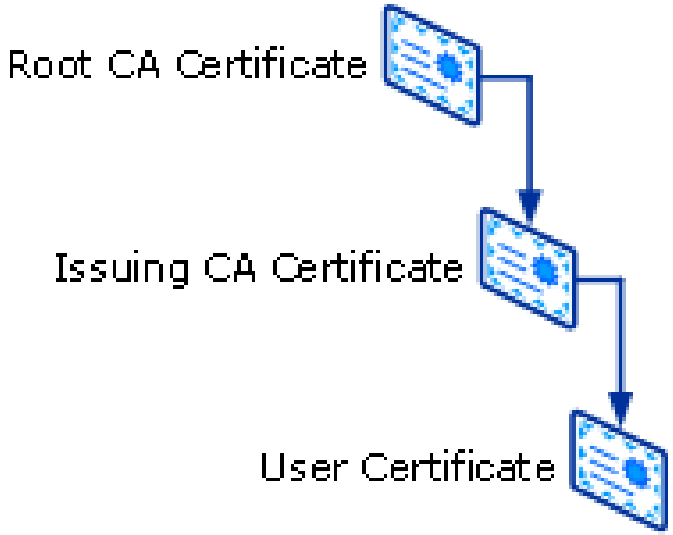
OpenPEPPOL TICC
eDelivery TLS certificates
London November 22, 2016

Juan Baldovi

Certificate Trust



Root certificate is the top-most certificate of the tree, the private key of which is used to "sign" other certificates.

All certificates immediately below the root certificate inherit the trustworthiness of the root certificate

The root certificate is usually made trustworthy by some mechanism other than a certificate, such as by secure physical distribution.

For example, some of the most well-known root certificates are distributed in the Internet browsers by their manufacturers.

OpenPEPPOL transport infraestructure specifications

PEPPOL PAN-EUROPEAN PUBLIC PROCUREMENT ONLINE

making procurement better.eu

ICT-Transport-AS2_Service_Specification-2014-01-15.pdf

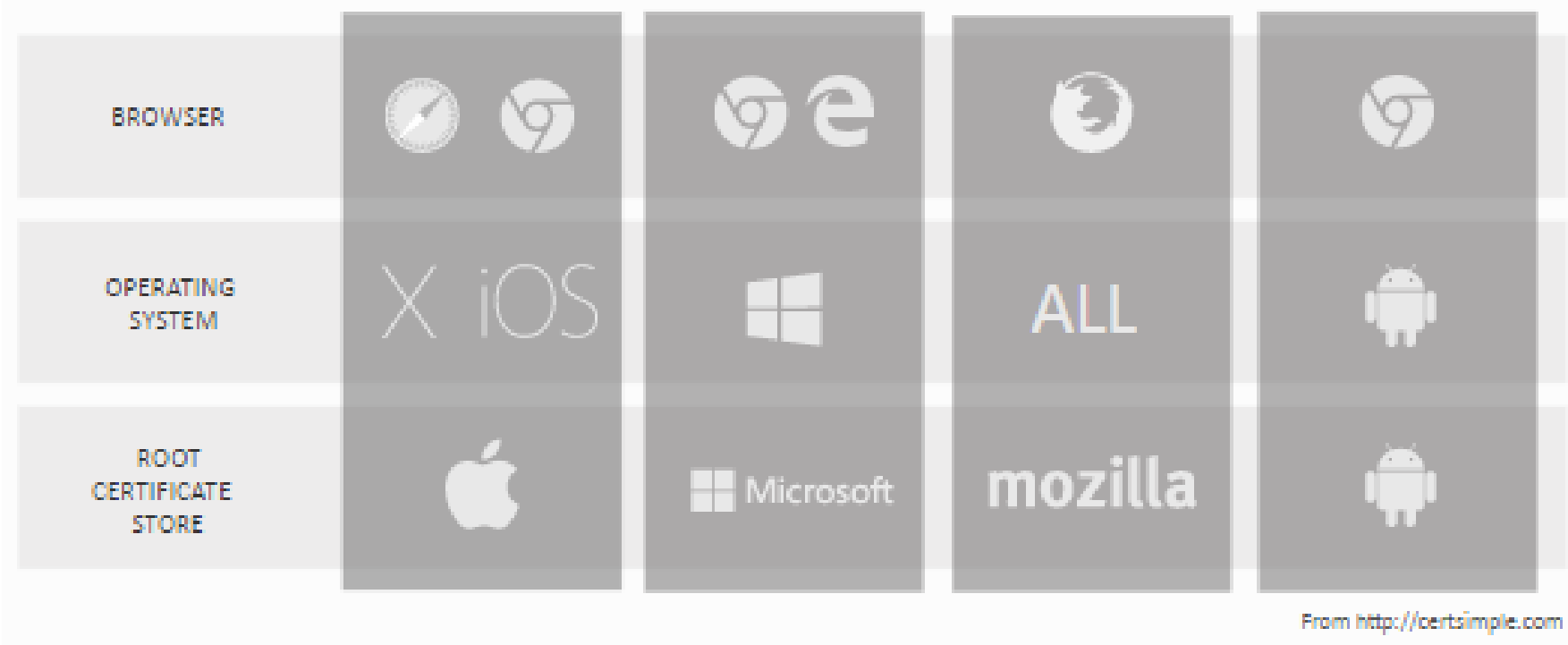
Item 3.6 in page 19

Use of HTTPS

Messages MUST be transmitted using HTTPS POST using trusted SSL certificates - which **prevents a "man-in-the-middle" attack** - as follows:

- The DestAP MUST implement HTTPS with certificate chains to certificate authorities which would be considered to be trusted by the PEPPOL community.
- It SHOULD be a 2048 bit Certificate or better.
- The certificate MUST correctly identify the DestAP URL e.g. no self-signed certificates.
- The certificate MUST NOT be expired or revoked.
- The DestAP MUST use a simple TLS handshake.
- It SHOULD use TLS v1.2 where possible as described in RFC 5246.
- The DestAP URL MUST only refer to HTTPS.
- The DestAP URL SHOULD use the default port 443. This assures firewall rules are often setup in advance.
- The DestAP MAY use wildcard certificates to facilitate multiple URLs under the same trusted domain.

Who we trust now?



Major root certificate stores

Apple	Microsoft	Mozilla	Oracle	Android

The current problem?

HTTPs interoperability not guaranteed between APs

- There's no consensus in OpenPEPPOL today about who should be trusted at the transport layer
- Different trust criteria depending on the AP because is being granted based on the default trust stores which is dependant on SO, software, etc
- AS2 over HTTPS is failing because of European CAs not being present in default trust stores

What is a TSL?

- TSL = Trust Service status List

Trusted lists are essential elements in building trust among electronic market operators by allowing users to determine the qualified status and the status history of trust service providers and their services.

- Based on ETSI TS 102 231

EU Trusted list

- Member States have the obligation to establish, maintain and publish trusted lists of qualified trust service providers and the qualified trust services provided by them. The lists are available for consultation on this page

- In order to allow access to the trusted lists of all Member States in an easy manner, the European Commission has published a central list with links to national “trusted lists”.

- Human readable
- Machine format

Proposed Solution

1) Use of the EU trusted list (TSL) in OpenPEPPOL

1) Create OpenPEPPOL addendum TSL for covering possible gaps in EU's

Implementation plan

April 1st 2017

1) OpenPEPPOL to publish TSL

1) APs to add OpenPEPPOL's TSL to truststore

1) APs to add EUs TSL to trustore

1)

PEPPOL

“The future of public procurement?”

For more information:
E-mail: info@peppol.eu
Web address: www.peppol.eu

Follow PEPPOL on

joinup

LinkedIn

YouTube

twitter