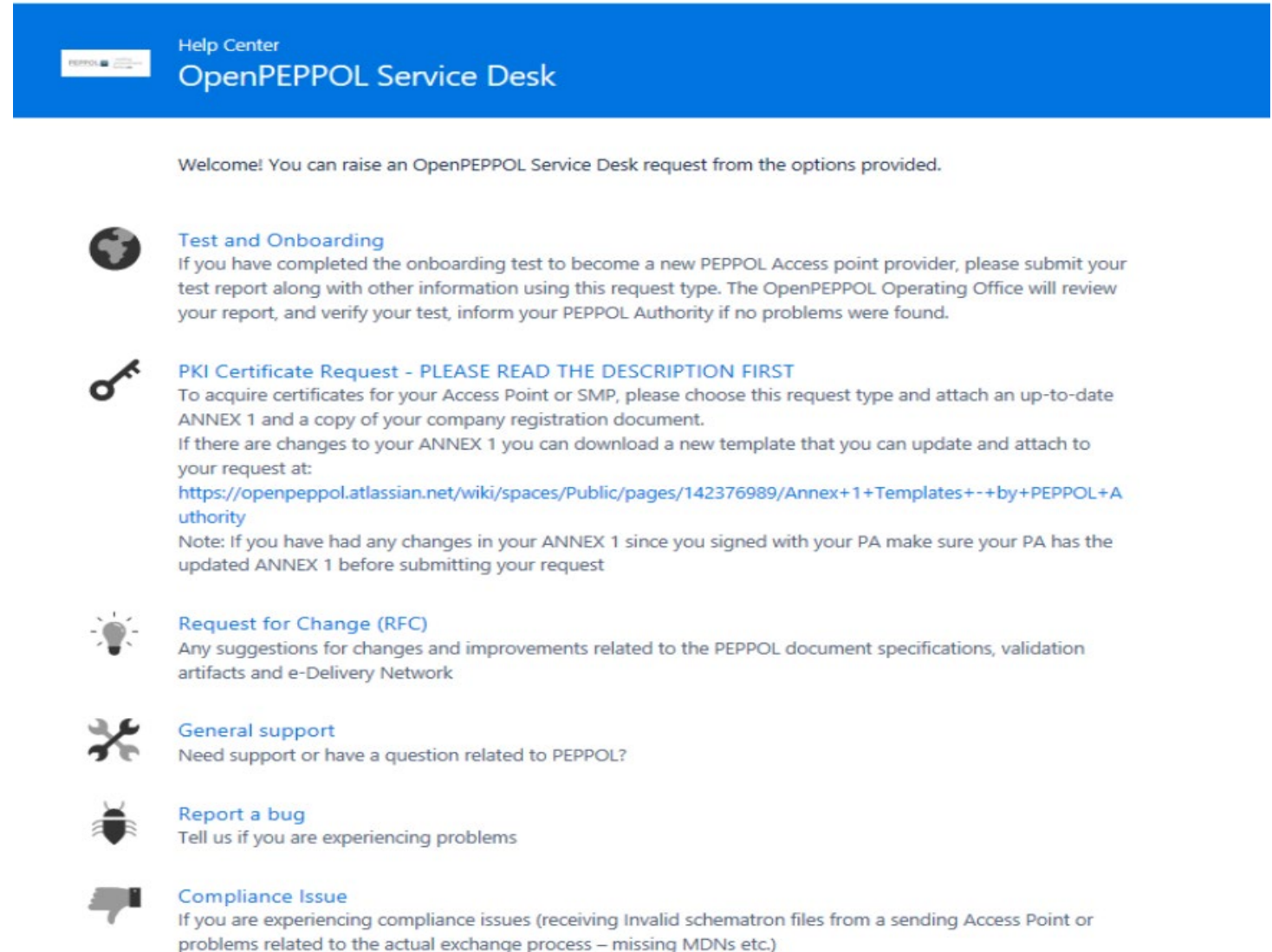
- ▶▶ Test and onboarding responsibility moving from DIFI to OpenPEPPOL
- ▶▶ Testbed as a service for AS2 and AS4 onboarding
- ▶▶ Onboarding will be done with as less human interference as possible. (Self explanatory and intuitive)
- ▶▶ Testbed will be rolled out in phases. Phase one cover the minimum (sending and receiving)

Before testing

- ▶▶ Complete and sign the OpenPEPPOL Membership form and await the formal acceptance email.
- ▶▶ Identify the PEPPOL Authority you wish to sign the Transport Infrastructure Agreement with (your National Authority is recommended) and complete the agreement.
- ▶▶ The PEPPOL Authority will review, approve and advise you to proceed with requesting your Test Access Point (AP) PKI Certificate request.
- ▶▶ Study the relevant PEPPOL eDelivery Network specifications. Create an understanding of the PEPPOL architecture
- ▶▶ Implement a conformant PEPPOL AP implementation (OpenSource, Hosted or build your own)

The PEPPOL Service Desk

- ▶▶ When your AP infrastructure is ready, you can request your Test AP PKI certificate through the OpenPEPPOL Service Desk.
- ▶▶ Upon approval from your PEPPOL Authority, your PKI certificate will be issued.
- ▶▶ The PKI certificate must be installed in your browser before initiating the Acceptance Test through the Centralised Test Facility.



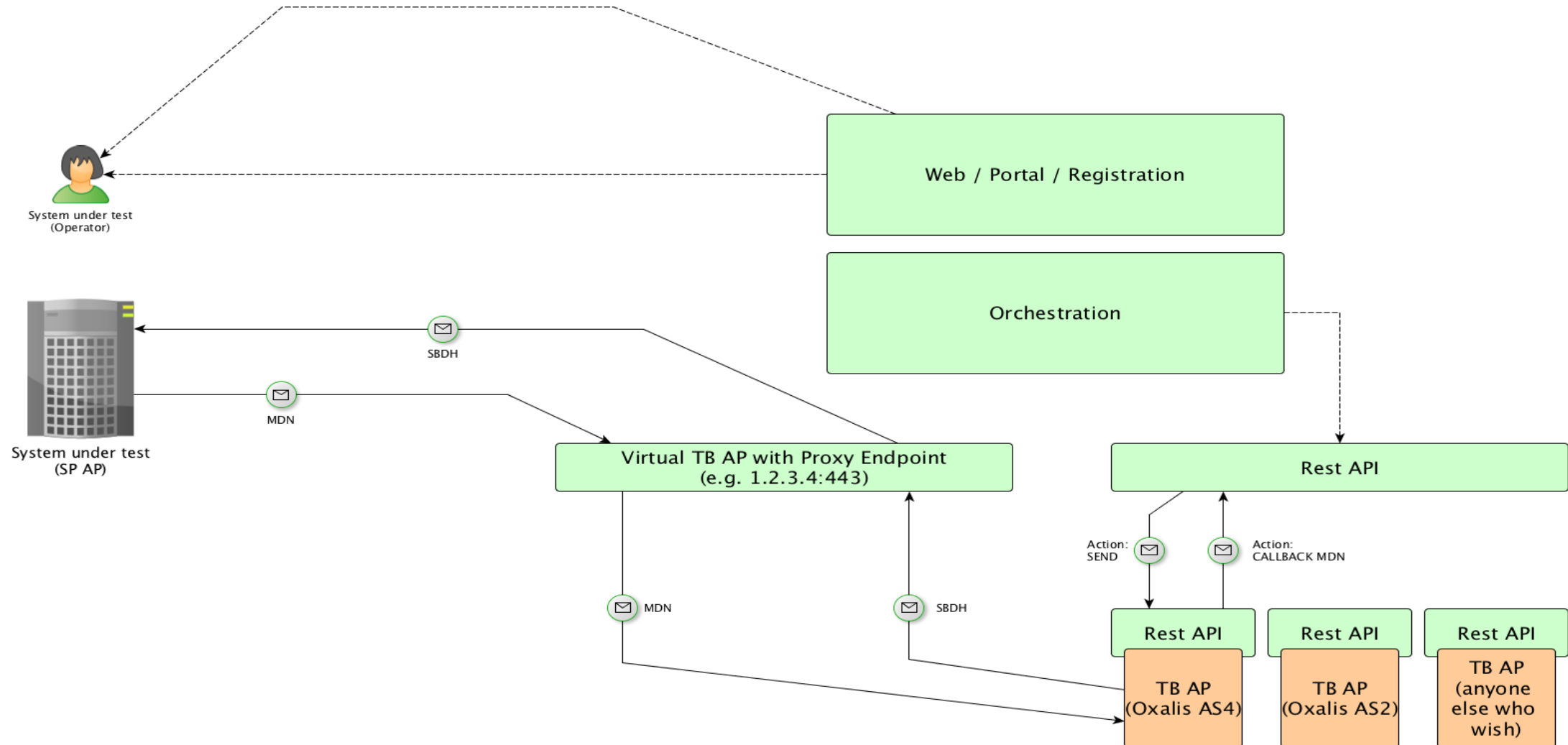
The screenshot shows the 'Help Center' for the 'OpenPEPPOL Service Desk'. It features a blue header with the PEPPOL logo and the text 'Help Center OpenPEPPOL Service Desk'. Below the header, a welcome message states: 'Welcome! You can raise an OpenPEPPOL Service Desk request from the options provided.' The main content area lists several request types, each with an icon and a brief description:

- Test and Onboarding** (Globe icon): If you have completed the onboarding test to become a new PEPPOL Access point provider, please submit your test report along with other information using this request type. The OpenPEPPOL Operating Office will review your report, and verify your test, inform your PEPPOL Authority if no problems were found.
- PKI Certificate Request - PLEASE READ THE DESCRIPTION FIRST** (Key icon): To acquire certificates for your Access Point or SMP, please choose this request type and attach an up-to-date ANNEX 1 and a copy of your company registration document. If there are changes to your ANNEX 1 you can download a new template that you can update and attach to your request at: <https://openpeppol.atlassian.net/wiki/spaces/Public/pages/142376989/Annex+1+Templates+-+by+PEPPOL+Authority>. Note: If you have had any changes in your ANNEX 1 since you signed with your PA make sure your PA has the updated ANNEX 1 before submitting your request.
- Request for Change (RFC)** (Lightbulb icon): Any suggestions for changes and improvements related to the PEPPOL document specifications, validation artifacts and e-Delivery Network.
- General support** (Wrench and screwdriver icon): Need support or have a question related to PEPPOL?
- Report a bug** (Bug icon): Tell us if you are experiencing problems.
- Compliance Issue** (Downward pointing hand icon): If you are experiencing compliance issues (receiving Invalid schematron files from a sending Access Point or problems related to the actual exchange process – missing MDNs etc.)

Pre-requisites for Onboard Testing

- ▶▶ The testing AP must use “**acc.edelivery.tech.ec.europa.eu**” as the SMK (test SML). Please consult the documentation for the access point software you are using.
- ▶▶ The AP **MUST** implement HTTPS with certificate chains to certificate authorities which are trusted by the PEPPOL community. OpenPEPPOL trusts Microsoft and Oracle CAs.
- ▶▶ You must have an SSL quality grade A (can be tested online and will be verified by OpenPEPPOL)
- ▶▶ The AP URL **MUST** use the default port 443.

Testbed architecture



Centralized testbed phase 1

DEMO

<https://testbed.peppol.eu/secure/suite/view>

Testing your Access Point 3

OpenPEPPOL TestBed Report

Test suite details

- AP Certificate: POP000055
- Test suite: [id=1] Conformance/onboarding test suite. Version 1.0
- Profile: AS2
- Endpoint: <http://www.example.com/as2>
- Receiver: 0088:1122334455 (GLN)
- Completed: Oct 04 2018 19:16:02 CEST

Completed test cases

Case	Direction	Type	Status	Completed	Audit
Testbed sends to testing AP	OUTBOUND	POSITIVE	COMPLETED	Oct 04 2018 19:15:35 CEST	1:1
Testing AP sends back to Testbed	INBOUND	POSITIVE	COMPLETED	Oct 04 2018 19:15:49 CEST	1:2
Testbed sends large file to testing AP	OUTBOUND	POSITIVE	COMPLETED	Oct 04 2018 19:15:52 CEST	1:3
Testing AP sends large file back to Testbed	INBOUND	POSITIVE	COMPLETED	Oct 04 2018 19:16:02 CEST	1:4

Welcome! You can raise an OpenPEPPOL Service Desk request from the options provided.



Test and Onboarding

If you have completed the onboarding test to become a new PEPPOL Access point provider, please submit your test report along with other information using this request type. The OpenPEPPOL Operating Office will review your report, and verify your test, inform your PEPPOL Authority if no problems were found.



PKI Certificate Request - PLEASE READ THE DESCRIPTION FIRST

To acquire certificates for your Access Point or SMP, please choose this request type and attach an up-to-date ANNEX 1 and a copy of your company registration document.

If there are changes to your ANNEX 1 you can download a new template that you can update and attach to your request at:

<https://openpeppol.atlassian.net/wiki/spaces/Public/pages/142376989/Annex+1+Templates+-+by+PEPPOL+Authority>

Note: If you have had any changes in your ANNEX 1 since you signed with your PA make sure your PA has the updated ANNEX 1 before submitting your request



Request for Change (RFC)

Any suggestions for changes and improvements related to the PEPPOL document specifications, validation artifacts and e-Delivery Network



General support

Need support or have a question related to PEPPOL?



Report a bug

Tell us if you are experiencing problems



Compliance Issue

If you are experiencing compliance issues (receiving Invalid schematron files from a sending Access Point or problems related to the actual exchange process – missing MDNs etc.)

OpenPEPPOL Accreditation

- ▶ Once you have successfully completed Acceptance Testing, your company name and external contact details will be added to the Certified Access Point listing on the OpenPEPPOL website.
- ▶ OpenPEPPOL will issue a Certified Access Point logo to be used on your website, marketing materials, etc.



Next phase – brainstorming

- ▶▶ Several testcases (negative)
- ▶▶ Several underlying AP implementations
- ▶▶ SMP onboarding test
- ▶▶ Document layer testing
- ▶▶ Multiple choice PEPPOL quiz (mini exam). Can only be passed if specs are read!!

Useful Links

PEPPOL Website: www.peppol.eu

PEPPOL Service Desk:

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

eDelivery Network specifications: <https://peppol.eu/downloads/the-peppol-edelivery-network-specifications/>

Post-Award BIS specifications: <https://peppol.eu/downloads/post-award/>

PEPPOL Directory: <http://directory.peppol.eu/public>

Questions

Questions?



Get involved

- PEPPOL members are invited to join any of the following:
- eDelivery Coordinating Community
- Post-Award Coordinating Community
- Pre-Award Coordinating Community
- Any number of active work groups