Nederlandse Peppolautoriteit
Ministerie van Binnenlandse Zaken en Koninkrijksrelaties

NPA best practice

End-user Identification

Version: 2.2

Status: Final

Table of contents

1. Introduction and goal

End-user Identification (EUI) is an important process for the reliability of the Peppol network. If this process is correctly performed, the following risks are greatly reduced:

- Fraud by end-users, where a malicious end-user for example, impersonates a legitimate end-user and sends fraudulent or otherwise malicious messages (as for example spam or malware). The main risk of fraud focusses on end-users who use the Peppol network to send messages.
- Errors by misplaced messages, that are sent to an unintended end-user. The main risk of errors focusses on end-users who use the Peppol network to receive messages and for which errors have been made in end-user Information in a Service Metadata Publisher (SMP). With the introduction of Invoice Response Messages (IRM) and the Message Level Responses (MLR), errors in end-user Information for sending end-users becomes even more relevant.

The goal of this document is to clarify the OpenPeppol regulations and give practical guidelines to Service Providers (SP). The best practice does **not** have any legal status from the OpenPeppol Interoperability framework, SP agreements or Peppol Authority Specific Requirements. The NPA will use a comply or explain approach for subjects in the best practice. SPs can choose to follow this guideline and gain certainty that EUI complies to regulations (if correctly implemented) or choose to implement EUI in another way.

Regulations regarding EUI have been described in the OpenPeppol Internal Regulations. Internal Regulations relevant to EUI for SPs have been included in attachment 1.

Based on SP agreements, SPs need to ensure that there is a contractual relationship (directly or through intermediaries), that includes specific requirements. These requirements have been included in attachment 2.

2. Relying on EUI

SPs need to perform EUI, before granting end-users access to the Peppol network.

When migrating an already registered end-user, the new SP must also execute the EUI process.

In the event of a bulk takeover, for example in the event of the termination of the activities of an SP, where the entire or the regular EUI process cannot be realised by the new SP in such a period and manner that it does not hinder the activities of the end-user, the initial EUI can take place in a more limited manner. The NPA wishes to be informed about this. By limited manner, the NPA means the application of the Chamber of Commerce API or VIES register control for number and name check. Within 6 months, the regular (full) EUI process of the new SP must still be completed.

3. Distinction between sending and receiving

Some SPs currently only have sending or receiving end-users as clients. The risks mitigated by EUI differ for sending and receiving Peppol messages (as described in paragraph 1). However, the NPA will use the same standards for EUI at all SPs, even if these SPs currently only receive invoices (and currently have less risk of fraud from their own end-users).

The reason that no distinction is made between sending and receiving is the OpenPeppol credo “Connect once, connect to all”. Connecting once is only possible if an end-user has full access to the Peppol network after EUI. Also, the scenario that additional checks are performed on end-users, when end-users switch roles (for example starting to send messages after firstly only receiving messages), doesn’t seem feasible and maintainable to the NPA. Finally, the migration of end-users between SPs (as set out in paragraph 2) is not possible if a distinction is made between EUI for sending and receiving end-users.

4. Distinction in implementation processes

A difference between SP solutions is that some offer an online (cloud / off the shelf / portal) solution while others offer software solutions that need to be installed and configured on site.

A general rule for the first type is that EU information is exchanged electronically, there is no personal contact and could even be (partly) free of charge.

A general rule for the second type of solutions is that they require a (relatively long) process of tendering, contracting and implementation. It is also plausible that there is an (extensive) CRM process that also includes aspects like creditworthiness, UBO and company history and -structure investigation.

5. Distinction in level of relation with end-user

Another distinction is that an SP acts directly, or it could act with intermediaries (partners), towards EU. Intermediaries such as (administrative) software suppliers or accounting services. Some SPs offer a solution to send/receive Peppol messages for these intermediaries. The intermediary offers the software to end-users. The SP has no direct contact with the end-users in this case and EUI is carried out by the intermediary.

All EUI conditions must be imposed on the intermediary. The responsibility that EUI is carried out correctly stays with the SP.

At having a relation with an intermediary we ask the SP to:

- request it's intermediary explicit confirmation and acceptance of an EUI working method that at least complies with the requirements set out in the OpenPeppol Internal Regulations;
- ask periodically proof with the intermediary of correct identification and its reassessment;
- do (as a minimum) a yearly (sample) check on the end-user information registered by an intermediary.

6. Proof of ownership

According to the OpenPeppol Internal Regulations, a SP must check if information has been provided by the entity it concerns. The Internal Regulations give no further elaboration on how this is carried out.

A representative from an entity gives information about the entity. Therefore, the goal of proof of ownership is to link a representative to an entity. The representative should be in a position within the entity to (legally) decide to enter the Peppol network.
The ways of linking a representative to an entity, used by SPs and supported by the NPA are as following:

- Bank check. The SP lets the end-user transfer a small payment (e.g. euro 0,01) and checks the entity name in the payment with the entity that the representative presumes to represent. This check confirms that the representative has access to the entities bank account. Following the Instant Payments Regulation European banks check IBAN vs. name of the payee, which makes this an adequate check.
- PSD2. An SP can have the possibility to get access to the bank account information under this EU Directive.
- Checking the name of a representative with legal documents (as an example: signed contract or a signed order) and linking this name to Chamber of Commerce documents. This check confirms that the representative is a legal representative for the entity.
- Electronic Identification. A product that is meant as a safe and reliable mean of login to various services for representatives of companies. As an example the use of eHerkenning provides an adequate link between the representative and the entity.
- Identity provider. A third party that supports the SP with identity verification of the entity.
- In case of an implementation process as described under 4: the information coming from the implementation process in combination with a (pre)payment. This should provide adequate certainty that representatives and the entity are linked. Regularly a signed contract is also available in such an implementation process.

7. Other end-user Information

The OpenPeppol Internal Regulations mention specific end-user information, that a SP needs to know for all end-users (included in attachment 1). Such as: the legal name, legal address, contact

information and identifiers used in the Peppol network. If legal identifiers are associated with different trade names or legal entities within the same organization, associations should be mapped similarly.

We advise to support automated models for checking the correctness of the identifiers: as an example a Netherlands Chamber of Commerce number has 8 positions, an OIN has 20 positions, a VAT-number meets the obliged structure, etc.

8. Periodical check on correctness of end-user information

For all end-user Information, the OpenPeppol Internal Regulations state that these must be collected and verified at the time of enrolment at the Peppol network, but also as it changes. Furthermore, the end-user Information must be checked periodically at least on an annual basis.

Checks can in general be carried out in several ways:

- Automated checks, for example: by retrieving Chamber of Commerce data via an API. This automated check should include a comparison between end-user Information and data retrieved from the source;
- Manual checks, where end-user Information is checked with for example: a Chamber of Commerce extract;
- VIES validation, where, the correctness of a VAT number can be checked (both manually as well as via a batch);
- Payments, is the payment for your services coming from the number registered in the Peppol network;
  and / or is the payment for your services coming from the registered name.

We advise the SP (and it's intermediaries) to, by contract, always ask the end-user to give notice of any changes in relation to the registration / identifiers.

9. End-user contracts

SP agreements specify some requirements that need to be included in contracts between SPs and end-users. These requirements are included in attachment 2. The NPA doesn't expect the literal text to be included in contracts, but expects the meaning of the text to be communicated clearly.

A SP is advised to include the requirements in annexes on end-user (incl. intermediaries) contracts or in terms and conditions.

10. Reasonable effort for retrieving end-user information

The Peppol Internal Regulations state: "Service Providers must verify the above information concerning end-users to which they provide Peppol Services, except in cases when this is not feasible with reasonable efforts."

The NPA expects that all end-user information, as described in this best practice, can be retrieved with reasonable effort.

Attachment 1: End-user identification in Internal Regulations

The Internal Regulations V3.0, as published per December 11th, 2024, include the following components that are relevant to end-user identification for SPs.

3.3 End-user Identification

3.3.1 Information to be Collected

Peppol Service Providers shall ensure that the following information is known for all end-users (senders and receivers) to which they provide Peppol services directly or indirectly through intermediaries. As an exception, Service Providers that offer Capability Lookup Services exclusively are not responsible for end-user identification, unless they have a direct contract with them:

1. Legal identifier of the end-user in the jurisdiction within which it is legally based, and legal identifier Type (e.g., VAT number, company registration number).
    a. The legal identifier has to be active, in jurisdictions when such distinction exists.
    b. In case of end-users that are public organisations and where legal identifiers as such do not exist, other officially issued codes are acceptable.
2. Legal name of the end-user, in the jurisdiction within which it is legally based.
3. Legal address, including as a minimum country and (where applicable) territory information.
4. End-user's capability to receive and/or send Peppol Dataset Types (Document Type ID).
5. All identifiers used in the Peppol Network by the end-user, related only to the Peppol Services which that particular Service Providers offers to them. If these are associated with different trade names or legal entities within the same organization, associations must likewise be mapped.
6. Contact information sufficient for the end-user to be reachable by the Service Provider.
7. Proof of ownership – i.e., that the information has been provided by the entity it concerns.
8. Which intermediaries, if any, intermediate the end-user's access to the Peppol Services. The following information must be known about each intermediary:
    a. Legal identifier of the Intermediary in the jurisdiction within which it is legally based, and legal identifier Type (e.g., VAT number, company registration number).
    b. Legal name of the Intermediary, in the jurisdiction within which it is legally based.
    c. Country and (where applicable) territory where the intermediate is legally based.

Service Providers must verify the above information concerning end-users to which they provide Peppol Services, except in cases when this is not feasible with reasonable efforts. Such cases may include, but are not limited to, the lack of automated means to retrieve or verify end-user information through lookup or API connection to authoritative sources of information in specific jurisdictions. Service Providers may not be held accountable for lack of proactive verification when they can demonstrate that this was not feasible with reasonable effort.

If and when it comes to the attention of a Service Provider that one of their end-users is trading under names different from its legal name, these may be documented. In particular, when the Service Provider becomes aware that different trade names, business units, etc. are associated with different endpoints, this should be adequately documented.

The Service Providers remain responsible for the correctness of end-user information for the time during which they provide Peppol Services to them. End-user information shall be collected and verified at the time of enrolment in the Peppol Network and when it changes. Furthermore, it must be periodically checked at least on an annual basis, provided that mechanisms to that effect are available, e.g., through lookup or API connection to authoritative sources of information in specific jurisdictions. For avoidance of doubt, this clause does not require the Service Providers to make such checks for each transaction or more generally in runtime.

Attachment 2: Specific Requirements from SP Agreements v4.0.2

SP agreements include the following specific requirements with regard to contracts between SPs and end-users.

9.2.
The Peppol Service Provider shall ensure that there is a contractual relationship in place with the End User, either directly with the Peppol Service Provider or indirectly through an intermediary with whom the Peppol Service Provider has a contractual relationship, clearly stating:

a) that the Peppol Service Provider is entitled to perform the relevant Peppol Services, including receipt and/or transfer of Peppol Dataset Types, on behalf of or for the benefit of End Users,

b) that the End User remains fully responsible for the business content of the datasets exchanged including their compliance to relevant law as well as for any resulting business commitment,

c) the existence and role of the Peppol Network, and a reference to where relevant contact points are available, and

d) that the End User will be blocked from the Peppol Network in case fraud, spam or other criminal acts are noted by or on behalf of the End User.

The Peppol Service Provider is responsible and liable for ensuring at all times that all parts of such contractual relationship with End Users respects the terms of this Agreement and the Peppol Interoperability Framework in general, and that the correct identity of the End User is verified in accordance with the Entity Identification provisions stipulated by the Internal Regulations and/or Operational Procedures and applicable PA Specific Requirements as part of onboarding of an End User. The Peppol Service Provider shall furthermore provide the Peppol Authority upon its reasonable request with adequate evidence of compliance with these obligations towards the End Users