PEPPOL
Pan-European Public Procurement Online

PEPPOL Deliverable D1.1
Requirements for Use of Signatures in Public Procurement Processes
Part 4: Architecture and Trust Models

Version 1.2

PEPPOL WP1 2009-04-30

Borderless eProcurement

Let's make it happen!

cip

Table of contents

1 Summary and Structure of Document

1.1 Scope and Structure of Deliverable D1.1

This document is a part of the multi-part deliverable D1.1 "Requirements for Use of Signatures in the Procurement Processes" issued by the PEPPOL[1] (Pan-European Public Procurement On-Line) project. PEPPOL is a three-year (May 2008 – May 2011) large scale pilot under the CIP (Competitiveness and Innovation Programme) initiative of the European Commission.

D1.1 consists of the following documents:

Part 1: Background and Scope

Part 2: 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 D1.1 deliverable is the first 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, if the resulting solution is successful it is believed that it will 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 guide the implementation, testing, and piloting of e-signature interoperability solutions to be done by PEPPOL. The specifications are publicly available and comments from any interested party are most welcome. Note that since the specifications of D1.1 by necessity will evolve as a result of further work in PEPPOL, any party using or referring to the specifications must ensure that the latest version is used; contact the PEPPOL project for information.

1.2 Scope and Structure of This Document

This document discusses architecture and trust issues for validation solutions for e-signatures and eIDs. Specifically, chapter 2 and appendix 1 discuss trust models, including the role of an authority. Chapter **Fehler! Verweisquelle konnte nicht gefunden werden.** raises the issues related to encryption. Chapter 4 describes technical integration of validation services. Use of Trust Status List (TSL) services in PEPPOL is described in chapter 5. A short discussion on use of Time Stamp Authority (TSA) services is included in chapter 6 and appendix 2. Appendix 3 discusses the possibilities for integration of validation interfaces on the sending side, conveying the validation information either by use of services provided by the PEPPOL infrastructure or in XAdES SDOs.

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

1.3 Version, List of Contributors

Version 1.0	2009/02/11	Complete version for internal quality assurance.
Version 1.1	2009/02/27	Submitted to PEPPOL project management, approved with comments at project management meeting 2009/03/27.
Version 1.2	2009/04/30	For publication, updated according to comments.

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

- **bremen online services, Germany,** http://www.bos-bremen.de
- **CNIPA, Italy** http://www.cnipa.it
- **DGME, French Ministry of Finance** http://www.references.modernisation.gouv.fr/
- **DNV, Norway** http://www.dnv.com

The following persons (alphabetical ordering for each participating organization) have contributed to the work:

Jörg Apitzsch	bos	Uwe Trostheide	bos	Dr. Daniele Tatti	CNIPA
Markus Ernst (co-editor)	bos	Jens Wothe	bos	Mario Terranova	CNIPA
Mark Horstmann	bos	Martine Schiavo	DGME	Anette Andresen	DNV
André Jens	bos	Stefano Arbia	CNIPA	Dr. Leif Buene	DNV
Dr. Jan Pelz	bos	Giovanni Manca	CNIPA	Jon Ølnes (editor)	DNV
Marco von der Pütten	bos	Adriano Rossi	CNIPA		

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. "Organizational 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 "organizational trust" from e-signatures is important and is covered by D1.1 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 authorizations? PEPPOL's work on VCD (Virtual Company Dossier) is one step in the direction of assessment of organizational trust; schemes for approval of actors that are allowed to connect to the PEPPOL infrastructure are another measure.

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

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

CAs issue assertions about subjects. 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 D1.1 part 3), notably that the quality and legal status are sufficient.

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 about CAs; their legal status and the quality of their eIDs and the signatures produced. Such services must be made available to the receiving side (the relying party) for e-signatures, since it is this actor that faces the challenge of asserting signature policy fulfilment with respect to a large number of CAs. The next section describes this in more detail.

Of other trusted services, the TSA (Time Stamp Authority) role and the need for trusted time are briefly discussed in chapter 6 and appendix 2. PEPPOL does not intend to work on time stamping.

The organizational trust aspects require other trusted services and other assertions but this is not discussed further in this document.

2.3 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 5. Several TSL issuers shall contribute to one European TSL system.
- Trusted validation services that validate eIDs and e-signatures and issue assertions about validity and signature policy adherence. Again, several validation services are most probably needed in a co-operative structure. Such co-operative structures are described in D1.1 part 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 apart from ensuring that all necessary information for archival is made available by the services offered.

2.4 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 will seek to explore both variants. 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.

2.5 Trust Anchors for Services and Authorities

An 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. An authority is usually well known to its customers, so this trust may be easily established. It may also be possible to look up authorities by means of registries or TSLs.

A technical service may on the other hand inherit trust from some other actor, e.g. sign using a certificate issued by some CA. Again, the service will be known to its customers.

Although a receiver selects a local, well-known and trusted validation service to call, all trusted 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 service may later have to be checked by other parties than the one that directly calls the trusted 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. Services may be provided by public (national) providers or by commercial (private) providers. Scope need not be national; degree of CA coverage may actually be a competitive edge for validation services.

The challenge arises when the local, trusted service is incapable of providing an answer on its own. Chapter 5 and D1.1 part 2 describe 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 in validation services is also possible.

In any case, the following rules are imposed by PEPPOL:

- The relying party calls its local, trusted validation service (unless a TSL is directly used).
- This service may relay the request to another validation service as needed; it is not anticipated that more than one step is necessary.
- Upon receiving the response from this remote validation service, the local validation service re-signs the response (and possibly adds information) before returning the response to the caller.
- I.e. to the relying party it always looks like the local validation service answers, even when the request is chained.

3 Encryption Is not Fully Supported by PEPPOL

3.1 Encryption of Business Documents Is not Supported

For end-to-end confidentiality, business documents should be encrypted. 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 may be too long-term for the PEPPOL pilots, may be to issue corporate certificates that can be used to both sign and encrypt – see D1.1 part 3 for some discussion on use of such certificates for signing. Such a solution, and its inherent trust issues such as being able to obtain and trust the encryption certificate of the receiver, are possibly for further study by PEPPOL WP1.

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 after a certain time. However such a solution is considered to be out of scope for PEPPOL.

The conclusion is that in general the transport channel must be trusted to preserve confidentiality of business documents. The PEPPOL transport infrastructure[2] (see D1.1 part 1 for a short description) guarantees such protection only for a part of the transport channel (see 3.2). Thus, the security must be assessed also for other parts of the transport channel. When the PEPPOL transport infrastructure is not used (e.g. tendering), use of a TLS/SSL protected channel is recommended.

3.2 PEPPOL Transport Infrastructure Protects Part of the Transport Channel

The PEPPOL transport infrastructure ensures integrity and confidentiality *between Access Points* (AP). 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, 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 actor may however have no means to assess trust in the (actor running an) AP service, if different from the operator system. If unsigned, clear text business documents are sent, one implicitly trusts the AP to be sufficiently secure and to itself not disclose or change documents. This trust may be perfectly

[2] See http://www.peppolinfrastructure.com

valid since APs must go through some kind of approval before being allowed to connect to the PEPPOL infrastructure.

Unsigned, clear text business documents are also available to the receiving side AP and to the receiving side operator system. This cannot be evaluated by the sender but it must be assumed 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 problem but actors should evaluate the trust issues in the given business scenario.

4 Validation Service Technical Integration

4.1 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 service providers (Operator systems in the figures below). 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 D1.1 respectively. Actors can use these interfaces to obtain the necessary verification information.

There is a need for underlying trust models to enable the system to scale and for "any" actor to be able to trust the verification information. This is described later in this document.

4.2 eID Validation by XKMS

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

1. The recipient selects an XKMS service to call. Presumably this will be a service selected and trusted by the recipient but it may also be selected from a TSL (Trust 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[3] 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 ValidateResponse that is signed and sent back to the local XKMS service.
6. The ValidateResult 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 2.5.

In both case 2 and 3-6, it is the local XKMS service that shall sign the ValidateResult returned to the recipient. This can include liability and other issues, depending on whether the service is a validation authority or a more technical validation service (see chapter 2). The XKMS interfaces (also when used for chaining) should adhere to the specifications in D1.1 part 5.

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

4.3 Signature Verification by OASIS DSS

4.3.1 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 ValidateResult from the remote responder is processed. A trust structure must exist to enable mutual trust between the two actors.

Note that there is no chaining of DSS requests. The service called by the recipient does all signature processing, 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 should adhere to the specifications in D1.1 part 6, and the XKMS interfaces for chaining should follow D1.1 part 5.

4.3.2 Validation Gateway

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

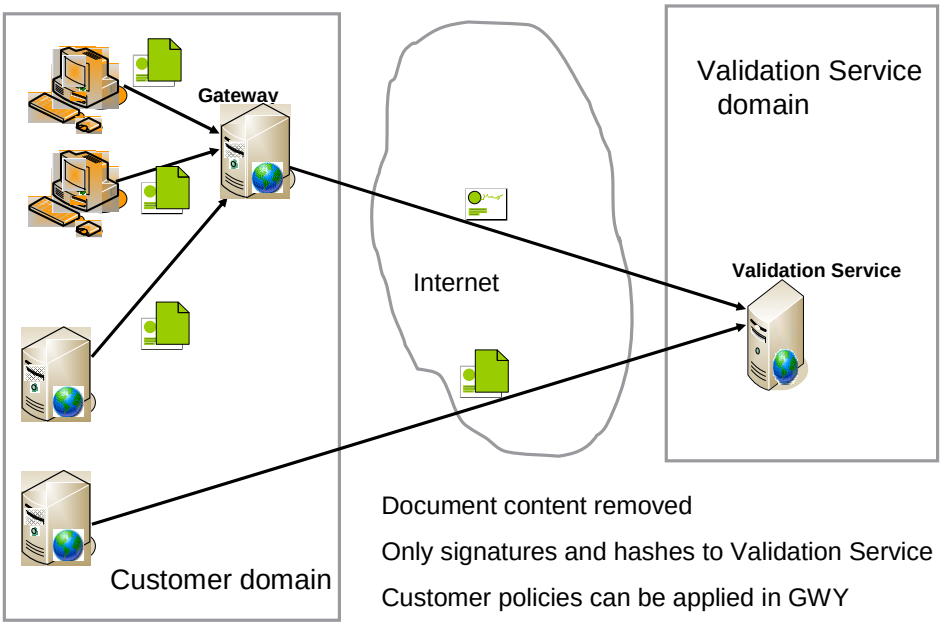

Figure 1: Validation gateway solution.

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

gateway removes the document, forwarding only signature fields and corresponding hash values to the validation service. Such a solution is described in [DNV01].

The gateway is installed (software with or without separate hardware) in the recipient's network and requests are directed to the gateway as shown in Figure 1 (the bottom arrow in Figure 1 shows that direct calls to the validation service may still be allowed). In the gateway, signatures are extracted and the corresponding hash values computed from the document. Only signatures and hash values are sent to the validation service; the content may be disposed of as soon as the request has been sent.

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

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

The interface to the gateway is internal at the recipient site. The gateway should offer the same OASIS DSS interface as the validation service, but requirements for request signing can be avoided (the 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 gateway as attachments; the response being attached to a response email.

5 Trust Models and Trust Status List (TSL)

5.1 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.

If TSLs are issued by national supervision bodies, then these will be national. However, other schemes for issuing of TSLs (such as a PEPPOL TSL) can well be envisaged.

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.

While this chapter refers to [ETSI-102-231], TSL specifications are also under development by the Commission's expert group for Service Directive implementation [SEALED01]. The revised specifications are used by PEPPOL.

5.2 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.

Note in particular that since TSL issuing services may not exist in the time frame of the PEPPOL pilots, 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 entirely 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 D1.1 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 be a separate trust anchor (a root-CA certificate of its own issuing a certificate to the TSL signer only) and/or show a certificate path to an EU top-level. The latter is only relevant if a model using a top-level EU TSL is used (see 5.5). In any case the TSL issuer's certificate shall not be issued by any "normal" CA.

In the model described in this chapter, knowledge of the certificate of the "local" TSL issuer, and the EU TSL issuer if used (see 5.5), is sufficient to obtain the information. Other TSL issuers will simply be listed as TSPs either in the local TSL or in the TSL issued by the EU.

Accreditation and trust in TSL issuers that are non-governmental (such as a PEPPOL TSL repository as described in 5.6) is for further study.

TSL issuers must archive the TSLs issued and/or otherwise maintain historical information about the CAs. 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.

5.3 Extending TSLs with Non-Qualified CAs

A TSL such as described in this chapter will only cover qualified CAs. A rather simple extension may be 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 D1.1 part 7 is recommended. This system is independent from the qualified state although qualified is clearly indicated. There is no ongoing work at including this quality classification system in TSL specifications but PEPPOL should initiate this topic.

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 quality parameters are used, and assessment is properly done, this can even be a replacement of today's lists of "approved" CAs in Microsoft and other operating systems.

Such TSL issuing is not discussed further in this document.

5.4 TSL Used by End System

In an ideal TSL Trust Model, a generic application X in Member State (MS) Y shall be able to use a TSL directly. On validation of a foreign (MS Z) end-user certificate, application X:

1. downloads an updated TSL from its Supervision/Accreditation Body (SB);
    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 URI (Pointers to other TSLs – clause 5.3.13 [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 - clause 5.3.13 [ETSI-102-231])
    a. searches the TSL's URI relative to the Country Code of the investigated CSP
3. downloads an updated TSL from the SB of the MS Z
    a. 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 5.5.4 [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, 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.

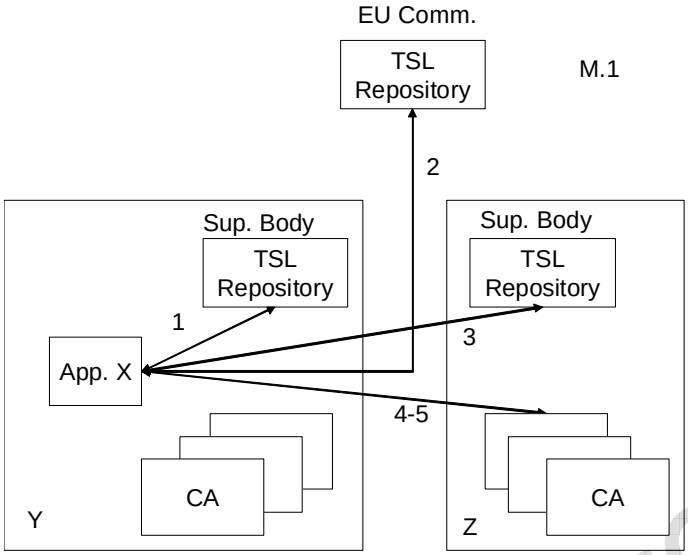

Figure 2: M.1 - Ideal TSL trust model

5.5 TSL Used by Validation Service

In the M.2 model, 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 mean of the VS's exposed interfaces. In this case the validation operations (steps 2-6) are performed by the VS in MS Y that at the end sends back the validation results to the application X.

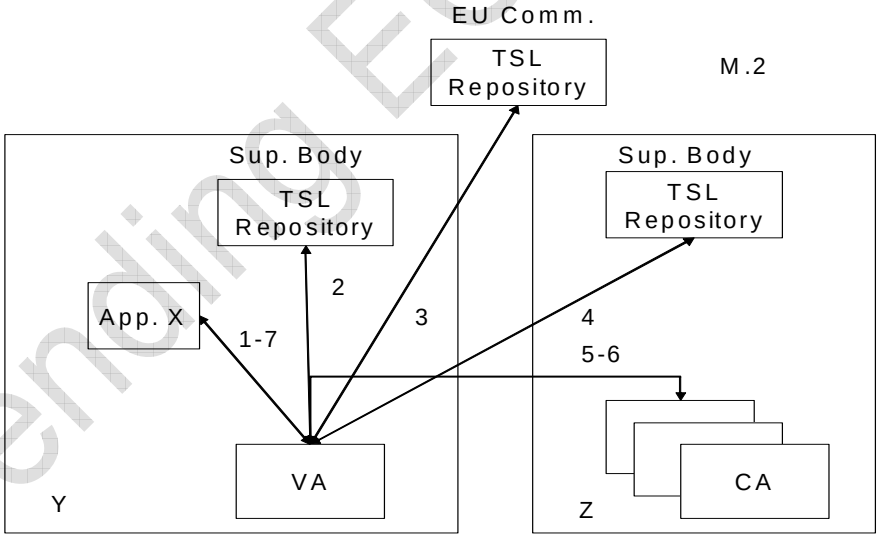

Figure 3: M.2 - Validation run by a Validation Service

The M.2.1 model is a simplified M.2 model where the SB's TSL of the MS Y contains direct links to other MS TSLs, including MS Z, avoiding to do the M.2 3rd passage.

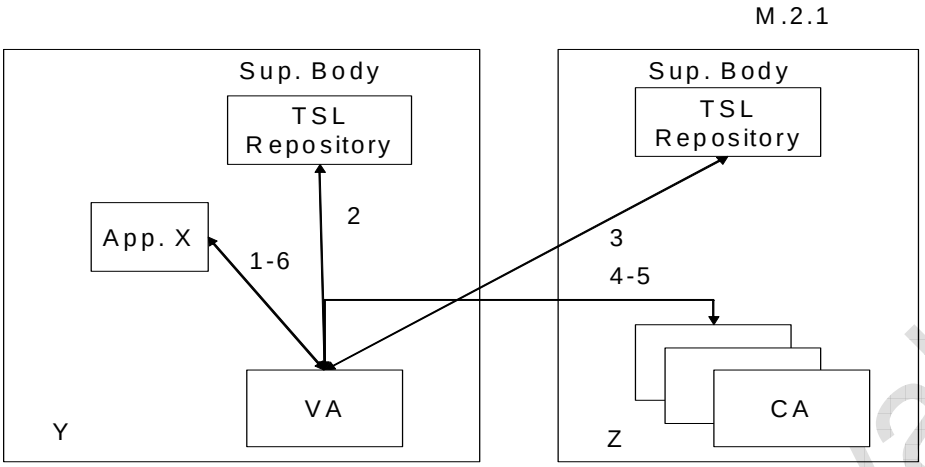

Figure 4: M.2.1 – MS TSLs contains links to other TSL

As further simplification, in PM.1 model, 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 policy) are taken in account.

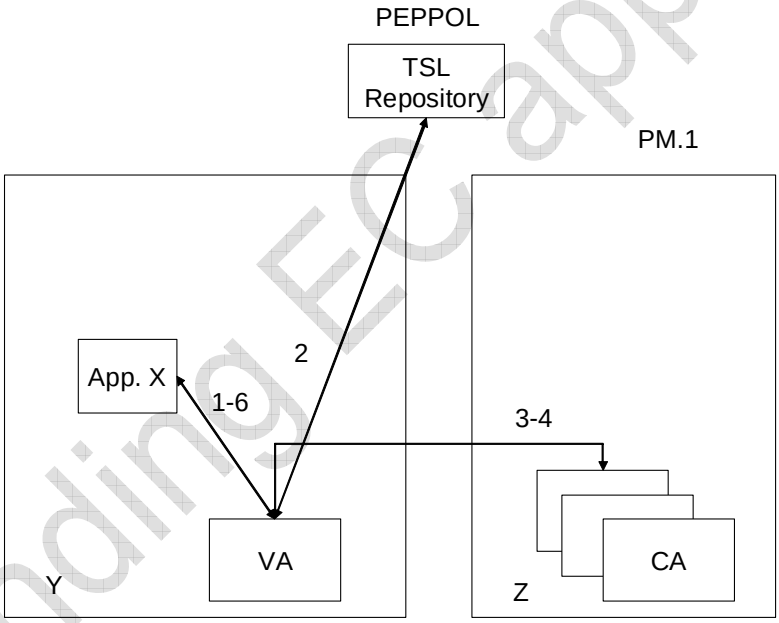

Figure 5: PM.1 – a single TSL

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 5.2).

5.6 PEPPOL Pilot Architecture

Since the VSs have in general a limited CPSs coverage, to extend this limit it is necessary to create a trusted network of VSs.

As one possible solution, a list of the available VSs in the PEPPOL Pilot is added to the single TSL (Figure 5). The sum of the two lists is called PEPPOL Public Registry Service (PPRS).

In this case the VS in the MS Y:

2. downloads from PPRS indications on how to contact and interrogate the VS in MS Z
3. asks VS in MS Z for the end-user certificate validation

VS in MS Z:

4. downloads from PPRS an updated TSL
    a. 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

VS in MS Y:

8. sends the validation results to the application X

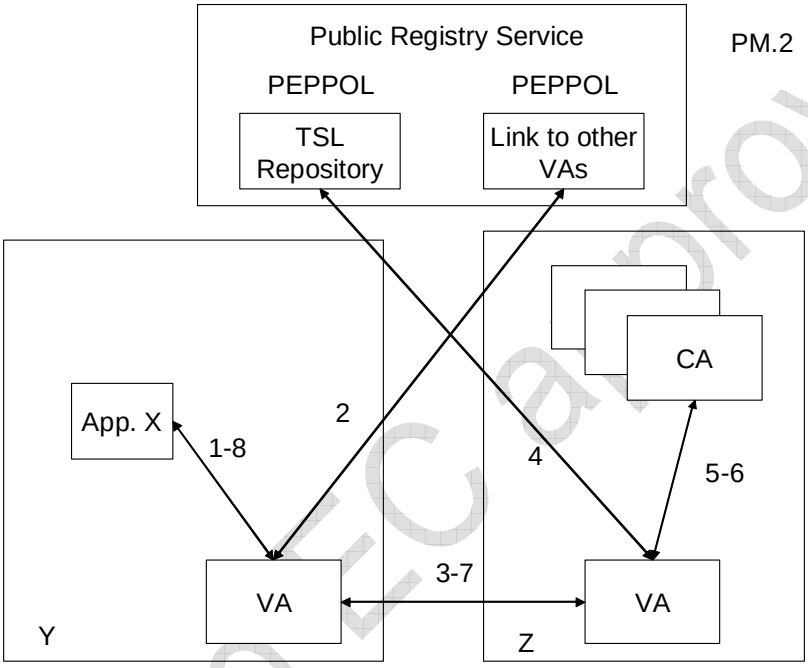

Figure 6: PM.2 - Public Registry Service

5.7 PEPPOL Transitory Architecture

5.7.1 Reference Validation Services

Unfortunately the use of TSL it still in an experimental state, no public implementation is available and existing VSs are not able to manage TSLs. In addition VS solutions are available only in a limited number of MSs.

Awaiting a complete implementation of model PM.2, as first and temporary solution WP1 proposes to realize the architecture as in Figure 7, where PPRS is manually implemented as VS configuration file/s.

In this preliminary phase, when a national VS does not exist in a MS Y, it could be reasonable to use a foreign VS that temporarily will extend its CPS coverage to MS Y. Such VS is termed a Reference VS (RVS).

In this model PM.2.1, the PEPPOL Consortium publishes the CSP TSL and the Links to other VS (LtoVA), and RVSs should maintain continuously updated information that is pertinent within their domains.

In practise:

1. Application X call its RVS for a validation of an end-user certificate
2. RVS for MS Y (if CSP is not in its domain as described in its PEPPOL TSL configuration file) calls the correct RVS as described in its LtoVA configuration file
3. RVS for MS Z checks, as found in its TSL configuration file, CSP service status, SSCD quality, end-user certificate quality (Qualified or Non-Qualified) and, if the CSP service is "in accordance", it checks the certificate revocation/suspension status following its business logic (e.g. downloading a CRL, performing a OCSP request or directly using its own database)
4. RVS for MS Z sends the validation results to RVS for MS Y
5. RVS for MS Y sends the validation results to the application X

Note: this solution does not exclude the possibility for an application to directly use the TSL in order to accomplish an end-user certificate validation by itself.

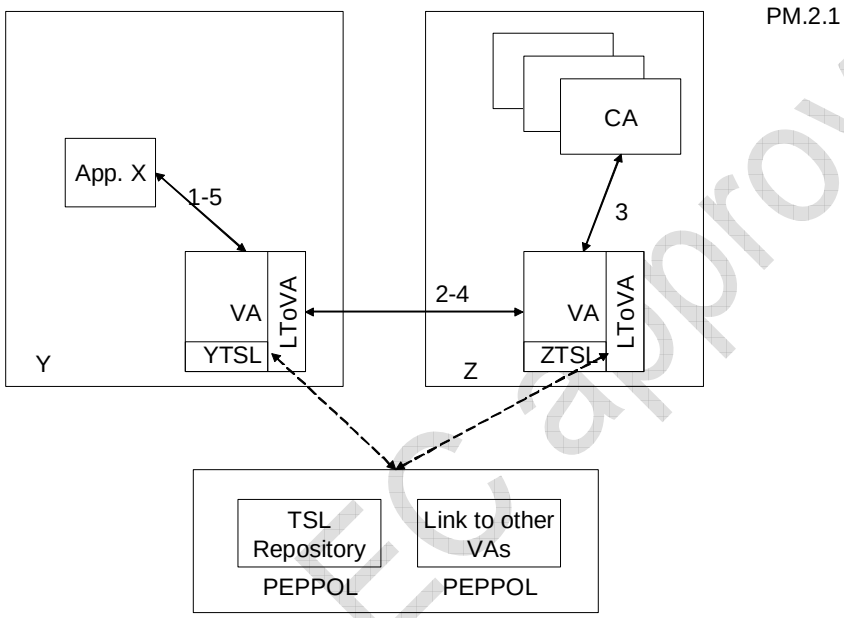

Figure 7: Transitory Solution

5.7.2 Public Registry Server Data Structure

5.7.2.1 Data Structures

We will now examine the two lists, the CSP TSL and the LtoVA lists. Considering the TSL data structure, it is possible to use TSL even to manage VS services considering them among other TSL services. In this case the *Service type identifier clause 5.5.1* [ETSI-102-231] will be filled with the value "*unspecified*".

Thus, if they have a common maintainer, the two list can be merged in a single list that we call PEPPOL TSL. This does not exclude the possibility to develop two different lists.

In the continuation we will refer to a single PEPPOL TSL.

5.7.2.2 PEPPOL TSL data structure

The PEPPOL TSL will be structured into the following categories of information:

- Information on the Trusted List issuing scheme;
    - Information about a/more Trusted Service Provider/s
        - Information about a/more specific trusted service/s
            - Information about the status of the trusted service on regard of the scheme policy

In case of TSP as CSP it is particularly important to assure:

- unambiguous identification of the issuing certification (CA) service provided by the CSP;
- for each issuing CA, an unambiguous Deterministic Set of Information to be Found in an end-entity certificate (DSIFC);

The indication of the DSIFC data per issuing CA service is necessary to avoid ambiguous situations where not enough information is available in the qualified certificate about its qualified status, its potential support by an SSCD and especially in order to cope with the additional fact that most of the (commercial) QCSPs are using one Qualified CA to issue several types of end-entity certificates, both qualified and non-qualified.

The number of entries in the list per recognised CSP might be reduced where one or several Upper CA services exist.

5.7.2.3 Information on the Trusted List Issuing Scheme

The following information will be part of this category:

- A Trusted List **tag** facilitating the identification of the Trusted List (if in Machine Processable (MP) format);
- A Trusted List **format and format version identifier** (e.g. TSL format version 2 when relying on TSL format defined by current version 2.1.1 of the ETSI TS 102 231 TSL specification);
- A Trusted List **sequence (or release) number**;
- A Trusted List **type** information (e.g. for identification of the fact that this Trusted List is providing information on the accepted status of the CSPs or VSs in the PEPPOL context);
- A 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 Trusted List is associated, including but not limited to:
    - o the MSs in which it applies,
    - o information or reference of location where information on the scheme can be found (scheme model, rules, criteria, applicable community, type, etc.),
    - o 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.**

5.7.2.4 Information about TSP

This set of information will include:

- The TSP organisation name as used in formal legal registrations;
- The TSP organisation UID as defined in formal legal registers (e.g., the same format can be used as the one proposed for the QEC profile[4]) ;
- 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.

5.7.2.5 Information about TSP's trusted services

This set of information will include at least the following:

[4] A UID scheme based 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 *"generic" – unspecified* for Validation Service services)
- (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.

The Service Directive expert group is proposing to adopt the "service information extensions" (clause 5.5.9 [ETSI-102-231]) when the information provided in the "Service digital identity" is not sufficient to unambiguously identify the qualified certificates issued by this service and/or the information present in the covered qualified certificates does not allow machine processable identification of the fact whether or not the QC is supported by an SSCD. In our project since the Peppol signature validation policy does not consider the use of SSCD (or QC) as mandatory constrain, PEPPOL TSL will not use this extension.

Moreover the Service Directive expert group by means of the *Service current status – 5.5.4 clause* [ETSI-102-231], specifies the kind of the CSP and its status (historical and current) through specific URIs (still to be defined e.g. trough ETSI):

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

For our scope we could consider this solution adding:

8. Contractual[5] accepted
9. Contractual accepted expired
10. Contractual accepted revoked
11. Validation Service[6] recognized
12. Validation Service recognized expired
13. Validation Service recognized revoked,

Of course, for each status must be specified the starting date and time.

In alternative for the scope of PEPPOL Pilot they could be simplified using an unique URI meaning "PEPPOL accepted/recognized TSP".

5.7.3 PEPPOL TSL Implementation

As first TSL implementation the PEPPOL Consortium will provide a TSL in a Human Readable (HR) format following the indication of Annex J of [ETSI-102-231]. The PEPPOL TSL:

- will be a document file, in an open format (e.g. ODF, Open Document Format).

[5] We use contractual to distinguish a CSP that is present in the list by mean of an approval by a Verification Service assessing the CSP properties (see D1.1 part 7).

[6] The same approach could be useful even in case of a VA since there is not a specific *Service type identifier,* the *Service Information extensions – 5.5.9 clause* could be filled identifying the PEPPOL VA service.

- to assure the authenticity of it, the file could be signed electronically using CADES-BES format [ETSI-101-733], in harmony with Service Directive expert group.

As successive implementation PEPPOL Consortium on its web site will provide a Machine Processable (MP) implementation following the Annex J [ETSI-102-231]. In this case the PEPPOL TSL:

- will be available in ASN.1 format as in Annex A [ETSI-102-231] and
- in XML format as in Annex B [ETSI-102-231][7].

The cited Annexes indicate also the format of electronic signature to assure TSL authenticity.

In both phases, the keys (end-user or machine and the root certificate) to perform the signature verification will be published on the same web site.

Could be sensible find out an alternative solution for publishing these key such as a official PEPPOL gazette available in a non electronic format.

5.7.4 PEPPOL TSL Human Readable Example

As example of a PEPPOL TSL, where there are a TSP providing CA (Qualified Certificates) service and a TSP providing a Validation Services, follows:

TSL type	http://uri.etsi.org/TrstSvc/TSLtype/generic
Scheme operator name	PEPPOL Consortium
Scheme operator address	10, Peppol rd – Anywhere in EU – EU – 00000 - EU
Scheme name	Peppol Consortium Pilot TSL
Scheme information URI	http://www.peppol.eu/PEPPOLTSL
Status determination approach	1 – Active - http://uri.etsi.org/TrstSvc/TSLtype/StatusDetn/Active
Scheme type/community/rules	
Scheme territory	EU
TSL policy/legal notice	http://www.peppol.eu/PEPPOLTSL/legalnotice.htm
Historical information period	65535 – indefinite
Pointers to other TSLs	
List issue date and time	2008-11-14T16:30:15Z
Scheme extension	
TSP information	
TSP name	VATIT 0101010101
TSP trade name	CSP 1.
TSP address	Via Flaminia 2000 – 00100 Rome (RM) – Italy
TSP information URI	http://www.CSP1.it
TSP information extension	

[7] The Service Directive expert group is considering to adopt a different kind of signature format, probably based on CADES-BES for ASN.1 format, and XADES-BES for XML format.

Service Information	
Service type identifier	2 – CA (QC)
Service name	C=IT/O=CSP1 S.p.A./CN=CSP1-Firma Digitale/emailAddress=certificazione@csp1.it
Service digital identity	MIIE7zCCA9egAwIBAgICFxYwDQYJKoZIhvcNAQEFBQAwgaAxCzAJBgNVBAYTAklUMSowKAYDVQQK EyFDb25zaWdsaW8gTmF6aW9uYWxlIGRlbCBOb3RhcmlhdG8xOTA3BgNVBAMTMENvbnNpZ2xpbyBO YXppb25hbGUgZGVsIE5vdGFyaWF0by1GaXJtYSBEaWdpdGFsZTEqMCgGCSqGSIb3DQEJARYbY2Vy dGlmaWNhemlvbmVAbm90YXJpYXRvLml0MB4XDTAyMDkzMDEwMjYxOVoXDTA4MDkzMDEwMjYxOVow gaAxCzAJBgNVBAYTAklUMSowKAYDVQQKEyFDb25zaWdsaW8gTmF6aW9uYWxlIGRlbCBOb3Rhcmlh dG8xOTA3BgNVBAMTMENvbnNpZ2xpbyBOYXppb25hbGUgZGVsIE5vdGFyaWF0by1GaXJtYSBEaWdp dGFsZTEqMCgGCSqGSIb3DQEJARYbY2VydGlmaWNhemlvbmVAbm90YXJpYXRvLml0MIIBIjANBgkq hkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQEA2ntn+Oo+p1l5U1K6/xHPKaBxqquPpZ1Wz9S6ozzm6pHV ItihMS415R/VSot1fRZkIKlub54igxPBiRrdf5QVIBzuMOtM+Dq2QUqZ0dLRc44JlhW0kTmx+jpC CTrqzBCeO7E1jBCpJh1/o/B5M+p0XY8dSXk+CwB0/zsfJVCyQSiYiT08se0SPl6zHz5EPwLu3OTw 0l4D+5ROro3JRFiz4Lg0rA65A9h5uzlvs0/GrNq5WCHiI69gSchHhiinZ3jQjnplmaFR0lt3DlhU CVuzaPbew9aezBCuV/aqCh1WZtJXk62Nprn2z8PznvS9ceXpfwSE0khMxY7Ht/yvQ7oLuwIDAQAB o4IBLzCCASswDwYDVR0TAQH/BAUwAwEB/zAOBgNVHQ8BAf8EBAMCAQYwXQYDVR0gBFYwVDBSBgor BgEEAcJOAQEBMEQwQgYIKwYBBQUHAgEWNmh0dHA6Ly93d3cubm90YXJpYXRvLml0L2Zpcm1hZGln aXRhbGUvbWFudWFsZW9wZXJhdGl2bzCBiQYDVR0fBIGBMH8wfaB7oHmGd2xkYXA6Ly9sZGFwLmNh Lm5vdGFyaWF0by5pdDozODkvb3U9Q29uc2lnbGlvIE5hemlvbmFsZSBkZWwgTm90YXJpYXRvLUZp cm1hIERpZ2l0YWxlLG89Q29uc2lnbGlvIE5hemlvbmFsZSBkZWwgTm90YXJpYXRvMB0GA1UdDgQW BBTe0Elw9+eCaWyCLW58cdUESdFGTTANBgkqhkiG9w0BAQUFAAOCAQEAHVI2pN/Sx3VobEaCERQ8 tA+V6PhAm0Wtqpc0w28yas0DbQK68xqfKbi0UKu+idhAjVwoa6zIuCM4Lu30OLueuhcPlTUuxQA7 swNEj3IyoZP2cUn3UU017dgyKjxa5lNDjMlQSBAtFqq/JRSQOApB0ggA14FlMlt8w43W2D9o8NKU RnrZpz3w3koueyidQOYCgch2Xb3PpxMMWZNQLLa4PFLIJHNdxKnACFamXl4N9o5pvNMv+0xC/Pog yBx4+OxTBzyp1llxvZzwhgKGxcN0CNv0ruzMtIa7iv4sArgDHmbCbJr5Hz6qmus8S2F79PwIuQL8 aIB2hrUxUVSKC5fu4Q==
Service current status	5 – Accredited
Current status starting date and time	2007-09-27T16:04:08Z
Scheme service definition URI	Scheme Service Definition URI
Service supply points	
TSP service definition URI	TSP Service Definition URI
Service information extension	
Historical service information	
Service type identifier	2 – CA (QC)
Service name	C=IT/O=CSP1 S.p.A./CN=CSP1-Firma Digitale/emailAddress=certificazione@csp1.it
Service digital identity	MIIE7zCCA9egAwIBAgICFxYwDQYJKoZIhvcNAQEFBQAwgaAxCzAJBgNVBAYTAklUMSowKAYDVQQK EyFDb25zaWdsaW8gTmF6aW9uYWxlIGRlbCBOb3RhcmlhdG8xOTA3BgNVBAMTMENvbnNpZ2xpbyBO YXppb25hbGUgZGVsIE5vdGFyaWF0by1GaXJtYSBEaWdpdGFsZTEqMCgGCSqGSIb3DQEJARYbY2Vy dGlmaWNhemlvbmVAbm90YXJpYXRvLml0MB4XDTAyMDkzMDEwMjYxOVoXDTA4MDkzMDEwMjYxOVow

	gaAxCzAJBgNVBAYTAklUMSowKAYDVQQKEyFDb25zaWdsaW8gTmF6aW9uYWxIIGRlbCBOb3Rhcmlh dG8xOTA3BgNVBAMTMENvbnNpZ2xpbyBOYXppb25hbGUgZGVsIE5vdGFyaWF0by1GaXJtYSBEaWdp dGFsZTEqMCgGCSqGSIb3DQEJARYbY2VydGlmaWNhemlvbmVAbm90YXJpYXRvLml0MIIBIjANBgkq hkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQEA2ntn+Oo+p1l5U1K6/xHPKaBxqquPpZ1Wz9S6ozzm6pHV ItihMS415R/VSot1fRZkIKlub54igxPBiRrdf5QVIBzuMOtM+Dq2QUqZ0dLRc44JlhW0kTmx+jpC CTrqzBCeO7E1jBCpJh1/o/B5M+p0XY8dSXk+CwB0/zsfJVCyQSiYiT08se0SPl6zHz5EPwLu3OTw 0l4D+5ROro3JRFiz4Lg0rA65A9h5uzlvs0/GrNq5WCHiI69gSchHhiinZ3jQjnplmaFR0lt3DlhU CVuzaPbew9aezBCuV/aqCh1WZtJXk62Nprn2z8PznvS9ceXpfwSE0khMxY7Ht/yvQ7oLuwIDAQAB o4IBLzCCASswDwYDVR0TAQH/BAUwAwEB/zAOBgNVHQ8BAf8EBAMCAQYwXQYDVR0gBFYwVDBSBgor BgEEAcJOAQEBMEQwQgYIKwYBBQUHAgEWNmh0dHA6Ly93d3cubm90YXJpYXRvLml0L2Zpcm1hZGln aXRhbGUvbWFudWFsZW9wZXJhdGl2bzCBiQYDVR0fBIGBMH8wfaB7oHmGd2xkYXA6Ly9sZGFwLmNh Lm5vdGFyaWF0by5pdDozODkvb3U9Q29uc2lnbGlvIE5hemlvbmFsZSBkZWwgTm90YXJpYXRvLUZp cm1hIERpZ2l0YWxlLG89Q29uc2lnbGlvIE5hemlvbmFsZSBkZWwgTm90YXJpYXRvMB0GA1UdDgQW BBTe0Elw9+eCaWyCLW58cdUESdFGTTANBgkqhkiG9w0BAQUFAAOCAQEAHVI2pN/Sx3VobEaCERQ8 tA+V6PhAm0Wtqpc0w28yas0DbQK68xqfKbi0UKu+idhAjVwoa6zIuCM4Lu30OLueuhcPlTUuxQA7 swNEj3IyoZP2cUn3UU017dgyKjxa5lNDjMlQSBAtFqq/JRSQOApB0ggA14FlMlt8w43W2D9o8NKU RnrZpz3w3koueyidQOYCgch2Xb3PpxMMWZNQLLa4PFLIJHNdxKnACFamXl4N9o5pvNMv+0xC/Pog yBx4+OxTBzyp1llxvZzwhgKGxcN0CNv0ruzMtIa7iv4sArgDHmbCbJr5Hz6qmus8S2F79PwIuQL8 aIB2hrUxUVSKC5fu4Q==
Service previous status	5 – Accredited
Previous status starting date and time	2006-04-27T17:04:18Z
TSP information	
TSP name	VATEU 12345678
TSP trade name	Validation Team Inc.
TSP address	15, Anywhere Str. – Anytown in EU - 00000 – EU - EU
TSP information URI	http://www.cspvteam.eu
TSP information extension	
Service Information	
Service type identifier	0 – unspecified (Validation Authority)
Service name	C=EU/O=CSP Validation Team Inc./CN=CSP VTEAM
Service digital identity	MIIEBTCCAu2gAwIBAgIEOdnX1zANBgkqhkiG9w0BAQUFADBXMQswCQYDVQQGEwJJVDEYMBYGA1UE ChMPUG9zdGVjb20gcy5wLmEuMRcwFQYDVQQLEw5DQSBIIFNpY3VyZXp6YTEVMBMGA1UEAxMMUG9z dGVjb20gQ0ExMB4XDTAwMTAwMzEzMDAyOFoXDTEwMTAwMTEyMDAyOFowVzELMAkGA1UEBhMCSVQx GDAWBgNVBAoTD1Bvc3RlY29tIHMucC5hLjAXMBUGA1UECxMOQ0EgZSBTaWN1cmV6emExFTATBgNV BAMTDFBvc3RlY29tIENBMTCCASIwDQYJKoZIhvcNAQEBBQADggEPADCCAQoCggEBAOVjO/c6v6jR H9pB2sJtvkWwr+5cRy9lk09ZNHih6wRgTdv4yxAy2LpAkH30N2oo6eZsZv7G0ibxDOLa4Uwh2vwm rxvr2imKq5eWEatDwmQAunI9hxbFdu9MjsjXg6ecvWgV7LcD+kjaapUavpiE46/gZ2wslfewEmj2 rsKO1uZ6thj7BJ8Q1ttSEJuHdiTVx84VRYjnYgNKxCw3XA/WUCqIEQFDuuX1EWr/WrG2Y+jpwd7L PNRaBMCVaUWb6uOUAVBP4n5vxK2qHr126iXOLAeL2Mt9XWOuSXzN1G4dTVq4JfcHZIFWjHCu2tnG Y/UY7j+JjAdMv5NdNTlgLPcqk4kCAwEAAaOB2DCB1TASBgNVHRMBAf8ECDAGAQH/AgEAMAwGA1Ud JAQFMAOAAQAwPQYDVR0gBDYwNDAyBgcrTAsBAgEBMCcwJQYIKwYBBQUHAgEWGWh0dHA6Ly9wb3N0 ZWNlcnQucG9zdGUuaXQwOgYDVR0fBDMwMTAvoC2gK4YpaHR0cDovL3Bvc3RlY2VydC5wb3N0ZS5p dC9wb3N0ZWNvbWNhMS9jcmwwEQYDVR0OBAoECEku+kddYQjMMBMGA1UdIwQMMAqACEku+kddYQjM MA4GA1UdDwEB/wQEAwIBBjANBgkqhkiG9w0BAQUFAAOCAQEAsIoJsI+dPRGXBhU6bMrgSb0g4dWH 6mIjjJL/2O/HYEDihhhNcKawVK4hrXYEkJMgTKcqKf7V4ZpDnWTYwZLtWeucmgAeUyc12xhldJhU

	jgMloes4Vi/hUFaDLknvIcBzuvyFflkjVj4e45D6vl99yP2s0yvIVnU9huri0hNV+FyPPsXq3CSt 6fDdgUXwuLW5cgK/01LMXDj3b5PBlJlrVoPJoqGZQDeDgDf/VWh5oc5XjHoZD06HVg1V2JxmDfr5 8EYyuP+yuU3HyazaabmIFHbR94H+6WHDc0oFwd6STvzZTAyupTo41JUnsXmfr1WtWkc/b+DqK2oL K9GsvYWwhA==
Service current status	11 – Validation Authority recognized
Current status starting date and time	2007-07-07T09:18:25Z
Scheme service definition URI	Scheme Service Definition URI
Service supply points	
TSP service definition URI	http://www. cspvteam.eu/access.htm
Service information extension	
Historical service information	
Service type identifier	
Service name	
Service digital identity	
Service previous status	
Previous status starting date and time	
TSL signature information	
Textual certificate detail, time and date of signing	SubjectDN:C=EU/O=PEPPOL Consortium/CN=PEPPOL TSL SIGNER Subject Key Identifier: 49EF4A3608C6108CC Serial:aa22ff1122 Autority Key Identifier: 49EF4A24568C6108CC Signing Date**:** 2008-11-18T09:18:25Z

5.7.5 PEPPOL TSL XML Example

As example of a PEPPOL TSL, where there are a TSP providing a CA (Qualified Certificates) service and a TSP providing a Validation Services, follows:

```
<?xml version="1.0" encoding="UTF-8" standalone="yes" ?>
- <tsl:TrustServiceStatusList xmlns:tsl="http://uri.etsi.org/02231/v2#"
    xmlns:ds="http://www.w3.org/2000/09/xmldsig#"
    xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
    xsi:schemaLocation="http://uri.etsi.org/02231/v2# ETSI_TS_102_231_v2.xsd"
    TSLTag="http://uri.etsi.org/02231/TSLTag" Id="ID0001">
- <tsl:SchemeInformation>
  <tsl:TSLVersionIdentifier>2</tsl:TSLVersionIdentifier>
```

```
<tsl:TSLSequenceNumber>78</tsl:TSLSequenceNumber>
<tsl:TSLType>http://uri.etsi.org/TrstSvc/TSLtype/generic</tsl:TSLType>
- <tsl:SchemeOperatorName>
<tsl:Name xml:lang="EN">Peppol Consortium</tsl:Name>
</tsl:SchemeOperatorName>
- <tsl:SchemeOperatorAddress>
- <tsl:PostalAddresses>
- <tsl:PostalAddress xml:lang="EN">
<tsl:StreetAddress>Peppol rd</tsl:StreetAddress>
<tsl:Locality>Anytown in EU</tsl:Locality>
<tsl:StateOrProvince>EU</tsl:StateOrProvince>
<tsl:PostalCode>00000</tsl:PostalCode>
<tsl:CountryName>EU</tsl:CountryName>
</tsl:PostalAddress>
</tsl:PostalAddresses>
- <tsl:ElectronicAddress>
<tsl:URI>info_TSL@peppol.eu</tsl:URI>
</tsl:ElectronicAddress>
</tsl:SchemeOperatorAddress>
- <tsl:SchemeName>
<tsl:Name xml:lang="EN">Peppol Consortium Pilot TSL</tsl:Name>
</tsl:SchemeName>
- <tsl:SchemeInformationURI>
<tsl:URI xml:lang="EN">http://www.peppol.eu/PEPPOLTSL</tsl:URI>
</tsl:SchemeInformationURI>

<tsl:StatusDeterminationApproach>http://uri.etsi.org/TrstSvc/TSLtype/StatusDetn/active</tsl:StatusDeterminationApproach>
<tsl:SchemeType>http://www.peppol.eu/PEPPOLTSL</tsl:SchemeType>
<tsl:SchemeTerritory>EU</tsl:SchemeTerritory>
- <tsl:PolicyOrLegalNotice>
<tsl:TSLLegalNotice
xml:lang="EN">http://www.peppol.eu/PEPPOLTSL/legalnotice.htm</tsl:TSLLegalNotice>
- <!--
# CSPs AND VAs VALID IN PEPPOL PILOT
-->
```

```
    </tsl:PolicyOrLegalNotice>
  <tsl:HistoricalInformationPeriod>65535</tsl:HistoricalInformationPeriod>
  <tsl:ListIssueDateTime>2008-11-14T16:30:15Z</tsl:ListIssueDateTime>
  <tsl:NextUpdate>2008-12-14T16:30:15Z</tsl:NextUpdate>
    </tsl:SchemeInformation>
- <tsl:TrustServiceProviderList>
- <tsl:TrustServiceProvider>
- <tsl:TSPInformation>
- <tsl:TSPName>
  <tsl:Name xml:lang="EN">VATIT 0101010101</tsl:Name>
  - <!--
   unique organisation name
    -->
    </tsl:TSPName>
- <tsl:TSPTradeName>
  <tsl:Name xml:lang="EN">CSP1</tsl:Name>
    </tsl:TSPTradeName>
- <tsl:TSPAddress>
- <tsl:PostalAddresses>
- <tsl:PostalAddress xml:lang="EN">
  <tsl:StreetAddress>via Flaminia, 2000</tsl:StreetAddress>
  <tsl:Locality>Roma</tsl:Locality>
  <tsl:StateOrProvince>RM</tsl:StateOrProvince>
  <tsl:PostalCode>00100</tsl:PostalCode>
  <tsl:CountryName>IT</tsl:CountryName>
    </tsl:PostalAddress>
    </tsl:PostalAddresses>
- <tsl:ElectronicAddress>
  <tsl:URI>info@csp1.it</tsl:URI>
    </tsl:ElectronicAddress>
    </tsl:TSPAddress>
- <tsl:TSPInformationURI>
  <tsl:URI xml:lang="EN">http://www.csp1.it</tsl:URI>
    </tsl:TSPInformationURI>
    </tsl:TSPInformation>
- <tsl:TSPServices>
```

- <tsl:TSPService>
- <tsl:ServiceInformation>

<tsl:ServiceTypeIdentifier>**http://uri.etsi.org/TrstSvc/Svctype/CA/QC**</tsl:ServiceTypeIdentifier>

- <!--
CA (QC)
-->

- <tsl:ServiceName>

<tsl:Name xml:lang="**EN**">**IT:CSP1 S.p.A./CN=CSP1-Firma Digitale/emailAddress=certificazione@csp1.it**</tsl:Name>

</tsl:ServiceName>

- <tsl:ServiceDigitalIdentity>
- <tsl:digitalId>

<tsl:X509Certificate>**MIIEkjCCA3qgAwIBAgIEQQYlHjANBgkqhkiG9w0BAQUFADCBhzELMAkGA1UEBhMCSVQxNDAy**
BgNVBAoTK0NlbnRybyBOYXppb25hbGUgcGVyIGwnSW5mb3JtYXRpY2EgbmVsbGEgUEExLjAs
BgNVBAsTJVNlcnZpemkgZGkgU2ljdXJlenphIGUgQ2VydGlmaWNhemlvbmUxEjAQBgNVBAMT
CUNOSVBBIENBMTAeFw0wNDA3MjcwOTQ5NDlaFw0yNDA3MjcwOTQ5NDlaMIGHMQswCQYDVQQG
EwJJVDE0MDIGA1UEChMrQ2VudHJvIE5hemlvbmFsZSBwZXIgbCdJbmZvcm1hdGljYSBuZWxs
YSBQQTEuMCwGA1UECxMlU2Vydml6aSBkaSBTaWN1cmV6emEgZSBDZXJ0aWZpY2F6aW9uZTES
MBAGA1UEAxMJQ05JUEEgQ0ExMIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQEAsZR8
USuYYROXAZGJ88QoZU0io8ldcrTQ29kvxlL9Dgd8pWoNth/mikKWaLo3Ce4YrEKC23lYN0gd
QhU6ZhIFf3UBFPiZydY5KOi8ef1NcArGvIS1tUMwr1CxjOXqX+z51g+VerDhr9lHEega3Fiz
JyW71XJJO8cUdXFXDSCx36o0I54zszdQ+Sb6TWQfqJhpVvJO9CsxjUPDuGgTWkaTH272N5PW
fkqjQGgY12A6XaZNptCuATRNMXdQm6DsXLUqGv4gFBCq2HfVZjIl1apL0TDy0oynX/YqAPzk
dbamNDx3jLfPqhxUuqOcTQYdKi9AwKUGhyHOayQDLBPpak7MhwIDAQABo4IBAjCB/zASBgNV
HRMBAf8ECDAGAQH/AgEAMAwGA1UdJAQFMAOAAQAwWgYDVR0gBFMwUTBPBgcrTBABAgEBMEQw
QgYIKwYBBQUHAgEWNmh0dHA6Ly93d3cuY25pcGEuZ292Lml0L2Zpcm1hZGlnaXRhbGUvbWFu
dWFsZW9wZXJhdGl2bzAvBgNVHR8EKDAmMCSgIqAghh5odHRwOi8vY2EuY25pcGEuZ292Lml0
L2NybC5jcmwwHQYDVR0OBBYEFJxv4XZoJ0KcwIBAcKAPCOnREv+kMB8GA1UdIwQYMBaAFJxv

4XZoJ0KcwIBAcKAPCOnREv+kMA4GA1UdDwEB/wQEAwIBBjANBgkqhkiG9w0BAQUFAAOCAQEA
TUqQwTPs7UqAbLLk5XoOwA8DjC8bUHyO+cRAlBPGEZo+OLP5S2vYuY95l2rLmWrCEZO2WxvN
FqpMhLV/HeCp8gltavHXe26eQusKRGr2WTyViL/9OAlP6rKM+hyJ8f48G+WAlVA2gpqxoWcJ
iyUUV05CnPy3fUmm7JoCumQqrKJVNbPVJ7GVcMR7wpz4PZigZp8cqXIpOKViSd66PubePas8
ZG1iUmCy0W6OLI/cM90qnOxFq4oLZWVy6X5EFARwbHt9ydYYPeAsX/bgeAxTjKrw8O98KDJr
MzdIx4n0LpsfCIDQyxFo1p4KTgX+FoYhz1XhK7urictJm/qj5m+o8g==</tsl:X509Certificate>
</tsl:digitalId>
</tsl:ServiceDigitalIdentity>

<tsl:ServiceStatus>http://uri.etsi.org/TrstSvc/Svcstatus/accredited</tsl:ServiceStatus>
- <!--
Accredited CSP
-->
<tsl:StatusStartingTime>2007-09-30T10:26:19Z</tsl:StatusStartingTime>
- <tsl:TSPServiceDefinitionURI>
<tsl:URI xml:lang="EN">http://www.peppol.eu/</tsl:URI>
</tsl:TSPServiceDefinitionURI>
</tsl:ServiceInformation>
- <tsl:ServiceHistory>
- <tsl:ServiceHistoryInstance>

<tsl:ServiceTypeIdentifier>http://uri.etsi.org/TrstSvc/Svctype/CA/QC</tsl:ServiceTypeIdentifier>
- <tsl:ServiceName>
<tsl:Name xml:lang="EN">IT:CSP1 S.p.A./CN=CSP1-Firma Digitale/emailAddress=certificazione@csp1.it</tsl:Name>
</tsl:ServiceName>
- <tsl:ServiceDigitalIdentity>
- <tsl:DigitalId>

<tsl:X509Certificate>MIIEkjCCA3qgAwIBAgIEQQYlHjANBgkqhkiG9w0BAQUFADCBhzELMAkGA1UEBhMCSVQxNDAy
BgNVBAoTK0NlbnRybyBOYXppb25hbGUgcGVyIGwnSW5mb3JtYXRpY2EgbmVsbGEgUEExLjAs
BgNVBAsTJVNlcnZpemkgZGkgU2ljdXJlenphIGUgQ2VydGlmaWNhemlvbmUxEjAQBgNVBAMT

CUNOSVBBIENBMTAeFw0wNDA3MjcwOTQ5NDlaFw0yNDA3MjcwOTQ5NDlaMIGH
MQswCQYDVQQG
EwJJVDE0MDIGA1UEChMrQ2VudHJvIE5hemlvbmFsZSBwZXIgbCdJbmZvcm1hdG
ljYSBuZWxs
YSBQQTEuMCwGA1UECxMlU2Vydml6aSBkaSBTaWN1cmV6emEgZSBDZXJ0aWZp
Y2F6aW9uZTES
MBAGA1UEAxMJQ05JUEEgQ0ExMIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIBCg
KCAQEAsZR8
USuYYROXAZGJ88QoZU0io8ldcrTQ29kvxlL9Dgd8pWoNth/mikKWaLo3Ce4YrEKC
23lYN0gd
QhU6ZhIFf3UBFPiZydY5KOi8ef1NcArGvIS1tUMwr1CxjOXqX+z51g+VerDhr9lHEe
ga3Fiz
JyW71XJJO8cUdXFXDSCx36o0I54zszdQ+Sb6TWQfqJhpVvJO9CsxjUPDuGgTWka
TH272N5PW
fkqjQGgY12A6XaZNptCuATRNMXdQm6DsXLUqGv4gFBCq2HfVZjII1apL0TDy0oyn
X/YqAPzk
dbamNDx3jLfPqhxUuqOcTQYdKi9AwKUGhyHOayQDLBPpak7MhwIDAQABo4IBAj
CB/zASBgNV
HRMBAf8ECDAGAQH/AgEAMAwGA1UdJAQFMAOAAQAwWgYDVR0gBFMwUTBPB
gcrTBABAgEBMEQw
QgYIKwYBBQUHAgEWNmh0dHA6Ly93d3cuY25pcGEuZ292Lml0L2Zpcm1hZGlna
XRhbGUvbWFu
dWFsZW9wZXJhdGl2bzAvBgNVHR8EKDAmMCSgIqAghh5odHRwOi8vY2EuY25pc
GEuZ292Lml0
L2NybC5jcmwwHQYDVR0OBBYEFJxv4XZoJ0KcwIBAcKAPCOnREv+kMB8GA1UdI
wQYMBaAFJxv
4XZoJ0KcwIBAcKAPCOnREv+kMA4GA1UdDwEB/wQEAwIBBjANBgkqhkiG9w0BA
QUFAAOCAQEA
TUqQwTPs7UqAbLLk5XoOwA8DjC8bUHyO+cRAlBPGEZo+OLP5S2vYuY95l2rLmW
rCEZO2WxvN
FqpMhLV/HeCp8gltavHXe26eQusKRGr2WTyViL/9OAlP6rKM+hyJ8f48G+WAlVA2
gpqxoWcJ
iyUUV05CnPy3fUmm7JoCumQqrKJVNbPVJ7GVcMR7wpz4PZigZp8cqXIpOKViSd6
6PubePas8
ZG1iUmCy0W6OLI/cM90qnOxFq4oLZWVy6X5EFARwbHt9ydYYPeAsX/bgeAxTjKr
w8O98KDJr
MzdIx4n0LpsfCIDQyxFo1p4KTgX+FoYhz1XhK7urictJm/qj5m+o8g==</tsl:X509Certificate>

</tsl:DigitalId>

</tsl:ServiceDigitalIdentity>

<tsl:ServiceStatus>http://uri.etsi.org/TrstSvc/Svcstatus/accredited</tsl:ServiceStatus>

<tsl:StatusStartingTime>2006-07-12T00:00:00Z</tsl:StatusStartingTime>

</tsl:ServiceHistoryInstance>

</tsl:ServiceHistory>

</tsl:TSPService>

</tsl:TSPServices>

```
    </tsl:TrustServiceProvider>
- <tsl:TrustServiceProvider>
- <tsl:TSPInformation>
- <tsl:TSPName>
  <tsl:Name xml:lang="EN">VATEU 12345678</tsl:Name>
    </tsl:TSPName>
- <tsl:TSPTradeName>
  <tsl:Name xml:lang="EN">Validation Team Inc.</tsl:Name>
    </tsl:TSPTradeName>
- <tsl:TSPAddress>
- <tsl:PostalAddresses>
- <tsl:PostalAddress xml:lang="EN">
  <tsl:StreetAddress>15, Anywhere Str.</tsl:StreetAddress>
  <tsl:Locality>Anytown</tsl:Locality>
  <tsl:StateOrProvince>EU</tsl:StateOrProvince>
  <tsl:PostalCode>00000</tsl:PostalCode>
  <tsl:CountryName>EU</tsl:CountryName>
    </tsl:PostalAddress>
    </tsl:PostalAddresses>
- <tsl:ElectronicAddress>
  <tsl:URI>info@cspvteam.eu</tsl:URI>
    </tsl:ElectronicAddress>
    </tsl:TSPAddress>
  <tsl:TSPInformationURI
    xml:lang="EN">http://www.cspvteam.eu</tsl:TSPInformationURI>
    </tsl:TSPInformation>
- <tsl:TSPServices>
- <tsl:TSPService>
- <tsl:ServiceInformation>
  <tsl:ServiceTypeIdentifier>0</tsl:ServiceTypeIdentifier>
  - <!--
   VALIDATION AUTHORITY SERVICES (unspecified)
    -->
- <tsl:ServiceName>
  <tsl:Name xml:lang="EN">EU:/O=CSP Validation Team Inc./CN=CSP
    VTEAM</tsl:Name>
```

```
    </tsl:ServiceName>
-   <tsl:ServiceDigitalIdentity>
-   <tsl:digitalId>

    <tsl:X509Certificate>MIIEBTCCAu2gAwIBAgIEOdnX1zANBgkqhkiG9w0BAQUFADB
    XMQswCQYDVQQGEwJJVDEYMBYGA1UE
    ChMPUG9zdGVjb20gcy5wLmEuMRcwFQYDVQQLEw5DQSBlIFNpY3VyZXp6YTEVM
    BMGA1UEAxMMUG9z
    dGVjb20gQ0ExMB4XDTAwMTAwMzEzMDAyOFoXDTEwMTAwMTEyMDAyOFowVzE
    LMAkGA1UEBhMCSVQx
    GDAWBgNVBAoTD1Bvc3RlY29tIHMucC5hLjAXMBUGA1UECxMOQ0EgZSBTaWN1c
    mV6emExFTATBgNV
    BAMTDFBvc3RlY29tIENBMTCCASIwDQYJKoZIhvcNAQEBBQADggEPADCCAQoCgg
    EBAOVjO/c6v6jR
    H9pB2sJtvkWwr+5cRy9lk09ZNHih6wRgTdv4yxAy2LpAkH30N2oo6eZsZv7G0ibx
    DOLa4Uwh2vwm
    rxvr2imKq5eWEatDwmQAunI9hxbFdu9MjsjXg6ecvWgV7LcD+kjaapUavpiE46/gZ
    2wslfewEmj2
    rsKO1uZ6thj7BJ8Q1ttSEJuHdiTVx84VRYjnYgNKxCw3XA/WUCqIEQFDuuX1EWr/
    WrG2Y+jpwd7L
    PNRaBMCVaUWb6uOUAVBP4n5vxK2qHr126iXOLAeL2Mt9XWOuSXzN1G4dTVq4J
    fcHZIFWjHCu2tnG
    Y/UY7j+JjAdMv5NdNTlgLPcqk4kCAwEAAaOB2DCB1TASBgNVHRMBAf8ECDAGAQ
    H/AgEAMAwGA1Ud
    JAQFMAOAAQAwPQYDVR0gBDYwNDAyBgcrTAsBAgEBMCcwJQYIKwYBBQUHAgE
    WGWh0dHA6Ly9wb3N0
    ZWNlcnQucG9zdGUuaXQwOgYDVR0fBDMwMTAvoC2gK4YpaHR0cDovL3Bvc3RlY
    2VydC5wb3N0ZS5p
    dC9wb3N0ZWNvbWNhMS9jcmwwEQYDVR0OBAoECEku+kddYQjMMBMGA1UdIw
    QMMAqACEku+kddYQjM
    MA4GA1UdDwEB/wQEAwIBBjANBgkqhkiG9w0BAQUFAAOCAQEAsIoJsI+dPRGXB
    hU6bMrgSb0g4dWH
    6mIjjJL/2O/HYEDihhhNcKawVK4hrXYEkJMgTKcqKf7V4ZpDnWTYwZLtWeucmgA
    eUyc12xhldJhU
    jgMloes4Vi/hUFaDLknvIcBzuvyFflkjVj4e45D6vl99yP2s0yvIVnU9huri0hNV+FyPP
    sXq3CSt
    6fDdgUXwuLW5cgK/01LMXDj3b5PBlJlrVoPJoqGZQDeDgDf/VWh5oc5XjHoZD06
    HVg1V2JxmDfr5
    8EYyuP+yuU3HyazaabmIFHbR94H+6WHDc0oFwd6STvzZTAyupTo41JUnsXmfr1
    WtWkc/b+DqK2oL K9GsvYWwhA==</tsl:X509Certificate>
    </tsl:digitalId>
    </tsl:ServiceDigitalIdentity>

    <tsl:ServiceStatus>http://uri.etsi.org/TrstSvc/Svcstatus/VArecognized</tsl:Serv
    iceStatus>
  - <!--
     Validation Authority recognized
    -->
```

```
<tsl:StatusStartingTime>2007-07-07T09:18:25Z</tsl:StatusStartingTime>
- <tsl:TSPServiceDefinitionURI>
<tsl:URI xml:lang="EN">http://www.peppol.eu/</tsl:URI>
</tsl:TSPServiceDefinitionURI>
</tsl:ServiceInformation>
</tsl:TSPService>
</tsl:TSPServices>
</tsl:TrustServiceProvider>
</tsl:TrustServiceProviderList>
- <ds:Signature>
- <ds:SignedInfo>
<ds:CanonicalizationMethod Algorithm="http://www.w3.org/TR/2001/REC-xml-c14n-20010315" />
<ds:SignatureMethod Algorithm="http://www.w3.org/2000/09/xmldsig#rsa-sha1" />
- <ds:Reference URI="">
- <ds:Transforms>
<ds:Transform Algorithm="http://www.w3.org/TR/2001/REC-xml-c14n-20010315" />
</ds:Transforms>
<ds:DigestMethod Algorithm="http://www.w3.org/2000/09/xmldsig#sha1" />
<ds:DigestValue>2jmj7l5rSw0yVb/vlWAYkK/YBwk=</ds:DigestValue>
</ds:Reference>
</ds:SignedInfo>

<ds:SignatureValue>MFgj+12dn5JD5VYmHwKkZ5gbjIN1L2Z4sd4MmnZ3Yi/xbr0T
yzP+im9uh2J6fk+YoV/s6DYhZBWT
Tbts6Pf8K4T8VyyoxTf8vFuf9Xr83VTjnV25lu8UTMuPKHEoOHnhPaT9+Pa82RomD
OhtcZ29nKHw OHGgsMcyt0XsvbMu/Lc=</ds:SignatureValue>
- <ds:KeyInfo>
- <ds:KeyValue>
- <ds:RSAKeyValue>

<ds:Modulus>tW/iq4Ee0HBo+IsXxBq0Muzag/cgk2wzc9JfPexrcoEXrL0xleP3aaD4
pPZitkVnsRCSEHMWOCuL
aUe84c7Zmqi+SIA0fiSCVBVnFJ6XI3sLB/JNIn8w//56zL98RlPa9K1V5OLpiOEYYx
4bIYc3zhyL IpYDh3KSbOFPwPupU+M=</ds:Modulus>
<ds:Exponent>AQAB</ds:Exponent>
</ds:RSAKeyValue>
```

```
</ds:KeyValue>
- <ds:X509Data>
<ds:X509Certificate>MIIEhzCCA2+gAwIBAgIERXZkeTANBgkqhkiG9w0BAQUFADC
BhzELMAkGA1UEBhMCSVQxNDAyBgNV
BAoTK0NlbnRybyBOYXppb25hbGUgcGVyIGwnSW5mb3JtYXRpY2EgbmVsbGEgUE
ExLjAsBgNVBAsT
JVNlcnZpemkgZGkgU2ljdXJlenphIGUgQ2VydGlmaWNhemlvbmUxEjAQBgNVBAM
TCUNOSVBBIENB
MTAeFw0wNjEyMDYwNjM0MzNaFw0wOTA4MDUwNjM0MzNaMIHUMQswCQYDV
QQGEwJJVDEaMBgGA1UE
CgwRQ05JUEEvOTcxMDM0MjA1ODAxJjAkBgNVBAsMHVVGRklDSU8gU1RBTkRBU
kQgRSBURUNOT0xP
R0lFMRYwFAYDVQQDDA1BUkJJQSBTVEVGQU5PMRwwGgYDVQQFExNJVDpSQkF
TRk42NFQzMEg1MDFI
MRAwDgYDVQQqDAdTVEVGQU5PMQ4wDAYDVQQEDAVBUkJJQTETMBEGA1UELh
MKMzAwMDIwMDgzNTEU
MBIGA1UEDAwLRlVOWklPTkFSSU8wgZ8wDQYJKoZIhvcNAQEBBQADgY0AMIGJA
oGBALVv4quBHtBw
aPiLF8QatDLs2oP3IJNsM3PSXz3sa3KBF6y9MZXj92mg+KT2YrZFZ7EQkhBzFjgri2
lHvOHO2Zqo
vkiANH4kglQVZxSelyN7CwfyTSJ/MP/+esy/fEZT2vStVeTi6YjhGGMeGyGHN84ciy
KWA4dykmzh
T8D7qVPjAgMBAAGjggEuMIIBKjAOBgNVHQ8BAf8EBAMCBkAwHQYDVR0OBBYEF
PLRqBl4d2Fabv7G
10fmQX6SoEFUMFoGA1UdIARTMFEwTwYHK0wQAQIBATBEMEIGCCsGAQUFBwIB
FjZodHRwOi8vd3d3
LmNuaXBhLmdvdi5pdC9maXJtYWRpZ2l0YWxlL21hbnVhbGVvcGVyYXRpdm8wM
AYDVR0fBCkwJzAl
COgIYYfaHR0cDovL2NhLmNuaXBhLmdvdi5pdC9jcmwzLmNybDAvBggrBgEFBQc
BAwQjMCEwCAYG
BACORgEBMAsGBgQAjkYBAwIBFDAIBgYEAI5GAQQwGQYDVR0RBBIwEIEOYXJia
WFAY25pcGEuaXQw
HwYDVR0jBBgwFoAUnG/hdmgnQpzAgEBwoA8I6dES/6QwDQYJKoZIhvcNAQEFB
QADggEBADeK7Qzt
YXwpvxC/wl/GOleeIBn+DXrRiRPokYDIUjl6d0HhLOGNfzlY//TtS/5A/OFPgRxpiU
3RE6bAZdmw
deenPw54q5eX5h6EG3ix3x/jwPsALh9nXVex8wvz/dafFPEQs+uREaauoDvyMbb+
EgbtvOKYlB51
Bteuf8jnhM1ycPxmlJdTD+ysmT8j07BCtgO+OCjG8HNhh79q66PbcrjUcHcJIAiP7b
tK2bCrMeJz
BKDvSwqlbJspvfvTtJgk0OeOv2gqvyqfvdswMEGGk9yLNbdhI4CWmdqDY8x3xm4
k0rKfq7RB5ATj M/NpukxLKsO4qr4d6+orD73axo/03bU=</ds:X509Certificate>
</ds:X509Data>
</ds:KeyInfo>
</ds:Signature>
</tsl:TrustServiceStatusList>
```

6 Time Stamps and TSA Services

6.1 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 recognize 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 D1.1 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.

6.2 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. TSA services should not be used by the sender. This relies on an assumption that no formal requirement exists for sending side TSA time stamps. PEPPOL WP1 is not aware of any such requirement.

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

7 Figures

8 References

[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

[DNV01] J.Ølnes et al., Making Digital Signatures Work across National Borders. ISSE/SECURE Conference, Warszawa, 2007.

[ETSI-101-903] ETSI TS 101 903 V.1.3.2 (2006-03) XML Advanced Electronic Signatures (XAdES).

[ETSI-102-231] ETSI: Electronic Signatures and Infrastructures; Provision of Harmonized Trust Service Provider Information. ETSI TS 102 231 v2.1.1,2006.

[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) XML Advanced Electronic Signatures (XAdES).

[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

[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.

[SEALED01] Sealed, Technical Specifications for the Proposed Common Template for the "Trusted List" of Supervised/Accredited QCSPs, version 0.72, January 2009 (to be published in version 1.0 later in 2009).

[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.

9 Appendix 1: Trust and Trust Models Theory

9.1 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. "Organizational 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 "organizational 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 organizations and humans.

9.2 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 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].

9.3 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.
- The electronic commerce protocols, defined as a sequence of exchange 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 must 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. Such requirements are investigated by PEPPOL WP1 in D1.1.

9.4 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 policy (see D1.1 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[8]. 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 D1.1 parts 3 and 7).

9.5 Electronic Signatures and Organizational 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 organizational 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 organizational attributes, and this may be used in the trust decision. Obviously there are no warranties that the information is updated.
- 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 registries).

[8] 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.

- Further information is obtained from independent, trusted sources; in which case the necessary services and infrastructure must be identified and specified.

PEPPOL WP1 will derive such framework policies, and this is further elaborated in D1.1 part 3.

9.6 E-signature and eID Interoperability

9.6.1 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 minimize 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 D1.1 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 utilize existing and future trust structures to the extent possible and will closely monitor progress in the area.

9.6.2 Trust Lists and Trust List Distribution Services

A trust list consists of named CAs 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 D1.1 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 the SPOCKS pilot [SEALED01]. 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 D1.1 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 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 relevant CAs in Europe may be in the order of 200 (the SPOCKS pilot lists 96 issuers of qualified eIDs in Europe). Bridge-CAs and hierarchies contribute to making the list shorter, and a trust list distribution service may cover all relevant CAs.

The scheme suggested by [COMM01] is a federated TSL (Trust Status List) system. The TSLs will be maintained by the respective Member State and these lists will either be aggregated or otherwise be made available to all parties that need the information.

Use of trust lists will be piloted by PEPPOL.

9.6.3 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 "un-known" CAs are handled by calls to the VA. This is a more technical approach to use of a VA.

PEPPOL will pilot 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.

10 Appendix 2: Time Stamp Requirements

10.1 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 is associated with events and documents 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.

10.2 EU Directives, Tendering Process Requirements

The EU Directives on public procurement [EU02] [EU03] require reliable time stamping of events in procurement processes. 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.

10.3 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 then has to collect them from a trusted source. The documents 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.

10.4 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).

10.5 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 are 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.

10.6 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 will 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.

10.7 Time Stamp Authority (TSA)

10.7.1 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.

10.7.2 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-CA certificates (public keys) must be maintained along with root-CAs for eID issuing. 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.

10.7.3 Qualified and Non-Qualified TSA Signatures, Accreditation

According to the EU Directive on Electronic Signatures [EU01], qualified certificates can only be issued to natural persons, 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 only 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.

10.8 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 recognize 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 D1.1 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 D1.1 part 3 is to not require "advanced" SDOs to be produced on the signing side.

10.9 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 D1.1 part 3). This relies on an assumption that no formal requirement exists for sending side TSA time stamps. PEPPOL WP1 is not aware of any such requirement.

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).

11 Appendix 3: Sending Side Validation

11.1 Requirements for Sending Side Integration

At earlier stages of the WP1 work, requirements for sending side integration to a validation service were raised. These requirements are now abandoned but the solution outline is kept in this appendix for documentation. Note that this type of integration is supported by the Governikus platform offered by bos for the pilots.

Requirements for sending side validation may be raised to ensure that the sender pays for the validation, and to ensure that, when a local CA is used, the information is validated close to that CA. This may reduce the need for distribution of information about CAs and their services.

There may be legislative requirements dictating receiving side validation in some countries, meaning that a sending side validation may have to be repeated at the receiving end in those cases. Sending side validation should therefore only be used if such requirements do not exost at the receiving side in order to avoid a double validation effort.

XKMS version 2 (see D1.1 part 5) is the protocol of choice also for sending side eID validation. OASIS DSS is not relevant in this case since the signature verification will anyway have to be repeated at the receiving side. Integration points can be established as follows:

- At the sending side, the sender's access point to the PEPPOL transport infrastructure performs the XKMS call and places the result as a token in the WS header. If the document has more than one signature, the process must be repeated.
- At the receiving side, the operator system or the recipient itself (depending on local choice) performs the XKMS call as a part of the signature verification process.

An XKMS ValidateResult should include the OCSP response (alternatively CRL but preferably not due to the potential size of a CRL) obtained from the CA. This may be needed at the recipient to build SDOs and archival records (see D1.1 part 3).

At the receiving side, OASIS DSS (see D1.1 part 6) is devised as an optional, alternative protocol if the receiver wants to outsource the entire signature processing and not only eID validation. This interface is not offered on the sending side since the receiver would anyway have to revalidate the signatures; only eID validation can be provided by sending side.

11.2 Sending Side eID Validation in PEPPOL Infrastructure

11.2.1 Sending Side Process

The process for sending side signing and eID validation is as follows:

1. The sender signs inside his own system or by use of an Operator system; in any case the signed business document is in the Operator system. Although encryption of the business document will be an exception (see 3.1), the validation process should allow use of encrypted documents. Multiple signatures can be applied.
2. The signed document is sent to the Access Point (AP) to the PEPPOL infrastructure. One of two conditions must be fulfilled for this interface:
    a. If encrypted documents are allowed, the certificate(s) supporting signatures must be conveyed separately over the interface.

b. Alternatively, for unencrypted documents only, one may rely on the AP's capability of extracting certificates from the signed document. For use of the PEPPOL infrastructure, XML-based signatures should be used, so this capability is rather straightforward.

3. The AP calls the XKMS responder obtaining an XKMS ValidateResult. When building the WSS document to be transported, the AP embeds the XKMS ValidateResult as a custom WSS XML token in the header. The process is repeated if the document has multiple signatures. The XKMS responder signs each ValidateResult individually.
4. The AP authenticates to the selected Security Token Service in the PEPPOL infrastructure to obtain a SAML token that is also placed in the message header, and the message is sent.

The following issues should be noted:

- For step 2a, the link between the certificates sent separately and the signatures on the encrypted document is only guaranteed by the Operator system. The possible scenarios that may emerge if this condition is not fulfilled are not yet studied but needs to be explored in order to determine if the protocol is sufficiently secure.
- For step 2a, one has to determine if it is necessary to send the entire certificate path or only the end user certificate. Possibly this can be determined by local policy but path validation may be a requirement imposed on/by the recipient.
- For step 3 it has to be determined if path validation or only end user certificate validation shall be used. If complete certificate path is included, one may have to do path validation. Possibly this can be determined by local policy but path validation may be a requirement imposed on/by the recipient.
- For step 3 the action to take in case an invalid or incomplete result is returned from the XKMS responder must be specified. The easiest solution is to not examine the result but just forward whatever is received from the XKMS responder and leave this to the receiver. Alternatives are to return to Operator system with an error message or (in the case of incomplete) to enter a time-out period and try again a specified number of times.

In addition to the fact that the validation costs in this case will be placed on the sender, which may be desired, the added advantage of sending side validation is that it is performed "close" to the sender and the sender's CA, eliminating chaining of requests to remote XKMS responders. Also, the trust model on the sending side is not an issue since the sending side selects a local, trusted XKMS responder. The XKMS interface should adhere to D1.1 part 5.

11.2.2 Receiving Side Process

The PEPPOL infrastructure interfaces must ensure that the XKMS ValidateResult (all of them if multiple) is conveyed together with the signed document to the receiving side AP and further on to the receiving system (Operator system or end receiver). The recipient has two options:

- If the sending side XKMS responder is trusted, the recipient may proceed by just verifying the ValidateResponse (the XKMS responder's signature and that the certificate status is valid), and then continue to verify only the signature.
- At its own discretion (sending side XKMS responder not trusted, legal requirements, other reasons) the recipient may discard the XKMS ValidateResponse and perform its own validation (receiving side validation as described otherwise in this document).

A main issue on the receiving side is how to establish trust in an XKMS responder selected by the sending side:

- Even though the XKMS responder should be independent and trusted, the fact that it is selected by the receivers "opponent" may be a problem. This may be more of a theoretical case.

- This aside, trust in an (potentially unknown) XKMS responder must lean on not only the ability to verify the XKMS responder's signature but also on knowledge of quality and other issues.
- The assessment done by the XKMS responder and the information in the ValidateResponse should be sufficient for the recipient to determine not only validity but also signature policy adherence (see D1.1 part 3).

Given that the ValidateResponse contains sufficient information (signature policy adherence), the issue is how the recipient can be able to verify the XKMS responder's signature and assess that the XKMS responder itself is trustworthy (organizational trust) and has sufficient quality. At present, the only possible solution seems to be that the XKMS responder needs to be somehow listed, preferably in a TSL issued by someone (directly or indirectly) trusted by the recipient.

11.3 Sending Side eID Validation without Use of PEPPOL Infrastructure

Instead of integrating to the XKMS responder from the AP, the integration may be done directly from the Operator system (or even from the sender's system). If the PEPPOL infrastructure is used for transport, one can then at least in theory mediate the XKMS ValidateResult over the interface between the Operator system and the AP and proceed as described in 11.2.

However, in this case a more natural way to proceed is to include the XKMS ValidateResult in an XAdES [ETSI-101-903] SDO (Signed Data Object). The XAdES SDO can then be sent by use of the PEPPOL infrastructure or be transferred using some other transport channel. Use of XAdES SDOs created on the sender side is neither recommended by the signature policies described in D1.1 part 3 nor anticipated in the time frame of the PEPPOL pilots. Thus, this alternative is not discussed further. The trust issues are the same as described in 11.2.