

**Specification**

**OpenPEPPOL AISBL**

**Transport Infrastructure Coordinating Community**

**ICT - Models**

**PEPPOL Policy for transport security**

**Version: 1.0.0**

**Status: Draft**

***Statement of copyright***

******

*This deliverable is released under the terms of the Creative Commons License accessed through the following link: http://creativecommons.org/licenses/by/3.0/.*

*In short, it is free to*

***Share*** *— to copy, distribute and transmit the work*

***Remix*** *— to adapt the work*

*Under the following conditions*

***Attribution*** *— You must attribute the work in the manner specified by the author or licensor (but not in any way that suggests that they endorse you or your use of the work).*

# Contributors

Hans Berg, Tickstar

Jerry Dimitriou, OpenPEPPOL Operating Office

Jesper Larsen, OpenPEPPOL Operating Office

Risto Collanus, Visma/Maventa

Philip Helger, Bundesrechenzentrum

Erlend Klakegg Bergheim, Difi

Bård Langöy, Pagero

# Version History

|  |  |  |
| --- | --- | --- |
| Version | Date | Change log |
| 1.0.0 | 2018-11-13 | Initial version |

# Introduction

Operators (SML, SMP, AP) within the PEPPOL Trust Network are required to manage 2 different types of certificates:

* TLS Certificate, used on transport level to provide a standard solution for securing server authentication, message confidentiality and authentication.
* OpenPEPPOL Certificate, used on application level, to secure that only authorized and approved operators are operating within the PEPPOL Trust Network.

The TLS Certificates, on the other hand, are managed and issued by third party Certificate Authorities.

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

* limit disruptions in traffic between operators
* provide good security requirements for both current and future demands

## 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].

### Notational conventions

Normative references

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

[SSL-LABS] SSLLabs Website performing SSL tests

[https://www.ssllabs.com/ssltest](https://www.ssllabs.com/ssltest/)

[TRST\_NET] ICT-Transport-Trust\_Network\_Certificate\_Policy

https://github.com/OpenPEPPOL/documentation/blob/master/TransportInfrastructure/ICT-Transport-Trust\_Network\_Certificate\_Policy-2.00.pdf

### Use of TLS

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.

# Policy for transport security

## Approved Certificate Authorities

TLS Certificates are not issued by OpenPEPPOL and would lead to security risks and trust issues between operators without any guiding policies. Trust issues have already been a problem within OpenPEPPOL for several years and to alleviate this, OpenPEPPOL restricts the Certificate Authorities allowed to issue certificates:

1. Approved Certificate Authorities

The TLS certificate MUST be trusted by both Oracle (Java) and Microsoft. The certificate store distributions MUST not be older than 6 months.

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

1. Self-signed certificates

Self-signed TLS certificates are not allowed.

## TLS Requirements

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

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

To address the fact that demands on keeping the TLS configurations up to date with the latest security standards and cover the areas stated above, without having to reissue this policy for every change, OpenPEPPOL has chosen to use the third-party analysis tool offered by SSL Labs.

1. TLS Requirements

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

An operator (SMP, AP) graded below "A" is considered to be unavailable with regards to the Transport Infrastructure Agreement.

## Customizations to TLS requirements and truststore

When encountering an operator breaking the policies stated in this document (concerning approved certificate authorities or TLS requirements) it SHOULD be reported to OpenPEPPOL Operations and MUST NOT lead to customizations or extensions of transport security configurations for this single operator.

1. Customizations to TLS configurations and Truststore

TLS configurations MUST NOT be modified in order to fix ongoing communication issues with operators violating the policies of this document.