# DELIVERABLE

**Project Acronym:** PEPPOL

**Grant Agreement number:** 224974

**Project Title:** Pan-European Public Procurement Online

## PEPPOL Deliverable D1.3 Demonstrator and functional Specifications for Cross-Border Use of eSignatures in Public Procurement

## Part 4: Architecture and Trust Models

**Revision: 1.9.5**


**Authors:**

**Germany: bremen online services**

**Norway: Difi**

**Italy: InfoCamere, InfoCert**

**France: ADETEF, DILA, Lex Persona, ANSSI, Esteral Consulting**

**Greece: University of Piraeus**




| 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 | |

# Revision History

| Revision | Date | Author | Organisation | Description |
|---|---|---|---|---|
| 1.0 | 2009/02/11 | | | Complete version for internal quality assurance. |
| 1.1 | 2009/02/27 | | | Submitted to PEPPOL project management, approved with comments at project management meeting 2009/03/27. |
| 1.2 | 2009/04/30 | | | For publication, updated according to comments. |
| 1.3 | 2009/11/06 | | | Formal update of D1.1 after EC approval. |
| 1.8 | 2010/09/23 | | | Complete D1.3 version edited from D1.1 part 4. For internal quality assurance. |
| 1.9 | 2010/09/30 | | | D1.3 submitted to PEPPOL project operating office (POO) for approval. |
| 1.9.5 | 2010/11/05 | | | D1.3 ready for publication, updated according to comments from POO. Uploaded for EC approval. |
| 2.0 | 2010/xx/xx | | | Formal update after EC approval. |

## 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This deliverable contains original unpublished work except where clearly indicated otherwise.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

# Table of contents

# 1 Summary and Structure of Document

## 1.1 Scope and Structure of Deliverable D1.3

This document is a part of the multi-part deliverable D1.3 "Functional Specifications for Cross-Border Use of eSignatures in Public Procurement" issued by the PEPPOL[1] (Pan-European Public Procurement On-Line) project. PEPPOL is a 4-year (May 2008 – end April 2012[2]) large scale pilot under the CIP (Competitiveness and Innovation Programme) initiative of the European Commission. D1.3 is an updated version of the deliverable D1.1 "Requirements for Use of Signatures in the Procurement Processes" [PEPPOL-D1.1].

D1.3 consists of the following documents:

**Part 1:** Background and Scope

**(Part 2:** Not included – was the D1.1 part on E-tendering Pilot Specifications)

**Part 3:** Signature Policies

**Part 4:** Architecture and Trust Models

**Part 5:** XKMS v2 Interface Specification

**Part 6:** OASIS DSS Interface Specification

**Part 7:** eID and eSignature Quality Classification

The D1.3 deliverable is the second version of **functional specifications** for cross-border interoperability of e-signatures in Europe. The specifications are specifically targeted at cross-border public procurement, the topic of PEPPOL. However, a successful solution should be applicable also to other application areas in need of e-signature interoperability.

Signature interoperability in PEPPOL focuses on verification of e-signatures and their associated eIDs. Interoperability of signing solutions is not handled as it is assumed that all actors are capable of signing documents within their corporate infrastructure.

The specifications in deliverable D1.1 has guided the implementation and testing of e-signature interoperability solutions in PEPPOL. In the course of this work, the specifications have by necessity evolved, leading to the revised version published in this deliverable D1.3. These are the specifications for the solutions used for the e-signature interoperability pilots in PEPPOL [PEPPOL-D1.2] in the period 1st November 2010 to 30th April 2012.

The specifications are publicly available and comments from any interested party are most welcome. Note that further evaluation of the specifications of D1.3 is expected as a result of further work in PEPPOL and any party using or referring to the specifications must ensure that the latest version is used; contact the PEPPOL project for information.

## 1.2 Demonstrator Software Components and Documentation

In addition to the specifications in this deliverable D1.3, PEPPOL WP1 provides software components for cross-border validation of e-signatures:

[1] http://www.peppol.eu

[2] Originally, PEPPOL was scheduled for 3 years. The project has been prolonged twice, both times by 6 months.

- PEPPOL XKMS responder component (server side component) according to the specifications of D1.3 part 5 is provided as open source. The software component, source code and documentation are available on OSOR[3],
- A free to use client side component for signature validation can be retrieved from bremen online services. The validation client is available as a standalone version and a version for integration into other software applications. To receive download permission, please use the following contact:

| **bremen online services**<br>Support and supply of<br>PEPPOL WP1 software components |
|---|
| • Phone: +49-421-20495-777<br>• E-Mail: support-wp1@peppol.eu |

The software components are used for PEPPOL's pilot demonstrators on e-signature interoperability as described in PEPPOL Deliverable D1.2 [PEPPOL-D1.2]. Attachments A and B to D1.2 provide documentation on respectively the XKMS responder and the validation client.

## 1.3 Scope and Structure of this Document

This document discusses architecture and trust issues for validation solutions for e-signatures and eIDs. Chapter 2 and appendix 1 discuss trust models, including the role of an authority. Chapter 3 shows the overall architecture of PEPPOL's validation solution. Chapter 4 raises issues related to transport security and encryption. Chapter 5 describes technical integration of validation services. Use of Trust Status List (TSL) services in PEPPOL is described in chapter 6. A short discussion on use of Time Stamp Authority (TSA) services is included in chapter 7 and appendix 2.

## 1.4 Evolution of this Document and Changes from D1.1

Note: This document, like the other parts of D1.3, continues the version numbers deriving from D1.1.

Parts of this document, in particular the sections on use of TSLs, may need updating as the status in the relevant area changes. However, most parts of this document are regarded as stable.

The main changes from [PEPPOL-D1.1] part 4 to this document are:

- A new chapter 3 has been added to explicitly present the architecture.
- Status on use of TSLs (chapter 6) has been updated to reflect recent development in the EU. Official EU TSLs covering issuers of qualified eIDs are now available.
- Chapter 4 is slightly expanded.
- D1.1 part 4 included an appendix 3 on sending side verification. This has been deleted as it is no more considered relevant.

[3] Open Source Observatory and Repository for European public administrations, http://www.osor.eu. Results from PEPPOL are available in http://www.osor.eu/projects/peppol.

## 1.5 List of Contributors

The following organisations, in alphabetical order, have contributed to Deliverable D1.1.

- **ADETEF, France** http://www.adetef.fr
- **ANSSI, French Network and Information Security Agency, France** http://www.ssi.gouv.fr
- **bos, bremen online services, Germany,** http://www.bos-bremen.de
- **Difi, Agency for Public Management and eGovernment, Norway** http://www.difi.no
- **DILA, Direction de l'Administration Légale et Administrative Of French Prime Minister Office, France** http://www.dila.premier-ministre.gouv.fr
- **Esteral Consulting, France** http://www.esteralconsulting.com
- **InfoCamere, Italy** http://www.infocamere.it
- **InfoCert, Italy** http://www.infocert.it
- **Lex Persona, France** http://www.lex-persona.com
- **University of Piraeus, Greece** http://www.unipi.gr

The following persons (alphabetical ordering for each participating organisation) have contributed to the D1.3 work:

| | | | | | |
|---|---|---|---|---|---|
| Jörg Apitzsch | bos | Piero Milani | InfoCamere | Alain Ducass | ADETEF |
| Nils Büngener | bos | Luca Boldrin | InfoCert | Ahmed Yacine | DILA |
| Mark Horstmann | bos | Daniele Mongiello | InfoCert | François Devoret | Lex Persona |
| Ralf Lindemann | bos | Lefteris Leontaridis | Univ. Piraeus | Julien Pasquier | Lex Persona |
| Dr Jan Pelz | bos | Dr Andriana Prentza | Univ. Piraeus | Sébastien Herniote | ANSSI |
| Lars Thölken | bos | Alain Esterle | Esteral Cons. | Jon Ølnes (editor) | Difi |

D1.3 is a revised version of D1.1. The D1.3 team acknowledges the contributions of organisations and persons that helped producing D1.1 but are no longer active in PEPPOL's e-signature work. These are not listed above; please refer to D1.1 for the names.

# 2 Trust Models and Trust Requirements

## 2.1 Levels of Trust

Appendix 1 to this document gives some background theory on trust issues. To sum up, trust can be seen at two levels [Olnes1]:

1. "Technical trust" in the technology used, i.e. computer systems and the means to communicate between these systems.
2. "Organisational trust" between the actors that eventually shall carry out the business transactions, e.g. enter a contractual relationship.

For e-signatures, the first level is about establishing means to cryptographically verify signatures and eIDs and to assess that quality and other signature policy requirements are fulfilled. This document is (mainly) about such "technical trust". Although human operation can be used, a goal of WP1 in PEPPOL is that it shall be possible to establish such trust by automated means; i.e. the criteria and mechanisms shall be processable.

The second level in general requires more than e-signatures; the means to assess that a given counterpart is trustworthy and has honest intent. However, the degree of ability to infer "organisational trust" from e-signatures is important and is covered by D1.3 part 3. Is a signature of good quality sufficient to trust the named counterpart (it is a strong proof binding to the document)? Can the name in the eID be linked to roles and authorisations? PEPPOL's work on VCD (Virtual Company Dossier) is one step in the direction of assessment of organisational trust; a scheme for approval of actors that are allowed to connect to the PEPPOL BusDox infrastructure is another measure.

## 2.2 Claims and the Need for Infrastructure

Actors that know one another can establish trust bilaterally by themselves assessing properties of the counterpart. This obviously does not scale to European level. Thus, there is a need for infrastructures of trusted services that can contribute to assessments about counterparts.

The starting point is a claims-based identity paradigm; see e.g. [Cameron], who defines a claim as "an assertion of the truth of something, typically one that is disputed or in doubt". For scaling, claims about identity attributes (names, identifiers, business roles etc.) must be backed by evidence from trusted infrastructure services that can be recognised across Europe or even globally.

A trusted service issues, validates or stores assessments of claims about properties of actors (such as a CA issuing an eID containing assertions about claimed identity attributes of the subject). By trusting the service, one can trust the assertions (claims) and derive the properties needed.

## 2.3 Trust Service Provider (TSP) Roles

### 2.3.1 TSPs Serving Users Directly

The basic trusted service provider (TSP) for e-signatures is of course the CA issuing eIDs. Such PKIs (public key infrastructure) exist in all countries in Europe, and PEPPOL WP1 relies on existing PKIs.

CAs issue certificates as assertions for the claims included in, or possibly also derived from, the certificates. By trusting the CA one trusts the assertions. CAs and their eIDs have different properties such as legal status (notably qualified or not) and may have different quality. In the PEPPOL context,

the cryptographic trust in the public key of the CA is not sufficient; one needs to know that the e-signature fulfils the signature policy (see D1.3 part 3).

A CA is an example of a TSP that directly serves the actors involved in the e-signature process: the sender/signer (the certificate holder) and the receiver/verifier (the relying party). Other relevant TSPs serving actors directly are:

- Validation Authority (VA), providing validation evidence to relying parties; this role is discussed further in the rest of chapter 2.
- Time-Stamp Authority (TSA), providing trusted time; this role is briefly discussed in chapter 7 and appendix 2. PEPPOL does very limited work on time stamping.
- Attribute Authority (AA), providing trusted attributes outside of those contained in the eID certificate of the signer. This role is not further elaborated by PEPPOL, except that a business register or a VCD provider (see below) may be said to take the role of an AA for attributes derived from an eID (certificate information) used for the lookup in the register.

The STORK[4] project has done a bulk of work on provisioning of identity attributes during a cross-border authentication procedure.

In a business protocol context, other trusted services may also be defined to handle claims related to the organisational trust aspects, such as:

- Notary, providing trusted attestation and/or storage of electronic documents,
- Virtual Company Dossier (VCD) issuer, a service defined by PEPPOL WP2.

A CA issuing qualified certificates is regulated by the EU's e-signature Directive. Depending on the interpretation of the Directive, other CAs and other roles may also be defined as Certificate Service Provider according to the Directive. TSPs may also be subject to other EU and/or national legislation, e.g. the TSA and Notary roles are defined in some Member States but not all.

### 2.3.2 Second Order TSPs

The number of relevant CAs in Europe depends on what one wants to include. The number of qualified CAs may be in the order of 100 but other CAs may also be included, and there may be several services (different policies) per CA actor. Experience has shown that this number is too high to be manageable to the individual actors involved e.g. in public procurement. And then one eventually also has to look outside of Europe, to a global scene.

The conclusion is that there is a need for further trusted services that can attest to assertions (claims) about CAs (and possibly other TSPs); their legal status and the quality of their eIDs and the signatures produced.

These TSPs can be considered "second order" services in the sense that they serve to establish trust in the service-providing TSPs. Notably the following can be mentioned:

- Supervision and accreditation body for TSPs, notably for CAs,
- Trust Status List (TSL) issuer (see chapter 6),
- Root-CA provider, acting as trust anchor for processing of certificates from underlying CAs (see Appendix 1),
- Bridge-CA provider, to link different PKIs through cross-certification with the bridge-CA (see Appendix 1),
- Product certification body, notably for certification of SSCD (Secure Signature Creation Device),

[4] http://www.eid-stork.eu

- Policy owner, where certificate policy or signature policy is governed by another body than the one responsible for the operational trust service,
- A Validation Authority may also be considered a second-order TSP to the extent that the purpose of the VA is to enable trust in certificates issued by a CA.

There are other TSP roles that may be defined, such as Registration Authority (RA) for identification and registration of entities before a CA issues a certificate. In the context of PEPPOL, the RA role is viewed as a part of the CA provisioning.

## 2.4 Validation Trust Models and Services

Appendix 1 describes common trust models in PKI: Cross-certification, hierarchy, and bridge-CA. There is no initiative at establishing such pan-European structures among CAs, and PEPPOL does not recommend any initiative in this direction.

PEPPOL instead recommends two other approaches that mutually enhance one another:

- TSL (Trust Status List) distribution services, as further described in chapter 6. A European TSL system has been established and will be utilised by PEPPOL, in the first run by import into PEPPOL validation services and possibly digested into a PEPPOL TSL (see chapter 6).
- Validation services that validate eIDs and e-signatures and issue assertions about validity and signature policy adherence. There may be a need for several validation services in a co-operative structure as described in this document and in [PEPPOL-D1.2].

The ultimate goals are:

- Any actor shall have available service(s) that enables validation and signature policy checks for any e-signature regardless of eID issuer (may be limited to a subset of eID issuers if relevant). The system must have real time properties.
- It must be possible to store/archive the assertions issued and validated for later reference by the actors involved or by other parties (such as an arbiter). The system must have persistent properties.

Persistence must be guaranteed by continued existence of the certificates of the validation services, preferably also of their entire service offering. PEPPOL does not intend to work on archival and persistence apart from ensuring that all necessary information for archival is made available by the services offered.

## 2.5 Services and Authorities, Risk Management

A service (TSL distribution, validation service) may be trusted only for its technical function, i.e. it provides “advise” that the relying party may choose to use to assess validity and signature policy adherence. If something is wrong, the service takes on little or no liability, limited to being responsible for its own negligence.

A service may also be provided as an authority, serving as a one-stop actor for all aspects of validation covering agreement, billing, trust, complaining, and liability (see Appendix 1 and [Olnes2].

PEPPOL looks at both variants, although it is likely that only the technical service approach will be demonstrated in the project’s pilots. A validation service can be offered as a software installation with an interface. For it to become an authority, it additionally needs to be governed by an actor that contractually takes on the necessary responsibilities. Thus, if the authority approach is taken, there is a need for an actor that is willing to take on this role.

To the relying party, an authority may be an advantage since this provides a manageable risk situation for acceptance of e-signatures. A uniform liability and a single point of contact is achieved for e-signatures of equal quality, On the other hand, with a service only one has to address the individual CA if anything goes wrong, and CAs' policies may vary in this aspect. Additionally, reading a foreign CA's policy may be difficult (language), and the policy may refer to national laws of the CA's country. A dispute may have to be settled in the CA's home country.

In short, the main virtue of an authority is that it transfers the situation of the relying party **from (many) national laws to a state of contract law.** The same argument is valid for both TSL distribution (at least if it feeds relying parties directly) and validation services.

It can be argued that as far as e-signature interoperability is limited to qualified signatures or advanced signatures using qualified eIDs, the risk situation from relying on each (in principle unknown) CA individually is acceptable since the e-signature Directive [EU01] ensures a uniform legal situation across all Member States.

## 2.6 Trust Anchors for Validation Services and Authorities

One may argue that a validation authority should in principle be its own trust anchor, i.e. it should have its own root-CA and be independently trusted for its signed assertions. A validation authority should be well known to its customers, so trust in such a root-CA may be easily established. On the other hand, one may also argue that the certificate used for signing assertions is only an authentication means; the independently trusted role is derived from contracts and policies. Thus, a validation authority may procure its certificates from a suitable CA in the market.

For a "technical" validation service, the issue of inheriting trust from a CA may on the other hand not be important.

Although a receiver selects a local, well-known and trusted validation service to call, all validation services are required to sign using publicly available and verifiable certificates of their own and using signatures of sufficient quality. The assertions issued by a trusted validation service may later have to be checked by other parties than the one that directly calls the validation service.

There is at present no accreditation scheme for validation authorities/services. Such a scheme may be established along the lines of the system in use for qualified CAs. Validation services may be provided by public (national) providers or by commercial (private) providers. Scope need not be national; degree of CA coverage on a global scale may actually be a competitive edge for validation services.

The challenge arises when the local, trusted validation service is incapable of providing an answer on its own. Chapter 6 describes how to use TSLs and registries to locate a validation service that is capable of handling a particular CA. If services are national, the service to call may be given by the CA's nationality. Local configuration is also possible.

# 3 PEPPOL Federated Validation Services Architecture

Based on the background presented in the previous chapter, the system architecture for the federated validation solution of PEPPOL WP1 is as shown in Figure 1 below.

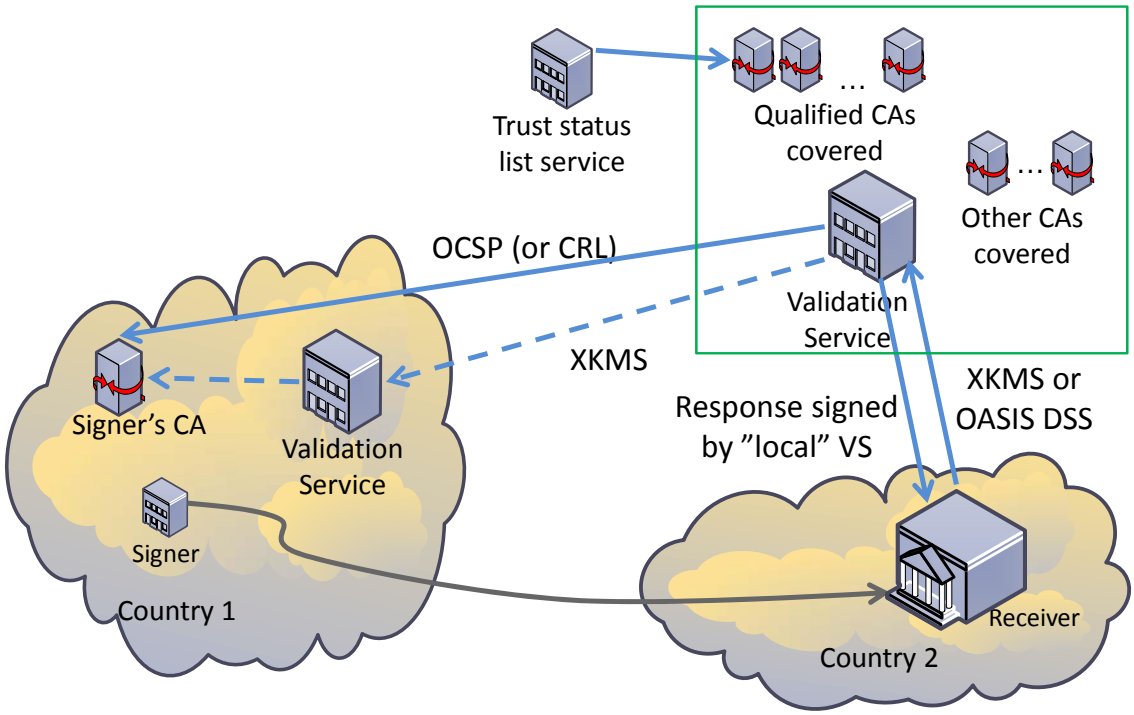


Figure 1: PEPPOL verification system architecture.

The figure shows a signer in Country 1 submitting a signed document to a receiver (relying party) in Country 2. The CA issuing the signer's eID is shown inside Country 1 assuming the usual case of a national CA, but this is not a requirement.

To validate the signed document, the receiver calls a locally trusted Validation Service (VS) using one of the interfaces specified by D1.3: XKMS interface (part 5) or OASIS DSS interface (part 6). Note that no plans exist for provisioning of the OASIS DSS interface, meaning that only the XKMS interface can be assumed to be available for PEPPOL pilots.

A VS may have a national scope as shown by the VS inside Country 1 in the figure, or it may operate on an international scale, as shown by the VS inside the rectangle in the upper right hand corner of the figure. In both cases, the VS should make use of all relevant TSLs to achieve coverage of all relevant qualified CAs (and possibly other CAs covered by the TSL system). The TSL usage might be possible by means of import of machine readable TSLs or manual configuration of VS on basis of human readable TSLs. However, the current state of available TSLs does not necessarily enable direct productive coverage of the listed CAs nor provide all relevant CAs; this is discussed further in chapter 6. Additionally, the VS may support other CAs through local configuration or additional PEPPOL specific TSLs specifying non qualified CAs.

When receiving a call from the receiver, the local VS checks if the CA in question is locally covered. In case, a revocation status check (OCSP or CRL) is done towards the CA, the response is locally produced and signed by the VS and returned to the receiver.

If the CA is not in the list of locally covered CAs, the VS has to locate another, remote VS able to answer for the CA. The mechanism and trust model for this look up and mapping is provided by the PEPPOL Public Registry Service (PPRS – not shown in the figure), this is discussed further in chapter 6. When located, the request is forwarded to the remote VS using the XKMS interface. Note that if the local VS is called using the OASIS DSS interface, all signature processing is done by the local VS and only eID validation by XKMS is "outsourced" to the remote VS.

The remote VS, e.g. national VS for the country of the CA as indicated in the figure, performs the eID validation and returns a signed XKMS response to the local VS.

Upon receiving the response from the remote VS, the local VS re-signs the response (and possibly adds information) before returning the response to the receiver; i.e. to the receiver (the relying party) it always looks like the local VS answers, even when the request is chained.

The goals fulfilled by the architecture are:

- The receiver shall only need to have a relationship to one VS provider.
- The VS system shall be able to validate eIDs from in principle any CA even though the local VS provider may have a limited coverage (e.g. it is required to take a national scope).
- The architecture shall not limit a VS' operation to a national or otherwise restricted scope.
- The architecture shall support both a VA (Validation Authority) approach and an approach where the VS is a technical integration service.

Note that this architecture explicitly supports verification initiated by the receiving side. Another option, which is deemed to be out of scope in PEPPOL, is to require verification information from the sending side. The sender can, e.g. at the time of signing, obtain an OCSP response and/or other information to embed in an advanced signed data object. The receiver can then decide to trust this information instead of performing extra revocation checking.

# 4 Transport Security and Encryption

## 4.1 The BusDox Transport Infrastructure, Trust and Trust Gaps

The BusDox[5] transport infrastructure specified and deployed by PEPPOL ensures integrity and confidentiality (by transport signatures and encryption) *between Access Points* (AP). See D1.3 part 1 for a figure and some more explanation.

An AP may be integrated into an originating or receiving system (e.g. a sending side ordering system and a corresponding system on the receiving side) but the AP may also be a separate service. In the latter case, the PEPPOL transport infrastructure will not protect the entire transport channel as the channels from systems to APs are not covered. Also, since business documents cannot in general be encrypted[6], they will be available in clear text in the APs.

If an actor uses an operator system outside its own control, the trust in this operator system must be assumed to have been evaluated (e.g. that the operator system is trusted to see content of business documents), and the same goes for the communication channel from the actor towards the operator system.

The first “trust gap” is the fact that the actor may have no means to assess trust in the (actor running) a separate AP service, different from the operator system, and in the communication channel between these two services. One implicitly trusts this AP to be sufficiently secure and to itself not disclose or change documents. This trust may be backed by a system where APs must go through some kind of approval before being allowed to connect to the PEPPOL infrastructure.

The second “trust gap” is that business documents (possibly unsigned and normally in clear text) will be available to the receiving side AP and to the receiving side operator system. This trust cannot be evaluated by the sender apart from an assumption that the receiver has taken sufficient precautions when selecting service providers.

Note that the most severe problem related to clear text, unprotected documents in intermediate systems need not be the direct risk of security breaches but the difficulty of proving what happened and who was responsible (and how to escape from accusations) if something goes wrong somewhere.

Again this may not be a major problem but actors should evaluate the trust issues in the given business scenario. An end-to-end signature on a business document prevents intermediaries from changing (or faking) content but does of course not contribute to confidentiality.

## 4.2 End-to-End Transport Protection

Use of e-signatures as specified by this deliverable is an end-to-end mechanism that is fully independent from use of the BusDox infrastructure. However, signatures are only a part of a reliable and secure end-to-end messaging solution.

Reliable messaging infrastructures are made available at a national level in quite a few countries. The bulk of this work is based on the REM (Registered Electronic Mail) standards [ETSI-102-640]; however note that neither REM nor most national infrastructures support encryption.



[5] See PEPPOL BusDox 1.0 specifications on http://www.peppol.eu/work_in_progress/wp8-Solutions%20architecture%2C%20design%20and%20validation/specifications/version-1-0-of-busdox-specifications-finalized

[6] This would be a matter of mutual agreements of business partners, to be handled on payload level.

The SPOCS project[7] has specified a solution to bridge these national infrastructures to enable end-to-end reliable messaging from an endpoint in one national infrastructure to an endpoint in another national infrastructure. It is noted that the BusDox infrastructure could be used in a similar way by interfacing the national messaging infrastructures to BusDox Access Points; however this is at present out of scope of PEPPOL.

## 4.3 Encryption of Business Documents (not Supported)

Since transport infrastructures do not provide end-to-end encryption, business documents should be encrypted on a message level end-to-end. Most signing software and signed data formats also support encryption but encryption is still not available in most cases.

To encrypt, the sender (signer) needs a trusted eID certificate for the receiver, where the certificate (key usage settings) allows encryption. Unfortunately, most public eID services (such as national ID cards) do not include certificates that can be used for encryption. Thus, end-to-end encryption of business documents between persons cannot be used in general.

Since personal eID certificates are the only certificates that can be assumed to be available, this means that PEPPOL cannot support encryption of business documents.

The solution, which will however not be explored by PEPPOL, may be to issue corporate certificates that can be used to both sign and encrypt – see D1.3 part 3 for some discussion on use of such certificates for signing.

For encryption, a major problem is how to locate and verify the correct encryption certificate for the receiver. In the PEPPOL context, it is noted that the Service Metadata Locator / Service Metadata Publisher system devised by BusDox could be used to store encryption certificates.

There are requirements (e.g. in France) for encryption of tendering documents until time of opening of the bids. In such cases, PEPPOL WP1 recommends tendering platforms to provide an “upload and encrypt” function to this effect. On upload over a protected channel, the receiving system will immediately encrypt all documents using a certificate and public key whose corresponding private key will only be made available to the receiver at a certain time. However such a solution is considered to be out of scope for PEPPOL and a matter of mutual agreements of business partners.

The conclusion is that in general the transport channel must be trusted to preserve confidentiality of business documents. In PEPPOL, this is only guaranteed for the parts of the channel covered by the BusDox infrastructure, see 4.1.

In some cases, use of an end-to-end TLS/SSL protected channel may be sufficient for protection.



[7] http://www.eu-spocs.eu

# 5 Validation Service technical Integration

## 5.1 Introduction

E-signature interoperability in PEPPOL focuses on the receiving side and verification of signatures, assuming that all actors are able to sign inside their corporate infrastructure or by use of the systems of their local service providers. Since interoperability requires more information and thus a richer interface than merely cryptographic verification and validity checking (OCSP or CRL), PEPPOL specifies two interfaces as profiles of XKMS v2 and OASIS DSS (Digital Signature Standard) in parts 5 and 6 of D1.3 respectively. Actors can use these interfaces to obtain the necessary verification information. There are at present no plans for provision of the OASIS DSS interface, meaning that actors for the PEPPOL pilots can only assume availability of the XKMS interface.

## 5.2 eID Validation by XKMS

Upon obtaining the signed document (sent over the BusDox transport infrastructure or otherwise), the validation process on the recipient side (see also chapter 3) 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 Status List) or by a registry lookup.
2. If the CA is known locally, the local XKMS service only has to perform an OCSP (or CRL) call to the CA that has issued the sender's eID.
3. If the CA 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 CA.
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[8] 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 CA (OCSP, CRL) and forms a Validate Response that is signed and sent back to the local XKMS service.
6. The Validate Result from the remote XKMS service is re-signed (possibly also further processed) by the local XKMS service 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 and discussed in 2.6.

In both case 2 and 3-6, it is the local XKMS service that shall sign the Validate Result returned to the recipient. This can include liability and other issues, depending on whether the service is a validation authority or a technical validation service (see chapter 2). The XKMS interfaces (also when used for chaining) shall adhere to the specifications in D1.3 part 5.



[8] Trusting the remote XKMS service's signature should not be a problem; its signing certificate can be obtained in a trusted way from the TSL or the registry.

## 5.3 Signature Verification by OASIS DSS

### 5.3.1 Interface and Process

This 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 CA is known locally, only an OCSP (or CRL) call to the CA is necessary.
- If the CA is not known, a registry (or perhaps TSL lookup or even local configuration) will reveal an XKMS service that can handle the CA. An XKMS request is forwarded and the Validate Result 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 processing of signatures, while 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. The OASIS DSS interface shall adhere to the specifications in D1.3 part 6, and the XKMS interface for chaining shall follow D1.3 part 5.

### 5.3.2 Validation Gateway

Sending the entire content of a signed document to a validation service may disclose 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.

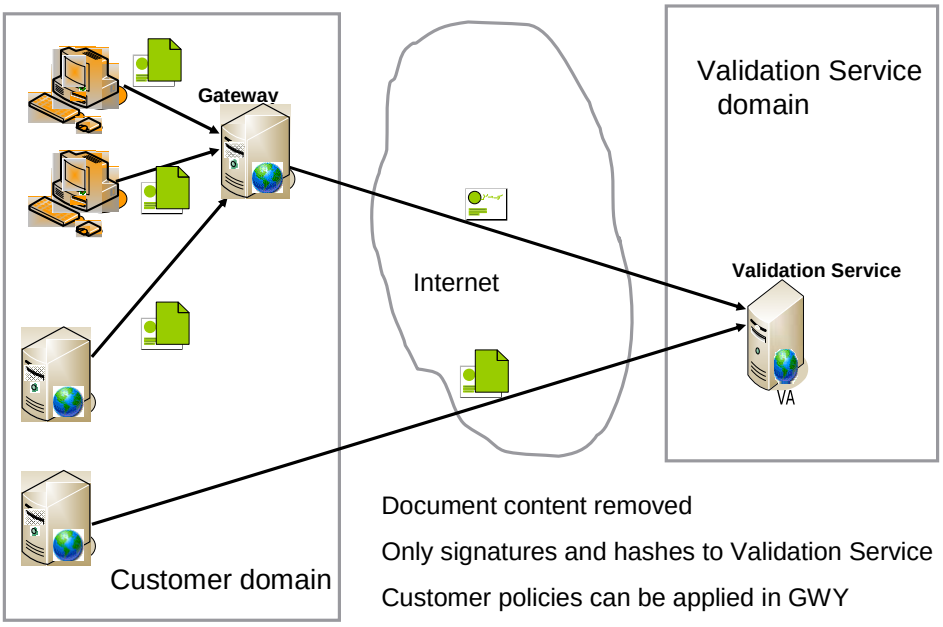


Figure 2: Validation gateway solution.

A possibility is to use a validation gateway deployed in the recipient's IT infrastructure (the possibility of offering a validation gateway as an external service of course also exists but is not discussed

further here), where the validation gateway removes the document, forwarding only signature fields and corresponding hash values to the validation service. Such a solution is described in [Olnes3].

The validation gateway is installed (software with or without separate hardware) in the recipient's network and requests are directed to the validation gateway as shown in Figure 2 (the bottom arrow in Figure 2 shows that direct calls to the validation service may still be allowed). In the validation gateway, signatures are extracted and the corresponding hash values computed from the document. Only signatures and hash values are 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 validation gateway, which in turn must direct the response to the correct end system. It is important that the validation service, not the validation gateway, signs responses since the validation service is the trusted actor. The validation gateway is only trusted with respect to correct functionality, not to provide assertions about validity of signatures and eIDs.

Additionally, a validation 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 the validation gateway is internal at the recipient site. The validation gateway should offer the same OASIS DSS interface as the validation service, but requirements for request signing can be avoided (the validation gateway will anyway sign the request). Additionally, a web GUI interface may be used, or even an email interface where signed documents can be sent to the validation gateway as attachments; the response being attached to a response email.

# 6 Trust Models and Trust Status List (TSL)

## 6.1 Introductory Notes

In this chapter, reference is frequently made to Member State (MS) and information and services that are MS specific. While national services is one possibility, the reference to MS should be read more as an indication of partition into several domains than literally as national. One validation service may perfectly well cover more than one MS, and there may in this case of course be overlap between the lists of CAs covered by different services.

TSLs issued by national supervision bodies will be national. However, other schemes for issuing of TSLs (such as a PEPPOL TSL) can well be envisaged and will be used in PEPPOL piloting.

The term Validation Service (VS) is mainly used below but the term Validation Authority (VA) is also used. VS is a more general term covering also technical validation services (not only real authorities, see chapter 2). In this chapter VS and VA can be read as the same term.

PEPPOL refers to the latest version of [ETSI-102-231] for content of TSLs.

PEPPOL WP1 has specified and established a certain infrastructure design and trust model for the federated validation services constituting the WP1 pilot. The specification and description of this set up is provided in [PEPPOL-D1.2] chapter 3.

The approach to establish a trusted network of service instances based on the ETSI TSL specification is also adopted by the large scale pilot SPOCS[9], where certain transmission gateway instances are governed by a central TSL component.

## 6.2 EU's TSL System

An immediate and prioritised action point in [COMM01] is establishment of a pan-European system of Trust Status Lists (TSL) covering qualified CAs. The format of the lists is according to [ETSI-102-231]. Both human readable (PDF) and machine processable (XML) lists shall be issued. Status is as follows:

- Establishment of the TSL system has been decided by the EU Commission [COMM02].
- The EU has established top level lists that include only pointers to the national TSLs: Human readable[10] and machine processable[11].
- All EU/EEA countries will establish national lists. Lists are issued (and will eventually be signed) by the national authorities responsible for accreditation or supervision of issuers of qualified certificates.
- Only issuers of qualified certificates are covered. There have been initiatives at extending coverage to non-qualified CAs but apparently no Member State has this in scope at present.
- The level of detail and the information content vary a lot from country to country. This also means that the usefulness of the information in different TSLs varies (see below).

[9] Simple Procedures Online for Cross-border Services, http://www.eu-spocs.eu

[10] https://ec.europa.eu/information_society/policy/esignature/trusted-list/tl-hr.pdf

[11] https://ec.europa.eu/information_society/policy/esignature/trusted-list/tl-mp.xml

- The national lists shall be updated every six months. Procedures should be in place for any national authority to issue a new list in case of change in status for a CA and furthermore to notify the top level authority at EU level about the new version.

Some examples:

- The German TSL lists only the national root-CAs operated by the accreditation authority. Since all accredited CAs are required to obtain a certificate from (one of) the root-CA(s), individual CAs may be traced to an accreditation status from the TSL, provided that the certificate path to this root-CA is available. In practice, this TSL may add very little value.
- The Italian TSL contains detailed information on each qualified CA individually; since path processing is not allowed in Italy, each CA must be represented by its own root-CA. In addition to the root-CA certificates, access points for status information, policy information etc. are also specified; more information than provided by most TSLs. This TSL may prove to provide all, or almost all, information that a VS needs to support Italian, qualified CAs.
- The Norwegian TSL contains all certificate issuing CAs but not necessarily the root-CAs; e.g. all qualified BankID CAs are listed individually including their CA-certificates issued by the BankID root-CA, but the BankID root-CA itself is not listed. Certificate status services are not specified.
- The Danish TSL is empty except for a policy notice stating that there is no issuer of qualified certificates in Denmark.

The conclusion is that while the TSL system is very useful to map qualified CAs in Europe, to a varying degree (depending on the level of detail of the TSL in question) supplementary information is needed (e.g. in most cases access points to certificate status information services), the TSLs must be explicitly monitored to detect changes in status of CAs, and the system covers only qualified CAs.

## 6.3 TSL Issuer Requirements

In this chapter, TSL issuers are usually national supervision agencies (or even EU agencies). Other models, such as issuing by private agencies, can also be used.

TSL issuing services apart from the official EU system covering issuers of qualified certificates as described above may not exist in the time frame of the PEPPOL pilots. Thus, PEPPOL must be able to take an active role in issuing TSLs for pilots. This is described below. This will be regarded as a temporary situation and governance, liability, and commercial issues related to such a PEPPOL service are not detailed; this will be more a situation of making the necessary functionality available.

TSL issuers must sign the TSLs applying a signature of sufficient quality. While a person name is irrelevant, this may still have to be a personal signature (possibly using a pseudonym like “TSL Issuer”) in order to make it a qualified signature. A corporate signature (see D1.3 part 3) at the same level as a qualified signature would be a better alternative if this can be agreed upon.

The TSL issuer should in principle be a separate trust anchor (a root-CA certificate of its own issuing a certificate to the TSL signer only) and/or use a certificate issued by a CA that is outside of the actual TSL. In practice, signing a TSL using a certificate issued by a CA on the TSL is accepted in most cases. For the EU TSL system, TSL issuers are required to publish their signing certificates in a trustworthy manner.

Since TLSs may (and will) contain pointers to other TSLs using an entry including the signing certificate, a user of a TSL system should not be required to know in advance the certificates of all TSL issuers.

Accreditation and trust in TSL issuers that are non-governmental (such as a PEPPOL TSL repository as described in 6.11) is for further study.

TSL issuers must archive the TSLs issued and/or otherwise maintain historical information about the CAs (or other trust service providers). This is necessary in order to prove the status of a CA at a particular point of time in retrospect. The TSL issuer should provide an on-line interface for access to old TSLs or old status information.

## 6.4 Extending TSLs with Non-Qualified CAs

The national TSLs will only cover qualified CAs. A rather simple extension is to cover even non-qualified CAs that have some national approval status. National TSL issuers will probably be reluctant to include more than these alternatives in their approved lists. This clearly does not cover all possible or all relevant CAs, in particular since a TSL system cannot be expected to exist outside of Europe.

With respect to listing of CAs, use of the quality classification system described in D1.3 part 7 should be considered. This system is independent from the qualified state although qualified is clearly indicated.

Since CAs without any national approval status, and CAs outside of Europe, will not be on any national TSL, some non-government (commercial or consortium or international body) TSL issuer must take on this responsibility if the TSL approach is to be expanded to such CAs. If quality parameters are used, and assessment is properly done, this can even be a replacement of today's lists of "approved" CAs used by Microsoft and other suppliers of operating systems.

Such TSL issuing is not discussed further in this document.

## 6.5 TSL Used by End System

An intended use of a TSL system and trust model is that a generic application X in Member State (MS) Y shall be able to use a TSL directly. Given the state of even the machine processable TSLs issued under the EU system (see 6.2), more effort is needed to achieve this goal. On validation of a foreign (MS Z) end-user certificate, application X:

1. downloads an updated machine processable TSL from its Supervision/Accreditation Body (SB) and verifies its digital signature;
    a. searches the Trust Service Provider (TSP) that have issued the end-user certificate (in this case we call it a Certification Service Provider or CSP) and upon not finding it, searches the Pointers to other TSLs as specified by [ETSI-102-231] for the available EU Commission TSL (EU TSL)
2. downloads an updated EU TSL, from the EU Commission, containing the URIs of MS TSLs (Pointers to other TSLs as specified by [ETSI-102-231]) and verifies its digital signature
    a. searches the TSL's URI relative to the Country Code of the CSP
3. downloads an updated TSL for MS Z and verifies its digital signature;
    b. checks CSP service status, SSCD quality, end-user Certificate quality (Qualified or Non-Qualified)
4. if CSP service is "in accordance" (Service Current Status clause according to [ETSI-102-231]), contacts the CSP and asks for the end-user certificate status (note: CRL or OCSP links are available only in the end-user certificate, usually not in the TSL);
5. checks via OCSP or CRL the current end-user certificate status.

Note that in this case the application X may be required to archive the TSL used to be able to prove that it checked not only validity but also quality at time of verification.

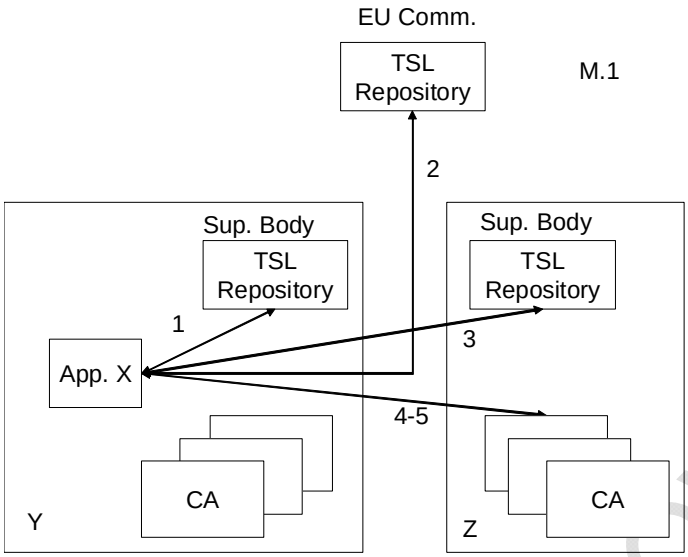


Figure 3: TSL used directly by end system

## 6.6 TSL Used by Validation Service

If the application X is not able to use TSLs by itself, or the application for other reasons has desired to outsource the validation functionality, it will use a Validation Service (VS). The application X contacts the VS as reference for its MS (step 1) by means of the VS's interface (e.g. XKMS as specified in D1.3 part 5). In this case the validation operations (steps 2-6 corresponding to steps 1-5 in 6.5) are performed by the VS in MS Y that at the end sends back the validation results to the application X.

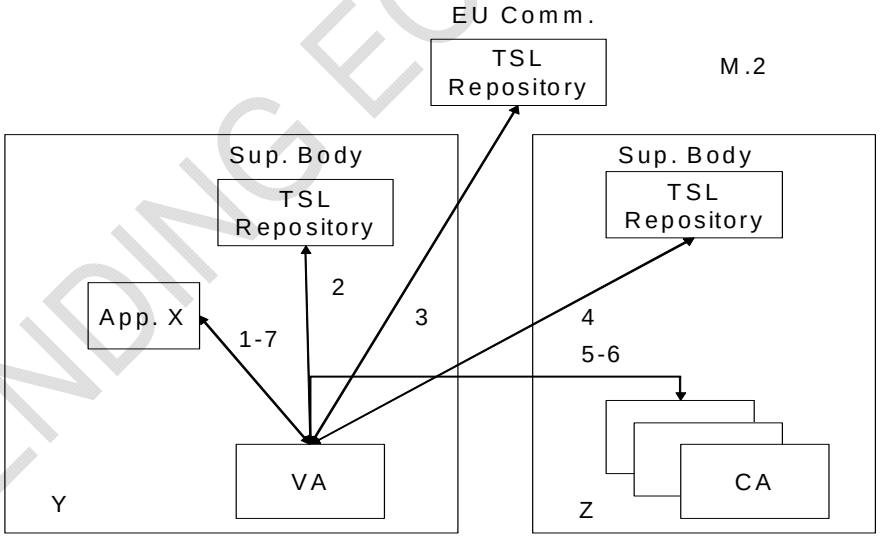


Figure 4: TSL used by a Validation Service

Note that this model relies only on use of TSLs and does not use request chaining between VAs as specified by this deliverable D1.3. Note also that a VA may pre-import or cache both TSLs and CA configuration elements fetched from TSLs in order to speed up processing.

In a simplified model, the national TSL of MS Y contains direct links to other MS TSLs, including MS Z, avoiding the step to the EU level.

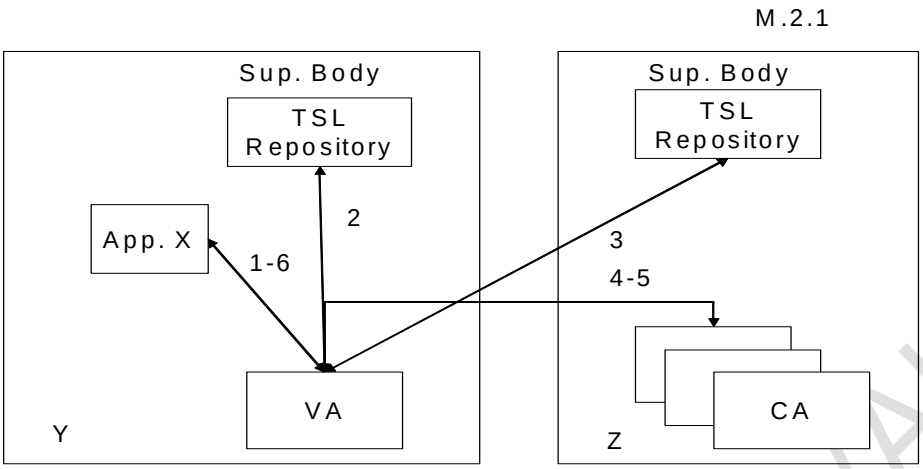


Figure 5: MS TSLs contains links to other TSL

As a further simplification, the managers of an application domain (e.g. PEPPOL Consortium) may decide to maintain a single TSL, where only CSPs in accordance with the application policy (e.g. PEPPOL signature policies) are taken in account.

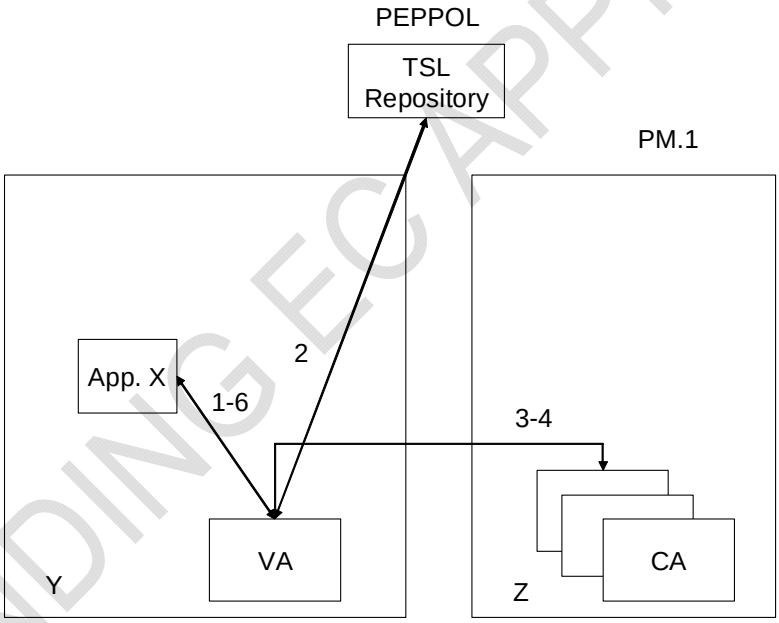


Figure 6: A single TSL

The TSL may be imported directly to the application or to a VS. Note that when a VS is used, the response signed by the VA (XKMS or OASIS DSS) shall include sufficient information to prove both quality and validity, thus there should be no need to convey the TSL to the application X. The VS may archive TSLs or rely on archival at the TSL issuer (see 6.3).

While in principle such a TSL issuer may aggregate information from the TSLs of the EU system into one list, the benefits of such an approach is questionable. However, a single list approach may be used for TSLs covering other services than those on the EU lists, e.g. validation services.

## 6.7 TSL Distribution for Information on VSs

Since each VS in PEPPOL may in general have a limited CSPs coverage, means shall be devised to create a trusted network of VSs (see chapter 3 and section 5.2). A central PEPPOL TSLs will be used to this effect.

The solution provides a list of the available VSs in the PEPPOL pilot and is distributed as a single TSL (Figure 7).

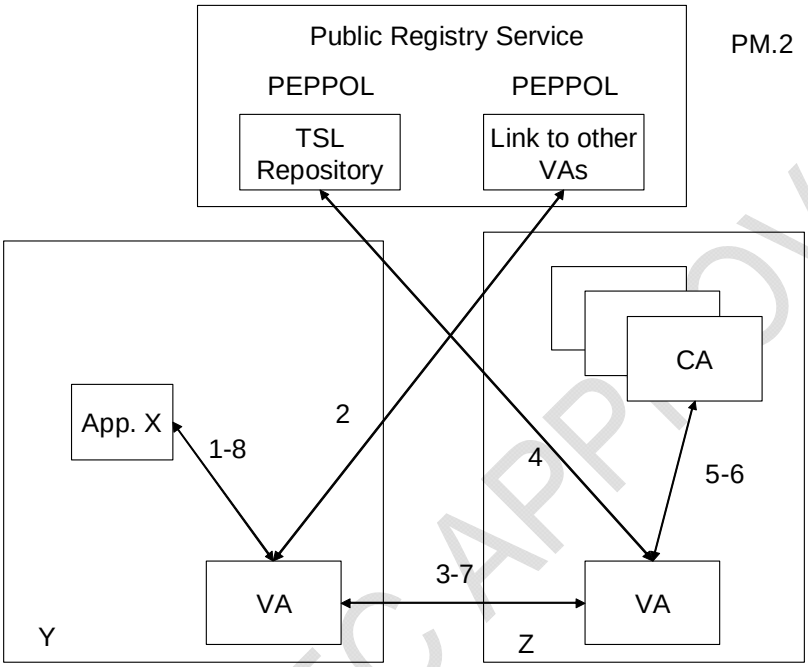


Figure 7: PEPPOL Public Registry Service (PPRS)

In this figure, a single TSL or TSL repository for "EU type" TSLs is also shown as an option. While this is not needed for qualified eID issuers, the approach could be used to include non-qualified eIDs in the TSL system.

The sum of the TSL for VSs and the optional TSL repository is called PEPPOL Public Registry Service (PPRS).

To establish trust between VSs, the PPRS can be used as follows by the VS in MS Y:

1. download from PPRS indications on how to contact and interrogate the VS in MS Z,
2. ask VS in MS Z for the end-user certificate validation.

VS in MS Z:

3. obtains an updated TSL (or uses a locally cached version)[12]; the figure shows downloading from the PPRS the EU system can also be used,
4. checks CSP service status, SSCD quality, end-user Certificate quality (Qualified or Non-Qualified),
5. if CSP service is "in accordance", contacts the CSP and asks the end-user certificate status,
6. checks via OCSP or CRL the current end-user status,
7. sends the validation results to VS in Y.

[12] The crucial purpose of this step is to bring the VS and information in the TSL in accordance, this process does not have to be dynamic, accordance can also be achieved by manual configuration.

VS in MS Y:

8. sends the validation results to the application X.

## 6.8 Need for Manual Configuration

The TSL use specified in sections 6.6 and 6.7 faces some immediate problems:

- Even the machine processable TSLs issued under the EU system may not be easily processable and may not contain all necessary information (see 6.2).
- A VA implementation cannot immediately be assumed to implement automated TSL import, at least not without a need for some additional, manual configuration.
- The TSL for VSs must be implemented and maintained (PEPPOL WP1 will take on this task).

The first approach may be manual configuration in each VS, mimicking a situation where an architecture as shown in Figure 7 exists.

Note also that for a start national VSs will not exist for all Member States. This can be managed by designating some VS to handle a particular MS even though this would normally be out of scope of the VS. Alternatively, and even as a permanent solution, a VS operating out of the national scope (see chapter 3) can take on the role of a “national VS” for specific countries.

This will have to be reflected in and maintained by the TSL for VSs, which is part of the PPRS.

## 6.9 Need for PEPPOL Member State TSLs

While availability and quality of Member State (MS) TSLs must be expected to improve, PEPPOL WP1 still needs to issue its own PEPPOL MS TSLs, which are part of the PPRS. The following reasons explain why this is necessary:

1.) The published MS TSLs do not contain all relevant TSPs issuing qualified certificates, for example the German one (see chapter 6.2) lacks information. Although the situation might change in near future, a solution has to be in place for the PEPPOL pilots as early as possible; PEPPOL MS TSLs provide a solution.

2.) The PEPPOL validation infrastructure aims at a maximum coverage of European TSPs, nevertheless some TSPs listed in national TSLs will not be covered by the validation infrastructure. There is a number of TSPs in several European countries (see as an example the description in section 6.2 of the Norwegian TSL) acting in the bank or health sector. Those are not expected or sensible to be used in cross border scenarios and will not be covered to save a relevant effort. The PEPPOL MS TSLs are closing this gap.

3.) The full coverage of the validation infrastructure cannot be achieved at once; the expansion of CA coverage is an ongoing process. This circumstance produces the requirement to reflect the productive current coverage of the validation infrastructure at a given time. PEPPOL MS TSLs provide this information.

4.) The national TSLs are limited to TSPs issuing qualified certificates. PEPPOL assumes the need to cover specific TSPs issuing non-qualified certificates as well, due to their usage in the procurement context. The PEPPOL MS TSLs issued by the appointed national authority or responsible PEPPOL partner can list those additional TSPs.

## 6.10 Extending TSL by VS Information

The TSL data structure defined by [ETSI-102-231] can be used to include VS services even though the VS role is not explicitly defined. In this case the *Service type identifier* as defined by [ETSI-102-

231] will be filled with the value "*unspecified*". Such entries may be added to existing TSLs (e.g. according to the EU system) or they may be gathered in a separate TSL. The latter is most relevant for the PEPPOL pilots.

Specification on how to include CAs in TSLs is not given below; this is supposed to be covered by the EU TSL system and by [ETSI-102-231], see also [CROBIES2.1] and [CROBIES2.2]. As stated in 6.7, the PPRS could include non-qualified CAs in the PEPPOL TSL in order to enrol such CAs in the TSL system, at least until such CAs are covered by "official" TSLs.

In the case of a separate TSL (issued by PEPPOL), the **Trusted List Issuing Scheme** must be specified. Note in particular the following elements that PEPPOL must handle:

- Trusted List **type** information (e.g. for identification of the fact that this TSL provides information on the accepted status of VSs in the PEPPOL context;
- Trusted List **owner information** (e.g., name, address, contact information, etc. of the Supervisory Body in charge of establishing, publishing securely and maintaining the list – in other words the PEPPOL Consortium);
- Information about the underlying **supervision/accreditation scheme** to which the TSL is associated, including but not limited to:
    - the MSs to which it applies,
    - information or reference of location where information on the scheme can be found (scheme model, rules, criteria, applicable community, type, etc.),
    - period of retention of (historical) information.
- **Trusted List policy** and/or legal notice, liabilities, responsibilities (e.g. PEPPOL Policy);
- Trusted List issue date and time and next foreseen update, i.e. an **update policy** is needed.

For each VS covered, the element on information about the TSP organisation must be filled in, in particular:

- The TSP organisation name as used in formal legal registrations;
- The TSP organisation UID as defined in formal legal registers (e.g., the proposed format for the qualified eID certificate profile[13] can be used);
- The TSP address and contact information;
- Additional information on the TSP either included directly or by reference to a location from where such information can be downloaded.

The VSs used by the PEPPOL pilots will not necessarily be run by formal authorities but the information should nonetheless be provided for each VS.

For each TSP organisation, further information must be provided for each trusted service provided. This set of information will include at least the following:



[13] A UID scheme can be based on a first part consisting of 3 initial characters specifying the type of organisation's identity reference, two characters of a country (according to ISO 3166), one blank space, and a second part consisting of data which type is defined by the three initial characters. One of the following set of three initial characters can be used as a mandatory formatting of such information:

1. "VAT" for identification based on VAT number,
2. "NTR" for identification based on National Trade Register.

Example: "VATBE 0876866142"

- An identifier about the type of service (e.g. *"generic" – CA(QC)* for Qualified Certification Authority services, *"generic" – CA(PKC)* for non-Qualified Certification Authority services, and *VS* for Validation Service)[14];
- (Trade) name of this issuing trusted service;
- For CSP (CA) services, an unambiguous unique identifier of the issuing CA service (i.e. the CA certificate supporting the issuing of end-entity EC;
- For TSP (VS) services, an unambiguous unique identifier of the VS services. This could be a digital identity like a company certificate.
- Additional information on the trusted service (e.g., directly included or included by reference to a location from which information can be downloaded, access information regarding the service.

Provisioning of adequate information for a VS should be relatively straightforward.

Moreover [ETSI-102-231] specifies the service current status in terms of defined parameters. The EU TSL system requires that historical information about CSP status is kept in TSLs. Status codes are:

1. Under Supervision
2. Supervision of Service in Cessation
3. Supervision Expired
4. Supervision Revoked
5. Accredited
6. Accreditation Expired
7. Accreditation Revoked

As no supervision/accreditation system exists for VSs, these status codes are nor relevant. One alternative is to add a URI meaning "PEPPOL accepted/recognised TSP". Alternatively one could consider adding for example:

8. Contractually accepted
9. Contractually accepted expired
10. Contractual accepted revoked
11. Validation Service recognised
12. Validation Service recognised expired
13. Validation Service recognised revoked

Contractual can be used to denote an approval, e.g. according to the "approval status" quality parameter defined in D1.3 part 7, while recognised can denote a VS otherwise incorporated.

## 6.11 PEPPOL TSL Issuing

PEPPOL will issue a TSL covering relevant VSs and MS TSLs covering the relevant qualified and non-qualified CAs. The TSL is made available in machine processable format according to [ETSI-102-231] with the modifications specified in the previous section. A human readable version of the PEPPOL TSL could be considered but is less relevant.

[14] A specification of the PEPPOL related customisations as used in the pilot is given in PEPPOL D1.2 chapter 3.

The machine readable format shall be XML according to Annex B of [ETSI-102-231]. The alternative ASN.1 format is considered out of scope.

Inclusion of pointers to the official EU TSL system can be considered. The TSL shall be published at a well-known URI. The certificate (possibly also path) used for signing the TSL shall be published along with the TSL.

The TSL shall be signed using an XML DSIG approach or preferably a XAdES-BES signature according to Annex B of [ETSI-102-231]. An official entity must be appointed by PEPPOL with authorisation to sign the TSL. Further requirements for the signature, e.g. whether or not a qualified signature is needed, must be determined.

# 7 Time Stamps and TSA Services

## 7.1 Validation of Time Stamp Issued by TSA on Sender Side

PEPPOL WP1 does not recommend use of TSA time stamps from the sending side but if such a time stamp is included in an SDO submitted e.g. as part of a tendering process, the recipient should be able to process this. This however requires that the recipient:

- Knows the public key of the TSA as a trust anchor;
- Is able to recognise the TSA as an accredited TSA acting accordingly;
- Is able to verify the time stamp format;
- Is able to verify the quality of the time stamp, possibly ignoring requirements for qualified signatures in cases when the TSA certificate is not issued to a physical person;
- Is able to judge the semantics implied by the time stamp.

The following challenges are noted:

- A TSA may constitute a separate trust anchor that will have to be recognised by the receiver in the same manner as a CA.
- This adds to the interoperability challenges that PEPPOL WP1 aims to solve, and PEPPOL has decided to not spend resources on TSA interoperability across Europe.
- The TSA role is not formally recognised in all Member States and the role does not even exist in some countries.
- A TSA signature will in many cases not be a qualified signature, meaning that interoperability is further complicated.

If an external validation service is used for the entire signature verification (OASIS DSS approach, see D1.3 part 6), the validation service should be able to handle this on behalf of the recipient, and to indicate time stamps and their signatures accordingly in responses.

Given recommendations below, these requirements are regarded as optional.

## 7.2 PEPPOL WP1 Recommendations for Time Stamps

Time stamps are important in procurement processes. Usually, time stamps are obtained by use of a local system clock but use of an external TSA may be required. The protocols and formats specified by PEPPOL must include time stamps and must address requirements related to trusted time. This is an issue that must be discussed with other WPs in PEPPOL. Each time stamp must have defined semantics, such as time of sending, time of reception etc. Appendix 2 discusses issues related to time information for e-procurement.

PEPPOL WP1 recommends as the main solution that if a time stamp from the sender is included with a signature, this should be generated locally by use of a system clock or another correct time source. A TSA service used by the sender is still an option.

The receiving side will typically obtain time stamps (from TSA or system clock whatever is considered necessary) to embed in more elaborate SDO structures such as XAdES [ETSI-101-903], CAdES [ETSI-101-733] or PAdES [ETSI-102-778] or in archival records for the signed documents. This is considered outside the scope of PEPPOL and TSA services will not be offered by PEPPOL for the pilots. There may however be mandatory requirements for use of a TSA (e.g. Italy and France). In

such cases, the receiver will select a TSA service that is locally known and regarded as trusted by the receiver.

# 8 Figures

# 9 References


[Cameron] K.Cameron, The Laws of Identity. 2005, http://www.identityblog.com/stories/2005/05/13/TheLawsOfIdentity.pdf

[COMM01] Commission of the European Communities, Action-Plan on e-Signatures and e-Identification to Facilitate the Provision of Cross-Border Public Services in the Single Market, Communication from the Commission to the Council, the European Parliament, the European Economic and Social Committee and the Committee of the Regions, November 2008, http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2008:0798:FIN:EN:PDF

[COMM02] Commission of the European Communities, Commission Decision of 16 October 2009 on 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, October 2009, http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2009:299:0018:0054:EN:PDF

[CROBIES2.1] Sealed, time.lex, Siemens: Study on Cross-Border Interoperability of eSignatures (CROBIES), Trusted Lists Implementer's Guide. CROBIES deliverable 2.1, July 2010, http://ec.europa.eu/information_society/policy/esignature/docs/crobies_deliverables/crobiesd2.1.pdf

[CROBIES2.2] Sealed, time.lex, Siemens: Study on Cross-Border Interoperability of eSignatures (CROBIES), Trusted Lists User's Guide. CROBIES deliverable 2.2, July 2010, http://ec.europa.eu/information_society/policy/esignature/docs/crobies_deliverables/crobiesd2.2.pdf

[ETSI-102-231] ETSI TS 102 231 v3.1.2 (2009-12) Electronic Signatures and Infrastructures (ESI) – Provision of Harmonised Trust Service Provider Information.

[ETSI-101-733] ETSI TS 101 733 V.1.7.4 (2008-07) Electronic Signature and Infrastructure (ESI) – CMS Advanced Electronic Signature (CAdES).

[ETSI-101-903] ETSI TS 101 903 V.1.3.2 (2006-03) Electronic Signature and Infrastructure (ESI) – XML Advanced Electronic Signatures (XAdES).

[ETSI-102-640] ETSI TS 102 640 V2.1.1 (2010-01) Electronic Signature and Infrastructure (ESI) – Registered Electronic Mail (REM) parts 1-5.

[ETSI-102-778] ETSI TS 102 778 V.1.1.1 (2009-07). Electronic Signature and Infrastructure (ESI) – PDF Advanced Electronic Signature Profiles (PAdES), Parts 1-5.

[EU01] EU, Community Framework for Electronic Signatures. Directive 1999/93/EC of the European Parliament and of the Council, December 1999, http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2000:013:0012:0020:EN:PDF

[EU02] EU, Coordination of Procedures for the Award of Public Works Contracts, Public Supply Contracts and Public Service Contracts. Directive 2004/18/EC of the European Parliament and of the Council, March 2004, http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2004:134:0114:0240:EN:PDF

[EU03] EU, Coordinating the Procurement Procedures of Entities Operating in the Water, Energy, Transport and Postal Services Sectors. Directive 2004/17/EC of the European Parliament and of the Council, March 2004, http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2004:134:0001:0113:EN:PDF

[IDABC01] Siemens, time.lex: Preliminary Study on Mutual Recognition of eSignatures for eGovernment Applications (Final Study and 29 Country Profiles). IDABC, 2007.

[IDABC02] e-Procurement specification (Functional Requirements for conducting electronic public procurement under the EU framework), IDABC 2005.

[Josang] A.Jøsang, The Right Type of Trust for Distributed Systems, Proceedings of the 1996 New Security Paradigms Workshop, 1996.

[OASIS1] OASIS, Understanding Certification Path Construction. White Paper from PKI Forum Technical Group, 2002.

[Olnes1] J.Ølnes, A Taxonomy for Trusted Services, First IFIP Conference on e-Commerce, e-Business, e-Government (I3E), Zurich, 2001.

[Olnes2] J.Ølnes: "PKI Interoperability by an Independent, Trusted Validation Authority", 5th Annual PKI R&D Workshop, NIST, Gaithersburgh, USA, 2006. http://middleware.internet2.edu/pki06/proceedings/olnes-interoperability.pdf

[Olnes3] J.Ølnes et al., Making Digital Signatures Work across National Borders. ISSE/SECURE Conference, Warszawa, 2007.

[PEPPOL-D1.1] PEPPOL project: Requirements for Use of Signatures in Public Procurement Processes. PEPPOL Deliverable D1.1, April 2009, http://www.peppol.eu/work_in_progress/wp-1-esignature/results/deliverable-1.1/first-deliverable-of-wp1-has-been-released

[PEPPOL-D1.2] PEPPOL project: Trans-national Verification Solution(s) – Prototype Documentation. PEPPOL Deliverable D1.2, April 2010, http://www.peppol.eu/work_in_progress/wp-1-esignature/results/deliverable-1.2/d1.2-trans-national-verification-solution-s-prototype-documentation

[RFC3161] C.Adams, P.Cain, D.Pinkas, R.Zuccerato. Internet X.509 Public Key Infrastructure Time-Stamp Protocol (TSP), RFC3161, 2001.

[RFC3379] D.Pinkas, R.Housley, Delegated Path Validation and Delegated Path Discovery Protocol Requirements. RFC3379, 2002.

[RFC3628] D.Pinkas, N.Pope, J.Ross, Policy Requirements for Time-Stamping Authorities (TSAs), RFC3628, 2003.

[Siemens] Siemens, time.lex, Preliminary Study on the Electronic Provision of Certificates and Attestations Usually Required in Public Procurement Procedures – Final Report – Strategy and Implementation Roadmaps. European Commission, Internal Market and Services DG, September 2008, http://ec.europa.eu/internal_market/publicprocurement/docs/eprocurement/ecertificates-study_en.pdf

[XML-DSig] D.Eastlake, J.Reagle, D.Solo. XMLSignature Syntax and Processing. W3C Recommendation. http://www.w3.org/TR/xmldsig-core/ 2002.

# 10 Appendix 1: Trust and Trust Models Theory

## 10.1 Aspects of Trust

In order to gain acceptance, electronic commerce must be trustworthy. There are two aspects of trust in this picture [Olnes1]:

3. "Technical trust" in the technology used, i.e. computer systems and the means to communicate between these systems.
4. "Organisational trust" between the actors that eventually shall carry out the business transactions, e.g. enter a contractual relationship.

[Josang] uses the terms trust in "rational" and "passionate" entities.

Both these aspects must be considered. If systems are not trustworthy (e.g. an e-signature with insufficient quality), the transaction cannot be carried out.

But even if trustworthy systems are used, the actors need to determine if the counterpart can be trusted to fulfil its duties according to the transaction in question; authenticating the crook or have him electronically sign something does not necessarily make him honest. If this "organisational trust" is too low, again the parties cannot carry out the transaction. Alternatively, the transaction can be carried out only if sufficient tracing mechanisms (electronic signatures may be important here) are in place to ensure that a distrusting actor can follow suit if the counterpart does not behave as expected.

Although one may measure trust on a scale from 0 (complete distrust) to 1 (complete trust), a concrete trust decision is always binary yes/no. Trust above a certain value yields a positive decision. This "calculation" is performed independently by the parties involved, meaning that they may end up with different conclusions based on the same situation; or rephrased: trust may be mutual or one-way. Trust can be viewed as a risk management decision relatively to the situation at hand – what is the risk of trusting this particular actor in this particular situation?

A trust decision is ultimately always a human decision; which however may be implemented in a computer system. It follows that a trust decision is subjective. The basis for the decision is knowledge and assumptions about the situation at hand. The decision is not necessarily rational, as the "knowledge and assumptions" may reflect a perceived, not real, risk situation. E.g. it is not sufficient that a system is trustworthy, it must also be perceived as trustworthy; likewise with organisations and humans.

## 10.2 The Role of TTPs – Direct and Indirect Trust

Trust decisions can be made more rational by increasing knowledge, decreasing the part based on assumptions only. On a small scale, actors can build knowledge themselves, resulting in direct trust between the actors.

On a large scale, such as faced by electronic public procurement across Europe, actors may have no prior knowledge of one another, and thus limited information to determine the trust to take in a counterpart or in the technical solutions (such as signature mechanism) used by the counterpart.

In this case, trust must be established indirectly by referring to infrastructures of trusted services, termed TTP (Trusted Third Party) services (although they do not necessarily have to be offered by independent, third parties). An actor derives direct trust in a TTP based on knowledge and assumptions about the quality of the TTP's services and possibly also other factors (nationality, financial situation, reputation etc.) related to the actor(s) that run the TTP.

TTPs produce, validate or store assertions [Olnes1] about statements that must be fulfilled. An eID is an identity assertion issued by a TTP (the CA). By trusting a TTP and its assertions, an actor can derive trust in counterparts. In this, trust is viewed as a transitive property.

This can (or must) be further expanded since not all actors will have direct trust in all TTPs. Thus, an actor must be able to refer to the TTPs it directly trusts, and based on this derive indirect trust in other TTPs. This is the rationale behind trust structures for PKI (cross-certification, hierarchies, bridge-CAs etc.) and also for the idea of independent validation authorities [Olnes2].

## 10.3 TTPs and Protocols

Communication with a TTP service can take one of three patterns:

- Off-line: The TTP produces its assertions in advance and is not directly involved in the communication between the actors. A CA issuing eIDs is an off-line TTP. (There is usually also on-line access to check revocation status of eIDs, however this is a validation step and not issuing of eIDs.)
- On-line: The TTP is involved in protocols as “side step” by one or both (all) actors. A validation service is one example, a time stamping service is another one, and a third example is a credit check statement issued by a trusted rating company.
- In-line: All communication goes through the TTP service. A service offering anonymity may work in this mode, as may certain broker services for electronic commerce.

There are two levels of protocols for electronic commerce transactions:

- The communication protocols between the IT systems. Although authentication and security are important for communication, this is not in focus here but rather a topic that is addressed by PEPPOL WP8 (see also chapter 4 of this document, D1.3 part 4)..
- The electronic commerce protocols, defined as a sequence of exchanges of defined messages/documents between the actors. This can be automated between computer systems, or the protocol may run (partly) under human control.

When TTP services are (optional or mandatory) elements in an electronic commerce protocol, the interactions with the TTPs should be modelled in the definition of the protocol. In particular for on-line services, the protocol to use towards the TTP service must also be defined.

The need for involvement of TTPs in commerce protocols can be derived from legal sources, business requirements, or security and risk management requirements.

## 10.4 Trust in Electronic Signatures

In itself, an eID and an advanced electronic signature only provides trust in the communication mechanism – integrity protection, authenticity, accountability, and authentication of signer. This does not necessarily provide trust in the person signing, see below.

The first issue then is to specify the conditions for trust in the signature itself, i.e. the signature validation policy (see D1.3 part 3) in force, specifically:

- Quality requirements such as qualified signature, qualified eID etc.
- Trust in the issuer of the eID.
- Requirements on signature formats etc.

Instead of having each actor derive these requirements alone, referral to common signature policies is beneficial. The idea of qualified signatures is exactly to have one such level that is legally admissible

across Europe and has sufficient security/quality level to fulfil all purposes[15]. The real situation is that products offering SSCD (secure signature creation device) with sufficient certification are not available in all European countries and where available the market penetration is highly variable. Thus, more signature policies may have to be specified in addition to qualified signatures but the number should be kept small.

An eID can only be trusted if the issuer (the CA) is trusted either directly or indirectly via some trust structure. It is strongly advised that signature policies shall be defined as general quality criteria and not as merely a list of acceptable CAs, at least not unless such a list is know to be exhaustive and non-discriminatory.

Further signature policy requirements can be defined with respect to signature formats and use of particular cryptographic algorithms or algorithms with a minimum security level (see D1.3 parts 3 and 7).

## 10.5 Electronic Signatures and Organisational Trust

This trust decision is not directly related to accepting the signature itself, but rather to acceptance of the contents of the signed document. The contribution of an electronic signature (or an eID used for authentication) to the organisational trust between actors depends on the situation:

- Is this a known counterpart, for which we have enough further knowledge on which to base the trust decision?
- Is this a previously unknown counterpart or a counterpart where the additional information is too limited?

In the first case, we are fine. In the second case, there are alternative actions to be taken:

- The signature provides a strong identity proof, and one may conclude that this is sufficient to trust the other actor and believe his honest intentions.
- The name authenticated by the eID may in some cases provide extra information such as organisational attributes, and this may be used in the trust decision.
- One may decide that further information or further assertions are needed for the trust decision.

Information may be obtained from the counterpart itself, or one may obtain assertions from other TTPs such as business registries, credit rating services, tax authorities etc. These services must be trusted, either directly or indirectly.

Guidelines for such trust decisions can be formulated as framework policies that can be referred to by actors. The number of policies must be limited. Alternatives may be:

- If an e-signature is above a certain quality level (e.g. qualified signature), the contents of the signed document is accepted as true.
- If the information is insufficient, the counterpart itself is asked to supply additional information, which may or may not be checked against authoritative sources (such as business registers).
- Further information is obtained from independent, trusted sources; in which case the necessary services and infrastructure must be identified and specified.

PEPPOL WP1 does some work on framework policies, and this is further elaborated in D1.3 part 3.

[15] With the exception of information that is classified for military or other (national) security purposes. Public procurement, e.g. of defence material, may in deed touch upon classified information but this is considered to be out of scope of PEPPOL.

## 10.6 E-signature and eID Interoperability

### 10.6.1 PKI Trust Models and Certificate Paths

Trust structures among CAs (issuers of eIDs) are constructed in three alternative ways:

- Cross-certification: Pairs of CAs issue certificates to one another. This model does not scale and is not discussed further in the following.
- Hierarchy: A root-CA issues certificates to other CAs. An eID issued by any CA in the hierarchy can be validated starting at the root-CA. (There are several ways of constructing hierarchies but the details are not relevant here.)
- Bridge-CA: CAs (may be the root-CA of a hierarchy) cross-certify with the bridge-CA, which does not issue end user eIDs but acts as a hub.

The idea is that an RP (relying party) shall be able to discover and validate a certificate path from a directly trusted CA to any CA that is a member of the same trust structure. The number of CAs directly trusted by an RP can be reduced.

General comments on trust structures are that certificate path discovery may be a very difficult task [OASIS1] and certificate path validation may be a resource demanding process due to the need for repetitive certificate processing. Validation services may be used to outsource path processing [RFC3379] or to minimise path processing [Olnes2].

For further discussion on trust structures, see [Olnes2], which states as the main problem the lack of liability taken on by actors running hierarchies or bridge-CAs. Liability remains an issue between the relying party and the individual (unknown) CA. Further problems are related to assessment of quality, where policy mapping or root-CA base policies may be used to assess a common quality level; however policy mapping requires equivalence of policies, not only comparable quality.

Both hierarchies and bridge-CAs are in use today but there is at present no pan-European trust structure for PKI. While a pan-European bridge-CA may be envisaged (see D1.3 part 1 for pilot initiatives in Europe), PEPPOL will not rely on such a structure being formed and will not actively push the creation of such a bridge-CA. However, PEPPOL will utilise existing and future trust structures to the extent possible and will closely monitor progress in the area.

### 10.6.2 Trust Lists and Trust List Distribution Services

A trust list consists of named CAs (other trusted services may also be covered) and their public keys. All CAs on the list are trusted. The CA may be the root of a hierarchy, in which case all CAs in the hierarchy can be trusted. An RP may manage a trust list entirely on its own or base the list on existing lists such as (adding or removing CAs from) Microsoft's standard list.

Trust list management may also be done by a third party, which should regularly distribute lists to its subscribers. Interoperability is achieved by installation of compatible trust lists at all actors. This has been tried in Europe by the IDABC Bridge/Gateway CA (EBGCA) pilot (see D1.3 part 1), and ETSI has developed a standard for a trust list distribution service [ETSI-102-231]. This approach has been continued by the EU Commission Action Plan on E-signatures and E-identification [COMM01] and a European system for TSL distribution is now established (see section 6.2 of this document, D1.3 part 4). The status of a CA (such as issuer of qualified certificates) is indicated as extra parameters of the trust list. Quality information (such as described in D1.3 part 7) is a fairly straightforward extension for any trust list.

The EBGCA pilot was particular in that it defined itself as a trust anchor for the RP and took on some liability with respect to the RP. In other cases, like Microsoft's embedded trust list, the CAs take the trust anchor role, and liability remains an issue between the RP and the individual CA. As for quality

information, liability information may in principle be distributed with the trust list; however there is no ongoing work in this direction as far as we know.

Since no all-encompassing PKI structure exists, an RP must today maintain a trust list with quite a lot of entries if many CAs shall be covered. E.g. the number of CAs in Europe issuing qualified certificates is above 100 and this is in many cases only a subset of the relevant CAs. Bridge-CAs and hierarchies contribute to making the list shorter, and a trust list distribution service may cover all relevant CAs.

Use of trust lists is piloted by PEPPOL.

### 10.6.3 Independent Validation Authorities

A further suggestion for PKI interoperability is the introduction of an independent VA as a separate trust anchor [Olnes2]. The VA offers a uniform interface for validation of eIDs and/or signed documents and returns an independent assessment of validity. The assessment should also cover issues such as quality, and the VA should take on liability for the answers.

Internally, the VA will maintain a (trust) list of the CAs it handles. Path processing should be avoided but can be used in the VA's internal processing if desired.

There are two major modes for use of a VA:

- The VA is used for all eID and e-signature processing, notably because the VA gives an independent assessment of validity and is a liable actor, thus providing better traceability and risk management.
- The RP maintains a trust list of local (in some meaning of that word) CAs, while "unknown" CAs are handled by calls to the VA. This is a more technical approach to use of a VA.

PEPPOL's trust models and architecture support validation services that may or may not be authorities. A technical validation service will provide technical trust in the correctness and quality of eIDs and e-signatures; however liability is referred to the CA. A validation authority will give the same answers but also acts as a "one-stop shopping" actor for validation, covering agreement, billing, trust, complaining, and liability.

# 11 Appendix 2: Time Stamp Requirements

## 11.1 Time in Documents and Associated Time

For digital documents meant for human reading (such as a PDF document), time may be part of the document content such as a date in a letter. The time is provided by the originator of the document and gives a time indication that may or may not be trusted by other parties.

For electronic processes one usually rather refers to time of events associated with documents, such as sending or receiving, rather than time in the document content. Time associated with events and documents is recorded either as metadata or indirectly by reference to logs and other system information. Metadata may be attached by any actor involved in the procurement process, including independent, trusted time stamping authorities (TSA) and other third parties.

## 11.2 EU Directives, Tendering Process Requirements

The EU Directives on public procurement [EU02] [EU03] require reliable time stamping of events in electronic tendering (the only procurement process covered by the Directives). This is a well-justified requirement since a tendering process typically involves strict deadlines that must be met. The Directives do not mandate use of an independent TSAs but allow time stamps to be done by other means that are considered sufficiently reliable; in practice this means by use of the local system clocks of the actors' IT systems. National legislation may however raise requirements for use of TSAs, e.g. Italian law states that a TSA should be used to time-stamp archival records.

The primary use of a time stamp is for verification in real time in the execution of a procurement process. However, time stamps must also be stored. The Directives state that traceability of processes must be guaranteed by archival of the original version of all documents along with records of all exchanges carried out, and it is difficult to see how sufficient traceability can be guaranteed unless reliable time stamps are also recorded.

## 11.3 Certificates and Attestations

The Siemens and time.lex study on "Preliminary Study on the electronic provision of certificates and attestations usually required in public procurement procedures" [Siemens] describes both the present situation and the desired future for such documents that typically accompany tenders. Certificates and attestation can be submitted ("pushed") by the economic operator, who firstly has to collect them from a trusted source. A document may also be fetched ("pulled") by the awarding entity (or an e-procurement system on behalf of the awarding entity) from the trusted source. In the push alternative, certificates and attestations should be signed by the trusted source. In the pull alternative, this is not necessarily the case since there is a direct link between the trusted source and the actor (the awarding entity) that needs to trust the information.

Certificates and attestations must include time of issuing and validity time. These time indications will be supplied by the issuer; if the issuer is trusted with respect to the documents, then it should be trusted to provide correct time as well.

A Virtual Company Dossier (VCD) is one example of such an attestation.

## 11.4 Requirements in Post Award Processes

These processes consist of orders, (possibly optional) order confirmations, and invoices. Catalogues may play an important role as reference documentation. PEPPOL WP1 does not anticipate any use of TSAs in these processes.

Catalogues will typically include information on validity period in particular for pricing. This is time information supplied by the issuer of the catalogue related to a time in the future, which cannot be attested to by a TSA. The only event that a TSA might attest is the issuing of the catalogue, but there should be no need for an independent time stamp for this event.

An order will typically have a time stamp indicating when the order was placed. If referring to a catalogue or other (pricing) information, there may be a need to prove that the order was sent within the validity period of the catalogue. One could envisage use of a TSA to prove that the order was placed in time. An order may also give a deadline for fulfilment of the request but this is again a time in the future that cannot be attested to by a TSA.

Similarly, an order confirmation will have a time stamp, and this might be issued by a TSA to prove that the order confirmation was issued within the deadline set by the order.

It is up to WP4 in PEPPOL to determine if use of TSA shall be piloted in ordering processes in PEPPOL but WP1 will not pose this as a requirement for the pilots. This should be a fairly straightforward addition to an ordering process if desired.

An invoice will have a time stamp for the issuing of the invoice and a deadline for due payment. The latter cannot be attested to by a TSA (it is in the future), and attesting the issuing time of an invoice adds very little value to the invoicing process.

Correspondingly, PEPPOL WP1 will limit work on time stamping to tendering (pre award) processes and related documents. The only general requirements imposed are that all system clocks must be reasonably correct and that all actors shall fill in time information correctly as demanded by the procurement processes (but note that other actors may not unquestionably trust this time information, and business protocols should state when requirements for trusted time apply).

## 11.5 Security Risks Related to Time Claims

If a time stamp is not sufficiently trustworthy, an actor can claim that some event happened before or after some threshold value. For procurement, the main issue is a tender being in time or too late. Another issue may be that tenders are not opened by the awarding authority before the time announced.

For tender submission, neither the economic operator nor the awarding authority can in principle be trusted, not even if they provide a TSA time stamp. A TSA time stamp requested by an economic operator only proves that the tender was finished at that time, not that it was submitted in time. An awarding authority can be accused of deliberately delaying the TSA request for tenders until after the deadline, in order to refuse certain tenders that were in fact delivered in time.

The requirements are further accentuated if “advanced” procurement methods such as auctions are used. Then, not only correct time but also sequence of offers is important.

The corollary is that TSA time stamps as such can be used to prove that an event happened before a certain time (given the context and business protocol in use) but not in general that something happened too late. The TSA time stamp is a positive proof but may not be a negative one.

## 11.6 Trust, System Clocks versus TSA

The security risks outlined above are only some of several trust issues related to electronic tendering; trust that the awarding authority handles tenders correctly and fair. There are several approaches to mediate sufficient trust:

1. Use an independent procurement service rather than a system controlled by the awarding authority itself. This is the situation in many countries today, not primarily for trust reasons but rather as a matter of convenience to avoid proliferation in the number of systems. However, the operator of the procurement system should be neutral and trusted with respect to the procurement processes, such as not giving access to tenders before the specified time.
2. Define the awarding authority as ultimately trusted and perform all communication towards a system controlled by the awarding authority.
3. Use an independent service at least for the submission of tenders as an in-line trusted service. All tender (and possibly all other communication) passes through the service.

In situation 1, the service provider is usually trusted with respect to time. All transactions are time stamped by the service provider and there is no need for use of a TSA.

Situation 2 is in general not recommended but in case it is used, TSA time stamps may not help as described in the section on security risks above.

In situation 3, the in-line service will surely add a time stamp but since the in-line service is already trusted with respect to the communication, a separate TSA will not be used.

In all scenarios TSA time stamps may be added to prove that something happened before a certain time as discussed above, and TSA time stamps may enhance the situations. But the situation is that TSA time stamps are rarely used today. The exception may be time stamping of long-term SDOs for archiving, see below.

## 11.7 Time Stamp Authority (TSA)

### 11.7.1 Base Standards for Time-stamp Protocol and TSAs

The protocol towards a TSA is the TSP (Time-Stamp Protocol) specified by [RFC3161]. See also [RFC3628] (also issued as ETSI TS 102 023) on “Policy Requirements for Time-Stamping Authorities (TSAs)”.

Note that a TSA can only time stamp current time. A TSA cannot attest to a time in the future, such as a deadline or a validity period. If such a time indication (e.g. the validity period of a catalogue) needs protection from tampering by other actors, the document in question (e.g. the catalogue) should be signed by the issuer.

### 11.7.2 TSAs as Trust Anchors, Accreditation

As stated by [RFC3628], a TSA is a certification-service-provider, as defined in the EU Directive on Electronic Signatures [EU01]. TSA services are typically offered by the same actors that offer eID issuing (CA) services; in Italy there is even a requirement that a CA issuing qualified certificates shall offer a TSA service. However, in principle a TSA service can be offered by other actors, independently from CA services.

A TSA is usually a separate trust anchor, i.e. the certificates for signing time stamps is issued under a separate root-CA. In Italy this is even a firm requirement. In this case, a time stamp signed by the TSA provides proof of authenticity and integrity even in the event of compromise of the CA (or root-CA) of any signer.

While thus providing an extra layer of security, this arrangement adds to the complexity of trust anchor management since a list of root- certificates (public keys) for TSAs must be maintained along with root-CAs for CAs. Note that in Italy keys used to sign time stamps can be valid for one month only. Frequent key changes increase confidence in the solutions.

### 11.7.3 Qualified and Non-Qualified TSA Signatures, Accreditation

In most countries in Europe, a qualified certificate can only be issued to a natural person, and a TSA is only a legal person. Thus, a TSA signature will usually not be a qualified signature.

There is no uniform scheme throughout Europe for accreditation of TSAs. Some countries (like Italy and Germany) have this in place, while the default situation is just that the TSA falls under the legislation that applies to certification-service providers. Since a TSA is usually not subject to requirements pertaining to qualified level, the TSA market may be entirely open in some countries; no accreditation and no supervision.

In principle this implies that the quality of a TSA signature can vary and cannot be measured against the requirements for qualified signatures. However, in practice all TSAs will fulfil all requirements for qualified signatures except for the qualified mark in the TSA's certificate. But if the signature policy in force calls for qualified signatures to be used, an exception may have to be made for TSA signatures.

One way to get around this problem is to name the TSA certificate by a pseudonym registered for a natural person (e.g. the managing director of the TSA service provider). Thus, the TSA certificate can be issued as a qualified certificate and its signatures will also be qualified. This solution is in use in Germany but cannot be expected to be applicable in all countries.

## 11.8 Time Stamp Validation

If a time stamp by a TSA is included in an SDO (Signed Data Object) submitted e.g. as part of a tendering process, the receiver should be able to process this. This however requires that the receiver:

- Knows the public key of the TSA as a trust anchor;
- Is able to recognise the TSA as an accredited TSA acting accordingly;
- Is able to verify the time stamp format;
- Is able to verify the quality of the time stamp, possibly ignoring requirements for qualified signatures in cases when TSA certificate is not issued to a physical person;
- Is able to judge the semantics implied by the time stamp.

If an external validation service is used for the entire signature verification (OASIS DSS approach, see D1.3 part 6), the validation service should be able to handle this on behalf of the receiver, and to indicate time stamps and their signatures accordingly in responses.

Given recommendations below, these requirements are regarded as optional, also because the signature policy recommendation in D1.3 part 3 is to not require "advanced" SDOs to be produced on the signing side.

## 11.9 PEPPOL Recommendations for Time Stamps

Time stamps are important in procurement processes. The protocols and formats specified by PEPPOL must include time stamps and must address requirements related to trusted time. This is an issue that must be discussed with other WPs in PEPPOL. Each time stamp must have defined semantics, such as time of sending, time of reception etc.

Use of independent TSAs should be allowed, but be optional, in protocols and formats. PEPPOL pilots will not prioritise involvement of TSAs on the sending side (see also D1.3 part 3).

The receiving side will typically obtain time stamps (from TSA or system clock whatever is considered necessary) to embed in more elaborate SDO structures such as XAdES [ETSI-101-903] or CAdES [ETSI-101-733] or in archival records for the signed documents. This is considered outside the scope of PEPPOL but may be a requirement in some countries (e.g. Italy).