DELIVERABLE

Project Acronym: PEPPOL

Grant Agreement number: 224974

Project Title: Pan-European Public Procurement Online

Deliverable 1.2
Trans-national verification solution(s)
Prototype Documentation

Revision: 1.01

Authors:

Frank Schipplick (bremen online services)

Lars Thölken (bremen online services)

Project co-funded by the European Commission within the ICT Policy Support Programme		
Dissemination Level		
P	Public	X
C	Confidential, only for members of the consortium and the Commission Services	

CC BY

Revision History

Revision	Date	Author	Organisation	Description
1.0	20100430	Lars Thölken	bos	First version (pending EC approval)
1.01	20101001	Klaus Vilstrup Pedersen	DIFI	EC Approved

Statement of originality

This deliverable contains original unpublished work except where clearly indicated otherwise. Acknowledgement of previously published material and of the work of others has been made through appropriate citation, quotation or both.

Statement of copyright

This deliverable is released under the terms of the **Creative Commons Licence** 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

Organisations

bremen online services (main editor), Germany, http://www.bos-bremen.de

CNIPA (Centro Nazionale per l'Informatica nella Pubblica Amministrazione[1]) , Italy, www.cnipa.gov.it

DIFI (Direktoratet for forvaltning og IKT[2]) , Norway, www.difi.no

DILA (Direction de l'Administration Légale et Administrative Of French Prime Minister Office), France

InfoCamere, Italy, www.infocamere.it

Persons

Adriano Rossi, CNIPA

Ahmed Yacine, DILA

Alexander Funk, bos

Andreas Wall, bos

André Jens, bos

Daniel Eggert, bos

Edgar Thiel, bos

Frank Olthhoff, bos

Frank Schipplick, bos

Jon Olnes, DIFI

Lars Thölken, bos (editor)

Nils Büngener, bos

Piero Milani, InfoCamere

[1] From 29th December 2009, CNIPA will be renamed DigitPA (Legislative Decree 1st December 2009, n. 177)

[2] English: Agency for Public Management and eGovernment

Table of Contents

CC BY

1 Introduction

1.1 Reading instructions

This deliverable sets the background for a set of common documents,. A list of used abbreviations and terms, with their definitions, can be found in Deliverable 7.3b. The basis for the implementation and the complete specification is given in deliverable 1.1[3].

This document includes the same common, generalized introduction as all other PEPPOL Infrastructure deliverables so this introduction can be assumed for subsequent Infrastucture deliverable documents. This deliberate duplication allows each Deliverable to be read in isolation.

This common introduction includes a description of the approach adopted for designing the infrastucture specifications.

Chapter 2 contains the description of the prototype architecture and the used components. Also important parts of the WP1 specification, given in deliverable D1.1, are presented there to underline the boundaries.

Chapter 3 provides a description and specification of the trust model of the PEPPOL validation infrastructure.

Chapter 4 provides the member state specific description and characteristic of the validation infrastructure.

Attachment A contains the documentation of the installation and administration guidelines for the PEPPOL open source component XKMS responder.

Attachment B contains the specifications for the validation client. It is mainly divided into a user guide for graphical use interface based, stand alone version, and specifications regarding the integration version, to enable developers to use this version for integration into other applications and platforms.

1.1.1 Target Audience

The prototype documentation will be used by PEPPOL consortium members and shall help them to handle the software components. These require different depths in information, due to the different character of the provided components. In general, basic knowledge in public key infrastructure should be given.

Standard Users

The Documentation of the stand alone validation software “Signer Basic Edition” as described in Annex B is documentation designed to serve users with no special technical knowledge. It is however, assumed that the readers have the ability to use standard software products.

Developers

The documentation of the “Signer Integration Edition” (the second part of annex B) is designed to enable developers to integrate the software functions into other applications. This ability requires a more profound knowledge of software engineering.

Administrators

[3] The current version of the deliverable can be found on www.peppol.eu in the section results.

CC BY

Annex A deals with the server component PEPPOL XKMS responder. The document will help server administrators to install, configure, maintain and host the component. To use the documentation requires general abilities in administering server applications.

1.2 Deliverable objective

This document represents Deliverable 1.2 (D1.2: Trans-national verification solution(s) - Prototype Documentation of the PEPPOL project (Pan-European Public Procurement OnLine), created by PEPPOL work package 1 (WP1) - eSignature.

The aim of this deliverable is to support the implementation of the PEPPOL eProcurement pilots by describing the components needed and building block provided for implementing eSignature validation into the PEPPOL Infrastructure. These descriptions are applicable to both Contracting Authorities and their Suppliers (Economic Operators) and their technology and/or service providers.

Implementation of these specifications, in conjunction with the PEPPOL Transport Infrastructure (Deliverables 8.2), addresses the PEPPOL Infrastucture on Technical interoperability layers of the European Interoperability Framework (EIF) version 2.0.

These descriptions were prepared by PEPPOL Work Package 1 as an outcome from PEPPOL's Proof-of-Concept for eSignature (D1.1). It is anticipated that updates will be required during the Test and Production Pilot phases of the PEPPOL project as part of PEPPOL's overall support and governance policy.

1.3 Deliverable summary

This documentation supports the usage of the provided software components and the setting up of test pilot implementations. Due to the character of the prototype, this document serves as a software handbook for users of the given components and as an interface description to enable developers to integrate functions of the provided components into other systems.

First of all this deliverable is documentation of the reference implementation of WP1 - eSignature. Hence, it depends on "PEPPOL Deliverable D1.1 Requirements for Use of Signatures in Public Procurement Processes", which provides the specifications.

The main character of the prototype provided by WP1 is the provision of a validation infrastructure for qualified certificates that can be used, not only within the PEPPOL project or for procurement processes, but in general for any request for certificate validation that may arise in a cross European context.

The PEPPOL Infrastructure Report and Prototype deliverables follow the same overall structure as outlined in Figure 1. The main document will describe the specifications and any reference implementations and refer to other common guidelines and/or software components.

CC BY

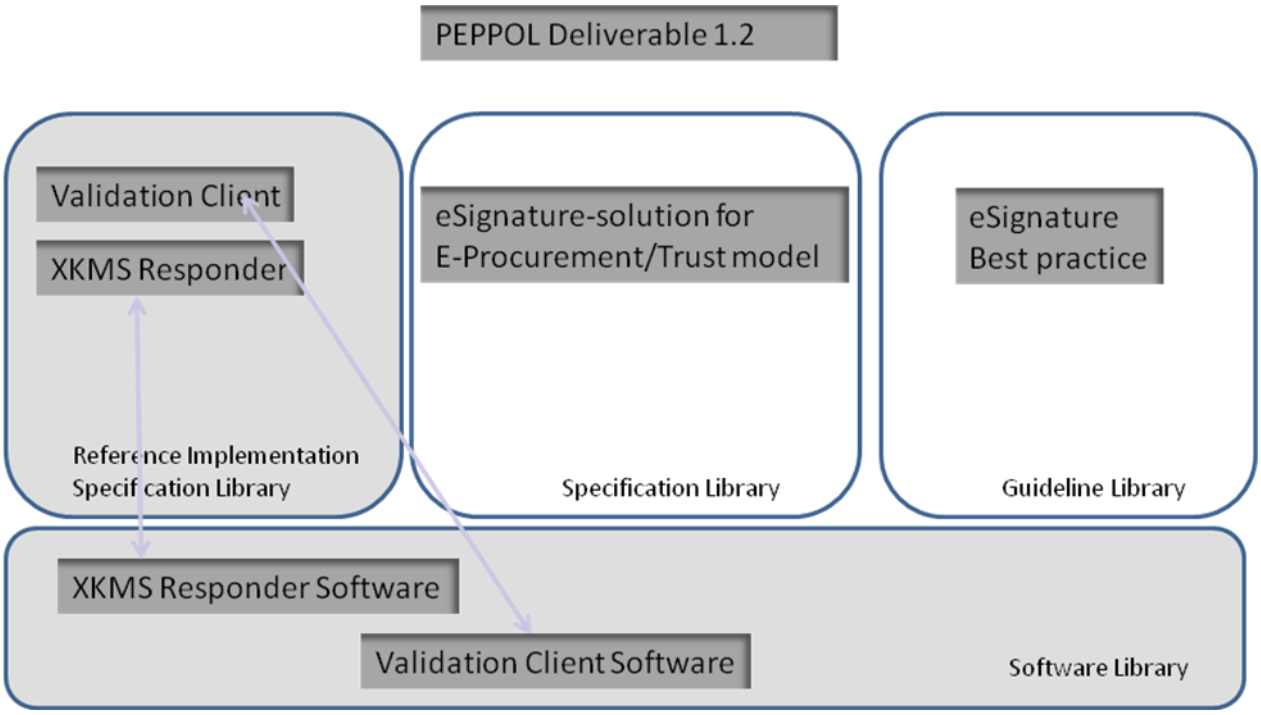

Figure 1: Structure of PEPPOL eSignature Validation Infrastructure Deliverable

As the figure depicts, the main deliverable is a document composed of various annexes (shown as shaded) categorised as Profiles, Reference Implementations, Common Guidelines and Software Components.

The deliverable describes a Reference Implementation and accompanying Software components based on WP1 deliverable 1.1 Specification of eSignature-solution for E-Procurement/Trust model (Both deliverables 1.1 and 1.2 will be evaluated during the test pilot phase and revised to form deliverable 1.3 Demonstrator and Revised Specification eSignature-solution for E-Procurement/Trust model)

1.4 The PEPPOL project

PEPPOL (Pan European Public Procurement On Line) is a 42 Month (May 1st 2008 – October 31st 2011) pilot project under the European Commission's CIP (Competitiveness and Innovation Programme) initiative.

The project aims to align business processes for eProcurement across all Government Agencies within Europe. The vision is that any company and in particular small and medium-sized enterprises (SMEs) in the EU can communicate electronically with any European governmental institution for the entire procurement process.

On May 1st 2010, following a specification phase and a development phase, PEPPOL entered its test pilot phase and from November 1st 2010 will be supporting production pilots.

The PEPPOL consortium comprises of the leading public eProcurement agencies in Austria, Denmark, Finland, France, Germany, Italy, Norway and Hungary. These have recently been joined by agencies from Greece, Portugal, the UK and Sweden.

The scope and structure of the PEPPOL project is shown in Figure 2. In addition to the work packages shown, WP6 provides project administration and WP7 supports awareness, training and consensus building.

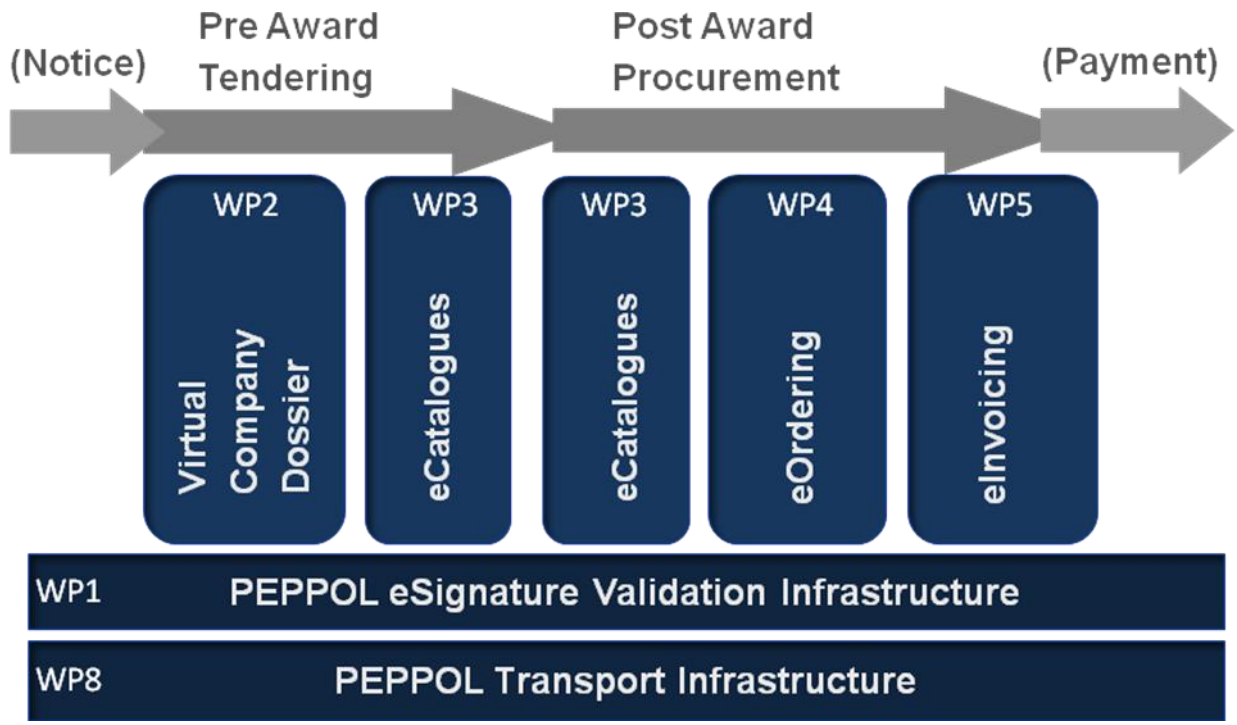

Figure 2: Structure of PEPPOL project

1.5 PEPPOL eProcurement Objectives

The broader vision for PEPPOL is that any company (incl. SMEs) in the EU can communicate electronically with any EU governmental institution for all procurement processes.

The objectives for eProcurement are set by PEPPOL stakeholders. These include:

- Project owners: The sponsors of PEPPOL i.e. EU commission and the beneficiary Member States.
- WP participants: Member States participating in specific PEPPOL work packages.
- Non-beneficiary Member State: stakeholders that gain benefits from the pilot i.e. EU member countries not participating in PEPPOL.

The project owner objectives can be deduced from the I2010[4] strategy, CIP ICT PSP[5] project call and country specific reasons for joining the project. Collectively this can be viewed as supporting a single European market, competiveness and innovation by...

- Removing barriers for cross-border eProcurement
- Learning through implementation and operation of eProcurement pilot systems
- Raising awareness of eProcurement benefits through a pilot

PEPPOL has adopted a broad definition for cross-border eProcurement. In a typical case a Contracting Authority and an Economic Operator (who may be an SME) are situated in different member states. However, there are also cases where an eProcurement platform is operated in a country different from either the Contracting Authority or the Economic Operator. In the scope of

[4] http://ec.europa.eu/information_society/eeurope/i2010/strategy/index_en.htm

[5] http://ec.europa.eu/information_society/activities/ict_psp/index_en.htm

CC BY

PEPPOL these are also considered as cases when the “cross-border” characteristic can be a barrier to interoperability.

Pilot participant objectives can be deduced from country specific reasons for participating in the project:

- Leveraging existing solutions to handle cross-border eProcurement
- Create traction on interoperability model, thereby securing the investment in the chosen eProcurement interoperability model
- Influence on standardization activities in such a way that they meet the requirements of the participant

There is a strong desire by both Contracting Authorities and Economic Operators for automation and efficiency across the procurement process. This requires good interoperability - that is a common information and process model ensuring a flow of meaningful information between different parties of the process. As mentioned above these interoperability requirements have been analyzed according to the European Interoperability Framework.

Non-beneficiary Member State objectives can be deduced from country specific reasons for joining the reference group, for example:

- Leveraging and building upon the experience of the PEPPOL eProcurement project.
- Cost saving by adopting a proven eProcurement interoperability model

Two separate outcomes for PEPPOL deliverables have been identified:

- Interconnecting the eProcurement platforms of Contracting Authorities in participating countries for engaging Economic Operators in other countries.
- Making available open source software together with tools to deal with eProcurement both for Contracting Authorities and Economic Operators (especially SME’s).

PEPPOL has built upon existing work in these areas and continues cooperation with current initiatives.

1.6 PEPPOL Interoperability Approach

The objective of a PEPPOL profile is to specify in details the interoperability requirements and solutions on all interoperability layers to (part-of) an eProcurement process.

The European Interoperability Framework’s[6] (EIF) goal is:

- To serve as the basis for European seamless interoperability in public services delivery, thereby providing better public services at EU level.
- To support the delivery of Pan-European eGovernment Services (PEGS) by furthering cross-border and cross-sector interoperability.
- To supplement the various National Interoperability Frameworks in the pan-European dimension.

Version 2.0 of the EIF defines these interoperability layers as Political, Legal, Organizational, Semantic and Technical. PEPPOL has specialised the EIF 2.0 as shown in figure 3. The Legal and Organisation Business Layer sets context, scope and requirements to the solutions classified into the layers: Organisation Process, Semantic, Technical Interaction and Tecnical Transport Layers.

[6] http://ec.europa.eu/idabc/servlets/Doc?id=31597

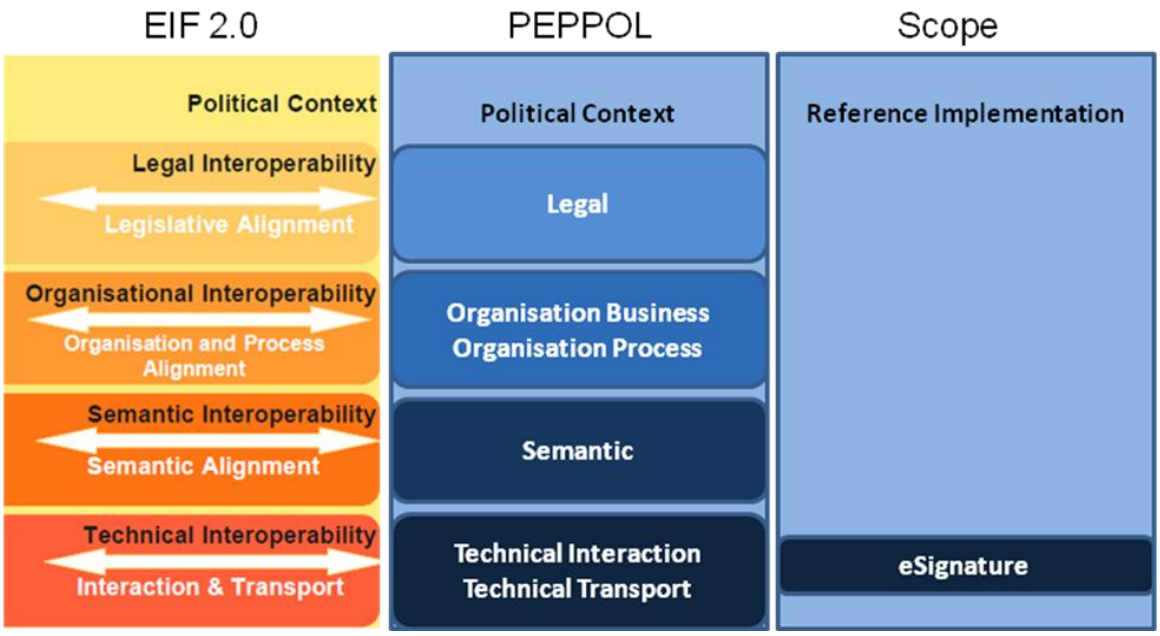

Figure 3: PEPPOL Interoperability approach

2 Introduction of the Prototype

This chapter introduces to the prototype architecture, the used components, their functions and the sourcing specification (WP1 D1.1). Chapters 2.5.2 and 2.5.3 are taken from the D1.1 specification and are not meant as a substitute for it, but to highlight the most important aspects for the implementation and the further possibilities of the PEPPOL validation infrastructure (even though the solutions might not yet be in place). The specification, which was the basis for the current implementation work, is currently under revision while this deliverable is being published. The next formal version of D1.1 will be delivered at the end of October 2010.

2.1 Abstract

This document describes the sample or Reference Implementation used to establish the validation infrastructure. The PEPPOL validation infrastructure is open to be implemented in several ways and will most likely have a different character at the end of the project, than it has in this first implementation. The building blocks created for this are issued with this document.

The PEPPOL prototype consists of several components which are part of this documentation:

- XKMS responders for certificate validation and
- PEPPOL public registry services for request mapping and configuration of servers.

Additional client components will be provided for the piloting:

- Stand-alone validation software and
- Validation software function libraries for integration.

In addition to describing the specific components, some explanations regarding other possibilities of implementing the PEPPOL validation infrastructure are also part of this document. For example, the description of the architecture mentions the “OASIS DSS interface option”. Although this will not be implemented for the first version of the PEPPOL test pilot, information about other options might be valuable for pilot participants, so these are includedin the more generic parts in the documentation.

The basis for the implementation of the components described in this documentation is mainly given in the first deliverable of work package 1 (D1.1). The main boundaries between D1.1 and the prototype are highlighted in this document.

The PEPPOL pilot will also include other software, such as procurement platforms or solutions, which will have to be connected to the PEPPOL validation infrastructure. These components are not part of the prototype and therefore not part of this documentation.

2.2 Definitions

Definition of the prototype

The topic of this document is the prototype as provided by Work Package 1. It consists of the technical components that establish the PEPPOL certificate validation infrastructure and is therefore the technical basis of the pilot.

The different components of the prototype have different characteristics regarding their significance and legal standing within the PEPPOL project. For instance, the PEPPOL XKMS responder will be made available as open source software, but the validation client will not. The validation client was

added to the project to enable project teams to use validation functionalities as easy and soon as possible, but it is not a necessary component to establish the validation infrastructure.

Definition of the demonstrator

The demonstrator is the prototype refined after the testing phase and revision of specification. The software components of the demonstrator are a formal deliverable of WP1.

Definition of the pilot

The WP1 pilot consists of the demonstrator, test, productive scenarios, data, and test and evaluation plan.

2.3 Prototype architecture

The PEPPOL validation infrastructure will consist of two main functional infrastructure components for the validation of certificates:

- Validation authority in two options: XKMS responder and OASIS-DSS interface,
- PEPPOL Public Registry Service.

The PEPPOL validation infrastructure is designed to deal with any document used in the procurement process. PEPPOL aims to explore both options for the validation authority; the first option (XKMS responder) is currently realised and described in this documentation. In the following the term “Validation Service” (VS) will be used, which means a more specific entity, like a XKMS responder.

To provide a maximum flexibility for the implementation of the PEPPOL validation infrastructure, different instances of validation services (VS) have to be assumed, which in general have a limited Certificate Service Provider (CSP) coverage. To extend this limit it is necessary to create a trusted network of VS, each with a different coverage of CSPs.

As a major characteristic of the PEPPOL validation infrastructure, any participant who requests a certificate validation needs to have access to only one validation service, which could be national, for example for one member state.

There are two possible cases:

1. The validation service of member state Y is able to handle requests locally, validates certificates against configured Certificate Service Provider and returns responses.
2. The validation service of member state Y is not configured to validate the given certificates; it mediates requests to an XKMS responder that can handle the request (presumably close to the sender). The recipient’s responder re-signs results to establish trust.

As soon as this validation service doesn’t have the coverage to validate the certificate in question, it forwards the request to another validation service that has. The information about a validation service that has the requested coverage will be provided through the PEPPOL Public Registry Service (PPRS).

The validation service in member state X is required to maintain updated information about all accredited/supervised CSPs in member state X, at least CSPs issuing qualified certificates. Updated information can be obtained by TSLs issued by the appropriate authority in member state X.

Given an unknown certificate the validation service in the member state Y:

1. Is configured via PPRS on how to contact and request the validation service in member state X
2. Asks validation service in member state X for the end-user certificate validation

Validation service in member state X:

3. Checks via OCSP or CRL the current end-user status
4. Sends the validation results to validation service in member state Y

Validation service in member state Y:

5. Sends the validation result to the requesting application. The recipient's validation service re-signs the result to establish trust.

The following figure describes the flow related to signatures for a tendering pilot with verification at receiving side, where the XKMS responder mediates the validation request to the responder of member state X.

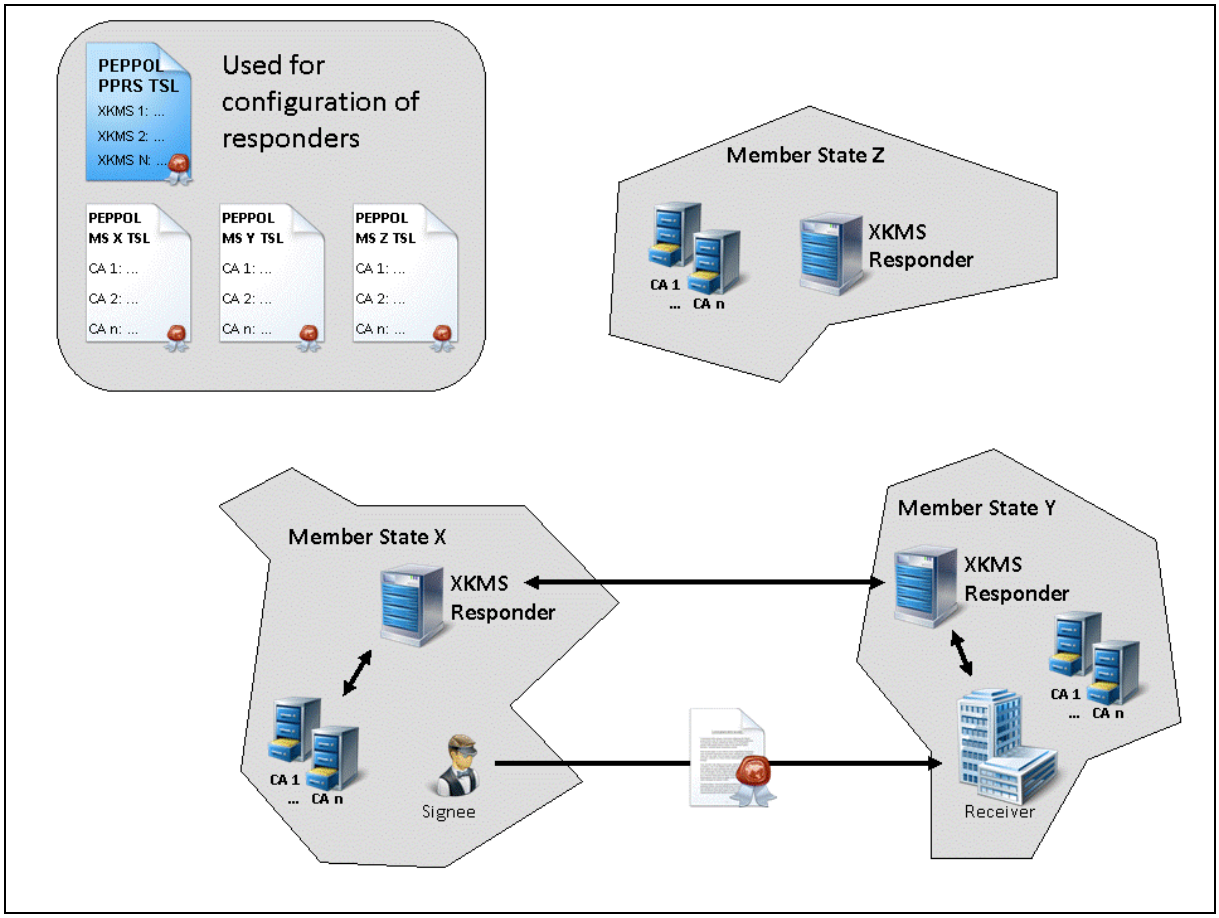

Figure 4: Overview of validation process

For the pilots Validation Services will be realised by different XKMS responder instances. The first version of the test pilot consisted of three member-state specific instances, which all have the coverage for several national CSPs (see chapter 4). The XKMS responders used were configured and tested in a lab-test before they were installed in the different member states.

2.4 Components used

The PEPPOL validation infrastructure is able to be used in many contexts. Requests can be generated by client software or procurement systems, at any point of the procurement process where certificate validation is needed. To facilitate the testing of the infrastructure for all parties and provide another possibility to integrate functions for validation into software systems, PEPPOL WP1 provides both the infrastructure components and the validation software.

CC BY

2.4.1 PEPPOL XKMS responder

For the pilots it is necessary to implement a PEPPOL XKMS responder. This infrastructure component has the following features:

- The PEPPOL XKMS responder can validate certificates against configured Certificate Authorities.
- It can use the PEPPOL Public Registry Service (see below) to pass XKMS requests towards other PEPPOL XKMS responders. Therefore it is crucial that the component can handle XKMS v2 requests and responses.

For further information concerning the XKMS responder please read Annex A.

2.4.2 PEPPOL Public Registry Service (PPRS)

The second infrastructure component of the PEPPOL validation infrastructure is the PEPPOL Public Registry Service (PPRS). This provides information about available VSs, organised in the form of a Trust-service Status List ("TSL" as defined by ETSI TS 102 231) as recommended by the IDABC expert group advising actions related to the EU Service Directive. The PPRS will contain a TSL of trusted XKMS responders to create a trusted network of validation services.

Initially, this will be published in a human readable format; and PEPPOL XKMS responder instances will be configured using this information. Eventually this will be published in a machine processable format (XML and possibly also ASN.1). In both stages the authenticity of the list will be assured by means of an electronic signature from the TSL issuer. Public keys of the TSL issuers will be published on the PEPPOL web site.

It will be structured into the following categories of information:

- Information on the trusted list issuing scheme
- Information about specific trusted service/s (XKMS)
- Information about the status of the trusted service regarding the scheme policy.

For Certificate Authority services, each EU member state is expected to make available a TSL about qualified (respective accredited) Certificate Authorities active in their region up until the end of 2009. These TSLs must be accessible online and must be maintained in the future by the respective authorities of the memberstates. When published, the national TSLs will be inspected with respect to their applicability for PEPPOL. Until then, the PEPPOL TSL will be self edited by the project members. For further information concerning the PPRS please read chapter 3.

2.4.3 Stand-alone validation software

As mentioned above, WP1 provides validation client software to enable pilot participants to use validation functionalities without creating software themselves. The software component is documented in this deliverable's Annex B and made available for the PEPPOL community for the project duration.

The validation client is based on a product of bremen online services, the "Governikus Signer" and has two versions: "Basic Edition" and "Integration Edition". In the context of PEPPOL, its main function is the validation.

Due to the fact that the product branding is hard to eliminate entirely, the name "Signer" appears often in the documentation. The reader of the documentation should bear in mind that the "Signer" or "Governikus Signer" in the context of this project means "PEPPOL validation client".

CC BY

Validation Client Basic and Integration Edition

The validation client exists as both a stand-alone solution and an integrable function library (Integration Edition) for integrating business process applications. Both include a verification component that allows verification of signatures and validation of signature certificates.

The *validation client* is a standalone application, that verifies signed documents and certificates through a graphical user interface. The verification results are summarized in a validation protocol (inspection sheet). This bulding block is a Java™ application, i.e. common operating systems such as MS Windows™ and SUSE Linux™ are supported.

The *validation client integration* allows functions to be called from a third application, providing a functional extension for business applications without complex changes. All functions (sign, verify, encrypt, decrypt) can be accessed either locally (via Java API, command line) or by means of a dynamic web call (with JNLP/JSP). A SOAP™ based interface is provided as well. All functions are called by pre-defined parameters, so that an existing business process application does not need modification.

Various kinds of document formats (for example, Word, Excel, PDF, XML data) are supported by the validation client. It can verify single documents, several documents or the contents of complete directories.

The validation client has been created by bremen online services GmbH & Co. KG, and declared as “foreground”. It is not planned to implement special features for the PEPPOL project. The Signer will be connected to the PEPPOL Infrastructure via a configured XKMS responder.

For the standalone edition, only verification and signing will be available. For further information concerning the validation client please see Annex B.

2.5 General Functions of Prototype

The main character of the prototype is the provision of services for certificate validation based on the XKMS protocol. These services are openly available, not only for PEPPOL but for any scenario where cross border certificate validation is requested.

To enable all PEPPOL participants to start piloting with electronic signatures, WP1 provides a software component (as mentioned above) that can validate certificates using the PEPPOL validation infrastructure. The prototype is also availiable to other applications or software systems that are used in the PEPPOL piloting.

2.5.1 Validation Service

eSignature interoperability for PEPPOL focuses on the receiving and verification of signatures. This assumes all participants are able to sign inside their corporate infrastructure or through their service providers (operator systems in the figures below). Since interoperability requires more than merely cryptographic verification and validity checking (OCSP or CRL), PEPPOL specify two interface profiles of XKMS v2 and OASIS DSS (Digital Signature Service) in parts 5 and 6 of D1.1 respectively. Participants can use these interfaces to obtain the necessary verification information.[7]

2.5.2 Certificate Validation by XKMS

2.5.2.1 PEPPOL XKMS responder

For the PEPPOL project the international characteristics concerning digital certificate validation is one of the challenges for the implementation, as there is a big number of certificate authorities with high

[7] The OASIS DSS interface will be realised at a later stage of the project.

diversity in certificates already in use. The PEPPOL XKMS Responder (XKMS Request/Response interfaces) can validate signatures certificates against known Certificate Authorities (Certificate Authorities). PEPPOL XKMS responders receive validation requests, verify certificates or mediate requests to other responder instances and return validation results to the requesting party. The PEPPOL XKMS responder is able to identify signature certificates and allocate them in terms of origin and method of validation. Depending on the given certificate, the XKMS responder requests the responsible Certificate Authority, validates the certificate or forwards the request to another XKMS responder within the PEPPOL infrastructure. The information about European certificates and responsible XKMS responders is stored in the PEPPOL TSL (see description below). For an unknown certificate, the given XKMS responder retrieves the information from the TSL about which XKMS responder is able to validate the certificate and forwards the request to that responder. This then validates the certificate and gives back the result to the mediating responder.

The XKMS responder will then sign the result of the certificate validation and return it back to the requester party. With this approach, the requester only needs one access point to the PEPPOL validation infrastructure (e.g. their national XKMS responder). This will respond with a signed validation result for any European signature certificate.

The communication between different XKMS responder instances is done according to a special profile of the XKMS 2.0 specification that was developed within the PEPPOL project, based on the XKISS subset of the XKMS protocol (http://www.w3.org/TR/xkms2/). PEPPOL has enriched the profile with several data fields to provide information about the quality of the certificate in question orthe reason for its suspension (if given).

The PEPPOL validation infrastructure is open for different implementations. It is possible to have a primary XKMS responder for each member state. These national XKMS responders can also be responsible for the validation of certificates of different member state, depending on agreements between them. The responsible XKMS responder can support the specific national Certificate Authorities and be configured to request validation according to the specific national regulations and laws. The model is also open to Validation Services that are not bound to the national level, e.g. commercial Validation Services covering a set of Certificate Authorities on an international level. Such a Validation Service may also in turn call national Validation Services obtained from the PPRS when encountering a Certificate Authority outside of its own domain.

A reference implementation of the PEPPOL XKMS responder has been developed in Bremen/Germany. This component can be used during the period of the project to provide the validation infrastructure. Bremen also offers the hosting of the responder instances or member states are able to host and develop their own, following the PEPPOL specification.

Upon obtaining a request (sent over the PEPPOL transport infrastructure or otherwise), the validation process on the recipient side is as follows:

1. The recipient selects an XKMS service to call. Presumably this will be a service selected and trusted by the recipient but it may also be selected from a TSL (Trust Service List) or by a registry lookup.
2. If the Certificate Authority is known locally, the local XKMS service only has to perform an OCSP (or CRL) call to the Certificate Authority that has issued the sender's electronic identity (eID).
3. If the Certificate Authority is not known, the local XKMS service does a TSL lookup (or perhaps registry lookup or even local configuration) to reveal some other XKMS service that can handle the Certificate Authority.
4. The request is forwarded to this remote XKMS service. This requires trust to be established between the two XKMS services. The local XKMS service must trust the remote one with respect to quality of service and liability in case of an erroneous answer, the remote XKMS service may have trust issues such as receiving payment.

5. The remote XKMS service obtains necessary information from the Certificate Authority (OCSP, CRL) and forms a ValidateResponse that is signed and sent back to the local XKMS service.
6. The validation result from the remote XKMS responder is re-signed (possibly also further processed) by the local XKMS responder since this is the one trusted by the recipient.

A trust structure must exist to enable mutual trust between the two XKMS responders as mentioned in point 4 above.

In both cases 2 and 3-6, it is the local XKMS service that shall sign the validation result returned to the recipient. This can include liability and other issues, depending on whether the service is a validation authority or a more technical validation service.

2.5.2.2 XKMS extensions defined for PEPPOL

For XKMS messages an abstract extension point (xkms:MessageExtension) is availiable to carry additional information. Some MS e.g. Germany, require detailed information on certificate quality and validity status as well as the validation process itself. If requested by a message extension in the respective validate request, an (/xkms:ValidateResult) should contain an extension block (/xkmsEU:ValidateResultExtLSP) as defined here,

Extended validation information is defined for:

- The quality of a certificate and the issuing CSP
- Details for the validation processing done by a XKMS responder instance
- Details about the Responder itself

It is complemented by possible fault information concerning the processing of the extensions.

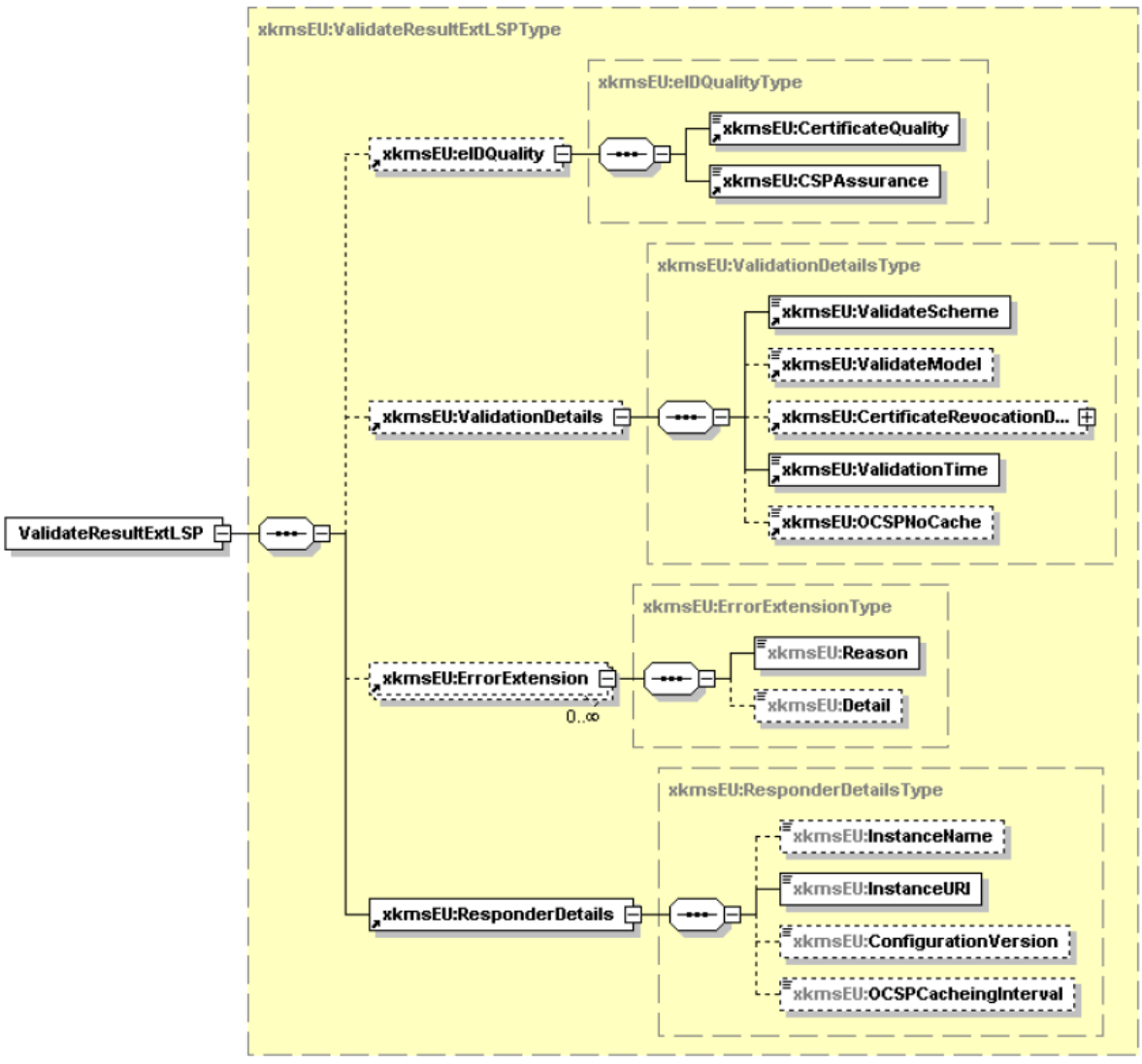

Figure 5: Extension scheme overview

Syntax for the xkmsEU:ValidateResultExtLSP element:

```
<xkmsEU:ValidateResultExtLSP>
      <xkmsEU:eIDQuality>
            <xkmsEU:CertificateQuality>
                  http://lsp.eu/2009/04/certquality#unknown |
                  http://lsp.eu/2009/04/certquality#low |
                  http://lsp.eu/2009/04/certquality#lcp |
                  http://lsp.eu/2009/04/certquality#ncp |
                  http://lsp.eu/2009/04/certquality#ncpplus |
                  http://lsp.eu/2009/04/certquality#qcp |
                  http://lsp.eu/2009/04/certquality#qcpplus
            </xkmsEU:CertificateQuality>
            <xkmsEU:CSPAssurance>
                  http://lsp.eu/2009/04/CSPAssurance#none |
                  http://lsp.eu/2009/04/CSPAssurance#IndependentDocumentReview |
                  http://lsp.eu/2009/04/CSPAssurance#InternalComplianceAudit |
                  http://lsp.eu/2009/04/CSPAssurance#SupervisionWithComplianceAudi
                  t |
                  http://lsp.eu/2009/04/CSPAssurance#ExternalComplianceAudit |
                  http://lsp.eu/2009/04/CSPAssurance#ExternalComplianceAuditCertif
                  ied |
```

```
                http://lsp.eu/2009/04/CSPAssurance#SupervisionWithExternalCompli
                ance Audit |
                http://lsp.eu/2009/04/CSPAssurance#AccreditationWithExternal
                ComplianceAudit
        </xkmsEU:CSPAssurance>
</xkmsEU:eIDQuality> ?

<xkmsEU:ValidationDetails>
        <xkmsEU:ValidateScheme>
                 http://www.lsp.eu/2009/04/valScheme#LOCAL |
                http://www.lsp.eu/2009/04/valScheme#OCSP |
                http://www.lsp.eu/2009/04/valScheme#CRL |
                http://www.lsp.eu/2009/04/valScheme#CRL_LDAP                    |
                http://www.lsp.eu/2009/04/valScheme#LDAP

        </xkmsEU:ValidateScheme>


        <xkmsEU:ValidateModel>
                http://www.lsp.eu/2009/04/valModel#PKIX |
                http://www.lsp.eu/2009/04/valModel#chain                        |
                http://www.lsp.eu/2009/04/valModel#escapeRoute |

        </xkmsEU:ValidateModel> ?


        <xkmsEU:CertificateRevocationDetails>
                <xkmsEU:RevocationTimeInstant>                          xs:dateTime
                </xkmsEU:RevocationTimeInstant>
                <xkmsEU:RevocationReason>
                        http://www.lsp.eu/2009/04/reason#unspecified |
                        http://www.lsp.eu/2009/04/reason#KeyCompromise |
                        http://www.lsp.eu/2009/04/reason#CACompromise            |
                        http://www.lsp.eu/2009/04/reason#AffiliationChanged |
                        http://www.lsp.eu/2009/04/reason#Superseded |
                        http://www.lsp.eu/2009/04/reason#CessationOfOperation |
                        http://www.lsp.eu/2009/04/reason#CertificateHold |
                        http://www.lsp.eu/2009/04/reason#RemoveFromCRL |
                        http://www.lsp.eu/2009/04/reason#PrivilegeWithdrawn |
                        http://www.lsp.eu/2009/04/reason#AACompromise |
                        http://www.lsp.eu/2009/04/reason#none

                 </xkmsEU:RevocationReason>
        </xkmsEU:CertificateRevocationDetails> ?
        <xkmsEU:ValidationTime> xs:dateTime </xkmsEU:ValidationTime>

</xkmsEI:ValidationDetails> ?


<xkmsEU:ResponderDetails>
        <xkmsEU:InstanceName> xs:string </xkmsEU:InstanceName> ?
        <xkmsEU:InstanceUri> xs:anyUri </xkmsEU:InstanceUri>
        <xkmsEU:ConfigurationVersion> xs:string
                </xkmsEU:ConfigurationVersion> ?
        <xkmsEU:OCSPCacheInterval> xs:duration
                </xkmsEU:OCSPCacheInterval> ?
        <xkmsEU:OCSPNoCache> xs:boolean </xkmsEU:OCSPNoCache> ?

</xkmsEU:ResponderDetails>


<xkmsEU:ErrorExtension
        <xkmsEU:Reason=
                http://www.lsp.eu/2009/04/reason#OpaqueClientDataTooLong        |
                http://www.lsp.eu/2009/04/reason#TrustCenterNotReachable        |
                http://www.lsp.eu/2009/04/reason#WrongCertificateFormat         |
                http://www.lsp.eu/2009/04/reason#WrongTimeInstant               |
                http://www.lsp.eu/2009/04/reason#UnkownCA                       |
                http://www.lsp.eu/2009/04/reason#SignatureKeyTooShort
                http://www.lsp.eu/2009/04/reason#Unknown
                http://www.lsp.eu/2009/04/reason#NotUnderstood
```

```
            </xkmsEU:Reason>
            <xkmsEU:Detail> xs:string </xkmsEU:Details>
        </xkmsEU:ErrorExtension> *
</xkmsEU:ValidateResultExtLSP> ?
```

Description of elements and attributes in the schema overview above:

.../xkmsEU:ValidateResultExtLSP ?

Container element carrying all items explained below.

.../xkmsEU:eIDQuality ?

This is an optional container element carrying assurances on certificate quality and issuing CSP status. It MUST be present if certificate validation could be processed. Explicitly requested by a xkms:RespondWith value of http://www.lsp.eu/2009/04/xkmsExt#edIDQuality

.../xkmsEU:eIDQuality/xkmsEU:CertificateQuality

Element of type xs:anyURI indicating the certificate quality. All values in the table below carry the prefix http://lsp.eu/2009/04/certquality#, which is omitted here for readability.

CertificateQuality URI ending	Meaning
unknown	Certificate quality can't be determined
low	Low confidence in certificate but certificate policy exists or quality assessment is possible by other means
lcp	Certificate governed by a certificate policy in compliance with the ETSI TS 102 042 standard for LCP or a similar standard
ncp	Certificate governed by a certificate policy in compliance with the ETSI TS 102 042 standard for NCP or a similar standard
ncpplus	Certificates governed by a certificate policy in compliance with the ETSI TS 102 042 standard for NCP+ or a similar standard (Use of a SSCD is mandated in the CP)
qcp	Certificates governed by a certificate policy in compliance with the ETSI TS 101 456 standard for QCP or a similar standard
qcpplus	Certificates governed by a certificate policy in compliance with the ETSI TS 101 456 standard for QCP+ or a similar standard. (Use of a SSCD is mandated in the CP)

Table 1: Quality of certificate

.../xkmsEU:eIDQuality/xkmsEU:CSPAssurance

Element of type xs:anyURI indicating the certificate issuing CSP status according to D1.1 Part 7, "eID and e-signature Quality Classification", chapter 3.2.3. All values in the table below carry the prefix http://lsp.eu/2009/04/CSPAssurance#, which is omitted here for readability.

CSPAssurance URI ending	Meaning

none	Self assessment only
IndependentDocument Review	Statement of compliance issued by an independent, external unit based on document review only
InternalCompliance Audit	Internal audit carried out periodically concludes compliance to applicable requirements
SupervisionWithout ComplianceAudit	Certificate Authority is supervised by a public, national or international authority according to applicable law to the Certificate Authority
ExternalCompliance Audit	Audit carried out periodically by external, independent auditor concludes compliance to applicable requirements
ExternalCompliance AuditCertified	Audit carried out periodically by external, independent auditor concludes compliance to applicable requirements. Certificate Authority operations are certified in accordance with a relevant standard; OR cross certification with a relevant bridge Certificate Authority has been made; OR the Certificate Authority has obtained membership in a PKI hierarchy as a result of appropriate assessment
SupervisionWith ExternalCompliance Audit	Audit carried out periodically by external, independent auditor concludes compliance to applicable requirements. Certificate Authority is supervised by a public, national or international authority according to applicable law to the Certificate Authority
AccreditationWith ExternalCompliance Audit	Audit carried out periodically by external, independent auditor concludes compliance to applicable requirements. **Certificate Authority is accredited** by a public, national or international authority according to applicable law to the Certificate Authority

Table 2: Certificate Authority Independent Assurance

.../xkmsEU:ValidationDetails ?

This is an optional container element carrying details on the certificate validation. It MUST be present if certificate validation could be processed. Explicitly requested by an xkms:RespondWith value of http://www.lsp.eu/2009/04/xkmsExt#ValidationDetails.

.../xkmsEU:ValidationDetails/xkmsEU:ValidateScheme

Element of type xs:anyURI indicating the mechanism respective the protocol a certificate was validated. All values in the table below carry the prefix http://lsp.eu/2009/04/valScheme#, which is omitted here for readability.

ValidateScheme URI ending	Meaning
LOCAL	Only local checked by responder instance
OCSP	Request to Certificate Authority OCSP responder

CRL	CRL used
CRL_LDAP	CRL and LDAP used
LDAP	Request to Certificate Authority LDAP certificate directory

Table 3: Certificate validation schemes

.../xkmsEU:ValidationDetails/xkmsEU:ValidateModel ?

Element of type xs:anyURI indicating the validation scheme used. All values in the table below carry the prefix http://lsp.eu/2009/04/valModel#, which is omitted here for readability.

ValidateModel URI ending	Validation Process
PKIX	Validation PKIX-conformant (shell-model)
chain	Strict certificate chain validation processing
escapeRoute	Mix of both above as described in [COMMPKI], part 9

Table 4: Certificate Validation Models

- .../xkmsEU:ValidationDetails/xkmsEU:CertificateRevocationDetails ?
    - Container holding details in case of a certificate revoked status.
- .../xkmsEU:ValidationDetails/xkmsEU:CertificateRevocationDetails/
    - xkmsEU:RevocationTimeInstant
    - Time of revocation; type is xs:dateTime.
- .../xkmsEU:ValidationDetails/xkmsEU:CertificateRevocationDetails/ xkmsEU:RevocationReason

Element of type xs:anyURI indicating one of the following revocation reasons outlines in the table below. All values carry the prefix http://lsp.eu/2009/04/reason#, which is omitted here for readability.

RevocationReason URI ending	Meaning
CACompromise	Issuer certificate is compromised
AffiliationChanged	Name or other attributes of certificate owner changed; certificate is not compromised
Superseded	Certificate marked as superseded; certificate is not compromised
CessationOfOperation	Certificate marked as no longer needed; certificate is not compromised
CertificateHold	Certificate withdrawn temporarily; certificate is not

	compromised
`RemoveFromCRL`	Certificate is withdrawn form CRL, reusable again
`PrivilegeWithdrawn`	A privilege documented in certificate is withdrawn
`AACompromise`	The private key of an attribute authority could be or is compromised
`None`	No revocation reason available

Table 5: Certificate Revocation Reasons

.../xkmsEU:ValidationDetails/xkmsEU:ValidationTime

Time of validation processing; element of type xs:dateTime.

.../xkmsEU:ValidationDetails/xkmsEU:OCSPNoCache ?

Optional element of type xs:boolean. It MUST be reported as true, if the OCSP response was not taken from the cache.

.../xkmsEU:ResponderDetails

This container MUST be present, indicating details to the XKMS responder used, otherwise corresponding attributes of the node generating this validation result.

.../xkmsEU:ResponderDetails/xkmsEU:InstanceName ?

Optional element of type xs:string carrying a responder name.

.../xkmsEU:ResponderDetails/xkmsEU:InstanceUri

Mandatory element of type xs:anyURI carrying the responder URI.

.../xkmsEU:ResponderDetails/xkmsEU:ConfigurationVersion ?

Optional element of type xs:string carrying information about the responders configuration version.11

.../xkmsEU:ResponderDetails/xkmsEU:OCSPCacheInterval ?

Optional element of type xs:duration. If a responder uses caching for OCSP responses, the caching interval time SHOULD be reported here.

.../xkmsEU:ErrorExtension *

This optional element is used to report errors concerning the validation process in the attribute:

.../xkmsEU:ErrorExtension/Reason

Element of type xs:anyURI with following possible values; all values carry the prefix http://lsp.eu/2009/04/reason#, which is omitted here for readability.

ErrorExtension/Reason URI ending	Semantics
`OpaqueClientData TooLong`	Length of value of /xkms:OpaqueClientData exceeds 256 byte
`TrustCenter NotReachable`	Responder of certificate issuer Certificate Authority not reached - time-out limit reached or other technical reasons
`WrongCertificateFormat`	Certificate defect or wrong coded

`WrongTimeInstant`	Validation time instant not recognisable or in future
`UnknownCA`	Certificate issuer not known
`SignatureKeyTooShort`	Key length of signature certificate is too short
`Unknown`	Error reason could not be determined
`NotUnderstood`	A request parameter could not be understood, but processing was (partially) possible. The indicated parameter SHOULD be outlined in the xkmsEU:Details element of this xkmsEU:ErrorExtension entry.

Table 6: XKMS error extension: reasons

2.5.3 Signature verification by OASIS DSS

The signature verification by OASIS DSS is still an option for piloting within the PEPPOL project. Eventhough a validation interface is not yet available, the following chapter 2.5.3 provides a brief introduction to the documentation, to give interested partys an implementation guide to the PEPPOL signature validation.

The provision of the OASIS DSS interface is an option within the Norwegian pilot actions, the description of the current situation is given in chapter 4.5 in the Norwegian pilot specification.

2.5.3.1 Interface and Process

The OASIS DSS process is quite similar to the XKMS process. The main difference is that the entire signed document is passed to the service.

The DSS service has the same two options as an XKMS responder for the processing:

- If the Certificate Authority is known locally, only an OCSP (or CRL) call to the Certificate Authority is necessary.
- If the Certificate Authority is not known, a registry (or perhaps TSL lookup or even local configuration) will reveal an XKMS service that can handle the Certificate Authority. An XKMS request is forwarded and the ValidateResult from the remote responder is processed. A trust structure must exist to enable mutual trust between the two actors.

Note that there is no chaining of DSS requests. The service called by the recipient does all signature-processing, although eID validation may be chained on to XKMS services. Thus the structure of co-operating XKMS services is exactly the same in both the XKMS and OASIS DSS cases. Therefore OASIS DSS interface should adhere to the specifications in D1.1 part 6, and the XKMS interfaces for chaining should follow D1.1 part 5.

2.5.3.2 Validation Gateway

Sending the entire content of a signed document to a validation service may reveal confidential information to the validation service and since documents may be large, response time may be slow due to the time needed to transmit the request.

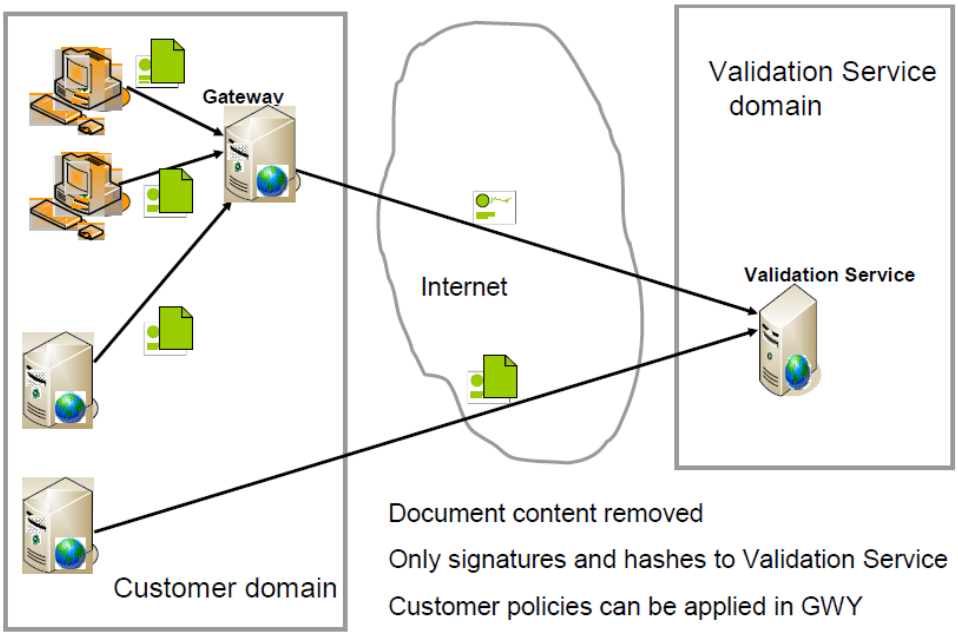

Figure 6: Validation gateway solution

An approach to address this would be to use a gateway deployed in the recipient's IT infrastructure (the possibility of offering a gateway as an external service of course also exists but is not discussed further here), where the gateway removes the document, forwarding only signature fields and corresponding hash values to the validation service.

Such a software gateway maybe installed (with or without separate hardware) in the recipient's network and requests are directed to the gateway as shown in figure 6 (the bottom arrow in figure 6 shows that direct calls to the validation service may still be allowed). In the gateway, signatures are extracted and the corresponding hash values computed from the document. Only signatures and hash values are then sent to the validation service. The content may be disposed of as soon as the request has been sent.

Responses are routed back to the gateway, which in turn must direct the response to the correct end system. It is important to note that the validation service, not the gateway, signs responses since the validation service is the trusted actor. The gateway is only trusted with respect to correct functionality, not to provide assertions about validity of signatures and eIDs.

Additionally, a gateway may be used to enforce recipient specific policies, e.g. ensure uniform quality requirements in all requests sent from the recipient.

The interface to such a gateway would be internal for the recipient. Thus the gateway would offer the same OASIS DSS interface as the validation service, but requirements for request signing can be avoided (the gateway will sign the request anyway). Additionally a web GUI interface may be used, or even an e-mail interface where signed documents can be sent to the gateway as attachments; with the response being attached to a response e-mail.

2.6 Requirements for integration of certificate authorities into the PEPPOL XKMS responder

To enable the PEPPOL XKMS responder to validate certificates of a specific Certificate Authority, technical information about the Certificate Authority and its certificates is required:

- Two "End Entity Certificates" (EE Certificates), (no test certificates)
- Root certificates
- Certificate Authority certificates
- Sub Certificate Authority certificates (if applicable)
- CRL and OCSP signer certificates and those of their certificate chain
- One signature card of the respective Certificate Authority (if possible)
- Signed documents (office documents, PDF, signed with own signature creation software), signed according to at least one of the following formats
  - PKCS#7
  - PDF inline
  - XAdES Basic / XAdES Timestamp / CAdES BES

CC BY

3 PEPPOL validation service trust model

3.1 Premise

This chapter wdescribes the trust model adopted for the PEPPOL pilots. Following the D.1.1. part 4 specifications, the model is based on the standard ETSI TS 102 231. This standard has been recently updated (v.3.3.1 October 2009) and defined by the European Commission, decision 16th Oct. 2009 n.767, the standard model to issue the national trust lists.

Decision 767/2009 Art.2

1. Each Member State shall establish, maintain and publish, in accordance with the technical specifications set out in the annex, a 'trusted list' containing the minimum information related to the certification service providers issuing qualified certificates to the public who are supervised/accredited by them.
2. Member states shall establish and publish, as a minimum, a human readable form of the trusted list in accordance with the specifications set out in the annex.

Decision 676/2009 annex. 1:

- (omitted) The proposed common template is compatible with an implementation based on the specifications from ETSI TS 102 231 that are used to address the establishment, publication, location, access, authentication and trusting of such kinds of lists.

It has to be noted that the present ETSI TSL plug tests, that are still in progress, commissioned by the European Commission, have highlighted some minor issues in implementing the standards. It means that it is reasonable that an update of the standard will be released in the mid-term, so it is probable that the term indicated in the art.3 (end of the year) for the MS TSLs, could be postponed. Based on knowledge of the challenges encountered, we believe that the above issues will not affect the actual specification of the pilot.

3.2 Member states TSLs and PEPPOL public registry server/service

With reference to D.1.1 part 4, § 5.6, we assumed that the WP1 framework was based of validation services anchored in a federation whose trust-relationships were established by the PEPPOL public registry service, containing both certification and validation services compliant to the PEPPOL e-signature verification policy.

In order to be compliant to the EU decision 767/2009 Art.2(1) as much as possible, considering that each member states should implement a TSL containing at least certification service providers issuing qualified certificates (perhaps for the end of the year 2009), it was considered unwise to adopt a different model for the pilot for certification services, so the PPRS will be limited only to validation services information. The pilot will hence provide two kinds of TSLs:

- Member State TSL (MS TSL)
- PEPPOL Public Registry Service TSL (PPRS TSL)

Due to the premises in 3.1, it is possible that such MS TSLs will not be available in time for the incoming PEPPOL pilot phases. Therefore, considering the need to have pilot CSPs not issuing Qualified Certificates, the PEPPOL WP1 may use (at least in the first phases), some PEPPOL MS TSLs that will include subsets of MS accredited/supervised CSPs plus some CSPs not issuing QCs.

CC BY

3.2.1 PEPPOL MS TSL

A PEPPOL MS TSL contains trust service providers, whose Certificate Authority services are compliant to the PEPPOL e-signature verification policy, the so called PEPPOL Certificate Authorities. The PEPPOL policy considers all TSPs compliant that are issuing qualified certificates following the e-signature directive. Since the MS TSLs are PEPPOL MS TSLs the TSL scheme information fields will be filled with reference to the PEPPOL context. In general a PEPPOL MS TSL contains only TSPs issuing qualified certificates, with the exception of the French TSL (and perhaps Norwegian TSL) due to the scarce use of QCs in eProcurement processes.

The PEPPOL MS TSLs are issued under the responsibility of their MS partner administration/company and the PEPPOL MS TSLs are issued in a XML format, compliant to the ETSI TS 102 231 annex B. To build the PEPPOL MS TSL the tool TSLEdit was used (www.osor.eu), plus some minor directly editing of the XML file. The PEPPOL MS TSL, even though in XML format, is intended for human readable purpose, as a trust source for manual setting server components of the XKMS responders. However it is not excluded that in the later pilot phases, the TSL is used for machine processable purposes, with consequent automatic update of the XKMS responders.

3.2.1.1 PEPPOL MS TSL template

URIs and customizations adopted in the template of PEPPOL MS TSL is listed below. The official language is English, hence all the fields with language extension begin with “EN:”. Even though the pilot introduces some limitations/extensions on the number of TSPs present in the trust list, a PEPPOL MS TSL contains only Certificate Authorities issuing qualified certificates in accordance to the e-signature directive and having an official voluntary accreditation scheme, hence only use special URIs or extensions referring to the real national context, apart from the following clauses:

Scheme information

- Clause 5.3.7 (Scheme Information URI)
  - URI:http://www.peppol.eu/wp1/uri/TrstSvc/PEPPOLMSTSL/[CC]/SchemeInformation/) where [CC]=Country Code – in this page it is present a disclaimer that refers to the official MS’s accreditation/supervision scheme and list the considered TSPs
- Clause 5.3.16 – Distribution Points
  - URI:http://www.peppol.eu/wp1/TrstSvc/PEPPOLMSTSL/[CC]/DistributionPoint/[CC]TSL.xml

While those PEPPOL MS TSLs not referring to a national official voluntary accreditation scheme use the additional following customizations

- Clause 5.3.4 – Scheme operator name
  - PEPPOL Consortium
- Clause 5.3.5 – Scheme operator address
  - PEPPOL Consortium Address (Country, City, Street Address, Postal Code, Electronic Address)
- Clause 5.3.6 – Scheme Name
  - Accreditation Status List of qualified certification services from Qualified Certification Service Providers issuing qualified certificates, established in the referenced PEPPOL Consortium Scheme as being compliant with the relevant provisions laid down in the e-signature European Commission Directive 1999/93/EC

CC BY

For those TSLs having non-QC issuers with several level of quality (e.g. French MS TSL), the TSL contains these extra customizations:

Service Information

- Clause 5.5.1 – Service type identifier
  - URI:http://uri.etsi.org/TrstSvc/Svctype/CA/PKC

Addition Service Information

- Clause 5.8.2 - additionalServiceInformation Extension (for quality level definition)
  - URI: http://uri.etsi.org/TrstSvc/eSigDir-1999-93-EC-TrustedList/schemerules/[CC]/[RULES] or more generically http://www.peppol.eu/TrstSvc/PEPPOLMSTSL/[CC]/[RULES]
  - InformationValue: [Level]

3.2.1.2 PEPPOL MS TSL signature

Every new version of a TSL will be signed compliant to ETSI TS 102 231 annex B. The certificates containing the public key to perform the TSL's e-signature verification will be published on the PEPPOL web site in the following URI:

- http://www.peppol.eu/wp1/TrstSvc/PEPPOLMSTSL/[CC]/TSLSignatureCertificate/[CC]TSLSignature.pem – in PEM format

3.2.1.3 Resources

To implement the above TSLs web spaces are to be created wherein the PEPPOL specific URIs and relative documents/files are collected

- http://www.peppol.eu/wp1/uri/TrstSvc/PEPPOLMSTSL/[CC]/SchemeInformation/
  - These pages contain disclaimers that refer to the official MS's accreditation/supervision schemes and list the considered MS TSPs
- http://www.peppol.eu/wp1/TrstSvc/PEPPOLMSTSL/[CC]/DistributionPoint/[CC]TSL.xml
  - Location to published the PEPPOL MS TSL
- http://www.peppol.eu/TrstSvc/PEPPOLMSTSL/[CC]/[RULES]
  - Location where the special MS rules to recognize the non-QC quality levels are published
- http://www.peppol.eu/wp1/TrstSvc/PEPPOLMSTSL/[CC]/TSLSignatureCertificate/[CC]TSLSignature.pem – in PEM format
  - Makes available the certificate containing the public key to perform the PEPPOL MS TSL e-signature verification

3.2.2 PEPPOL public registry service - PPRS

As said above the PPRS is the trust model of the PEPPOL validation services federation. It provides links and rules for requests to the PEPPOL validation service (PEPPOL VS) for the relevant status information about PEPPOL Certificate Authorities. The PPRS is issued under the responsibility of the PEPPOL consortium by means of the WP1 team. The PPRS is issued using the XML format, compliant to the ETSI TS 102 231 annex B. To build the PPRS, the tool TSLEdit is used (www.osor.eu) with some minor directly editing of the XML file.

As for the MS PEPPOL TSLs, the PPRS is intended for human readable use when manually configuring the XMKM responders. This does not exclude further use as machine processable TSL.

Before explaining the components of this special TSL, the following is emphasized:

- Each PEPPOL VS is a national VS. Each VS supports all the PEPPOL Certificate Authorities within its country (and present in its PEPPOL MS TSL).
- If a partner MS doesn't have its own VS, it can delegate it to a foreign partner. In this case the foreign VS must support all the PEPPOL Certificate Authorities within the delegating country.
- It is possible to have more than one VS in a Member State, due to VS's business model or service level agreement reasons.
- A VS can support some foreign PEPPOL Certificate Authorities.
- The federation is also based on a trusted backbone where each service is authenticated using an X.509v3 XKMS server certificate.

The PPRS contains:

- VS general identifiers: names, country, city, street address, postal code, electronic address
- VS digital identifier : digital identifier used to authenticate the service
- VS supply points: where and how to access the service
- VS descriptors: service specific information.

3.2.2.1 PPRS template

In the following the list of ETSI TS 102 231 customisations, adopted for the PPRS, is presented. Since the use of the ETSI standard to describe validation services is not planned to be in the standard itself, all the URIs are PEPPOL relevant. The official language is English, so all the fields with language extension begin with "EN:"

Scheme Information

- Clause 5.3.3 – TSL type
  - URI:http://www.peppol.eu/wp1/uri/TrstSvc/TSLtype/genericTSL/generic/PublicRegistryService-TrustedList
- Clause 5.3.4 – Scheme operator name
  - PEPPOL consortium
- Clause 5.3.5 – Scheme operator address
  - bremen online service CED address (country, city, street address, postal code, electronic address)
- Clause 5.3.6 – scheme name
  - PEPPOL public registry service – PEPPOL federated services
- Clause 5.3.7 – Scheme information URI
  - URI: http://www.peppol.eu/wp1/TrstSvc/Policy/PEPPOLPolicy.htm
- Clause 5.3.8 - Status determination approach
  - URI:http://www.peppol.eu/wp1/uri/TrstSvc/TSLType/StatusDetn/PEPPOLPublicRegistryService /appropriate
- Clause 5.3.9 - Scheme type/community/rules

  - URI: http://www.peppol.eu/wp1/TrstSvc/Policy/PEPPOLPolicy.htm
- Clause 5.3.10 - Scheme territory
  - EU
- Clause 5.3.11 – TSL policy/legal notice
  - The applicable legal framework for the present TSL implementation of the trusted list of national validation services providers for PEPPOL pilot is the PEPPOL policy
- Clause 5.3.16 – distribution points
  - URI:http://www.peppol.eu/wp1/TrstSvc/PEPPOLPublicRegistryService /DistributionPoint/PPRSTSL.xml

TSP Information

Since support of member state Certificate Authorities by multiple PEPPOL VSs, all with the same MS PEPPOL Certificate Authorities coverage, such VSs are collected under a virtual MS validation service. The virtual MS validation service is under the responsibility of the partner MS that manages the eventual agreements with foreign VSs or multiple national VSs. Therefore the virtual MS validation service is described with a standardised name that uses the country code in the search key when browsing the TSL.

- Clause 5.4.1 - TSP name
  - [CC]:PVEIDVS – (see TSP trade name)
- Clause 5.4.2 - TSP trade name
  - PEPPOL [CC] virtual eID validation service
- Clause 5.4.3 - TSP address
  - Physical addresses by the MS partner administration/company
- Clause 5.4.4 - TSP information URI
  - URI: http://www.peppol.eu/wp1/TrstSvc/Policy/PEPPOLPolicy.htm

Service Information

In the actual implementation of the PPRS all XKMS responders use the same WSDL template. Thus contacting them only differs in their IP addresses and ports of the server service. To allow having more than a service for each virtual validation service, the services of PPRS are structured as follows:

- TSP (virtual national VS – one for MS)
  - Validation service 1
    - Service digital Identity 1
    - Service supply points 1
    - Service information extensions 1
  - ….
  - Validation service n
    - Service digital Identity n
    - Service supply points n
    - Service information extensions n

It means that if a VS supports more than an MS, it has entries among the services of all supported MSs. In particular

- Clause 5.5.1 - Service type identifier
  - URI:http://www.peppol.eu/wp1/uri/TrstSvc/Svctype/VS
- Clause 5.5.2 - service name
  - PEPPOL [CC] virtual eID validation service
- Clause 5.5.3 - service digital identity
  - X.509v3 XKMS responder server certificate
- Clause 5.5.4 - service current status
  - URI:http://www.peppol.eu/wp1/uri/TrstSvc/Svcstatus/PEPPOLPublicRegistryService /acceptedvalidationservice
- Clause 5.5.5 - current status starting date and time
  - Pilot phase 2 start date
- Clause 5.5.6 - scheme service definition URI
  - URI: http://www.peppol.eu/wp1/TrstSvc/Policy/PEPPOLPolicy.htm
- Clause 5.5.7 - service supply points
  - URI:[IP address]:[port number]
- Clause 5.5.9 - service information extensions

The use of this field is dedicated to specify special service features such as service fees or SLAs. The optional entry are pairs of URIs, where the first is to declare the type of extension, the second to specify the URI where to find out the relevant service policy.

- URI:http://www.peppol.eu/wp1/uri/TrstSvc/PEPPOLPublicRegistryService /SvcInfoExt/ServiceFee
  - URI:URI to service policy
- URI: http://www.peppol.eu/wp1/uri/TrstSvc/PEPPOLPublicRegistryService /SvcInfoExt/ServiceLevelAgreement
  - URI:URI to service policy

All the pairs are marked as critical compliant to the EU Decision 767/2009 Annex.

3.2.2.2 PPRS TSL signature

Every new version of TSL will be signed compliant to ETSI TS 102 231 annex B. The certificates containing the public key to perform the TSL's e-signature verification will be published on the PEPPOL web site in the following URI:

- http://www.peppol.eu/wp1/TrstSvc/PEPPOLPublicRegistryService /TSLSignatureCertificate/PPRSignature.pem – in PEM format

3.2.2.3 Resources

To implement the above TSLs web spaces must be created wherein the PEPPOL specific URIs and relative documents/files are collected:

- http://www.peppol.eu/wp1/uri/TrstSvc/TSLtype/genericTSL/generic/PublicRegistryService-TrustedList
  - Meaning: The PEPPOL public registry service is the list of trusted validation service within the PEPPOL pilot context/environment
- http://www.peppol.eu/wp1/TrstSvc/Policy/PEPPOLPolicy.htm
  - Where it is published the PEPPOL e-signature verification policy
- http://www.peppol.eu/wp1/uri/TrstSvc/Svctype/VS
  - Meaning: this service provides status information about eID certificates issued by a set of supported certification service. Note: this service is not planned to be in the ETSI TS 102 231 standard. Thus as alternative the service could be treated with the standard URI: http://uri.etsi.org/TrstSvc/Svctype/unspecified, but it would require a further specification as validation service in the clause 5.5.9 - service information extensions (e.g. URI:http://www.peppol.eu/wp1/uri/TrstSvc/PEPPOLPublicRegistryService /SvcInfoExt/VS).
- http://www.peppol.eu/wp1/uri/TrstSvc/TSLType/StatusDetn/PEPPOLPublicRegistryService /appropriate
  - Meaning: Services listed have their status determined by the PEPPOL consortium.
- http://www.peppol.eu/wp1/TrstSvc/PEPPOLPublicRegistryService /DistributionPoint/PPRSTSL.xml
  - Where it is published the PPRS TSL.
- http://www.peppol.eu/wp1/uri/TrstSvc/Svcstatus/PEPPOLPublicRegistryService /acceptedvalidationservice
  - Meaning: the Validation service, for its reference Member State, supports the validation of eID certificates (QC or non-QC) issued by all the Certification Service Providers present in relative PEPPOL Member States TSLs.
- http://www.peppol.eu/wp1/uri/TrstSvc/PEPPOLPublicRegistryService /SvcInfoExt/ServiceFee
  - Meaning: When a VS is provided under service fees the URI is followed by a URI pointing to a service policy indicating fees and conditions.
- http://www.peppol.eu/wp1/uri/TrstSvc/PEPPOLPublicRegistryService /SvcInfoExt/ServiceLevelAgreement
  - Meaning: If this extension (optional) is filled for a VS, it means that the service maintainer wants to specify its availability (and consequently liability) in restricted days of the year or times of the day or of the week. This extension (critical) is followed by a URI pointing to a service policy regarding availability times of the service.
- http://www.peppol.eu/wp1/TrstSvc/PEPPOLPublicRegistryService /TSLSignatureCertificate/PPRSignature.pem – in PEM format
  - Where is available the certificate containing the public key to perform the PPRS TSL e-signature verification

4 PEPPOL MS pilot specification

4.1 French pilot specification

For the French contribution, DILA (Direction de l'Administration Légale et Administrative Of French Prime Minister Office) is responsible for

- hosting of the French PEPPOL XKMS responder and
- implementation and hosting of the French PEPPOL TSL.

4.1.1 French PEPPOL TSL

The French PEPPOL TSL contains accredited Certification Service Providers issuing Qualified Certificates

- Certinomis
- BANQUE POPULAIRE - CLICK AND TRUST
- Dhimyotis (Certigna)

4.1.2 French PEPPOL validation service

The French PEPPOL Validation Service will be hosted by DILA (Direction de l'Administration Légale et Administrative Of French Prime Minister Office)

4.2 German pilot specification

For the German contribution, bremen online services is responsible for

- Implementation of PEPPOL XKMS responder server components,
- Hosting of the German PEPPOL XKMS responder,
- Implementation of PEPPOL validation client and
- Implementation of the German PEPPOL TSL.

4.2.1 German PEPPOL TSL

The German PEPPOL TSL contains accredited certification service providers issuing qualified certificates.

- TeleSec
- TC-Trust
- Bundesnotarkammer

4.2.2 German PEPPOL validation service

The German PEPPOL Validation Service will be hosted by bremen online services GmbH & Co. KG

CC BY

4.3 Greek pilot specification

When this version of the documentation was finalised, information about the Greece pilot specification was not available. It will be added most likely in the next version of the documentation.

4.4 Italian pilot specification

Italy initially was represented by two beneficiaries: CNIPA[8] and InfoCamere. Unfortunately CNIPA (DigitPA in the following) left the PEPPOL consortium during the preparation of the documentation. Due to this fact, the Italian pilot specification is devided in a generic Italian part regarding the Italian PEPPOL TSL, as also DigitPA contributed to prepare the information, and a InfoCamere relating part for the rest, as infoCamere is currently the only Italian WP1 member.

4.4.1.1 Italian PEPPOL TSL

The Italian PEPPOL TSL contains only Italian accredited Certification Service Providers issuing Qualified Certificate compliant to the CNIPA's Decree 21th May 2009, n. 45.

For Phase 1 it has been considered the CSP InfoCert (www.infocert.it) that is the first in term of number of Qualified Certificates issued.

For Phase 2 the following CSPs will be added:

- Actalis S.p.A. – www.actalis.it - with relevance in the Italian National Service Card context;
- Lombardia Integrata S.p.A. Servizi Infotelematici per il Territorio (LISIT) – www.lisit.it - with relevance in the Lombard Regional Service Card context.

For the following Pilot phases will be taken in account at least the following further important CSPs:

- I.T. Telecom S.r.l. – http://www.ittelecom.it
- Postecom S.r.l. – www.poste.it
- ARUBA Posta Elettronica Certificata S.p.A. – ca.arubapec.it

The relevant data and test files/certificates have been gathered by mean of the questionnaire supplied by bos the last July 2009.

4.4.1.2 PPRS TSL

See 3.2.1.3.

4.4.2 Pilot Specification by InfoCamere

InfoCamere will establish the necessary infrastructure to run the WP1 piloting phases as stated by the Peppol Piloting strategy. They include:

- The activation of the PEPPOL XKMS Responder for Italy
- The cooperation with the WP1 Core team for the management of the Peppol MS TSL
- The management of the Italian Peppol MS TSL (in cooperation with DigitPA)
- The setup of an XKMS Client application to run Certificate Validation tasks

[8] From 29th December 2009, CNIPA will be renamed DigitPA (Legislative Decree 1st December 2009, n. 177)

The XKMS Client application: invokes certificate validation by the local XKMS Responder. It requires :

- XKMS Request preparation,
- Submission into the Local XKMS Responder,
- preparation for receiving and interpreting the reply from the server
- Activation and handling of the synchronous operation mode
- Activation of SOAP protocol 1.2
- Signed Message
- The X.509 must be in the Message
- Making of a JAVA Library (web interface / java-application) for reuse by organizations interested into the validation system

The PEPPOL XKMS Responder will operate according to the management and operation rules defined by the Peppol WP1 core team.

4.4.3 Pilot Use Case by InfoCamere

InfoCamere will also set up a specific use case for test purposes. The case will serve to the WP1 infrastructure a specific business document created within Peppol WP2, i.e. The “VCD – Virtual Company Dossier”. The VCD lies on two separated XML files and a variable set of electronic documents. The set is featured by a large set of “digital signatures” conforming to the standards CAdES, XAdES, PAdES.

The use case will focus on the XAdES sign and verify operation.

The case will run an integrated activity between WP1 and WP2 bringing some specific signature functions into the WP2 scenario. These functions are the Sign and Verify operation.

4.4.4 Resources activated by InfoCamere

The resources assigned by InfoCamere to enable the piloting activity are those recommended by the chapter 4.2 of the present specification document for what affects the XKMS Responder infrastructure.

4.5 Norwegian Pilot Specification

4.5.1 Procurement of Commercial Validation Service, Scope

During May 2010, Difi, Norwegian participant in PEPPOL WP1, will place a call in the market to buy validation services from a commercial service provider. The set of potential providers is as a start identified by the solution profiles of IDABC’s EFVS (European Federated Validation Service) study. Following award of a contract for service provisioning, the plan is to have an operational service by 1st November 2010, in time for the PEPPOL operational pilot phase. The schedule is tight, so this deadline should be regarded as a goal rather than a hard deadline; but if a delay is faced, the delay cannot be more than some weeks.

The requirements and scope for the service are as follows:

- The validation service interfaces shall be according to the PEPPOL D1.1 specifications, i.e. XKMS and OASIS DSS. The XKMS interface is mandatory, probably also the OASIS DSS interface (to be finally determined). This means that the integration task is the same as for use of the bos XKMS responder, and available client software should be reusable.

- The validation service is offered as part of the Norwegian national infrastructure for eID in the public sector and will be made available to any Norwegian public agency (this is outside of the PEPPOL scope).
- The validation service shall be offered free of charge to PEPPOL partners specifically for use in PEPPOL demonstrators and lasting until end of the PEPPOL project. This will cover Norwegian demonstrator scenarios and actors/services but may be extended to similar scenarios in other countries if desired.
- The selected service provider will take a subcontractor role in PEPPOL with Difi as contract partner (Norwegian consortium agreement). A designated amount of PEPPOL resources will be allocated (from WP1 Norway resources) to the service provider.
- Optionally, Difi may also offer subcontractor roles in other CIP pilot projects, notably STORK and SPOCS (if Norway enters the SPOCS project).
- It has not yet been decided if the validation service provider shall take an authority role (see PEPPOL D1.1, part 4, section 2.4) or provide a technical integration service with limited liability. An authority may be preferred but the call in the market may allow both alternatives (too be decided); decision based also on the cost picture implied by the two alternatives.

The legal possibilities to base public sector infrastructure on commercial services from private actors will vary from country to country. In Norway, this is a valid scenario, while some countries will require such a service to be run under government control. Thus, not all PEPPOL countries can be expected to be able to utilise the offer given by the third bullet point above.

4.5.2 Architecture and Interplay with other WP1 Components

Referring to the figure below, the service contracted by Difi will take the role of the validation service inside the rectangle in the upper right hand corner. This service is not shown as a “national” validation service, rather it is expected to provide as broad coverage as possible of the European (and possibly global) eID scene. The number of relevant Certificate Authorities directly covered by the service provider is an important criterion when the contract is awarded, as well as mechanisms to enrol new Certificate Authorities in the service.

In particular, qualified Certificate Authorities are most important, shown also by the reference to import of TSLs issued by the relevant authorities of the Member States.

As shown in the figure, the validation service contracted by Difi will be required to interplay with the national XKMS responders established by other PEPPOL participants. If a Certificate Authority is not directly covered by the commercial validation service, the ability to call a national XKMS responder shall be offered. In this respect, the service acts just like any “national” XKMS responder in the system.

Correspondingly, the validation service shall be able to take the role of a Norwegian XKMS responder in the PEPPOL system. As an example, if the Italian XKMS responder is in need of validating a Norwegian eID, the request can be chained to the Norwegian (commercial) validation service in the same manner as requests are chained to other “national” XKMS responders. In the context of PEPPOL demonstrators, the validation service provider will not charge for such requests.

CC BY

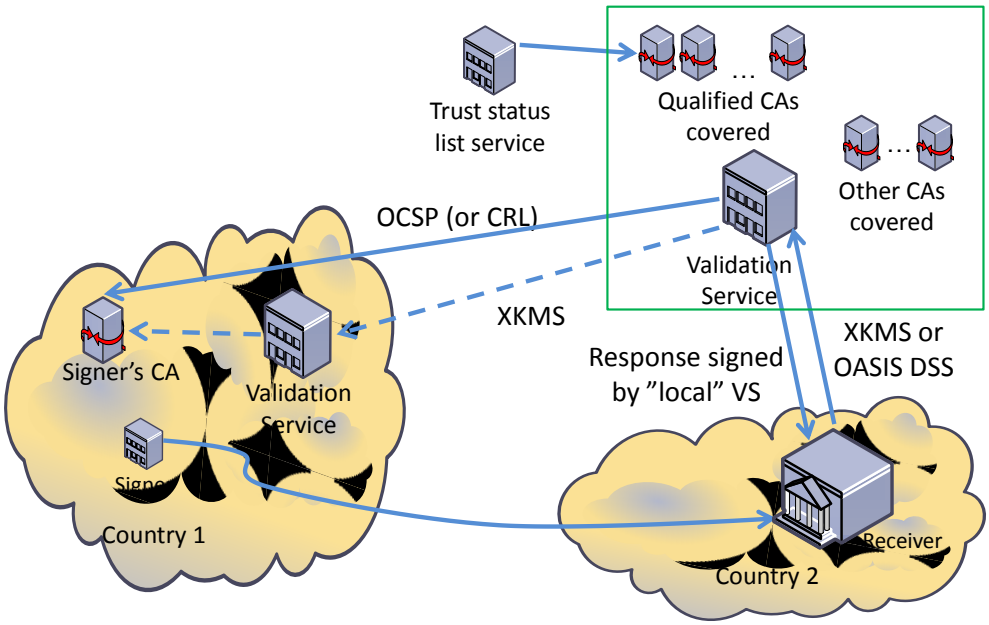

Figure 7: Norwegian validation service

4.5.3 Temporary Solution until the Validation Service is Operational

Until the procured validation service is operational, Norwegian Certificate Authorities can be handled by another XKMS responder in the PEPPOL infrastructure. The two most relevant Certificate Authorities, Buypass and Commfides, are already being tested in conjunction with the German XKMS responder. This allows Norwegian economic operators to participate using signed documents in procurement processes in other Member States, as far as the PEPPOL WP1 validation solution encompasses.

Until the validation service is operational, Norwegian contracting authorities (using the ehandel.no solutions, see below) will not be able to receive signed documents from economic operators in other Member States. If a Norwegian actor needs to test or operate according to WP1's solutions before this time, integration will have to be done towards an XKMS responder in the system, subject to availability.

Another possibility is to temporary instantiate a Norwegian XKMS responder in Norway but this will incur extra cost and work that should only be taken on if absolutely necessary.

4.5.4 Integration for WP1 Demonstrators

The validation service as described above will be integrated with services offered in the framework of ehandel.no (the Norwegian Public Procurement Portal). The services in ehandel.no are offered by commercial operators subject to contracts with Difi as responsible agency.

e-tendering services

The most relevant integration is towards the e-tendering services in ehandel.no. There are two such services, operated by Visma and Mercell. These actors have been allocated one man-month each from Norwegian PEPPOL WP1 resources to implement the integration. It is likely that both will choose to integrate with the XKMS interface, not with OASIS DSS, although this has to be finally determined.

According to Norwegian legislation on public procurement, electronic tenders must have an advanced (but not necessarily qualified) electronic signature supported by:

- Either an eID from a Certificate Authority that has a registered for supervision according to a self-declaration of conformance with the Norwegian requirements specification for PKI in the public sector (will apply to Norwegian Certificate Authorities), or
- A qualified eID issued by a Certificate Authority in any EU/EEA Member State.

Visma and Mercell currently use the BBS Global Validation Authority[9] subject to a temporary contract entered by Difi, ending 31st December 2010. The use of the BBS GVA service will be replaced by use of the validation service contracted by Difi as explained above.

Post-award services

Ordering (including catalogues) and invoicing is offered in ehandel.no by IBX subject to contract with Difi. Integration of the validation service with the IBX platform will enable signed documents in ordering and invoicing processes. Such integration is being discussed but has not been decided.

IBX has a subcontractor role in PEPPOL, working in the relevant post-award work packages.

Future e-invoicing for the Norwegian public sector

Work is in progress to make e-invoices mandatory for all suppliers to the Norwegian public sector (as has been done in Denmark). The recently established e-invoice project is led by Difi. The mandate and goals of the project have not been fixed, meaning that the following information shall not be taken as definite:

- The common solution shall be in place at the latest 1st July 2011. If this is the real date, the solution will have limited value to PEPPOL. This is however a last date given by political decisions. If the project can manage delivery at an earlier date, use in PEPPOL demonstrators should be considered.
- It is likely that the e-invoicing system will be implemented in the Altinn portal10. If the system is to be used for PEPPOL demonstrators, Altinn will have to be interfaced to the PEPPOL transport infrastructure, likely through its own access point. Through the PEPPOL metadata distribution system, all invoices to any Norwegian public agency will then be routed to Altinn.
- The e-invoicing solution should (regardless of PEPPOL) be able to handle signed invoices originating in any European country. Thus, Altinn should integrate with the validation service contracted by Difi.
- In the meantime, invoicing can be done through IBX' service in ehandel.no; this may also be a more permanent, parallel solution.

The Altinn portal is a single point of access for all reporting obligations from businesses to the Norwegian public sector. Altinn is run by the Brønnøysund Register Centre. The scope of Altinn is steadily increasing. Altinn is integrated towards the Norwegian business registers.Altinn is operational in version 1. Altinn 2 is being developed with planned release 1st November 2010. Thus the integration described by this note relates to the forthcoming Altinn 2.

Other services in Altinn

Outside of the PEPPOL scope, but inside the scope of the validation service, other services in Altinn will have a need for validation services. Notably, the Brønnøysund Register Centre has several roles

[9] http://www.bbs-nordic.com/en/Solutions-and-Services/eSecurity/Global-Validation-Service

[10] https://www.altinn.no/en

related to foreign enterprises (like the Norwegian Point of Single Contact for the Services Directive) and foreign individuals having roles (like board member) in Norwegian companies.

These services provide further arguments for integration of the validation service in Altinn. Integration in place for the Altinn release 1st November 2010 may be a goal but can by no means be guaranteed. Integration in Altinn may pave the way for a Norwegian pilot scenario in SPOCS, if and when the Brønnøysund Register Centre enters SPOCS as Norwegian partner.

CC BY

5 References

ETSI TS 102 231 v.3.1.1 (2009/10) - Electronic Signatures and Infrastructures (ESI); Provision of harmonized Trust-service status information

COMMISSION DECISION of 16th October 2009 setting out measures facilitating the use of procedures by electronic means through the 'points of single contact' under Directive 2006/123/EC of the European Parliament and of the Council on services in the internal market

First deliverable of PEPPOL workpackage 1: "D1.1 Requirements for Use of Signatures in Public Procurement Processes", revision 1.3 from November 6th 2009

6 Index of figures

7 Index of tables

Attachment A: XKMS Responder Prototype Documentation

CC BY

Attachment B: Validation Client Components

CC BY