PEPPOL
PAN-EUROPEAN PUBLIC PROCUREMENT ONLINE

Specification

OpenPEPPOL AISBL

Transport Infrastructure Coordinating Community

ICT - Models

PEPPOL Policy for Transport Security

Author:

Bård Langøy, Pagero, Sweden

Version: 1.0.0

Status: Scheduled for use

Statement of originality

This deliverable contains original unpublished work except where clearly indicated otherwise. Acknowledgement of previously published material and of the work of others has been made through appropriate citation, quotation or both.

Statement of copyright

Contributors

Bård Langøy, Pagero

Hans Berg, Tickstar

Risto Collanus, Visma

Philip Helger, Bundesrechenzentrum

Jerry Dimitriou, OpenPEPPOL Operating Office

Jesper Larsen, OpenPEPPOL Operating Office

Erlend Klakegg Bergheim, Difi

Version History

Version	Date	Change log
1.0.0	2019-01-31	Initial version

1 Introduction

Actors within the PEPPOL eDelivery Network are required to manage two different types of electronic certificates:

1. TLS certificates, used on transport level to provide a standard solution for securing server authentication and message confidentiality.
2. OpenPEPPOL certificates, used on application level, to secure that only authorized and approved actors are operating within the PEPPOL eDelivery Network.

The TLS Certificates are not provided by OpenPEPPOL and MUST be issued by third party Certificate Authorities.

This document covers the policies on the use of TLS certificates and TLS configurations in order to:

- limit disruptions in traffic between actors
- provide good security requirements for both current and future demands

1.1 Terminology

The keywords "MUST", "MUST NOT", "REQUIRED", "SHALL", "SHALL NOT", "SHOULD", "SHOULD NOT", "RECOMMENDED", "MAY", and "OPTIONAL" in this document are to be interpreted as described in RFC 2119 [RFC2119].

The term TLS is used through the entire document instead of SSL to highlight the fact that the TLS protocol is the successor of the SSL protocol.

1.2 Normative references

[RFC2119] Key words for use in RFCs to Indicate Requirement Levels, https://www.ietf.org/rfc/rfc2119.txt

[NSS] Mozilla Network Security Services, https://developer.mozilla.org/en-US/docs/Mozilla/Projects/NSS

[CACERTS] List of pre-loaded CA certificates of NSS, https://wiki.mozilla.org/CA/Included_Certificates

[SSL-LABS] SSL Labs Website performing SSL tests, https://www.ssllabs.com/ssltest

2 Policy for Transport Security

2.1 Approved Certificate Authorities

TLS Certificates are not issued by OpenPEPPOL and would lead to security risks and trust issues between actors without any guiding policies. Trust issues have already been a problem within the PEPPOL eDelivery Network for quite some time and to solve these issues, OpenPEPPOL restricts the usage of TLS Certificates as follows:

POLICY 1 Approved Certificate Authorities

Each TLS certificate used in the PEPPOL eDelivery Network MUST be issued (directly or indirectly) only by a root certificate contained in the latest version of the "List of pre-loaded CA certificates" [CACERTS] of the "Mozilla Network Security Services" [NSS].

It's the responsibility of the actor in the PEPPOL eDelivery Network to use a TLS certificate that adheres to this policy and to verify that only TLS certificates adhering to this policy are allowed to connect.

POLICY 2 Self-signed certificates

Self-signed TLS certificates are not allowed.

Self-signed TLS certificates are not allowed, because man-in-the-middle-attacks could be performed unnoticed.

2.2 TLS Requirements

TLS configurations SHOULD be constantly updated in order to keep the PEPPOL eDelivery Network secure. TLS configurations covers areas like:

- Software versions (security patches)
- Hash algorithms
- Key exchange algorithms
- Certificate requirements
- Cipher suites

POLICY 3 TLS Configuration Requirements

The TLS configuration MUST constantly be of at least grade 'A' according to SSL Labs [SSL-LABS].

To address the fact that requirements to keep the TLS configurations up-to-date, without having to re-issue this policy frequently, the third-party analysis tool offered by SSL Labs is used to verify the TLS configuration.

Every actor graded below "A" in SSL Labs is considered to be “unavailable” with regards to the Transport Infrastructure Agreement.

Note: this applies to all AccessPoints, for all transport protocols supported in the PEPPOL eDelivery Network (AS2 and AS4 at the time of writing of this document). This also applies to all SML instances. SMP instances are currently not affected because they are not using TLS certificates.

2.3 Customizations to TLS configurations

POLICY 4 Customizations to TLS configurations

TLS configurations MUST NOT be modified in order to allow communication with actors violating the policies of this document.

If an actor breaks at one or more of the policies stated in this document it SHOULD be reported to OpenPEPPOL Operations.

If an actor breaks at one or more of the policies stated in this document it MUST NOT lead to configuration changes for communicating with that specific actor.