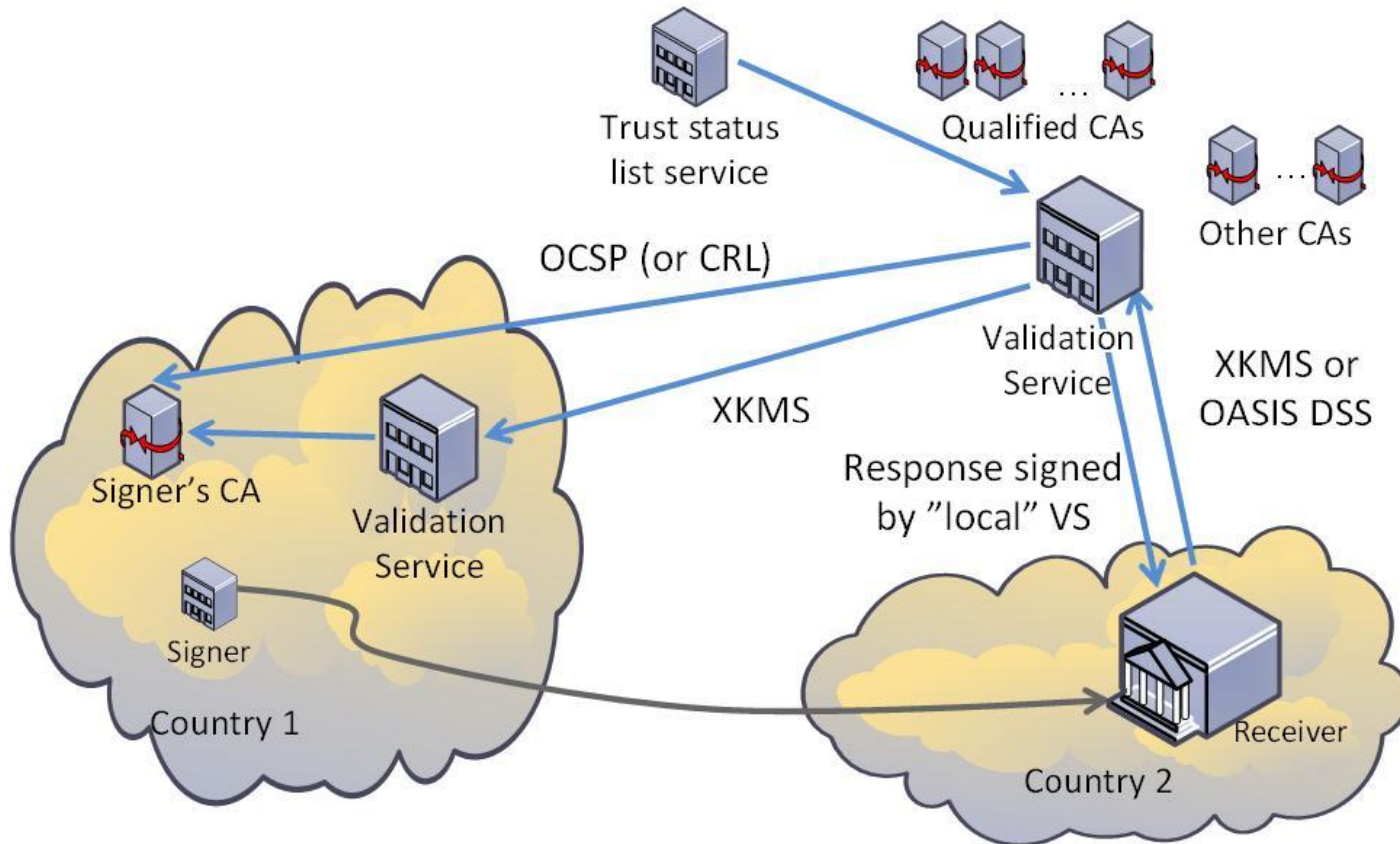




**eSignature
Infrastructure
ICT
Architecture
Framework**

Overall concept: Architecture of WP1 - solution



Infrastructure Components

1.) PEPPOL XKMS Responder:

- ▶ can validate certificates against configured CAs and use the PPRS to pass XKMS request towards other PEPPOL XKMS responders.

2.) PEPPOL Public Registry Service (PPRS)

- ▶ Service that provides information about Trusted Service Providers and their services.
- ▶ Organised according Trust-service Status List (TSL, ETSI TS 102 231)
- ▶ It will be aligned with the EU Commission project on establishing an European List of CSP.

Use Case description

- ▶ Sender applies digital signature, and transmits signed document to tender portal.
- ▶ Validation Service (VS) trusted by recipient is used to validate certificate.
- ▶ The requested VS can validate respective certificate directly or
- ▶ VS asks PEPPOL Public Registry Service (PPRS) which trusted VS is able to validate current foreign certificate.
- ▶ In the latter the VS mediates the validation request towards foreign VS covering respective CA.
- ▶ Foreign VS validates certificate against CA and sends validation result back to local VS.
- ▶ Local VS resigns XKMS respond and sends validation result back to recipient.

ICT Architecture Dependencies

- ▶▶ Available services of national certificate authorities
- ▶▶ Providers of validation services

- ▶▶ Central (need to have): PEPPOL Public Registry Service TSL (PPRS)
 - ▶▶ The trust model of the PEPPOL validation services federation
 - ▶▶ Provides links and rules to invoke the PEPPOL validation services
 - ▶▶ Issued in XML format according to ETSI TSL specification
- ▶▶ Decentral (need to have): Validation Services (VA, XKMS responders)
 - ▶▶ Validation of digital signature certificates
 - ▶▶ Local validation against configured Certificate Authorities (CA)
 - ▶▶ Forwarding of validation requests to other VS

eProcurement without borders in Europe

www.peppol.eu

