PEPPOL e-Signature Validation Service Agreements
Annex 3 – Services and Service Levels

Table of contents

1. Scope for this document 2
2. PEPPOL Services related to e-Signature Validation Infrastructure 2
3. Definition of Availability 5
4. PEPPOL PPRS availability 5
5. PEPPOL Validation Service Availability 6
6. Response time requirements 6
7. Capacity 6
8. Support services 7
9. Reporting 7
10. Exceptions 7

PEPPOL e-Signature Validation Service Agreements
Annex 3 – Services and Service Levels

1. Scope for this document

1.1. This document identifies services in the PEPPOL e-signature validation infrastructure and their minimum service levels required.

1.2. The scope includes services provided by the PEPPOL-VS coordinating authority and the PEPPOL validation services.

1.3. The stated service level is considered a minimum level for service providers in the PEPPOL validation infrastructure. Service providers may offer higher level of services as part of their offerings.

1.4. The performance of the PEPPOL e-signature validation infrastructure depends on the service levels of the certification authorities, which are not under control of the validation services providers or the PEPPOL e-signature validation infrastructure in total. The defined service levels in this document set requirements, which are achievable according to history experiences and under normal circumstances. A validation service provider may not be liable for poor response times of the CAs or remote validation services, he depends on.

2. PEPPOL Services related to e-Signature Validation Infrastructure

2.1. The technical services of the PEPPOL e-signature validation infrastructure

- PEPPOL Public Registry Service (PPRS)
- PEPPOL Validation Service (XKMS responder)

2.1.1. The PPRS provides the entries of validation services (XKMS responders) available in the e-signature validation infrastructure and their national coverage of certification authorities. It is not a critical service in runtime when validating digital signature certificates. The entries in the PPRS are considered to be rather stable, changes to the PPRS are expected to happen on monthly basis, as a rough estimation.

2.1.2. PEPPOL validation services are providing essential services for processing digital signature certificate validations by conducting the validation whether a) locally against configured certification authorities or b) by forwarding the validation request to another validation service in the infrastructure, using the PPRS for routing.

2.2. The parties, their roles and non technical services within the validation infrastructure

- PEPPOL-VS Coordinating Authority
- PEPPOL Validation Service Provider
- PEPPOL-VS Regional Authority

2.3. PEPPOL-VS Coordinating Authority

- Has the sole authority over the PPRS and is responsible for its entries.
- Signs the PEPPOL Validation Service Provider Agreement with the respective providers.
- Signs the community agreement with the PEPPOL Regional Authority in case this is applicable, and provides an arbitration body for PEPPOL e-Signature Validation related conflicts.
- Enters in to agreements with and provide support for Validation Service Providers in domains where no PEPPOL Regional Authority has been delegated.
- Provides a website with listing of all PEPPOL-VS Regional Authorities, Validation Service Providers and other contact information from Annex 1.
- Is responsible for providing the PPRS (compiling the PPRS TSL and publishing it online).
- Makes sure, that active validation services are listed in the PPRS and retired services are deleted.
- Makes sure that the most recent version of the PPRS is available in due time.
- Provides a mailing list containing all Validation Service Providers support e-mail addresses as written in Annex 1.

2.4. PEPPOL-VS Regional Authority

- Signs agreements with validation service providers.
- Signs the community agreement with the PEPPOL-VS Coordinating Authority.
- Provides support for Validation Service Providers it is contracted to.
- Reports PEPPOL validation service providers with issued contracts including contact information to the PEPPOL Coordinating Authority.
- Registers support incidents and respond/resolve according to locally defined service levels, and escalates to the PEPPOL-VS Coordinating Authority those not resolvable.
- Reports the inclusion or exclusion of validation services under its authority to the PEPPOL-VS Coordinating Authority in due time.
- Provides contact information of the contracted validation services providers as written in Annex 1 to the PEPPOL-VS Coordinating Authority.

2.5. PEPPOL Validation Service Provider

- Provides support to participants using the services offered.
- Performs logging of their services for support and trace purposes.
- Engages with other PEPPOL validation service provides to resolve issues related to connection problems between them.
- Reports service level compliance and significant operation disruptions to the PEPPOL-VS Coordinating Authority or PEPPOL Regional Authority issuing the service provider contract.
- Escalates support issues the service provider cannot resolve to the PEPPOL-VS Coordinating Authority or PEPPOL Regional Authority.
- Performs the necessary testing required to insure compliance with the relevant technical standards and specifications defined by PEPPOL e-Signature.

3. Definition of Availability

Availability is defined as availability of the service interface. Specifically availability of the validation service does not guarantee that requests involving a specific certification authority can be processed, as the connection to the certification authority may be unavailable and not under control of the validation service provider.

The availability window (the period over which availability is computed) is working days in the period 08.00 – 17.00 CET. Down time is the number of minutes of service unavailability, not measuring down time caused by force majeure situations.

As an additional availability requirement, the service SHALL NOT be unavailable for more than 3 consecutive hours within the availability window.

Percent availability is computed, all measurements in minutes, as follows:

$$\text{Percent availability} = \frac{(\text{Availability window} - \text{Down time}) \times 100}{\text{Availability window}}$$

The measures in the following chapters are defining the minimum requirements.

4. PEPPOL PPRS availability

4.1. The PPRS must be available on average:

- 98.5% of the time from Monday - Friday from 8:00 to 17:00 CET (business hours)
- 99% of the remaining period.

4.2. Availability is measured monthly and service windows are included in "down time".

4.3. Planned down times within and outside the business hours have to be announced 3 days in advance to the mailing list provided by the coordinating authority containing all support e-mail addresses.

4.4. Major incidents as breaches in the security have to be communicated within 4 hours to the mailing list provided by the coordinating authority containing all support e-mail addresses.

5. PEPPOL Validation Service Availability

5.1. PEPPOL validation services must be available on average:

- 98.5% of the time from Monday - Friday from 8:00 to 17:00 CET (business hours)
- 98.5% of the remaining period.

5.2. Availability is measured monthly and service windows are included in "down time".

5.3. A PEPPOL validation service provider must have an escalation procedure and a contingency plan to handle service disruption.

5.4. Major incidents as breaches in the security which could have an impact on other service providers have to be communicated within 4 hours to the mailing list provided by the coordinating authority containing all support e-mail addresses according to the annexes 1.

6. Response time requirements

6.1. A receiving validation service must return the validation result within 10 seconds after having received the request. If the response time exceeds 10 seconds measured at the interface between the validation service and external networks, the validation service SHALL be considered unavailable.

6.2. Unavailability of a validation service may not always be owed by the validation service provider the initial request was sent to, as the performance of a validation service is always dependent on other entities, which are not under direct control of a validation service provider, i.e. the certification authorities and other validation services in the infrastructure.

6.3. Persistent unavailability must be reported to the validation service provider after ascertained within 1 hour after the first occurrence of unavailability to the support e-mail address as written in Annex 1. Persistent unavailability occurs in case a validation service is unavailable in 3 consecutive validation requests within 3 minutes.

7. Capacity

7.1. Validation service providers must establish their systems with sufficient capacity to serve customers and other validation service providers within the required service levels.

7.2. If response time or availability requirements cannot be met due to insufficient capacity, validation

service providers shall scale their systems to a level appropriate for handling the workload.

8. Support services

8.1. PEPPOL validation service providers must name an e-mail address and telephone number that can be used for reporting of incidents such as system failures, security incidents or other emergency situations. This information is to be provided with annex 1.

8.2. The telephone contact must be available during defined business hours. If English language is not supported by the telephone contact, a call-back service must be established to facilitate efficient dialogue on the incident can be initiated within 2 hours.

8.3. Local language is preferred during analysis and resolution of reported incidents if both parties agree on this. If not English language is default.

8.4. A **critical incident** reported must be responded to within 4 hours after reporting. A critical incident is defined as the occurrence of wrongly valid validation results from a validation service.

8.5. An **incident** reported must be responded to within 1 working day after reporting.

9. Reporting

9.1. In case of major system failures causing more than 4 hours of down-time, the PEPPOL-VS coordinating or regional authority must be notified.

9.2. PEPPOL validation service providers may be required to provide documentation on service level on a monthly basis to the PEPPOL-VS regional or coordinating authority. A reporting template will be provided by the PEPPOL-VS regional or coordinating authority.

9.3. If service levels are not deemed sufficient by the PEPPOL-VS regional authority, validation service provider can be instructed to take appropriate measures to restore service quality.

9.4. PEPPOL validation service providers may be required by the PEPPOL coordinating or regional authority to report on the number of transactions (i.e. the received requests and provided responses).

10. Exceptions

10.1. An validation service provider does not have to fulfil the service levels defined in this agreement in the following situations:

- The validation service is under a virulent attack.
- Lack of service level fulfilment results in force majeure.
- Special conditions apply and the PEPPOL coordinating or regional authority has approved lowering the service levels for a specific time period and under specific conditions.

10.2. Validation service providers must document the reasons for not fulfilling the required service levels.