eDelivery CMB status update

Hans Berg, Tickstar
Bård Langøy, Pagero
Risto Collanus, Visma
Philip Helger, BRZ

Transport Security Policy 1.0

- The TSP document covers the policies on the use of TLS certificates and TLS configurations
  - Covering policies for certificates not maintained by OpenPEPPOL
  - Provide good security requirements for both current and future demands

Why do we need this policy?

- To limit disruptions in traffic between actors
- Open PEPPOL provides a platform for indirect interoperability agreements between Access Points through the TIA.
  - Access Points might not have any established contact points between each other.
  - New Access Points might join the network at any time.
  - Updates to certificates might cause disruptions within PEPPOL and force other Access Points into incorrectly updating their trust store.
  - This has happened on several occasions already

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].***
- Providing a technology agnostic distribution
- It is the responsibility of the actor (AccessPoint) to ensure that the TLS certificate is allowed.

Policy 2 - Self-signed certificates

- ***Self-signed TLS certificates are not allowed***
- A consequence of Policy 1.

Policy 3 - TLS Configuration Requirements

- ***The TLS configuration MUST constantly be of at least grade 'A' according to SSL Labs [SSL-LABS].***
- Use SSL Labs in order to keep updated with latest security standards without having to update the specification regularly.
  - Software versions (security patches)
  - Certificate requirements
  - Cipher suites
- Actors graded below "A" is considered unavailable with regards to the TIA
- Applies to both AS2 and AS4 protocols for AccessPoints
- Applies to SML.

Policy 4 - Customizations to TLS configs

- ***TLS configurations MUST NOT be modified in order to allow communication with actors violating the policies of this document.***
- If an actor breaks one or more of the policies stated in this document it SHOULD be reported to OpenPEPPOL Operations.
- If an actor breaks one or more of the policies stated in this document it MUST NOT lead to configuration changes for communicating with that specific actor.