Peppol CNAME to NAPTR Migration Process

V 1.0.0

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

info@peppol.eu
www.peppol.org
Last updated: 17.04.2025

Contents

1 Introduction 3
2 Summary of Changes 3
2.1 Changes to Peppol Policy for use of Identifiers....3
2.1.1 Changes to POLICY 1 3
2.1.2 Changes to POLICY 7 3
2.2 Changes to Peppol Service Metadata Locator specification 4
2.2.1 Chapter 2.1 4
2.2.2 Chapter 2.1.1 4
2.2.3 Chapter 3.1.1 5
2.2.4 Other Changes 5
2.3 Changes to Peppol Service Metadata Publisher specification 5
2.3.1 Chapter 5 5
2.3.2 Other Changes 6
3 Intended Impact for different Actors 6
3.1 Peppol SMP Providers 6
3.2 Peppol AP Providers 7
3.3 OpenPeppol Operating Office 8
3.4 SML Operator 9
3.5 Third-party API users 9
4 Migration Plan 9
4.1 Peppol SMP Providers 10
4.2 Peppol AP Providers 11
4.3 OpenPeppol Operating Office 12
4.4 SML Operator 13
4.5 Third-party API users 13

1 Introduction

This document is a guideline to support implementing the changes described and defined by the following approved specification changes:

- Peppol Policy for use of Identifiers v4.4.0 updating v4.3.0
- Peppol Service Metadata Locator v1.3.0 updating v1.2.0
- Peppol Service Metadata Publishing v1.4.0 updating v1.3.0

The target audience of this document are primarily Peppol Service Providers, as they are directly impacted by the changes. Additionally, Peppol Authorities and Software vendors might scan through this document to better support Peppol Service Providers in implementing the changes.

2 Summary of Changes

This section contains a summary of the changes, grouped by specification documents.

2.1 Changes to Peppol Policy for use of Identifiers

2.1.1 Changes to POLICY 1

The **maximum length** of Participant Identifiers and Party Identifiers was **increased from 50 to 130** characters.

Additionally, it was clarified that the identifier length excludes the numerical identifier scheme.

Example: `iso6523-actorid-upis::9930:de162463073`

The change affects solely the green part of the above Identifier. Other parts of the Identifier are not impacted.

This change is not directly related to the CNAME to NAPTR changes but primarily focuses on French participant identifier requirements.

2.1.2 Changes to POLICY 7

The algorithm used to lookup Peppol Participants in the DNS was adopted.

The old algorithm looks like this (in pseudo code):

```
"B-"+hexstring(md5(lowercase(ID-VALUE)))+"."+ID-SCHEME+"."+SML-ZONE-NAME
```

The new algorithm looks like this (in pseudo code):

```
strip-trailing(base32(sha256(lowercase(ID-VALUE))),"=")+"."+ID-SCHEME+"."+SML-ZONE-NAME
```

The most important thing is, that the required parameters have not changed between the old and the new algorithm.

Example for Participant Identifier `iso6523-actorid-upis::0088:123abc` on the production SML:

- Old algorithm creates:
  - B-f5e78500450d37de5aabe6648ac3bb70.iso6523-actorid-upis.edelivery.tech.ec.europa.eu
- New algorithm creates:
  - Y7DZFXAF3D4CJZ4KCGRXTEC6TWVCGA4KY7ZWA5BOIF6MSWD4TDRQ.iso6523-actorid-upis.edelivery.tech.ec.europa.eu

As shown, the ID-SCHEME (in red) and SML-ZONE-NAME (in blue) are unchanged.

Note: All parts of URL domain names are case insensitive.

Note: This particular change only refers to the domain name algorithm but makes no statement on the DNS record type to query.

2.2 Changes to Peppol Service Metadata Locator specification

This section covers the relevant changes to the Peppol SML specification.

2.2.1 Chapter 2.1

The overall flow how SMP URLs are determined, was updated to include the specific DNS NAPTR lookup as an extra step.

2.2.2 Chapter 2.1.1

This chapter was added to add special constraints that apply to all SMP URLs.

- use only the “https” URL scheme
  - This is in line with the general requirement to enforce the usage of HTTPS
- NOT use username and/or password in the domain authority section
  - This should prevent URLs that require authentication
  - Example restricted SMP URLs are:
    - `https://user@pw:smp.example.org`
- NOT include query or fragment parts, in addition to the domain authority and path parts
  - This should prevent URLs that cannot be used as a prefix for SMP querying
  - Example restricted SMP URLs are:
    - `https://smp.example.org/smp?param=value`
    - `https://smp.example.org/smp#anchor`

Valid intended URLs according to the rules are e.g.

- `https://smp.example.org`
- `https://smp.example.org/`
- `https://server.example.org/smp`
- `https://server.example.org/smp/`
- `https://server.very.complex.example.org/path/to/my/smp`

2.2.3 Chapter 3.1.1

References the new lookup algorithm for DNS Lookup URLs (see Policy for use of Identifiers POLICY 7 changes described in section 2.1.2)

2.2.4 Other Changes

- The links to the bibliographic references were updated (only editorial)
- All occurrences of “BUSDOX” were removed (only editorial)
- The WSDL files were removed from the appendix, as they are published separately on https://docs.peppol.eu/edelivery

It is important to note, that the data model does not change. The interface between SMP and SML does not change either.

2.3 Changes to Peppol Service Metadata Publisher specification

This section covers the relevant changes to the Peppol SMP specification.

2.3.1 Chapter 5

This chapter contains the primary changes to this specification:

- Requirement to operate an SMP only using the scheme “https” and not anymore via “http”.
  - This is a breaking change
  - This implies, that servers running a Peppol SMP also need a TLS certificate
- Requirement to operate an SMP only using port 443 and not anymore on port 80.
  - This is a breaking change and consistent to the change in URL scheme
- The limitation to operate the SMP in the root path (“/”) was replaced with the possibility to choose an arbitrary URL path in combination with the domain.
  - This is an opportunity to better fit SMP deployments in common infrastructure patterns

Note: According to RFC 2616 (HTTP/1.1) there is no hard limit for URL lengths, so none was imposed in the specification. If this will lead to operational problems, OpenPeppol may limit the maximum allowed path length in a later version of the specification.

2.3.2 Other Changes

- The textual descriptions and diagrams were updated to use “U-NAPTR” instead of “CNAME”
- Links to references were updated (only editorial)
- All occurrences of “BUSDOX” were removed (only editorial)
- It is important to note, that the data model does not change. The interfaces between SMP and SML as well as Peppol Directory does not change either.

3 Intended Impact for different Actors

This section tries to summarize the anticipated changes foreseen for different actors in the Peppol Network. This section only focuses on the activities but does not make statements about the timing of implementation. The migration plan with the dates and durations can be found in chapter 4.

3.1 Peppol SMP Providers

The following list of activities is specific to Peppol SMP Providers. Please also refer to specific migration guidelines of your SMP solution provider.

- Prepare to handle longer Participant Identifier Values. This could imply enlengthening fields in a database schema as well as adopting local validation rules when dealing with Participant Identifier Values. The usage of longer Participant Identifier Values needs coordination, as it requires sender and receiver to be capable of dealing with it.
- Prepare the operations of the SMP solution to be operated via https:
  - This requires a TLS certificate for the domain the SMP is operated on. This may be a TLS wildcard certificate (e.g. for the domain `*.example.org`). The Peppol Policy for Transport Security applies here. Please note, that the Peppol SMP certificate CAN NOT be used as a TLS certificate.
  - It is possible to run the AP and the SMP on the same domain, if they are accessible through different paths (e.g. `/smp` and `/ap`). In this case they can share the same TLS certificate.
  - During some part of the migration, an SMP may be operated using the http and the https protocol in parallel.
  - Make sure that inbound firewall rules allow traffic on TCP port 443 for protocol https from all IP addresses.
- Once the hosting using the http protocol is turned off the following things need to be considered:

- The specific server aliases for the dynamic host names in reverse proxy configurations should be deleted (e.g. nginx configuration `server_name *.acc.edelivery.tech.ec.europa.eu;`)
- The reverse proxy configuration should be adopted, so that only https access is allowed
- Specific reverse proxy configuration that was necessary for the previous setup (e.g. running specific parts of the SMP under https) should be removed to ensure no unwanted insecure access remains possible
- At the right point in time during the migration, the SMP must update its registration at the SMK/SML, so that it is registered with the https URL instead of the http URL. If a query base path is used, it must be part of this registration call (see below). This refers to the SOAP call of method `update` on service `ManageServiceMetadata` in the SMP to SMK/SML interface.

The following activities are considered best practices for using the new possibilities provided by the updated specifications:

- Configure your SMP solution to be accessed in a server-relative path instead of the root (`/`) directory. This makes sure that multiple applications can easily be solved on the same host name.
- Additionally, SMP solutions might now define base URIs for querying only (as in e.g. `/smpquery`). This allows for a clear separation of URLs between the standardised querying APIs and the implementation specific other APIs. It also allows to easily limit access to only the mandatory APIs (as in “allow TCP port 443 from all hosts via HTTP GET on path /smpquery/*”). If this path is part of the SMP registration (see above) it can be used as the baseline for all standardised queries:
  - Example: register an SMP with the URL `http://smp.example.org/smpquery` at the SMK/SML. Querying all document types of a participant would be done using this URL `http://smp.example.org/smpquery/{ppid}` and the URL for querying the service metadata of the participant for a specific document type would be `http://smp.example.org/smpquery/{ppid}/service/{doctype}`
  - This would also apply for the standardised Business Card query: `http://smp.example.org/smpquery/businesscard/{ppid}`

Note: Don’t forget that Port 80 (http) is still needed to download CRL (Certificate Revocation Lists) or to access the OCSP server of Peppol X.509 certificates.

3.2 Peppol AP Providers

The following list of activities is specific to Peppol AP Providers. Please also refer to specific migration guidelines of your AP and/or AS4 solution provider.

- Prepare to handle longer Participant Identifier Values. This could imply enlengthening fields in a database schema as well as adopting local validation rules when dealing with Participant Identifier Values. The usage of longer Participant Identifier Values needs coordination, as it requires sender and receiver to be capable of dealing with it.
    - Please remember to test the usage of longer Participant Identifier Values in all processing steps, including at least: Document validation, SMP lookup, SBDH creation and Document transmission
- Prepare to use the U-NAPTR based SMP URL resolution instead of the CNAME based SMP URL resolution. This is one of the few activities that may be initiated very early in the migration process.
    - Note: initially, the resulting SMP URL MUST still be using the http protocol. Any SMP returning a URL using the https protocol is non-compliant.
- Later in the process, a Peppol AP must be able to deal with SMPs that are operated using the https protocol. This includes, but is not limited to, the following considerations:
    - Make sure that any check on the “http” protocol as well as on the usage of port 80 is adopted accordingly. During a migration phase it will be required to handle http and https in parallel.
    - Use a TLS trust store like the one used for AP-to-AP communication
    - Note: No additional firewall rules are needed, as APs already need to open TCP port 443 to any IP address.
    - Note: Don’t close the firewall for http port 80 too early, as it depends on the availability of all other SMPs under https.
    - Note: Don’t forget that Port 80 (http) is still needed to download CRL (Certificate Revocation Lists) or to access the Peppol-required OCSP server.

3.3 OpenPeppol Operating Office

The following list contains the high-level activities where the Operating Office will support the migration.

- Testbed
    - Adopt test cases for the new Participant Identifier Value maximum length
    - Adopt test cases that ensure the new DNS name algorithm is implemented correctly (String based, not exchanged based)
    - Adopt test cases that ensure that the lookup via U-NAPTR DNS records works as expected
- Peppol Directory

- Must be updated to support the new Participant Identifier Value maximum length
- Must be updated to support the new lookup algorithm

- All the changes for SMP and AP providers apply accordingly for the SMPs and APs operated by the OO
- The Service Desk will of course answer specific questions to the changed specifications and this migration document

3.4 SML Operator

The following list contains the high-level activities that the SML Operator needs to perform. This applies to SMK and SML in the same way.

- After the migration was performed, the existing CNAME entries may be removed from the DNS domains. This is the primary goal.
- After the migration, the SML implementation may be simplified by removing the code that creates, updates and deletes CNAME and U-NAPTR records in parallel.
- Note: The SML implementation already today creates both CNAME and U-NAPTR records in parallel, that's why there is no activity needed in this area.
- Note: The SML implementation already supports Participant Identifier Values with the new length, so no changes are needed.

3.5 Third-party API users

The following list contains the high-level activities required by third-party tools that use or access the Peppol Network interfaces and APIs:

- SMP accessors
  - See section 3.2 on Peppol AP Provider above
- Peppol Directory accessors
  - No changes are envisioned in this migration

4 Migration Plan

This section contains the overall migration plan for the changes described in this document.

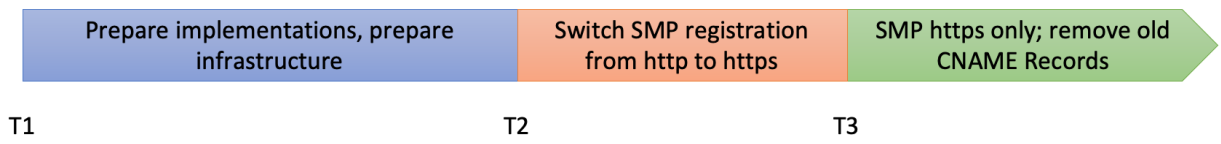

Figure 1: Overall Migration Plan

This migration contains the following milestones:

- T1: Start point (May 1st, 2025)
- T2: T1 plus 6 months (implementation time) (November 1st, 2025)
- T3: T2 plus 3 months (change time) (February 1st, 2026)

The primary activities for Peppol SMP Providers and Peppol AP Providers are outlined in respective subsections below.

The main action items for the duration between the milestones are as follows:

- Between T1 and T2:
  - Implement SMP and AP changes
  - Prepare SMP infrastructure changes
- Between T2 and T3:
  - Switch SMP operations from http to https
- After T3
  - Clean up old DNS entries

4.1 Peppol SMP Providers

This section contains all the activities for Peppol SMP Providers during this migration in context with the timeline:

- Participant Identifier Values with new maximum length
  - Before T2: implement the changes
  - From T2 onwards: the new values must be usable in production (for querying and registration)
- Change SMP operations from http to https
  - Before T2: prepare the changes
    - make sure your SMP implementation can run on https
    - organize a TLS certificate
    - prepare the https configuration
    - decide on the new query base URL
    - eventually test the migration in the Peppol Test Network
  - Between T2 and T3: swap from http to https in production by
    - enabling the https configuration
    - make sure SMP inbound firewalls are open on TCP port 443

- updating the SMP base URL with the SMK/SML.
  IMPORTANT: if you have an SMP installation with more than 10000 (ten thousand) Service Groups, please align individually with the SML Operator via email (EC-EDELIVERY-SUPPORT@ec.europa.eu). The reason for this is, that the NAPTR structure does not have the “publisher” in-between domain name which means that each participant record needs to be updated separately. In combination with DNSSEC this would create too much load on the SMK/SML.
- and afterwards removing the http support from the configuration. This also means, that an SMP MAY run on http and https in parallel for a limited amount of time.

- From T3 onwards: all SMPs MUST run solely on https (and no longer on http)

4.2 Peppol AP Providers

This section contains all the activities for Peppol SMP Providers during this migration in context with the timeline:

- Participant Identifier Values with new maximum length
  - Before T2: implement the changes
  - From T2 onwards: the new values must be usable in production
- Use DNS U-NAPTR record to find the SMP base URL
  - From T1: start implementing these changes from T1 onwards to ensure the DNS U-NAPTR lookup is used before T2. The SML already today creates the necessary DNS records
  - From T2: all SMP lookups MUST use the U-NAPTR based lookup, because using CNAME records does not allow to properly differentiate between http and https registrations. From this point on, the lookup via CNAME is forbidden.
- Change SMP lookup from http to https
  - Before T2:
    - All SMP lookups MUST result in http URLs. The usage of https URLs is still forbidden before that milestone
    - Implement the code changes, that SMP connections may use https as well as http and https in parallel
    - Eventually test the lookup in the Peppol Test Network
  - Between T2 and T3:

        - An SMP lookup may result in an http or an https URL – the AP must be able to deal with both protocols in parallel
    - From T3 onwards:
        - An SMP lookup must result in an https URL
        - It is recommended (but not mandated), that APs stay resilient and accept http URLs for at least 6 months afterwards

4.3 OpenPeppol Operating Office

This section contains all the activities for the Peppol Operating Office during this migration in context with the timeline:

- Peppol Directory
    - Participant Identifier Values with new maximum length
        - Before T2: implement the changes
        - From T2 onwards: the new values must be usable in production (for querying and registration)
    - Use DNS U-NAPTR record to find the SMP base URL
        - Same as for Peppol AP Provider (see section 4.2)
    - Change SMP lookup from http to https
        - Same as for Peppol AP Provider (see section 4.2)
- Peppol Testbed
    - Implement a new Test Suite
        - Before T2: the new Test Suite should be implemented and in production
    - Participant Identifier Values with new maximum length
        - Before T2: implement the changes
        - From T2 onwards: the new values must be usable in production (for querying and test suite creation)
    - Use DNS U-NAPTR record to find the SMP base URL
        - Same as for Peppol AP Provider (see section 4.2)
    - Change SMP lookup from http to https
        - Same as for Peppol AP Provider (see section 4.2)
- OpenPeppol APs
    - Same as for Peppol AP Provider (see section 4.2)
- OpenPeppol SMPs

- Same as for Peppol SMP Provider (see section 4.24.1)

4.4 SML Operator

This section contains all the activities for the SML Operator during this migration in context with the timeline:

- Participant Identifier Values with new maximum length
  - No action needed
- Create registrations with CNAME and U-NAPTR records in parallel
  - Before T3:
    - Continue to register each Service Group using both record types
    - Prepare the coding changes to remove the parallel DNS record creation
  - From T3 onwards:
    - Coordinate with the Peppol Operating Office on a timeline to stop creating both DNS record types in parallel as well as to remove all Peppol-CNAME records
- Create a replacement for the DNS “publisher” record that works with U-NAPTR
  - Note: this is an informal recommendation and up to the SML Operator

4.5 Third-party API users

Third-party API users should refer to the respective sections for Peppol SMP Providers (4.1) as well as Peppol AP Providers (4.2).