PASR Approval 2022
Decision Background – 21.06.2022

Peppol Authority Specific Requirements – Approval 2022

MC167 Decision Background – 2022.06.21

Table of Contents

1 Introduction

This document is intended as background for a Managing Committee decision to approve the updated PA Specific Requirements (PASR) for use within the new Peppol Interoperability Framework as of 1 July 2022, when the new Peppol Agreements enter into force.

The document will cover the following topics:

1. Process for defining PASR
2. Main issues encountered
3. Recommendations for MC approval

2 Process and approach

2.1 Requirements from Internal Regulations

Under the new Internal Regulations for Use of the Peppol Network, the PASR have to be reviewed by OpenPeppol members. This obligation created a new landscape where the definition and approval of PASR is no longer a matter exclusively between each PA and the MC, but it is a matter that concerns the entire Association.

The new Peppol Agreements and Internal Regulations make it clear that PASR apply automatically to all Service Providers that have customers (receivers or senders contracted, not receivers reached through other Service Providers) in the territorial jurisdiction of a Peppol Authority, therefore apply without the need to sign an agreement with that Peppol Authority. This feature of the new Agreement Framework was taken very seriously by the Service Providers, who took a much closer and more thorough look to the proposed PASR, mindful that they could apply to them without signing an Annex 5 as before.

2.2 Process walkthrough

The process to define and approve the new PASR went through the following steps:

a. Initial definition of PASR by each Peppol Authority
b. Review by OpenPeppol members
c. Discussion of the comments between Peppol Authorities and the Operating Office
d. Assessment of PASR quality and compliance with the IR, performed by the OO in cooperation with the Peppol Authorities

e. Approval by the Managing Committee and entry into force.

The Member review took place between 21 February and 21 March 2022. A total of 589 comments were received.

Clause ->	Identifier schemes	Information security	Reporting	Mandatory use	SLR	Local interoperability specs	Accredi-tation	Applicable jurisdiction	General	Terms and conditions	Total
Applicable for all countries	2	1	2	2	1	4	1	1	17		31
Australia	3	9	11	4		4	7		3		41
Australia New Zealand		1							2		3
Australia New Zealand Singapore			1								1
Belgium	4			13							17
Germany	2					13					15
Iceland	8					24			5		37
Italy	20			11		1			2		34
Japan		9									9
New Zealand	3	4	6	4		4	7		3		31
Norway	21	6	9	5	51	6					98
Overall									1		1
Poland	12	1				17			2		32
Portugal									2	39	41
Singapore	5	3	4	5	6	3	7		1		34
The Netherlands	17	82	9	4	8	29	11				160
The Netherlands Germany (from 11/22)						4					1
Total	**97**	**116**	**42**	**48**	**66**	**109**	**33**	**1**	**38**	**39**	589

The comments were all assessed and tabulated, and the analysis resulted in the identification of 38 issues which capture the main concerns expressed. These issues were also tabulated in terms of

- Issue description
- Issue category according to the IR
- Issue sub-category (where relevant)
- Service Provider reaction (high/low)
- Peppol Authorities to which the issue is relevant, based on the comments received on their PASR
- Status of issues per PA after comment resolution and OO-PA discussions (remaining, changed, removed)

The consolidated comment and issue log is available for reference https://openpeppol.atlassian.net/wiki/spaces/AF/pages/2756772112/2022.02.21+-+Review+of+PA+Specific+Requirements+Wave+1

3 Issues encountered

3.1 Applicable or allowed identifier or identification schemes

There have been many cases where Peppol Authorities request the national use of specific identifiers and identification schemes within their jurisdiction.

Surprisingly, quit a few of these PASR have raised reactions from Service Providers. But they are in line with the Internal Regulations, where the category is clearly foreseen, and they are also part of the Peppol tradition to allow to Peppol Authorities some control over identifier schemes, particularly when they implement national policy.

It should also be understood that most of the PASR in this category should be considered as PA guidance on end user identification requirements as foreseen by the Internal Regulations section 3.3.1.

3.2 Information security

The category of PASR is one of the most contentious, since variable security requirements across a global network are challenging for Service Providers who want to be present in many markets.

3.2.1.1 Third-party certification

Some Peppol Authorities require ISO27001 certificate or equivalent (Australia, Japan, New Zealand, Netherlands). Different arguments are being made but it seems that Service Providers within these countries are not the ones that are reacting the strongest – those from other countries voice the loudest objections. The reason is that the PAs have been working with SPs in the local communities, but the international ones are not yet part of that consensus process.

The Peppol Authorities that have this requirement have already been cooperating and aligning, and there is room to be more uniform in their approach to international SPs, for example by recognising those accredited by other PAs with equivalent certifications that may not be very well known in their part of the world. This will help smooth the path for cross-jurisdiction accreditation.

There is a common goal to adopt a Peppol -wide Security policy with a phase in period that will make security-related PASR obsolete. This will happen in a 3-year period, according to estimates at the outset of the WG on Security, which has recently been launched.

3.2.2 Mandatory end-to-end security in Post-award

The PASR for end-to-end security in the Netherlands has raised many objections, mainly because it seeks to prescribe obligations to a part of the ecosystem where Peppol is deliberately not specifying the behaviour of Service Providers and End Users: The communication between C1-C2 as well as the communication between C3-C4.

In IR section 7.3.1 p3 states that

“PA specific requirements cannot be used to impose changes to any component of the Peppol Interoperability Framework but may be used to constrain their use, such as making an optional Peppol Dataset Type mandatory.”

This criterion seems to imply that key design choices of the Peppol architecture should not be changed through PASR, either by changing current globally applicable building blocks or by introducing building blocks (such as end to end encryption) where none are intended. There are Service Domains such as Pre-award (eTendering) where this is a domain requirement, however for eInvoicing this is not considered to be a global requirement, (except when invoice content is sensitive, as may happen in healthcare, where higher requirements may apply).

On a more practical level, the requirement is defined in the abstract sense and therefore it is difficult for legal departments of Service Providers to have sufficient clarity on how to comply with it. Many SPs have quite robust security in their communication with End Users but would still not know whether it would be sufficient, because there are no details. As a result, SPs cannot even know the cost of complying.

In IR section 7.3.1 p2 states that

“When defining and enforcing PA specific requirements, Peppol Authorities should strive to minimize the additional compliance costs and increased regulatory burden that such requirements will place on Service Providers.”

It has been argued that the national SPs agree with this goal and indeed it is worth increasing the security and reliability of the network, provided there are no significant adverse effects. The business goal of promoting a higher level of security might be better supported by positive incentives rather than a punitive approach through mandatory PASR.

3.3 Reporting on End User information and transaction statistics

There are Peppol Authorities that require reporting, and they still continue to do so. This requirement will be phased out when the centralised reporting mechanism of OpenPeppol is put in place in early 2023.

During the transition period until the new mechanism is implemented, the obligation for jurisdiction-specific reporting will also apply to Service Providers which have not been reporting to those PAs until now because they had not signed Annex 5 or gone through accreditation in those jurisdictions. Some of the Peppol Authorities applying this requirement have shown to be pragmatic and address SP concerns during the transition period.

3.4 Mandatory use of centralised services and global specifications

3.4.1 Peppol Directory

The Peppol Directory is gaining in popularity and an increasing number of Peppol Authority wishes to make it mandatory.

The challenge is that the Peppol Directory 1.0 has been a (not very reliable) service provided “as is” without any service guarantees and without any checks. Under the new Peppol Interoperability Framework, the Directory 2.0 will be a service that will be provided by OpenPeppol, and OpenPeppol will have responsibility for this data even though they will be provided by SMPs as is done now.

OpenPeppol has not performed a legal analysis of its responsibilities regarding the quality and accessibility of the data the Directory holds, and there are questions for example about the automated queries which are now allowed. In the new version of the Peppol ecosystem that includes a more robust compliance policy that will have to be enforced, it is not advisable that OpenPeppol attaches any legally binding obligations on the use of the Peppol Directory without a legal analysis of the conditions that may have to be applied, for example in relation to the business-related or privacy-related controls of End Users and also who has access and what is the purpose of the service.

The legal analysis has to be done in tandem with the legal review of the reporting requirements and encompass every use of data that OpenPeppol as a legal entity is related with.

3.4.2 Message Level Response

MLR is widely considered a way to ensure better quality in the Peppol Network, where the problem of invalid messages is still existing even though there is a clear and explicit obligation in the new SP Agreement that only valid documents should be exchanged on the Peppol Network. As a result, Peppol Authorities are starting to require that MLR becomes mandatory.

It is true that Peppol has not solved the error correction problem and has still to establish a comprehensive environment with response messages at the transport level and the business level, the former to ensure technical interoperability and quality between Access Points and the latter to ensure business interoperability between End Users.

These will be the goals of a new cross-Community work group that will be established shortly and will aim to develop a policy to be applied throughout the Peppol Network. For this reason, it may be premature to introduce MLR obligations at a national level, something that will have to be phased in at any case. It would be far better if the Peppol Authorities and the Service Providers were to devote their efforts to a common policy and its implementation.

3.5 Service Level Requirements

After considerable efforts and discussions between OO and PAs, there are fewer PASR on SLRs now.

3.6 Use of local interoperability specifications

There is extensive use of local specifications which the Peppol Authorities have defined over the year and continue to maintain, as well as introduce new ones.

It is interesting that this category of PASR does not raise considerable objections and is one of the least contentious categories of PASR.

3.7 Service Provider Accreditation

Local accreditation schemes continue to exist, even though they can be seen as obstacles to operating across borders. The latest PA to introduce a national accreditation process is Japan.

It seems, however, that SPs want to have visibility with the local Peppol Authorities and therefore are willing to go through these procedures.

The introduction of BIS testing in the next version of the centralized Peppol Testbed, already being piloted with Japan, is expected to reduce the additional procedures that SPs have to go through for local accreditation purposes. Most of the remaining checks are intended to satisfy, as the Peppol Authorities claim, requirements that are based on national legislation and public-private sector relations, which vary from country to country.

4 Proposal for an MC167 decision

4.1 Considerations for the MC

4.1.1 The new process of review and debate

With the new Internal Regulations, PASR were reviewed for the first time and Service Providers throughout Peppol have had the chance to comment. This is a new step towards visibility and ownership.

Peppol still lacks a fully fledged change management process for PASR, since the current IR only describe the outline of an approval process. A detailed and robust change management policy is needed. The APP CMB can play a significant role in the execution of such procedures.

4.1.2 Regulation through PASR and legal basis

The most contentious PASR are those that are not based on national legislation but appear as Peppol rules, imposed through PASR. However, many PASR are actually defined in an effort of Peppol Authorities in order to help Service Providers, particularly those outside their jurisdiction – but having a market presence there – to comply with the spirit, not only the letter of national regulation.

This is in line with the IR section 7.3.1-point 1a:

"…they need to ensure compliance with legislation, regulation, or market conditions particular to that jurisdiction…"

In order to give more clarity to the motivation behind PASR and the context in which they are defined, the 2022 update can be distinguished in three categories:

- Type 1 - Based on national legislation or regulation
- Type 2 - Guidance on how to comply in a jurisdiction with the Peppol requirements
- Type 3 - Above and beyond national legislation or regulation

With this distinction, PASR of Type 1 and Type 2 should be more acceptable, although of course opinions may differ when interpreting the law and other regulatory revisions.

4.1.3 Timing of a decision

The process of discussing with the Peppol Authorities has been quite fruitful as there is a better understanding of PASR and quite a few have been revised or even removed. There could be a higher degree of convergence with the views of Service Providers if the process could continue.

On the other hand, PASR need to be approved so that the last legal uncertainties can be removed, and the Service Providers are aware of all their obligations when they sign the new SPA. This means that the MC must take a decision soon.

4.1.4 PASR going forward

With the introduction of a change management process and the evolution of the global interoperability framework, the vision can be that the views of stakeholders will converge more and more towards a vision where PASR are only based in legislation or non-existent.

4.2 Decision of the Managing Committee

The Managing Committee discussed the PA Specific Requirements in two meetings over three different sessions: MC165 (24.05.2022) and MC166 (31.05.2022, continued on 07.06.2022). After detailed deliberations, it decided the following:

1. Decision to approve PASR
    a. All Peppol Authorities Specific Requirements from Australia, Belgium, Germany, Iceland, Italy, Japan, New Zealand, the Netherlands, Norway, Poland, and Singapore are hereby approved, with some exception
    b. Exceptions are stated in point 2 below and are based on comments by MC members, having as starting point recommendations from the Operating Office included in the Assessment and Compliance Reports which have been provided to the MC ahead of the meetings.
    c. As part of this decision, the MC agreed on certain guidelines that should be considered by Peppol Authorities in future development, refinement, and update of PA Specific Requirements, but also in the manner in which they will enforce them. These guideiines are stated in point 3 below.
2. Exceptions include:
    a. Mandatory Use of the Peppol Directory (Australia, Germany, New Zealand, Netherlands, Italy, Belgium):
        i. Approval postponed until a legal opinion has been obtained by OpenPeppol about the possible liability of the Association and the conditions, if any, that must be applied to the notification of end users and their explicit consent, if needed.
        ii. The MC instructs the OO to prioritize such legal analysis and have it completed until September 2022.
    b. Mandatory use of the Message Level Response (Germany, Netherlands):

   i. Approval postponed until the beginning of 2023 until progress is made in a new work group that is being initiated shortly by PoAC, SPC and PAC.

   ii. The MC urges the Communities to speed up work and adopt a policy for the entire Peppol Network so that there is no need for individual PASR going forward and the Network takes the time to migrate and adapt with minimal disruptions

c. End-to end security (encryption, authentication) in the Post-award Service Domain (Netherlands):

   i. The MC requests that NPa provide more details regarding the impact on the global Peppol Network, the mechanisms that can be used to comply with this requirement, the way to enforce it and the cost incurred by Service Providers offering services, particularly those outside NL.

   ii. The MC also suggest that the NPa consider promoting enhanced end-to-end security through positive incentives and market awareness measures.

d. Data Quality in the Post-award Service Domain (Netherlands):

   i. The MC requests that NPa provide more details regarding the impact on the global Peppol Network, the mechanisms that can be used to comply with this requirement, the way to enforce it and the cost incurred by Service Providers offering services, particularly those outside NL.

   ii. The MC also suggest that the NPa consider promoting enhanced data quality through positive incentives and market awareness measures.

e. Mandatory use of the AS4 transmission protocol (Netherlands):

   i. The MC recommends that the NPa reconsider the wording of the requirement and confirm what is the actual intention, given that mandatory support of AS4 is a global rule for Peppol.

   ii. The MC instructs the OO to ensure that there are no SPs remaining in the Peppol Network after 1 July, unless they are confirmed as compliant with AS4.

   iii. The MC requests from eDEC to take the necessary steps to phase out AS2 completely.

3. Guidelines for the future:

    a. Guidance: The Peppol Authorities should clearly separate the actual rule, to be considered as obligations, from guidance offered to Service Providers on how to comply. Ideally, there should be different documents for PA Specific Requirements (PASR) and PA Specific Guidance (PASG)

    b. Identifiers: When Peppol Authorities mandate specific identifier schemes for their jurisdiction, they should also make all reasonable efforts to support market requirements expressed by Service Providers, such as the registration on lower-level units within a legal entity using different identifiers (e.g., in retail sector). The topic should be further discussed in the Communities.

    c. Centralized SMPs: When mandating the use of a centralized SMP in their jurisdiction, Peppol Authorities shall provide guidance to Service Providers on how to use it, particularly when Service Providers are based outside their jurisdiction.

    d. Reporting: Given that OpenPeppol is in the process of establishing a centralized reporting mechanism, national reporting schemes now approved as PASR should be phased out when the centralized mechanism is operational and implemented by Service Providers in the following months. In the interim transition period, Peppol Authorities shall have a pragmatic approach and ideally not to extend these schemes to Service Provider that have not been reporting to them under the TIA framework.

    e. Security: Given that there is a Security work group now operational, aiming to adopt a Peppol-wide security policy, Peppol Authorities should refrain from introducing through PASR new security requirements from what go beyond what they have today.

    f. Accreditation Policies: As clearly stated in clause 11.3 of the PA Agreement (The Peppol Authorities should use national Accreditation Policies in order to ensure compliance with their other PASR and not to introduce new PASR through Accreditation. In particular, certain business requirements that are currently part of national Accreditation Policies should be expressed as a different category of PASR. Since this is not currently foreseen in the Internal Regulations, it could be introduced following the provisions of the Change Management Policy.

    g. Local interoperability specifications: When Peppol Authorities introduce local interoperability specifications as part of their PASR they should make sure they apply them only to Service Providers that offer relevant services. For example, if there is a local invoice specification in a jurisdiction, the Peppol Authority should not ask compliance from a Service Provider that offers only eOrders.

4. Future handling of PA Specific Requirements:
   a. The MC instructs the OO to develop a proposal for a change management policy with respect to PA Specific Requirement.
   b. In doing so the OO should consult all relevant stakeholders and especially the APP CMB, which should be requested to review and approve the policy.