fact sheet

PEPPOL
PAN-EUROPEAN PUBLIC PROCUREMENT ONLINE

eProcurement without borders in Europe!

PEPPOL and eSignature

The PEPPOL eSignature Validation Infrastructure provides contracting authorities with the ability to validate digital signature certificates cross border. PEPPOL eSignature doesn't help you to sign but – more important – helps you to verify a digital signature from another European country!

The PEPPOL project: eProcurement without borders in Europe

The PEPPOL project (Pan European Public eProcurement On-Line) is an EC project facilitating EU-wide interoperability in public eProcurement aiming at setting up pan-European pilot solutions that conjointly exist with national infrastructures.

The PEPPOL project envisages a future where any company in the EU, and in particular small and medium-sized enterprises (SME), can communicate electronically with any European governmental institution for the entire procurement process. The project will set up integrated pilot solutions for cross border procurement.

It consists of eight work packages and is co-funded by the European Commission within the Competitiveness Innovation Programme (CIP). The PEPPOL consortium currently comprises 17 leading public eProcurement agencies in 11 countries (Austria, Denmark, Finland, France, Germany, Greece, Italy, Norway, Portugal, Sweden and the United Kingdom).
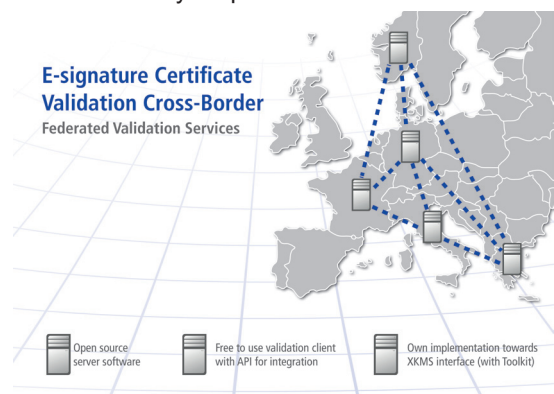Further information on PEPPOL: http://www.peppol.eu

eSignature

Electronic signatures based on electronic certificates are in common use already. They allow the secure identification of the sender of a document and ensure that a document has not been modified. PEPPOL aims to create **interoperability** between the different national schemes, so that in practice a public sector entity can validate certificates issued in other member states, allowing for electronic submission of tenders cross borders.
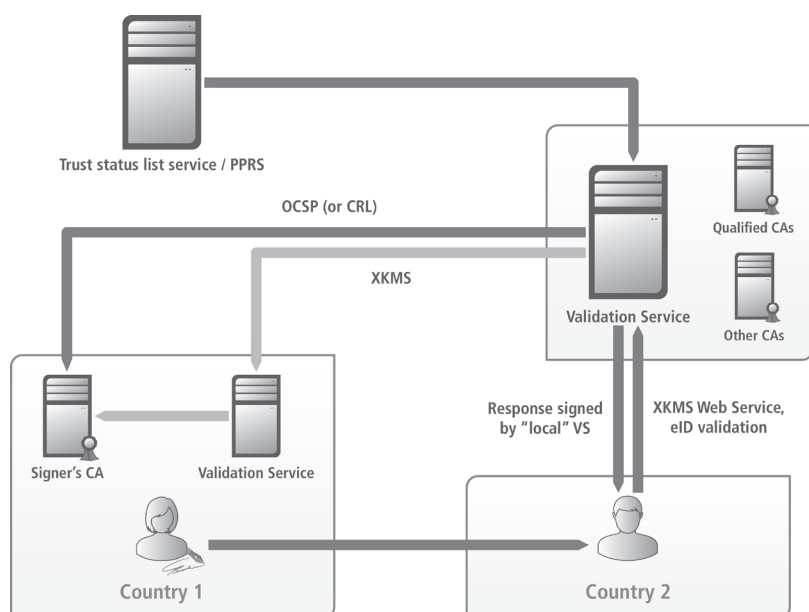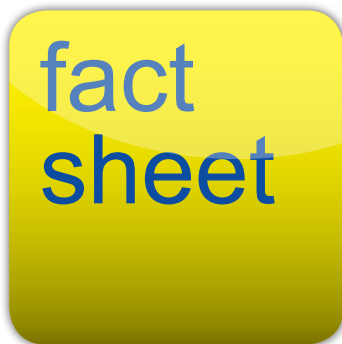
The **PEPPOL Validation Infrastructure** consists of a network of federated validation services, the **PEPPOL XKMS Responders** and a central component, the **PEPPOL Public Registry Service (PPRS)**, which establishes trust between the decentral responders and provides information about the Certification Authorities that the responders can validate. In case a validation request can not be handled by the initially called responder, it will be automatically forwarded to the responder in the network which can validate against the Certification Authority in question.

E-signature Certificate Validation Cross-Border
Federated Validation Services

Open source server software | Free to use validation client with API for integration | Own implementation towards XKMS interface (with Toolkit)

A contracting authority needs access to one of the validation services in the network to achieve the **full coverage** of the validation infrastructure. A validation service can validate the certificate itself, or forward a request to another service in the network. The PEPPOL Public Registry Service provides the information, which service can validate the respective certificate. The chaining process **runs automatically**, the receiver gets back the validation result from the service he called.

Covered Certification Authorities

Today the PEPPOL validation infrastructure covers **100% of the qualified certification authorities** of Europe.

fact sheet

PEPPOL
PAN-EUROPEAN PUBLIC PROCUREMENT ONLINE

Trust status list service / PPRS

OCSP (or CRL)

XKMS

Qualified CAs

Validation Service

Other CAs

Signer's CA

Validation Service

Response signed by "local" VS

XKMS Web Service, eID validation

Country 1

Country 2

Client Components for Validation

▶▶ Validation Client: Ready to use GUI based validation software usable as
- stand alone application and
- integration version with APIs for integration into other software applications

▶▶ Validation Toolkit: Set of function libraries to enable digital signature validation and generate XKMS requests to invoke the validation infrastructure for own development.

Central infrastructure component

▶▶ The **PEPPOL Public Registry Service (PPRS)** is the central server component of the validation infrastructure. It **establishes trust** between the different validation service instances, information how to access the services and information about which service is able to validate a certain certificate. Validation services use this information to forward a XKMS validation request to another service.

▶▶ The component is hosted and maintained by the PEPPOL consortium, **free to use** and will be maintained by the European Commission after project termination.

Decentral Server Component

▶▶ XKMS Responder: The component is available as **ready to use open source server software**, which can be used to set up an own validation service.

Join a Pilot Project

Taking advantage of PEPPOL's implementation experts, organisations in the EU can now set up a transaction pilot, realising significant cost and time savings immediately.

A PEPPOL pilot project must facilitate trade between contracting authorities as buyers and one or more economic operators as suppliers, supported by different technology solutions or service providers. The pilot can operate across national or regional borders in Europe, and connect eProcurement communities using the PEPPOL technology.

For further information on joining a pilot project, go to

http://www.peppol.eu/about_peppol/user_groups/join-peppol