PEPPOL
Pan-European Public Procurement Online

PEPPOL Deliverable D1.1
Requirements for Use of Signatures in Public Procurement Processes
Part 3: Signature Policies

Version 1.2

PEPPOL WP1 2009-04-30

Borderless eProcurement

Let's make it happen!

cip competitiveness and innovation framework programme 2007-2013

Table of contents

1 Introduction

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 – April 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 part of D1.1 describes signature policy requirements to enable cross-border interoperability of e-signatures. The purpose of a signature policy is to clearly describe the requirements imposed on the actors with respect to the following issues:

- Authorization and commitment implied by a signature or a set of signatures;
- Application of signatures in e-procurement processes – the documents that should be signed and at what stages of the process;
- Signature validation policies that specify the required quality levels and approval status (e.g. qualified) for eID and e-signatures, the validation process, and other requirements imposed on the actors.

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

Following signature policy definitions in chapter 1.3, the scope of such policies in PEPPOL is further refined in chapter 3. Commitment rules are specified in chapter 4 and application of e-signatures in business processes in chapter 5. Extensive specifications of signature validation policies are given in chapter 6 and Appendix 1, and conclusions are drawn in chapter 7. Appendix 2 gives some considerations for signature formats.

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 Signature Policy Definitions

2.1 Signature Policy

Quoting [ETSI-102-038], chapter 6:

*The **Signature Policy** is a set of rules for the creation and validation of an electronic signature, under which the signature can be determined to be valid. A given legal/contractual context may recognize a particular signature policy as meeting its requirements.*

The signature policy may be explicitly identified or may be implied by the semantics of the data being signed and other external data like a contract being referenced which itself refers to a signature policy.

An explicit signature policy has a globally unique reference, which is bound to an electronic signature by the signer as part of the signature calculation.

The signature policy needs to be available in human readable form so that it can be assessed to meet the requirements of the legal and contractual context in which it is being applied. To facilitate the automatic processing of an electronic signature the parts of the signature policy which specify the electronic rules for the creation and validation of the electronic signature also needs to be in a computer processable form.

2.2 Signature Validation Policy

The signature policy rules that apply to functionality are termed **Signature Validation Policy** [ETSI-102-038]. Further rules may place requirements on elements of certificate policies for the eIDs used with the signatures (e.g. requirements for protection of private keys), and to the signing environment used by the signer.

A signature validation policy [ETSI-102-038] includes:

- Rules to be followed by signer,
- Rules to be followed by verifier,
- Rules for use of CAs (Certificate Authority, i.e. eID issuer),
- Rules regarding use of TSAs (Time Stamping Authority),
- Rules on use of AAs (Attribute Authority) issuing attribute certificates,
- Rules on use of algorithms.

2.3 Commitment Rules

An electronic signature produced under a security policy supports a number of commitments. Rules may be specified in a signature policy either referring to the whole set of commitments made by the signer or to a certain given commitment.

An example is a rule stating that the signer must have certain authorizations on behalf of an organization in order to produce a signature that complies with the signature policy.

Use of signatures (which documents are signed, at what steps of the process) in business processes should be defined in conjunction with the definition of the process (the protocol). This may also be viewed as part of the signature policy in force. A signature policy may refer to a protocol specification or the other way around.

[ETSI-TR-102-045] discusses signature policies for “extended business model”, defined as: *a business or commercial transaction, which may involve several actors/participants and/or multiple actions in its process and which may require multiple signatures to give it effect.*

Examples of such extended business scenarios are:

- two (or more) primary signatures, such as buyer and seller on a contract;
- a countersignature as “authorization” or witnessing of a primary signature;
- signatures which are applied as part of a document flow, i.e. which assume a responsibility for a defined part of a document or transactional process;
- a combination of signatures all of which may be signed by another party, e.g. a notarial signature.

2.4 Signature Policy Representation

As stated by [ETSI-102-038], a *signature policy needs to be available in human readable form so that it can be assessed to meet the requirements of the legal and contractual context in which it is being applied. To facilitate the automatic processing of an electronic signature the parts of the signature policy which specify the electronic rules for the creation and validation of the electronic signature also needs to be in a computer processable form.*

[ETSI-102-041] suggests content of a signature policy. This can be used to form a template for the mandatory human readable policy. The technical reports [ETSI-102-38] and [ETSI-102-272] define signature policy elements in XML and ASN.1 format respectively.

Note that whenever several representations of one signature policy exist, one of them must be denoted as the authoritative version.

3 Scope of Signature Policies in PEPPOL

3.1 State on Use of Signature Policies

The concept of signature policies was introduced around the year 2000, and standards were published by ETSI in the years 2002-2003. It is fair to say that the idea of formalizing signature policies has not caught on. Standards are fairly old and not much referred to. Possible reasons, such as weaknesses in the approach, lack of market maturity etc. are not discussed here.

3.2 PEPPOL's Pragmatic Approach

When developing specifications for e-signature interoperability in PEPPOL, it became clear that the concept of signature policies is exactly what is needed to describe the rules for signature acceptance (as opposed to signature verification, which is merely an assurance that the signature is correct).

With respect to the constituents of a signature policy as described above, PEPPOL's approach for the pilots is:

- Commitment rules for business protocols must be described in human readable form[2] as parts of the protocol descriptions.
- Signing environment is (largely, but see D1.1 part 2, Appendix 1) out of scope of PEPPOL and no requirements are posed apart from those that follow from signature validation policies.
- Signature validation policies consist of a limited set of parameters for quality and approval status (notably qualified or not) that can be mediated across validation interfaces. These are defined as data structures that can be referred to by interface descriptions (see e.g. part 7 of D1.1).

PEPPOL does not (at least not at this stage) define complete, comprehensive signature policies that are given unique references. Given the points above, the important part is to uniquely define the parts that are machine processable, not to uniquely identify complete signature policies.

Annex A of this document describes how requirements from the eSignature Directive [EU-01] are addressed and which standards that must be applied.

3.3 Commitment Rules and Business Protocols

For a tendering process, it is very important that the awarding authority clearly states the signature requirements imposed on the economic operators. These requirements are at present best stated in a human readable form as parts of the instructions for tendering. Requirements must have three parts:

- Which documents must be signed at which stages of the procurement process?
- What shall these signatures imply in terms of commitment, and/or what authorizations (roles) are implied by the signatures?
- What are the quality requirements for the signatures themselves (signature validation policy)?

Quality requirements must be non-discriminatory and stated in general terms rather than (the present practice in most cases) referring to a list of eID issuers that are accepted. The requirements shall then

[2] For some protocols this may be defined along with a processable definition of the protocols. This may be further explored in PEPPOL at later stages of the project, e.g. an e-invoice protocol including use of e-signatures.

also be represented by parameters used for signature verification processes and across validation interfaces.

If business protocols are represented in a processable way, the representations should include an automated representation of all the signature requirements. If processable business protocol descriptions are introduced, PEPPOL WP1 is prepared to work with other WPs in PEPPOL on the signature parts.

A further requirement is that the policy should select one of the following alternatives:

- Signature verification is always done relatively to current time, which implies that eID certificates must be valid (not expired nor revoked) until the end of the business process (e.g. tendering). Such a requirement must be made clear to the signer since it requires caution in the signing process and action if a need to revoke an eID emerges.
- Signature verification is done relatively to the time when the signed document was originally received, i.e. a signature valid at that time remains valid even if the eID certificate is later revoked or expired.
- Signature verification is done relatively to the time of signing. This can only be achieved if the sender obtains a TSA time stamp at that time and conveys the time stamp to the receiver. Note that the signature may be applied “a long time” before sending the document. PEPPOL recommends not placing any requirements for TSA time stamps on the sender, meaning that this alternative should not be used.

Use of a revocation grace period where signature/eID verification is delayed until after the next scheduled issuing of revocation information by the eID issuer, is considered a local policy decision by PEPPOL and is not discussed further. Note that there may be national requirements for such delayed verification.

3.4 Signature Validation Policy

As described above, a signature validation policy may include the following:

- Rules to be followed by signer,
- Rules to be followed by verifier,
- Rules for use of CAs (eID issuer),
- Rules regarding use of TSAs (Time Stamping Authority),
- Rules on use of AAs (Attribute Authority) issuing attribute certificates,
- Rules on use of algorithms.

In short, the following approach is taken by PEPPOL:

- Signer rules are not made explicit since signing is essentially out of scope[3] in PEPPOL; however the rules for use of CAs must be adhered to by the signer. A signer may be required to produce a certain signature format; however requirements should be kept low to ensure a low barrier to economic operators.
- Verifier rules are the checks necessary for signature verification and signature acceptance (i.e. signature policy adherence) on receiving a signed document, rules that govern information

[3] It is assumed that all actors are able to sign inside their corporate infrastructure. Issues such as signing a form for a tender in a web interface are not entirely out of scope of a tendering pilot but will not be particularly addressed by PEPPOL.

collection at the time of verification, and rules for storing a signed document and collected information in an archival record (usually a signed data object – SDO).

- Rules for use of CAs shall be given in a non-discriminatory way. There are two important parameters: approval status of CA (qualified or not is the most important issue), and quality of eID and e-signatures (qualified signature or not, and other quality issues).
- For tendering pilots in PEPPOL, a TSA may be used on the receiving side (the awarding authority) as part of SDO creation. This is not mandated and not particularly focussed by PEPPOL. Use of TSAs on the sending side is not a prioritized topic for PEPPOL.
- Attribute certificates are not included in the PEPPOL pilots since such certificates are not at present in use in practical procurement processes, so assuming their existence or introducing them is not feasible. PEPPOL may however look into use of corporate (organizational) signatures where the signing certificates binds to an identified organization and not to a person inside that organization.
- Quality of hash algorithm and public key cryptography (algorithm and key length) should be parts of signature validation policies. Note that the hash algorithm used for the signature is controlled by the signing software and cannot be selected through the eID. Public key algorithm and key length are specified by the eID (the CA) but should be mediated as a separate quality parameter[4]. This is discussed further in part 7 of D1.1.

[4] Germany has already abandoned use of RSA-1024 for qualified certificates but common practice in the rest of Europe is to still accept RSA-1024 for the subject's public key. Merely checking the qualified status may therefore not be sufficient.

4 Commitment Rules – Names, Roles, Authorizations

4.1 Introduction

With respect to commitment and authorization, the usual requirement in Member States is that, when a signature is required, a personal signature from an authorized person is needed. A signature binds to the name in the eID, usually a person name only. The receiver will then usually need additional assurance that this signature also represents the signer's organization and that the person has the required role and authorizations.

The acceptance criteria with respect to commitment and authorization must be made clear. In the following sections, six approaches for use of e-signatures in tendering are outlined. Conclusions are then presented. The alternatives are:

- A signature of sufficient quality is accepted as legally binding. The risk of mistakes is low and if something is wrong a strong proof exists through the signature.
- A registration process binds names in eIDs to roles and authorization for the organization. The process as such is not described in this document, only requirements to the process.
- Binding between names and roles/authorizations are "automatically" established by means of a VCD (Virtual Company Dossier, studied by PEPPOL WP2) or by use of business registers.
- Use of employee eID that includes an organization's name (and unique identifier) in addition to the name of the person.
- Use of corporate eID that includes only organization name and unique identifier, no person name.
- Combination of an inner, personal signature and an outer signature by a corporate eID.

Note that it is strongly discouraged to include authorizations and roles in eID certificates. If such short-lived attributes are included, very cumbersome eID management (frequent revocations) will result. Some long-lived authorizations that follow a person (accredited lawyer, broker, medical practitioner) may still be included in eID certificates, but e-procurement needs management of short-lived authorizations.

Note also that the use of attribute certificates is not discussed in this document as this is regarded as a too experimental approach to be used in the PEPPOL pilots. An attribute certificate is a short-lived certificate that is used in conjunction with an eID certificate to convey authorizations.

4.2 Rules to Be Defined along with Pilot Scenarios

Rather that postulating specific commitment rules at the specification stage, PEPPOL will refine requirements and rules as a part of the pilot implementations and trials. In particular this applies to the tendering pilots to be run by WP1 (see D1.1 part 2); however the same approach will be taken for post-award processes (order, order confirmation, catalogues, invoicing) in co-operation with the PEPPOL WPs responsible for these processes.

4.3 Alternative 1: Accept Signed Documents

When a signature purports to be by a person in an authorized role, this claim is accepted.

In this alternative, a valid signature and an eID of sufficient quality is regarded as sufficiently trustworthy to prove the honest intent of the signer. This risk management decision has two elements:

- The risk of someone making false claims and signing them with e.g. a qualified signature is small. Besides, an attacker has little to gain.
- If something is wrong, there is a strong proof identifying the responsible actor.

This approach is based on a very high level of confidence on contractor parties, but the risk to expose the entire e-procurement system to mistakes and frauds is significant. This model offers simplification of technological solutions but could introduce an organizational overhead in case of further disputes even though these should be resolvable with the proof of signature.

Actors active in the Norwegian public e-procurement solution were queried about the implications of a signed tender. The answers indicate that an economic operator will normally be liable for a signed tender even if it turns out that the signer has acted outside of his authorizations. The claim is simply that the economic operator must be expected to exercise sufficient control within its own organization. On the other hand, if it turns out that a signature does not carry the necessary authorizations, an awarding authority will normally be expected to still accept the tender. A new, correct signature will be requested at time of contract signing. Competitors may dispute this but will normally not win such a case. These considerations may be different in other countries.

4.4 Alternative 2: Registration Procedure

A registration procedure to verify the link between a person with a given eID and roles within economic operators is carried out as a step of the tendering process.

In this alternative, the economic operator is forced to go through a registration procedure where e.g. persons as identified by eIDs are linked to economic operator enterprises and related roles and authorizations. The registered information may be accepted as a self-declaration (subject to some of the same considerations as for alternative 1 above), or it may wholly or partially be verified against independent sources such as business registries.

So, in this approach the links among eID and roles are established directly in the e-procurement process, in the registration phase.

Example Italian Approach (CONSIP eTender – Ministry of Economy and Finance)
Q. In which phases of the eProcurement process (e.g. notification, tendering, awarding, etc.) is there a need for signatures?
A. For the registration procedure and the final offering

When an economic operator, or a consortium, wants to participate to a public tender, it has to register to the awarding authority services (web sites). The registration will end with a signature of an agreement. After certain controls, the eID used for that signature will be the same for the offering phase.

Similarly in an e-order application the economic operator (seller) and the awarding authority (buyer) have to register to the service and link their eIDs to their roles by means of a similar agreement.

Example Italian Approach (CONSIP eOrder – Ministry of Economy and Finance)
Q. Who signs, and which authorizations are represented by the signatures?
A. A person, the linking with an organization is stated by the registration document.

In both cases the link established in the registration phase is used in the verification process in the finalization phases such as order confirmation (eOrder). This approach may be followed even if the order process is automated between the systems of the organizations such as envisioned by PEPPOL.

Referring to the previous approach this model, accepting only the registered signers, eliminates the risk to expose the entire e-procurement system to mistakes and frauds. This model does not introduce specific requirements about roles encoding because the link is made during the registration phase. The whole weight of this model is loaded on any local awarding authorities. This could introduce cross border barriers due to restrictive registration requirements.

Registration processes should be language neutral or at least offered in English along with the native language of the awarding authority.

4.5 Alternative 3: Attestations and VCD

Registration is done through a trusted identity service provider.

In this alternative, independent proofs of roles and authorizations are required for all or parts of the information. This may be mediated by virtual company dossiers (VCD) as studied by PEPPOL WP2, by reference to business registries, or by separate certificates and attestations.

This case generalizes the previous alternative in order to reuse an existing registration. Instead of registering to each awarding authority (or each tendering service provider), the company or consortium will attend to a registration service where associations among eIDs and roles are managed and updated. If the register is trusted, the information is assumed to be correct.

At least in some countries (e.g. Norway), companies have a legal obligation to maintain correct information in public business registers. If the information is wrong, the company itself is liable.

Business registers (national or regional, or run by other actors such as chambers of commerce) at least to some extent contain role information and authorizations. The missing links here are:

- Syntax and semantics of attributes representing roles and authorizations must be standardized and agreed among all users of a register.
- Roles and authorizations must be linked in the register to name used in the eID, or to a unique attribute of that name. National identifiers for persons are used to this effect but use of such identifiers across borders is not straightforward, and identifiers do not exist in all countries.

Information from a register may be obtained according to two models:

- The economic operator fetches the information from its local register, obtaining a data structure or document that should be signed by the register authority.
- The (tendering solution used by the) awarding authority requests the information, possibly through a chain of registers such as devised by the BRITE project[5]. In this case, authenticating the register should normally be sufficient; if the register is trusted, no signature is necessary (signature from register may still be an option).

The latter approach is recommended as this will imply more updated information and a simpler procedure since the awarding authority does not have to check that the economic operator has forwarded correct and updated information. However, paper-based procedures usually demand that the economic operator obtains the information, and it may be the case that such procedures are inherited by and enforced by legislation even for e-tendering.

It is also possible to register attributes at an identity provider and have the attributes conveyed e.g. in a SAML token when a user authenticates to the e-tendering service. This will not be tried in PEPPOL as the approach is too far from common practice to be useful in a pilot. In yet another approach, a company may itself make some of its internal directory information concerning names, authorizations

[5] Business Register Interoperability Throughout Europe, http://www.briteproject.net

and roles available to external parties, who in that case must be able to understand the information. This approach places too high requirements on economic operators and is not recommended.

4.6 Alternative 4: Employee eID Binding Person To Company

Within corporate PKIs, eIDs will usually identify the company in addition to the person. Such eIDs may also be issued by external eID issuers, if allowed by the company in questions since the registration procedure must ensure not only that the name of the person is correct but also that the binding to the company is correct. Most corporate PKIs are at a modest quality level but exceptions do exist such as the qualified eIDs that will be issued to employees of the Norway-based oil company StatoilHydro.

As discussed above, eIDs should never include short-lived authorizations or role attributes, so only the binding to company is attested by an employee eID.

Semantics of names in eIDs is a problem in general. In this case, even the encoding and the semantics of the organizational naming attributes must be defined.

While employee eIDs may be used in public procurement, they will at least in the time frame of PEPPOL remain a special case. Such eIDs may be handled along with person eIDs but procurement processes cannot rely on their existence in the hands of counterparts. Thus, PEPPOL does not venture further into use of employee eIDs.

4.7 Alternative 5: Corporate eID without Person Name

Using invoicing as an example, one is really not concerned about any person issuing the invoice, only about the issuing organization. One may say that it makes little sense to demand that a person signs the e-invoice; however procedures are frequently inherited from paper procedures. Only a person can sign by hand, as opposed to an e-signature that binds to the name in the eID, which does not have to be a person name. The term “seal” is often used instead of “signature” for such corporate signatures.

Example Italian Law – Legislative Decree 20 February 2004, n. 52 Art.1 c. 3 – (omissis) “non repudiation of date and invoice content is granted by mean of a time stamp and a qualified e-signature on a single or a set of invoices of the invoice issuer (omissis)”

Note that the E-signature Directive [EU01] does not prohibit issuing of qualified certificates to legal (i.e. non-physical) persons; however in most countries the implementation of the E-signature Directive restricts issuing of qualified certificates to physical persons.

For example, since a qualified signature in Italy must be by a person, use of a corporate eID to sign invoices is not allowed in Italy. Such requirements exist in a sufficient number of Member States, yielding the use of corporate signatures (or seals) infeasible in general – although this would be acceptable in some countries.

4.8 Alternative 6: Combination Personal and Corporate Signature

An alternative use of corporate eIDs and signatures is more realistic in the time frame of the PEPPOL pilots:

- The business document (e.g. an invoice) is first signed using a person eID as required.
- Then, on sending the document, a signature (seal) using a corporate eID is added; the semantics of this operation being that the corporate seal attests that the signing person belongs to the company and acts according to authorizations.

If the seal is sufficient according to the legislation in force, the inner, personal signature may be omitted.

While this approach is promising, and there is some attention to the possibilities of corporate signatures, it is not yet decided if PEPPOL shall dive further into this approach.

4.9 Conclusions, Tendering

For a start, the “accept signed document” alternative is a pragmatic choice. This can well be used for PEPPOL pilots.

Registration procedures are out of scope of PEPPOL since these must be offered independently by e-procurement systems. Consequently this alternative will not be tested by PEPPOL.

Attestations and VCD will not be worked upon in particular by PEPPOL WP1; however the results of PEPPOL WP2 on VCD will be studied and a co-operation with WP2 initiated if deemed feasible.

Employee eIDs (both person name and corporate name in same eID) will not be studied.

Corporate signatures, and in particular the model using an inner person signature and an outer corporate signature (seal) may be tested by PEPPOL A decision on whether or not to prioritize work on this topic is to be taken at a later stage, when the requirements of tendering and other processes are more clear.

4.10 Post-Award Processes

Post-award processes such as ordering and invoicing will usually refer to a contract between the buyer (awarding authority) and seller (economic operator). In addition to the alternatives above, the contract may include provisions on who are entitled to sign (kind of a registration process), and the eID used for a signature may be checked against the contract.

Corporate eIDs may be an even more promising alternative for post-award processes but as stated above:

- Personal signatures may still be needed for legislative reasons;
- It is not decided whether or not PEPPOL will work on corporate signatures.

Apart from this, the conclusions above hold for post-award processes as well.

5 Business Protocols – What Must Be Signed?

5.1 Business Process (Organizational) Interoperability

Organizational interoperability is about alignment of business processes between actors. For e-signatures, the main questions are: Which documents must be signed (if signatures are required at all), and what shall these signatures imply in terms of commitment and authorization? The latter question was discussed in chapter 4 above.

This implies that use of signatures shall be defined as part of the definition of the business process (transaction chain). The intention is not that processes must be the same across all actors but that requirements must be transparent and non-discriminatory.

Note that requirements for use of e-signatures in procurement processes are not specified in documents such as [EDYN].

5.2 Rules to Be Defined along with Pilot Scenarios

Rather that postulating specific protocols at the specification stage, PEPPOL will refine requirements and rules as a part of the pilot implementations and trials. In particular this applies to the tendering pilots to be run by WP1; however the same approach will be taken for post-award processes (order, order confirmation, catalogues, invoicing) in co-operation with the PEPPOL WPs responsible for these processes.

Use of signatures in business protocols should for a start be described in a human readable form only. If protocols are formalized by other WPs in PEPPOL in a processable language, then use of signatures should be part of these specifications. It is not assumed that tendering processes will be specified in a processable way in the time frame of PEPPOL.

5.3 Tendering

In the time frame of PEPPOL, e-tendering is still assumed to be a largely manual process consisting of manual downloading and submission (usually uploading) of documents. Consequently, tendering will not use the PEPPOL infrastructure[6], which supports system to system communication.

A requirement for public procurement solutions, at least in the long term, is the ability to deal with complex tenders [COMM01]. A complex tender may be delivered by a consortium of multiple parties in different roles, providing documents that potentially should be signed separately or jointly by members of the consortium. Additional documents may accompany a tender, such as certificates and attestations [Siemens], which may in turn be signed by the entities issuing the documents. Examples of yet more actors that may apply signatures related to a tender are time stamping authorities, notaries, and operators of e-procurement platforms.

In conjunction with specifications for the tendering pilots, PEPPOL will describe a few alternative strategies for signatures in tendering processes. Examples are: All documents signed, cover letter signed – see 5.7 below.

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

5.4 Post-Award Processes

For other procurement processes, a minimum requirement is that it must be possible to sign documents, and that it must be possible to convey signed documents end to end over the PEPPOL infrastructure (i.e. what is signed at the sending side is delivered in a verifiable way at the receiving side).

The post-award processes are usually considerably simpler than tendering. An order process consists usually of one document (which may be signed) containing the order. There may be accompanying documents such as a catalogue, which in turn may or may not be signed. The optional order confirmation may also be signed. An e-invoice is usually just one, preferably signed, document.

5.5 Conversion and Use of Signatures

A particular challenge that must be addressed for such processes is conversion services in concert with e-signatures. An e-signature binds not only to content but also to the document format. Thus, if e.g. an invoice is converted from EDIFACT to XML on its way from sender to receiver, the signature on the original EDIFACT message cannot be transferred to the XML document.

There are four possible solutions:

- Conversion is done before signing. In this case, the signer must know the format required by the receiver; such capabilities may be conveyed by use of information in PEPPOL registries. This is the recommended approach if possible.
- When a signed document is converted, the original, signed version is forwarded along with the converted version, enabling the receiver (at least in theory) to check both versions. This is recommended if the first alternative is not possible.
- When a signed document is converted, the conversion service adds metadata about the original signature(s) and re-signs the converted document with metadata. Since this signature is not from the originator, it may not be accepted as legally binding in many countries.
- A conversion service simply discards original signatures in the conversion process, forwarding an unsigned document, but logging the verification results internally for later reference.

The latter two alternatives are not recommended in general although they may work in some cases.

5.6 Phases of Public Procurement Procedures, Signatures

As examples of typical public procurement procedures may be used e-tendering and e-ordering.

The typical phases of a public e-tender are:

1. registration
2. tendering
3. awarding
4. contracting (when platform managed)
5. invoicing (when platform managed)

The typical phases of an e-order process are:

1. registration
2. catalogue (by the seller)
3. choice of article:

a) direct choice of article in a catalogue (by the buyer)

b) request for Quotation:

i. offer (by the seller)

ii. choice of best answer (by the buyer)

4. order confirmation (by the buyer)
5. invoicing (when platform managed)

An interview study with awarding authorities in some selected countries shows that in these two typical e-procurement processes the phases where a signature is requested are:

- registration (eTender/eOrder)
- catalogue (eOrder)
- order confirmation (eOrder)
- tender submission – in time (eTender)
- awarding (eTender)
- final offer confirmation (eTender)
- contracting (eTender)
- invoicing (eOrder/eTender)

In the eTender registration phase (if applied, see 4.4) the economic operators, even when joining a consortium, register their data and link an eID to the roles played in the tender process, with the effects described. To create that link, the participant signs an agreement with the awarding authority.

In the eOrder registration phase the seller and the buyer, as above, register their data and link an eID to the roles played in the eOrder process.

Example Italian CONSIP eTender – Ministry of Economy and Finance
Q. Is there a registration procedure to verify the link between a person with a given eID and roles within companies?
A. The registration form is used to insert information and to upload documents that identify the person, the person's role in the company, and the company itself.

The awarding authority verifies the signature and gives access to its application.

In some cases "to give access" means provide credentials for the on-line application access, and a PIN for intermediate operations (tendering phase) confirmation.

Example Italian CONSIP eTender – Ministry of Economy and Finance
Q. In which phases of the eProcurement process (e.g. notification, tendering, awarding, etc.) is there a need for signatures?
A. For the registration procedure and the final offering.
During tendering the bidder is required to insert a Personal Identification Number (PIN) to meet the non repudiation of data. The PIN is chosen by the bidder during registration. It is valid for 90 days and the bidder can renew it.

In this Italian case, the final offer confirmation (eTender), the document has to be signed by the tender winner and in case of a consortium by all its members. In the last case multiple signatures are necessary.

In the Italian case, for e-ordering the catalogue submission or in the order confirmation the documents have to be signed by the seller (eCatalogue) or the buyer (eOrder).

5.7 Documents to Sign

5.7.1 Approach All Documents Signed

When signatures are used, the main requirement at present seems to be that all submitted documents must be signed. The motivation may be for legal reasons or for safe archiving needs, preserving integrity and authenticity of the whole process documentation. A time stamp from a TSA (Time Stamping Authority) can be used to guarantee the time of submission.

Example Italian CONSIP eTender/eOrder – Ministry of Economy and Finance
Q. How is the verification data and/or the signed documents themselves processed and stored/archived?
A. Only the signed documents are archived.

Example Italian CONSIP eTender/eOrder – Ministry of Economy and Finance
Q. What is the purpose of the signature (to meet legislative requirements, authenticity of data, integrity of data, etc.)?
A. To meet authenticity, integrity and non-repudiation of data

The usual requirement at present also seems to be that all documents shall be individually signed. An approach where e.g. the documents are gathered in a zip-file, which is then signed, seems to be discouraged in particular since this approach poses challenges on archival of such “signed documents”.

5.7.2 Approach Cover Letter Signed

In this approach only the main document of a tender (or other business documents) is signed while attachments go unsigned. There seems to be some use of this approach, which technically is very similar to the “all documents signed” case.

5.7.3 Approach Document with Hash Values Signed

This approach is an option in the Norwegian, public e-tendering solution. The e-tender platform creates a document consisting of identification and hash values of all documents constituting the tender, and this document is in turn signed by the economic operator. (In the Norwegian approach it is even possible to print this document and sign it by hand.)

While clearly a simplified approach at signing all documents, this solution will not be tested in PEPPOL.

5.7.4 Approach Authentication, Simple e-Signature

According to the IDABC Study [IDABC01] two Member States (Finland, Estonia) accepts simple electronic signatures for tendering. The economic operator has to log on to the tender management system using an eID of sufficient strength (may be an eID at qualified level). Documents can then be uploaded. Submission is done by an explicit “submit” action. The link through logs of authentication, the documents, and the explicit submit action is regarded as an e-signature (but not advanced).

Authentication has the value of an electronic signature (art. 5.2 of the E-signature Directive [EU01]). In most Member States, such an approach can only be used at intermediate steps of processes. At defined steps, advanced/qualified e-signatures will be required.

Example Italian CONSIP eTender – Ministry of Economy and Finance
Q. In which phases of the eProcurement process (e.g. notification, tendering, awarding, etc.) is there a need for signatures?
A. For the registration procedure and the final offering. During tendering the bidder is required to insert a Personal Identification Number (PIN) to meet the non repudiation of data. The PIN is chosen by the bidder during registration. It is valid for 90 days and the bidder can renew it.

The Public Procurement Directives [EU02] [EU03] state that neither signatures nor encryption shall be used by economic operators unless they are invited to do so by the awarding authority. Thus, when submitting a tender in e.g. Finland, in principle an Italian economic operator should not sign the tender. In reality, the Italian economic operator may insist on signing the tender, and it may be argued that according to the e-Signature Directive [EU01] the Finnish awarding authority will be obliged to accept this if the signature is qualified.

PEPPOL WP1 will only work on advanced e-signatures. Interoperability of authentication solutions is out of scope[7].

5.7.5 One signature

One signature is used when documents need to be signed only by one of the parties, and only one signature is needed from this party. This is the usual case when documents bind only one party (tender, order, invoice), while multiple signatures are needed when several parties are involved (tender by consortium, contract on awarding).

The signature (this applies also to multiple signatures) may be done in “attached” or “detached” (external signature) form. The most widely used is the attached form, providing a self consistent object containing also the signature. A document with a detached signature can be viewed as two separate objects, document and signature, where the document is unchanged even if the signature is removed. This is typically used in document flow applications (e.g. document flow using XML signature).

5.7.6 Multiple signatures

A previously signed document may be re-signed in principle in three different ways:

- The new signature is done over a data set made by data and previous signature(s) (sequential signature);
- The new signature covers the data set only, meaning signatures are at the same level (parallel signature);
- The new signature covers old signature(s) only, the latter signature attesting to the first signature only and not to the content of the document (countersignature).

Sequential signature is simply a signature where signed data are formed by data already signed. Sequential signature is therefore supported by any verification software which is able to verify a signature. To be noted is that data signed n times need n verification processes to be displayed. Deleting a signature (except for the last) invalidates signatures applied later in the sequence.

Parallel signatures are all affixed to data (information contained into the document), not against previous signature(s). Deleting a signature does not invalidate the others. This type of signature is

[7] The STORK project will address authentication, see http://www.eid-stork.eu

generally preferred because there is not any hierarchy in signatures. Moreover signed data are directly available even without performing the verification process.

Countersignature is a signature of a signature or of another countersignature. It is possible to delete a countersignature without invalidating the previous signature. Even though the countersignature has a natural place in many processes (attesting to a signature), it is not widely used.

Example Italian CONSIP eTender – Ministry of Economy and Finance
Q. Is there a need for multiple signatures (parallel, sequential)?
A. Sequential multiple signatures are already used for the final offering in some cases of consortium of multiple parties

PEPPOL needs to support multiple signatures. While in principle all three alternatives should be supported, use of countersignatures may create interoperability problems due to lack of support in software products (both for signing and verification).

For pilots a reasonable compromise is to accept sequential or parallel signatures on equal terms without delving into the in principle different semantics of the three alternatives.

6 Signature Validation Policy

6.1 Introduction

The elements of a signature validation policy in the PEPPOL case are as stated in 3.4 above:

- Signer requirements are kept at a minimum apart from adherence to CA policy and quality requirements. The signer may be required to produce certain signature formats.
- Requirements for the verification process performed by the receiver should be stated.
- Quality requirements and approval status (in particular qualified or not) of eIDs and signatures should be assessed.
- Quality requirements for cryptography (hash and public key algorithms and key length) should be assessed.

These elements are outlined in the following.

6.2 Signer Requirements, Signature Formats

6.2.1 Signature Format and Quality Requirements

A clear recommendation from PEPPOL is to impose few requirements on the signer (sender of a signed document). The signer must be able to fulfil the quality requirements of the receiver (see 6.4) with respect to eID and cryptography.

PEPPOL recommends flexibility with respect to signature formats although this places more demands on the receiver's ability to handle multiple formats.

For post-award procedures, which in PEPPOL imply exchange of structured XML documents between the systems of the actors, there is really no alternative to XML DSIG [RFC3275]. The only discussion point is the possible addition of further information to comply with some XAdES [ETSI-101-903] profile. For a start, it is reasonable to require only the XML DSIG and leave construction of XAdES SDOs (Signed Data Object) to the receiver. The use of CMS/PKCS#7 [RFC3852] [RFC2315] is not recommended but pilots may in practice have to support this if it turns out that there is too limited software support for XML DSIG.

For tendering the situation is more complex. While a desired situation would be XML DSIG for documents in XML format and PDF signatures [PDF(v1.6)] for documents in text format, the real situation is that CMS/PKCS#7 will have to be accepted. One reason is that signed PDF requires documents to be in PDF format (which may not be desired) and it requires the signer to possess commercial PDF software. For XML DSIG, the same considerations as for post-award procedures apply. It may be desirable to require XAdES or CAdES [ETSI-101-733] formats but a safe approach is to leave the requirements for pilots to the simple variants and construct such structures only at the receiving side.

Correspondingly, external time stamps (TSA) should not be required from the sender as their use would imply a need for XAdES or CAdES created by the sender.

PEPPOL requires signature formats to include signing certificates. End user certificates or full path are both allowed. (While this is common practice, in theory it is an option for most signature formats, the alternative being just a certificate reference in the form of issuer name and serial number.)

6.3 Receiver Requirements

6.3.1 Introduction

In PEPPOL's approach, few strict requirements are imposed on the signer/sender. This raises higher requirements for flexibility on the verification/receiver side. This is where the complexity is faced.

A receiver may handle all verification on its own or it may rely on trusted, external services (technical services or authorities) as described in D1.1 part 4. Trusted services described in D1.1 are eID validation services (XKMS v2 interface, D1.1 part 5), signature verification services (OASIS DSS, D1.1 part 6), and TSL distribution services (Trust Status List, see D1.1 part 4). Additionally, TSA (Time Stamp Authority) services may be used as described in 6.3.4.4.

In the following, requirements imposed on the receiver of a signed document are outlined. It is recommended to outsource parts of the processing to trusted services.

6.3.2 Signature Verification Process

The signature verification process needs to perform:

- Cryptographic verification of the e-signature, repeated if multiple signatures on document;
- This includes validation of all eID certificates used (see 6.3.3);
- Verification of Signature Validation Policy adherence;
- Validation of the certificate of the CA issuing the subscriber's certificate as discussed below.

A verification process may end positive today but not tomorrow, depending on the expiry date and the revocation status of the certificate. It must be made clear if signatures are verified relatively to current time or to time of receiving the signed document (or time of signing), see 3.3 above.

Since PEPPOL does not recommend use of TSA time stamps obtained by the signer, there is no requirement for the receiver to be able to process such time stamps (although this may be done).

In any case, the result of a verification process must be logged with the verification time as part of the information. The system clock or a TSA may be used depending on local requirements.

The output status of a verification process is usually:

- Valid – passed cryptographic verification, depending on the semantics this may also imply that the signature policy is fulfilled;
- Invalid – meaning that something is wrong in the processing (signature format, eID, integrity check etc.), depending on semantics this may also be the status if signature policy is not fulfilled;
- Incomplete – meaning that validation has not failed but insufficient information is available to complete the process, e.g. OCSP responder or CRL distribution point is not reachable.

In case of incomplete validation, it may be possible to request a repeated signature validation, as soon as additional validation information has become available. Also, in the case of incomplete validation, additional information may be made available to the application or user in alternative ways, thus allowing the application or user to decide what to do with partially correct electronic signatures.

PEPPOL (see D1.1 part 6) proposes to add the following status:

- Insufficient quality – verification valid but signature policy rules are not fulfilled.

Adding this status clearly separates the valid/invalid decisions from the signature policy decisions. This enables for example raising an exception in the case of insufficient quality to trigger a manual process evaluation on whether or not the signature should still be accepted.

Output status should be indicated for each signature individually and as an aggregate value. The aggregate shall be in order of evaluation:

- Invalid if one or more signatures are invalid;
- Insufficient quality if one or more signatures have this status;
- Incomplete if one or more signatures have this status; and
- Valid only if all signatures are valid.

In addition to the status, various reason codes can be used in particular in case of invalid results. This is described in D1.1 parts 5 and 6.

6.3.3 Certificate Validation Process

6.3.3.1 The Process

The process to be done for complete validation of an eID certificate is as follows:

- Parsing and syntax checking of the certificate and its contents, including some semantic checking like use of certificate compared to allowed use (key usage settings) and presence of mandatory fields and critical extensions.
- Assessment of the risk implied by accepting the certificate, determined by trustworthiness of the CA's, the quality of the certificate, and the liability situation, relatively to the operation in question.
- Validation of the CA's signature on the certificate. This requires a trusted copy of the CA's own public key, either directly available, or obtained from further certificates in a certificate path.
- A check that the certificate is within its validity period, given by timestamps in the certificate. For real-time checking, this must be compared against the current time. For old, signed documents, it is the time of signing (or time of receiving the signed document) that is of interest.
- A check that the certificate is not revoked, i.e. declared invalid by the CA before the end of the validity period. For real-time checking, the current revocation status is checked. For old, signed documents, status at the time of signing (or time of receiving) is checked.
- Semantic processing of the certificate content, extracting information that shall be used either for presentation in a user interface or as parameters for further processing by programs. The name (or names) in the certificate and interpretation of naming attributes are particularly important.
- In the case of certificate paths, this processing must be repeated for each certificate in the path up to a trusted root-CA.

Syntactic parsing and checking of validity period are usually straightforward operations. All other steps in the certificate processing more or less have problems related to scaling, i.e. handling of certificates from a high number of CAs and in particular when CAs are from different countries.

It is essential that if a validated certificate contains a critical extension, whose meaning is unknown, it must not be accepted (state: incomplete).

Requirements for use of certificate paths may vary, e.g. path processing is not allowed in Italy (all CAs must have their own root certificate), while path processing may be required in Germany up to the common, national root for issuers of qualified certificates.

PEPPOL's requirement is that path processing should be supported but if trust in the CA's certificate can be established directly, then path processing is only required if national rules dictate this.

6.3.3.2 Certificate Content

The X.509v3 standard defines syntax of certificates, but leaves many options, and only partly defines semantics of fields, attributes and extensions. Even though recommended profiles for X.509 certificates exist, certificates from different CAs often differ in content. This particularly applies to naming of subjects. A study of certificates in use in Europe will reveal a wide variety of encoding of names and attributes such as unique identifiers.

The eID and e-signature action plan [COMM-02] suggests establishing profiles for qualified certificates. However, even if a common profile was established today, the eID issuers must be allowed as a minimum a full life cycle of their eID products to implement this (certificate validity is usually 2-3 years before renewal is needed). Thus, for the PEPPOL pilots the requirement is to handle the certificates available in the market.

PEPPOL recommends two actions but the project will not initiate own work on certificate profiles:

- Establish common European profiles for certificates and in particular for encoding of names.
- Establish the same profile as an XML and/or ASN.1 structure to enable mapping of the different naming schemes of the eID issuers to a common structure (one mapping per eID issuer).

Such mapping can then be done by identity providers, validation services or even by local implementation if software for the mapping is made available.

A validation solution shall not pose requirements on certificate content apart from those that follow from adherence to standards.

A validation solution must return sufficient information to uniquely identify the certificate (issuer name and certificate serial number) and must return the subject name in the certificate. If the receiver is able to process certificate content, then this information is directly available.

A receiver must either be able to use (parts of) names in a certificate directly for identification, or a name in a certificate must be reliably translated to a derived name that is useful to the receiver. The security/quality of the translation process must preserve the quality of the certificate, i.e. the confidence in the derived name must be as if the derived name had been included in the certificate.

A particular issue for cross-border use of eID is that there is no pan-European linking of different national identifiers for persons. A receiver cannot require national identifiers to be present in foreign certificates and should be able to accept certificates without such identifiers or with identifiers that are unknown.

6.3.3.3 Visualization of Signature Verification Results

If signature validation results are presented to a human user, the following should be noted. Annex IV of the e-Signature Directive [EU-01] describes recommendations for a secure signature validation. It should be ensured with reasonable certainty that:

- the signature is reliably verified and the result of that verification is correctly displayed (status as indicated above);
- the authenticity and validity of the certificate required at the time of signature verification are reliably verified;
- the result of verification and the signatory's identity are correctly displayed;
- the use of a pseudonym is clearly indicated.

In the validation protocol it has to be clarified, which information on validation refer to which signed content. Adherence to the signature validation policy in force should also be displayed.

Visualization and display should adhere to the requirements on accessibility as defined by the Web Content Accessibility Guidelines of the World Wide Web Consortium (universal access).

Above all, the user must be provided with sufficient information on the context and for navigation. The mechanisms for navigation have to be clear and coherent. As the content is very technical, adequate means like help texts should be used.

6.3.3.4 Visualization of Certificate Content

Annex I of [EU-01] defines requirements for qualified certificates, which must contain:

a) an indication that the certificate is issued as a qualified certificate;

b) the identification of the certification-service-provider and the State in which it is established;

c) the name of the signatory or a pseudonym, which shall be identified as such;

d) provision for a specific attribute of the signatory to be included if relevant, depending on the purpose for which the certificate is intended;

e) signature-verification data which correspond to signature-creation data under the control of the signatory;

f) an indication of the beginning and end of the period of validity of the certificate;

g) the identity code of the certificate;

h) the advanced electronic signature of the certification-service-provider issuing it;

i) limitations on the scope of use of the certificate, if applicable; and

j) limits on the value of transactions for which the certificate can be used, if applicable.

From a legal perspective it must be assured that at least the data in the verification process can be displayed for each validated user certificate. Following the X509v3 standard (and the [RFC5280] profile), all critical extensions have to be displayed. If necessary, the whole certificate content is to be reported, at least when the text is displayed.

6.3.3.5 Automated Processing of Validation Data

The signature verification process (“validation protocol”) must be an integral part of the e-procurement process. The common goal is to ensure the integrity and authentication and authorization implied by a signed document.

It is intrinsic to many e-procurement processes that the processing of validation data should be automated. Therefore the validation data should be accessible in a machine-readable format such as XML and should be highly standardized to ease the effort of implementation. The XKMS and OASIS DSS specifications in D1.1 parts 5 and 6 specifically target this goal.

The verification process includes typically three steps:

1. Validation

The first thing to do is obviously to generate the validation data by validating the signature(s) and accompanying eID(s).

2. Drawing conclusions

Based of the validation data various conclusions can be made automatically, e.g.

- If the validation data yields a “valid” result, then the e-procurement document (that was signed) may be processed further by the receiving system.

- If the validation data yields “invalid” or “insufficient quality”, the e-procurement document may be discarded; however this should also generate an error message to the sender (reliable protocol). Another alternative is to notify a human operator.
- If the validation data yields “incomplete”, the validation can be automatically retried at a later stage, or a human operator can be notified. If a configured number of retries are unsuccessful, then a human operator must be notified.

3. Archiving

The archiving (see 6.3.6) of the validation data is essential due to legal requirements. If the data is not stored at all or is stored without a relation to the e-procurement documents, it is impossible to prove the signature validity at a later point in time. Archival should be an automated process.

6.3.4 Interfaces and Protocols

6.3.4.1 External Interfaces towards CAs

As for names in certificates, PEPPOL is in the time frame of the pilots required to accept present service offers of the CAs. PEPPOL thus imposes only the following minimum requirements to CAs:

- An OCSP interface for revocation checking and/or a CRL distribution point (preferably both) must be available to validation services and preferably publicly available.
- The CA’s own root certificate must be available to validation services and preferably publicly available in a trusted way.
- The CA must have a published certificate policy that is adhered to.

OCSP and CRL download are the only two interfaces that can be assumed to be exposed by a CA. If interfacing directly to CAs, an actor needs trusted copies of all CA public keys and must know where to obtain the OCSP interface or a CRL (this can be conveyed by certificate extensions but it is a bit too optimistic to rely on this to always work). The certificate policy is needed to be able to assess quality of the eIDs. A TSL can be used to improve the situation.

PEPPOL requires signed documents to have signing certificates attached and thus does not require that a CA needs to have (LDAP or other) directory services for certificates. If available, it is of course allowed to use directories or more advanced interfaces like SCVP [RFC5055] or XKMS [XKMS].

6.3.4.2 Validation Interfaces

More argued elsewhere in D.1.1 (in particular parts 5 and 6), PEPPOL needs richer validation interfaces than bare OCSP or CRL. PEPPOL will make available certificate validation services offering an XKMS v2 interface as described in D1.1 part 5. PEPPOL may also make available signature verification services offering an OASIS DSS interface as described in D1.1 part 6.

A receiver should be able to use such interfaces unless it performs all validation locally. Trust models for validation are presented in D1.1 part 4.

An alternative protocol could be SCVP [RFC5055]. There are two reasons for not choosing this protocol:

- There is very limited software support available;
- Use of XML-based protocols such as XKMS and OASIS DSS fits much better with the general service oriented approach taken by PEPPOL.

6.3.4.3 Trust Status List Interface

TSLs consisting of issuers of qualified certificates will be made available in humanly readable form (to be configured into systems by local effort) and preferably also in machine readable form. The protocol and interface is not yet defined; this is a topic addressed by the Services Directive pilot[8]. Interface for human readable version may be just a web GUI.

TSLs are further described in D1.1 part 4. See also [SEALED01].

6.3.4.4 Time Stamp Authority Interface

This interface shall follow the Time Stamp Protocol specified by [RFC3161].

Trust models for TSAs are not further described in D1.1. It is assumed that the receiver calls a well-known TSA when needed. See however D1.1 part 4, chapter 7 and appendix 2.

If a time stamp by a TSA is included in an SDO 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 since in most countries a qualified certificate can only be issued to a physical person;
- Is able to judge the semantics implied by the time stamp.

A TSA will usually have its own root certificate (in Italy this is a requirement). Thus, a TSA may well be included in a TSL.

If an external validation service is used for the entire signature verification (OASIS DSS approach), 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.

6.3.5 Time Stamps

Time stamps are important in procurement processes. Since no requirement (meaning this is optional) is imposed on the sender to supply time stamps, the requirements are on the receiver. The receiver must time stamp all events and all validation processes. Each time stamp must have defined semantics, such as time of sending, time of reception etc.

If the sender supplies time stamps, these should only be trusted by the receiver following a thorough evaluation, or if they are supplied by a TSA known by the receiver. D1.1 part 4 has more information on the issue of trusted time and TSA, notably also an appendix on the subject.

The receiving side will typically obtain time stamps (from TSA or system clock whatever is considered necessary – note that e.g. in Italy a TSA time stamp is required) to embed in more elaborate SDO structures such as XAdES or CAdES or in archival records for the signed documents. This is considered outside the scope of PEPPOL (see next section).

PEPPOL is not aware of any formal requirement for use of TSAs on the sending side of procurement processes.

[8] SPOCS – Simple Procedures Online for Crossborder Services

6.3.6 Logging, Archival, Records Creation

The e-procurement systems must perform sufficient, reliable logging of events, including time of events, e.g. sending or receiving a message, establishing a communication channel for the transfer etc. This may involve operating system logs and logging in the e-procurement systems or other business software. Logging may be sufficient to trace events during the business process execution and shortly afterwards. However, trying to solve retention requirements such as those imposed by the public procurement Directives [EU-02] [EU-03] (typically 10 years) by retaining logs is not advisable. At some point the (original) documents must be preserved as archival records with the necessary time information and validation information as metadata.

In archive records, time stamps are associated to documents as metadata. Records may be used in the execution of a business process, or be created at a later stage based on logs and other information collected during the process. An example of a record structure is a signed data object (SDO) such as XAdES [ETSI-101-903] or CAdES [ETSI-101-733] archive formats.

Long term archival as such, and specifically use of “advanced” archival formats of XAdES and CAdES, will not be addressed by PEPPOL, being defined as a local matter to the receiving e-procurement system. But the solutions piloted must ensure that sufficient information is gathered and retained in a reliable and authentic way in order to enable creation of archive records.

The concept of “original electronic document” may be interpreted differently in different jurisdictions. Does this mean archival of the exact bit stream received, or can operations such as format conversion be carried out? For electronic signatures, three strategies are possible:

1. Archive documents unchanged with signatures intact;
2. Remove signatures but record verification traces as metadata;
3. Remove and forget signatures, essentially using them for integrity protection only.

The first alternative may be mandated by national jurisdiction (e.g. Belgium [Dekeyser]) but causes problems [Olnes-Seip] with respect to: Format obsolescence (continued support for document format, signature format, SDO format, and certificate format), cryptographic algorithm obsolescence (keys and algorithms weakened over time, old algorithms no longer supported or no longer secure), capture and reconstruction of state at time of signing, and possibly also existence of actors that one relies upon for verification.

Chemical Industry Data Exchange (CIDX) has surveyed requirements for e-invoicing [CIDX], summing up country specific archiving requirements in a table. This table indicates requirements across EU for storage period (varies from 4/5 to 10 years – ultimately 20 years in Switzerland), format received or format issued to be archived (in some cases both, probably meaning that they should be the same), requirements to store signatures (all countries require this but details, refer alternatives 1 and 2 above, are not known), and requirements for full on-line access to archive (all but 8 countries).

The main strategy today for long-term storage of signed documents is to capture sufficient state information (verification information) as metadata in the SDO (XAdES/CAdES). An alternative approach is to ensure that the state information (such as CRLs) is stored separately in a trusted way and referred to by the SDO. In any case, trusted time stamps are needed. To avoid placing requirements on the sender, PEPPOL requires archival records and “advanced” SDOs to be constructed on the receiving side. If a TSA time stamp is required, this shall be obtained by the receiver.

Verification in retrospect of an archival SDO is usually done by verifying the outer (archival) signature only. This signature is then trusted to attest to the correctness of the other information in the SDO; that this information was checked and found to be correct at the time when the outer signature was made. In principle, all other information in the SDO may also be verified but the process may be more or less

cumbersome. Several software products, including the Governikus platform used in Germany, support processing of such SDOs.

A validation service may support “historical verification and validation”, i.e. verification of a signed document or validation of an eID relatively to either a time indicated in the request or to time stamps in the SDO submitted in the request. In order to achieve this, the validation service must either rely on revocation information (OCSP response or CRL) mediated in the SDO, or it must have access to old CRLs (a CRL archive) for the CAs in question. Note that reliance on external actors (such as a validation service or a CA) for long-term verification/validation implies a risk since the external actor may go out of business or change its service offering. This must be weighted against the simplifications obtained by use of such actors.

Another approach to long term archival is specified by [RFC4998]. Here, a hash tree is constructed starting from hash values of the SDOs (or other leaf nodes) in a way that allows easy maintenance while still providing sufficient tamper detection.

6.4 Quality Requirements and Approval Status

6.4.1 Present Status

Quality and approval requirements vary significantly across member states for e-procurement. IDABC [IDABC01] finds 15 countries with e-procurement services for tendering in operation, where 6 require qualified signatures, 7 require advanced signatures (sometimes with the additional requirement of a qualified eID), while two countries require only authentication. The services furthermore either list one or a few eID issuers or are able to accept all domestic issuers and perhaps a few foreign issuers.

Correspondingly, CIDX (Chemical Industry Data Exchange) has surveyed requirements for signatures on e-invoices [CIDX], finding 11 countries requiring qualified signatures for e-invoices; the rest presumably then accepting other signatures although requirements are not explicitly stated.

PEPPOL must consider also voluntary, national accreditation schemes that exist in many countries in addition to registration as qualified. These are strongly related to national laws and for this reason it is practically infeasible for eID issuers to declare conformance with specific national requirements in a lot of different countries. PEPPOL’s recommendation is that such accreditations schemes are either abandoned or kept at a national level, where requirements are not imposed on eID issuers registered in other countries.

In PEPPOL’s view, differences in national legislation as well as different requirements for different e-procurement processes necessitate development of a framework to enable specification of the crucial elements of signature policies. The specification must provide non-discriminatory rules for acceptance of eIDs to replace present policies for national solutions, which refer to domestic issuers or national accreditation schemes.

As a part of the quality requirements, quality profiles for eID issuers and their certificate policies shall be developed. To determine if an eID fulfils quality requirements, the issuer and its policy must be assessed towards the corresponding quality profile. This is described in D1.1 Part 7.

For complex tenders one will usually measure all signatures from all parties towards the same signature policy; however signatures from time stamping authorities and issuers of certificates and attestations [Siemens] may need to be addressed separately; these cannot in general be qualified signatures since they are not applied by natural persons.

6.4.2 eID Quality and Assurance Level

6.4.2.1 Requirements

We can consider that the goal described in REC03 of the IDABC study [IDABC01] to be one of the most important for PEPPOL. In particular:

"Application owners should be advised to shift from the current situation of ad hoc decisions for each application, to a system where they require their users to employ a certain security/reliability level, such as the appropriate legal classification under the eSignatures Directive, rather than a specific certificate or CSP".

The eID and e-signature action plan [COMM-02] recommends as an "easy win" to emphasise two alternatives:

- Qualified signatures;
- Advanced signatures using qualified certificates (i.e. no SSCD used).

Assuming that both alternatives use proper strength cryptography and otherwise offer sufficient quality, a first approach at quality requirements could be to distinguish only between these two.

6.4.2.2 Comprehensive Quality Assessment

However, one may need to consider non-qualified certificates, there may be a need to assess sufficient quality even for qualified solutions, and there is a need to be able to incorporate non-European certificates ("qualified" is a European concept). A more comprehensive quality classification system is described in part 7 of D1.1. Certificate quality is defined as follows:

0. Very low or non-determined level: Very low confidence or assessment not possible, usually because a certificate policy does not exist.

1. Low level: Low confidence in certificate but certificate policy exists or quality assessment is possible by other means.

2. Medium level: Certificates governed by a Certificate Policy in compliance with the ETSI TS 102 042 standard for LCP or a similar standard.

3. High level: Certificates governed by a Certificate Policy in compliance with the ETSI TS 102 042 standard for NCP or a similar standard.

4. High level +: Certificates governed by a Certificate Policy in compliance with the ETSI TS 102 042 standard for NCP+ or a similar standard. (Use of a SSCD is mandated in the CP.)

5. Very high level: Certificates governed by a Certificate Policy in compliance with the ETSI TS 101 456 standard for QCP or a similar standard.

6. Very high level +: Certificates governed by a Certificate Policy in compliance with the ETSI TS 101 456 standard for QCP+ or a similar standard. (Use of a SSCD is mandated in the CP. Thus, this level supports qualified signatures according to the EU Directive on electronic signatures.)

LCP = Lightweight Certificate Policy
NCP = Normalized Certificate Policy
QCP = Qualified Certificate Policy
SSCD = Secure Signature Creation Device

The "or similar standard" clauses allow later inclusion of non-European eIDs. An annex to D1.1 part 7 shows a mapping from US Federal Bridge policies to the system. Note that it is suggested to assess quality and approval status / assurance level independently. Thus, a certificate may end up as quality 6 even if it is not marked as qualified – provided that the QCP+ requirements are fulfilled.

6.4.2.3 Assurance Level, Approval Status

The approval status / assurance level of a certificate can be classified as follows (see D1.1 part 7):

0. No independent assurance: self assessment only.

1. Independent document review: Statement of compliance issued by an independent external unit based on document review only.

2. Internal compliance audit: Internal audit carried out periodically concludes compliance to applicable requirements.

3. Supervision without compliance audit: CA is supervised by a public national or international authority according to applicable law to the issuer.

4. External compliance audit: Audit carried out periodically by external independent auditors concludes compliance to applicable requirements.

5. External compliance audit and certification: Audit carried out periodically by external independent auditors concludes compliance to applicable requirements. CA operations are certified in accordance with a relevant standard; OR cross certification with a relevant bridge CA has been made; OR the CA has obtained membership in a PKI hierarchy as a result of appropriate assessment.

> *Note:* Relevant standards include ETSI TS101 456, ETSI TS 102 042, WebTrust Program for CAs, tScheme Approval Profile for CAs, ISO9001, ISO27001.

6. Supervision with external compliance audit: Audit carried out periodically by external independent auditors concludes compliance to applicable requirements. CA is supervised by a public national or international authority according to applicable law to the issuer.

7. Accreditation with external compliance audit: Audit carried out periodically by external independent auditors concludes compliance to applicable requirements. CA is accredited by a public national or international authority according to applicable law to the issuer.

> *Comment:* Supervision and/or accreditation by a public international authority (levels 3, 6 and 7) is not relevant at present, but will become relevant in the future if international schemes for such supervision/accreditation are established, e.g. by the EU Commission.

In this scheme, qualified certificates have assurance levels 6 or 7 depending on whether supervision or accreditation scheme is selected by the country in question. This scheme then extends the assurance level to other schemes and other methods than qualified levels.

Note also that non-qualified certificates may have a national approval status indicating levels 6 or 7.

Certificate quality is then indicated as {quality, assurance}. Examples:

- {5, 6} is a qualified certificate with no SSCD (not qualified signature), issuer under supervision.
- {6, 7} is a qualified certificate with SSCD (QC), issuer accredited.

6.4.3 Cryptographic Quality

Adapted from US recommendations [NIST] that seem to be agreed to by most European countries as well, quality classification of cryptographic algorithms can be mediated as follows:

Quality 0: Inadequate – should not be trusted.

Quality 1: Reasonably secure for 3 years.

Quality 2: Regarded as trustworthy for 5-10 years.

Quality 3-5: Increasing levels of security.

There seem to be agreed judgements about which algorithms should go in which classes. This assumes no inherent (undetected) weakness in the algorithms and no implementation flaws. Examples of algorithm classifications are:

- Hash algorithms: MD5 = 0, SHA-1 = 1, SHA-224/256/384/512 = 2/3/4/5.
- Public key algorithms with key lengths: RSA-1024 = 1; RSA-2048 = 2; RSA-4096 = 4.

6.4.4 Signature Quality

Excluding implementation issues of signing software and hardware, the quality of a signature consists of the three parameters: eID quality (in the scheme described in this document consisting of the two parameters quality and assurance level), hash quality, public key quality.

Each of these parameters should be above a certain quality for the signature to be accepted; this should be defined in the signature policy. The signature policy should normally not refer to specific algorithms, only to quality parameters.

The PEPPOL profile for digital signatures is then defined by the following parameters:

- **eID quality**, consisting of a certificate quality parameter ranging from 0 to 6 and an independent assurance parameter ranging from 0 to 7,
- **Hash quality**, ranging from 0 to 5,
- **Public key quality**, ranging from 0 to 5.

PEPPOL suggests a notation for the signature quality as follows

Signature quality = {eID quality, hash quality, public key quality}

= {(certificate quality, independent assurance), hash quality, public key quality}

By way of example, a qualified signature created by a qualified certificate issued by an accredited CA and using the SHA-224 hash algorithm and a cryptographic key length of 2048, would have signature quality parameters as follows:

- **eID quality:** (6,7) – meaning certificate quality level 6 and independent assurance level 7
- **Hash quality:** 2 – regarded as trustworthy for 5-10 years
- **Public key quality:** 2 – regarded as trustworthy for 5-10 years

With the notation suggested above, this signature example would have a signature quality:

signature quality = {(6,7),2,2}

6.4.5 Quality of the Actor Issuing an eID

If desired, quality requirements may be imposed on the actor running an eID issuing service, such as:

- Financial strength (will it survive and can it face liability claims),
- Insurance coverage,
- Owners and organization structure (may include judgements about independence with respect to third party roles),
- Market penetration (number of eIDs and their usage frequency),
- Company reputation,
- Competence and knowledge,
- Processes and procedures (including issues like ISO9001, ISO27001 and other certifications),

- Infrastructure.

Such requirements are considered out of scope of PEPPOL.

7 Conclusions

Based on the requirements outlined in this document, signature policies that enable cross-border use of e-signatures can be defined. Most requirements described are imposed on the receiver of a signed document (signature validation policy), who in turn may “outsource” parts of the processing to validation services.

In the first run, emphasis should be put on two alternatives:

- Qualified signatures;
- Advanced (non-qualified) signatures using qualified eIDs.

Since qualified signatures can be assumed to be in use in only about half the Member States, this requirement may be viewed as too strict. Qualified eIDs are available in almost all Member States.

Use of the quality classification system presented in D1.1 part 7 will give more information as basis for signature acceptance decisions.

For business processes, it is necessary to specify which documents that shall be signed and at which stages of the protocol. It is also necessary to specify what signatures mean in terms of authorizations and commitments, linking personal signatures to roles and authorizations.

Few requirements are imposed on the signer/sender. This is a pragmatic choice since making too many assumptions about the functionality of the signer’s software may lead to requirements that are difficult to fulfil in the time frame of PEPPOL’s pilots.

8 References

[CIDX] Chemical Industry Data Exchange, White Paper, EU Compliant Digital Signatures, 2008. http://75.43.29.149/Portals/0/Publications/CIDX_EU_Compliant_Digital_Signatures_2008-11-12.pdf

[COMM01] Commission of the European Communities: Requirements for Conducting Public Procurement Using Electronic Means under the New Public Procurement Directives 2004/18/EC and 2004/17/EC. Commission staff working document, 2005.

[COMM-02] 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

[Dekeyser] Hannelore Dekeyser, Preservation of Signed Electronic Records. DLM Conference, Budapest, 2005.

[EDYN] European Dynamics SA, Functional Requirements for Conducting Electronic Public Procurement under the EU Framework (Volume 1 and 2). January 2005. http://ec.europa.eu/idabc/servlets/Doc?id=22191 and http://ec.europa.eu/idabc/servlets/Doc?id=22192

[ETSI-102-038] ETSI TR 102 038 V.1.1.1 (2002-04) Electronic Signature and Infrastructure (ESI) – XML Format for Signature Policies.

[ETSI-102-041] ETSI TR 102 041 V.1.1.1 (2002-02) Electronic Signature and Infrastructure (ESI) – Signature Policies Report.

[ETSI-102-045] ETSI TR 102 045 V.1.1.1 (2003-03) Electronic Signature and Infrastructure (ESI) – Signature Policy for Extended Business Model

[ETSI-102-272] ETSI TR 102 272 V.1.1.1 (2003-12) Electronic Signature and Infrastructure (ESI) – ASN.1 Format for Signature Policies.

[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, 1999.

[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, 2004.

[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, 2004.

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

[NIST] B. Burr: NIST Cryptographic Standards Status Report, April 2006, http://middleware.internet2.edu/pki06/proceedings/burr-nist_crypto_standards.ppt

[Olnes-Seip] Jon Ølnes and Anne Karen Seip, On Long Term Storage of Digitally Signed Documents. Second IFIP Conference on e-Commerce, e-Business, e-Government (I3E), Lisboa, 2002.

[PDF(v1.6)] Adobe Systems Inc., PDF Reference – Fifth Edition – Adobe Portable Document Format Version 1.6. http://partners.adobe.com/public/developer/en/pdf/PDFReference16.pdf 2004.

[RFC2315] B.Kaliski, PKCS#7: Cryptographic Message Syntax Standard - Version 1.5, RFC2315, http://www.ietf.org/rfc/rfc2315.txt 1998.

[RFC1521] N.Borenstein, N.Freed. MIME (Multipurpose Internet Mail Extensions) Part One: Mechanisms for Specifying and Describing the Format of Internet Message Bodies. RFC1521. http://www.ietf.org/rfc/rfc1521.txt 1993.

[RFC1847] J.Galvin, S.Murphy, S.Crocker, N.Freed. Security Multiparts for MIME: Multipart/Signed and Multipart/Encrypted. RFC1847. http://www.ietf.org/rfc/rfc1847.txt 1995.

[RFC2632] B. Ramsdell, S/MIME Version 3 Certificate Handling. RFC2632. http://www.ietf.org/rfc/rfc2632.txt 1999.

[RFC2633] B. RAMSDELL. S/MIME Version 3 Message Specification. RFC2633. http://www.ietf.org/rfc/rfc2633.txt 1999.

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

[RFC3275] D.Eastlake, J.Reagle, D.Solo, (Extensible Markup Language) XML-Signature Syntax and Processing, RFC3275. http://www.ietf.org/rfc/rfc3275.txt 2002.

[RFC3852] R. Housley. Cryptographic Message Syntax (CMS). RFC3852 http://www.ietf.org/rfc/rfc3852.txt 2004.

[RFC4998] T.Gondrom, R.Brandner, U.Pordesch, Evidence Record Syntax (ERS). RFC4998, http://www.ietf.org/rfc/rfc4998.txt 2007.

[RFC5055] T.Freeman, R.Housley, A.Malpani, D.Cooper, W.Polk, Server-Based Certificate Validation Protocol (SCVP), RFC5055 http://www.ietf.org/rfc/rfc5055.txt 2007.

[RFC5280] D.Cooper, S.Santesson, S.Farrell, S.Boeyen, R.Housley, W.Polk, Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile, RFC5280 http://www.ietf.org/rfc/rfc5280.txt 2008.

[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

[XKMS] XML Key Management Specification (XKMS 2.0) Version 2.0, W3C Recommendation, http://www.w3.org/TR/2005/REC-xkms2-20050628/ 2005.

[XPath] J.Clark, S.Derose, XML Path Language (XPath) Version 1.0. W3C Recommendation. http://www.w3.org/TR/1999/REC-xpath-19991116 1999.

[XSL] S.Adler, A.Bergl, J.Caruso, S.Deach, P.Grosso, E.Gutentag, A.Milowski, S.Parnell, J.Richman, S.Zilles, Extensible Stylesheet Language (XSL). W3C Proposed Recommendation. http://www.w3.org/TR/2001/PR-xsl-20010828/ 2001.

[XSLT] J.Clark, XSL Transforms (XSLT) Version 1.0. W3C Recommendation. http://www.w3.org/TR/1999/REC-xslt-19991116.html 1999.

9 Appendix 1: Signature Policy Template

9.1 Intellectual Property Rights

If appropriate, else it is simply stated that this is not relevant.

9.2 Foreword

This technical and organizational specification[9] has been produced by Pan European Procurement On Line (PEPPOL) WP1 (eSignature) expert group. It describes a format suitable for description of comprehensive signature policies and poses a first set of requirements for such policies.

9.3 Policy Maintenance

The PEPPOL policy is maintained by the PEPPOL Consortium by mean of WP1 expert group. This is the release v.1.0.

The document is published in http://www.peppol.eu/

9.4 Legal consideration

National laws have supreme value in national context, the present policy, in harmony with the spirit of the Service Directive and the eSignature Directive has value limited to the scope of the PEPPOL WP1 Pilot. Further developments and uses outside the present pilot need a general agreement of all Members State, but this is outside PEPPOL's scopes

9.5 Introduction

As indicated in [1] "*an important requirement of electronic commerce is the ability to identify the originator of electronic information in the same way that documents are signed using a hand-written signature*". This is realized using electronic signature, compliant to EU eSignature Directive [2], which is supported by a Certification Service Provider (CSP), so called Certification Authority (CA).

In the EU Member States, even in complete accordance to the eSignature Directive, private companies and Public Administrations have developed such certification services but adopted different (technical/organizational) signature solutions with a result of very low interoperability among them.

The Guidelines to Common Specifications for Cross Border use of Public eProcurement [3] documents states: "The lack of interoperability between the different national schemes for electronically signing tender documents is the single most important blocking factor to cross-border eProcurement". The vision of the PEPPOL project is that any company and in particular small and medium-sized enterprises (SMEs) in the EU can communicate electronically with any European governmental institution for the entire procurement process. One outcome of the PEPPOL project will be a set of guidelines, specifications and technical solutions to face this interoperability challenge.

[9] I.e. this appendix, which is written in a way that enables it to be used as basis for stand-alone documents later on. Note that for this reason, the appendix has its own reference list. Not all requirements described in the text of the main part of this document are at present translated into specific requirements.

9.6 Scope

Even though a simple electronic signature should be accepted (Article 5.2 of eSignature Directive), and there should not be any limitation that will interfere with the free circulation of goods and service among EU (Article 8 Service Directive [4]), in a ICT context it is barely impossible to open a service to all available solutions, so PEPPOL scope is to specify a minimum set of organizational/technical requirements that enable an acceptable level of interoperability.

The present document specifies these requirements to declare a CSP's policy and tools valid to participate in the PEPPOL eProcurement Pilot.

The requirements are defined in terms of:
- CSP's organizational status
- CPS's user identification policy
- Certificate fields
- Electronic Signature features
- eID security

9.7 Major Parties

Before starting to list the minimal requirements, it is necessary to give a short review on main parties involved in a electronic signature validation process, which are (see ETSI TS 101 733 [5]):
- the signer
- the verifier
- the Trust Service Providers

The signer, or the signers in case of multiple signatures, generates/e the document signature.

The verifier is the entity that validates the electronic signature; it may be a single entity or more entities.

The Trust Service Providers are one or more entities that help to build trust relationship among the signers and the verifier.

The Trust Service Providers that takes part on the actual process are:
- Certification Authorities
- Registration Authorities
- CRL Issuers
- OCSP Responders
- Signature Policy Issuers
- Validation Authorities

Certification Authorities provide keys, end-user (signer) certificates and revocation services.

Registration Authorities allow the identification and registration of entities before a CA issues a certificate.

CRL Issuers publish revocation/suspension status information about end-user certificates.

OCSP Responders publish end-user certificates status information.

Signature Policy Issuers define the signature policy to be used by signers and verifiers.

Validation Authorities provide validation information to verifiers that are not able to perform a validation by themselves.

9.8 Signature Policy

When in an electronic transaction a signature policy is declared both from the signer and the verifier, the result of the signature validation cannot be uncertain, but absolutely consistent and equally understood or interpreted by both the actors. In this case we will speak of “comprehensive” policy.

But in Europe where several electronic signature policies do exist, even though all legally equivalent, their technical equivalence and consequent interoperability are limited.

Thus the PEPPOL platform has to be open to these different policies but it has also to assure an unequivocal validation result. So the PEPPOL approach is to establish those minimal requirements and procedures, published, well known and accepted by the signer and the verifier, in the way that a verifier could receive an unique answer “under PEPPOL policy” corresponding to the signer’s intentions.

So the PEPPOL signature policy is intended to be a set of organisational/technical requirements that could be met by a particularly defined or existing electronic signature policy.

9.9 The PEPPOL policy requirements

9.9.1 Type of signature

The article 5.2 of the Directive 1999/93/EC of the European Parliament and of the Council of 13 December 1999 on a Community framework for electronic signatures [2] (eSignature Directive) states:

“*Member States shall ensure that an electronic signature is not denied legal effectiveness and admissibility as evidence in legal proceedings solely on the grounds that it is:*

- *in electronic form, or*
- *not based upon a qualified certificate, or*
- *not based upon a qualified certificate issued by an accredited certification-service-provider, or*
- *not created by a secure signature-creation device*.

The above article establishes a non-discriminatory principle for the free circulation of signed documents among MSs, recognizing their full legal effectiveness.

But the eSignature Directive, with this article, solves the interoperability question partly and only on a legal level leaving open all the technical/organisational issues regarding an applicative implementation.

The IDABC Study [6], but also the Questionnaire by Service Directive expert group [7] have shown that the kind of signature that is most recognized to be able to assure both the signer identity and the confidence on interoperability level is the Advanced Electronic Signature (AdES) as defined in the Article 2.2 of the eSignature Directive:

“an electronic signature which meets the following requirements:

a) it is uniquely linked to the signatory;

b) it is capable of identifying the signatory

c) it is created using means that the signatory can maintain under his sole control; and

d) it is linked to the data to which it relates in such a manner that any subsequent change of the data is detectable”.

Considering the available technology, we can fulfil the above requirements only using a Public Key Infrastructure (PKI) based on X.509v3 (RFC 3280 [11]) certificates.

REQ.1. A valid PEPPOL electronic signature is an Advanced Electronic Signature (AdES) based on Public Key Infrastructure (PKI) and X.509v3 certificates.

9.9.2 Identification of the signer

The first problem we must approach is the issuance of the electronic ID (eID). It is obvious that the link between the natural person holding an eID and the information in the eID is a relevant aspect. For a strong eID the usual situation is that this link is made with the personal appearance of the owner. But can issuance based on remote presentation of an identity document be acceptable?

From these first questions we can assure that this critical problem has great impact with the national regulation on identification and its solution is not obvious.

Our concern is that the identity of the signer must be guaranteed by a national registration authority under the specific rules for identification of that country.

Since a Trust Service Provider issuing end-user certificates operates following rules fixed in a document called Certificate Practice Statement, PEPPOL policy will consider only CPSs where it is clearly declared that the registration of the user is made in full accordance with the national identification rules.

This is especially relevant when the kind of certificates is non-qualified, when the issuer has not specific responsibilities.

REQ.2. A TSP's CPS must declare conformity of identification rules with country legislation.

9.9.3 Type of certificate

Since it is necessary to have a secure identification of the owner, PEPPOL allows only certificates for natural person which meet the following standard:

- ETSI TS 102 280 or
- ETSI TS 101 862 in case of Qualified Certificate

Use of corporate certificate identifying an organization and not a person is for further study in PEPPOL. This is accepted in some member states and is a promising approach for some procurement processes (e.g. invoicing) but can only be used if it is assessed that the use is allowed.

REQ.3. Certificates issued for natural person (ETSI TS 102 280 or ETSI TS 101 862) are required. Certificates issued to a legal person can be used but only when their legal status for the application in question has been assessed.

9.9.4 Certificate features and extensions

Even if a certificate is compliant to the above standards it is necessary to define other details in order to give to the verifier a sensible set of information.

Having the necessity to support any MS alphabet, the Issuer and Subject field must be in UTF-8 coding, even though PRINTABLESTRING coding is supported.

The certificate must contain the Name and Surname of the end-user. This could be present in the Subject commonName attribute but it is recommended to use the Subject surname and givenName.

Certificate with alias in Subject commonName or in Subject surname and Subject givenName are little supported and deprecated.

It is desirable the use a unique identifier of the end user (UID)[10]. If national laws do not allow use of national UID, an end user certificate must indicate at least a unique identifier valid for its CSP. The recommended field for the UID is the Subject serialNumber. The Service Directive expert group is evaluating a proposal for a European Qualified Electronic Certificate profile where the structure of such UIDs is defined. When available PEPPOL will address such profile as recommended.

In case of Qualified Certificate compliant to ETSI TS 101 862, the Qualified Certificate Statements (qcStatements) must be managed. The use of these extensions helps the understanding of the quality and security of the signature informing, for example, if the signature device is a SSCD.

REQ.4. The Subject and Issuer field should be coded in UTF-8 coding.

REQ.5. An end user certificate must contain the subject's given name and surname.

REQ.6. An end user certificate must contain an identifier unique at least for its CSP.

REQ.7. The use of qcStatements is strongly recommended.

9.9.5 Cryptographic requirements

A particular attention is taken in account on regard of the quality and security of the keys and algorithms used in the signature creation process. This is motivated on proofed, or estimated [8], duration of a signature in the middle-long period.

These requirement are expressed in terms of:

- Hashing algorithm
- Cryptographic algorithm
- Key size

Even [8] recommends to respect the following deadline:

Signature Generation Date	Public Key Algorithms and Key Sizes	Hash Algorithms	Padding Scheme
Through 12/31/2009	RSA (2048, 3072, or 4096 bits)	SHA-1	PKCS #1 v1.5
	RSA (2048, 3072, or 4096 bits)	SHA-256 (expect limited interoperability)	PKCS #1 v1.5
	ECDSA (Curve P-256)	SHA-256	N/A
	ECDSA (Curve P-384)	SHA-384	N/A
1/1/2010 through 12/31/2010	RSA (2048, 3072, or 4096 bits)	SHA-1	PKCS #1 v1.5
		SHA-256	PKCS #1 v1.5, PSS
	ECDSA (Curve P-256)	SHA-256	N/A
	ECDSA (Curve P-384)	SHA-384	N/A

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

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

Example: "VATIT RSSDRN67E28H501E

After 12/31/2010	RSA (2048, 3072, or 4096 bits)	SHA-256	PKCS #1 v1.5, PSS
	ECDSA (Curve P-256)	SHA-256	N/A
	ECDSA (Curve P-384)	SHA-384	N/A

Figure 1 - Signature algorithms and key sizes for PIV Information

In the real world only few MSs have updated their algorithms and key sizes, others are planning progressive modifications with a different time schedule, others have not approached the problem yet.

For interoperability, requirements for a qualified signature and its accompanying eID shall be set by the country of origin; if accepted as qualified in this country other member states should also accept this, even though the other member state itself has set stricter requirements. However, cryptographic algorithms must be at least at level 1 of the scheme in D1.1 part 7, else even a qualified signature should not be trusted for security reasons.

PEPPOL will encourage MSs that have implemented a high secure environment to also ensure electronic document circulation. Moreover since a certificate lasts in average two years, PEPPOL will support all the certificates issued before the adoption of the above improvements.

So trying to mediate all present MSs initiatives, a reliable environment may be:

Trough 12/31/2009:

- Cryptographic algorithm should be at least RSA (1024), RSA (2048) and ECDSA (Curve P-256) will be managed
- Hash algorithm should be at least SHA-1, SHA-256 will be managed

From 1/1/2010

- Cryptographic algorithm should be at least RSA (2048), ECDSA (Curve P-256) will be managed
- Hash algorithm should be at least SHA-256
- Cryptographic algorithm equal to RSA (1024) and hash algorithm equal to SHA-1 are deprecated but supported.

Note that these are recommendations and deviations may be accepted, e.g. for certificates that have a longer life time. Note also that strength of algorithms is given relatively to SHA-x and RSA but other algorithms should be accepted as long as they are supported by commonly available software and are not subject to licensing or other conditions that restrict their use for cross-border e-signatures.

REQ.8. If a certificate is issued before 1/1/2010 the hashing algorithm must have a strength at least equal to SHA-1 and the cryptographic algorithm must have a strength at least equal to RSA with a key size of 1024 bits. Certificates issued after 1/1/2010 should use a hashing algorithm of strength at least equal to SHA-256 and the cryptographic algorithm should be of strength at least equal to RSA with a key size of 2048 bits

9.9.6 Certification Service Providers

In establishing which TSP providing certification authority services are allowed to operate in PEPPOL environment, as starting point, if a TSP (CSP) is linked (directly or indirectly) in the page http://ec.europa.eu/information_society/eeurope/2005/all_about/security/esignatures/index_en.htm,

maintained by the EU Commission, it is automatically considered a valid PEPPOL CSP, being a supervised or an accredited CSP.

On that page, following the Art. 11 of eSignature Directive:

"*Member States shall notify to the Commission and the other Member States the following:*

a) *information on national voluntary accreditation schemes, including any additional requirements pursuant to Article 3(7);*
b) *the names and addresses of the national bodies responsible for accreditation and supervision as well as of the bodies referred to in Article 3(4);*
c) *the names and addresses of all accredited national certification service providers."*

The European List indeed links to the MSs national, voluntary accreditation/supervision schemes and respective Certification Service Providers that so are nationally recognized to possess all the organizational/technical requirements to provide digital certificates to their customers with full legal effectiveness. In particular it is assumed that those CSPs perform end-user authentication in adherence with national identification legislations. Such a kind of CSPs, whose services should be recognized among MSs (art. 4 of the eSignature Directive), will be identified as:

- Accredited CSP (ACSP)
- Supervised CSP (SCSP)

If they provide Qualified Electronic Certificates (QC) they will identified as:

- Accredited QCSP (AQCSP)
- Supervised QCSP (SQCSP)

As further source of trustworthiness PEPPOL will consider the use of the professional services offered by Validation Authorities like DNV. In this case the PEPPOL Consortium will sign an agreement with such VA in order to verify if a CSP, not included in any voluntary supervision/accreditation MS's schema, possesses the PEPPOL Policy requirements. In a positive case the VA signs an agreement with the investigated CSP. In such a way the legal trustworthiness (legal recognition) is based on a contractual level.

Such CSP will be identified as:

- Contractual accepted CSP (CCSP)

As in the previous case, if the CCSP provides qualified certificates, it will be addressed as CQCSP

REQ.9. A CSP should be at least a SCSP or a CCSP.

9.9.7 PEPPOL TSL

As TSP trustworthiness model PEPPOL Consortium has chosen the ETSI model ETSI TS 102 231 V.2.1.1, known as Trust-service Status List or more easily TSL, following the Service Directive expert group recommendations.

For the Pilot an unique PEPPOL TSL will be managed. It 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 the Pilot is foreseen a wide use of Validation Authority services. Even the TSL standard doesn't categorize such services, PEPPOL would consider them among the other trusted services using the "Service Type Identifier" equal to "generic – unspecified". A further clarification is possible to obtain by mean of the "Service information extension" equal to "PEPPOL VA".

The PEPPOL TSL will contain for the moment only the TSP CA services compliant with the previous paragraph. Moreover it will contain only TSPs working in Pilot Participant MSs. Further limitations to main MS TSPs may occur.

In a initial and transitory phase, PEPPOL TSL will be published in a Human Readable (HR) format.

It means a list organized following ETSI TS 102 231 Annex J as OpenDocument (ODF) electronically signed (CMS RFC 3739 – ETSI TS 102 231 Annex A) for authenticity reasons. The keys (certificates) and software, to perform its verification should be available on PEPPOL web sites.

In a further pilot phase, when available and updated to the Service Directive requirements, a TSL in machine readable format will be used.

For any changes will occur in the list (e.g. new TSP or status changes) PEPPOL will publish a new list.

REQ.10. A verifier must use the PEPPOL TSL as CSPs and VAs trustworthiness reliable source.

9.9.8 Signature creation devices

Looking back to c) feature of a AdES it is necessary that the signer must use a tool that "can maintain under his sole control". Also for this matter there isn't a unique solution. In real world we are using a token that is not a secure-signature-creation-device or we are unlocking with a PIN a software signature procedure. Probably the keys are stored in a PSE (Personal Security Environment) installed on the terminal hard disk.

The problem that now we are facing is the link between the "signature creation machine" and the natural person.

The solution for this problem can be that the natural person that sign, accepts the risk of a misuse of the signature-creation-device due to incorrect management of the credentials that are used to unlock that device.

REQ.11. A signer must use at least a Personal Secure Environment pass phrase protected but he should have accepted the risk of a misuse of the non-secure-signature-creation-device due to incorrect management of the credentials that are used to unlock that device.

9.9.9 Signature formats

In a recent survey done by the Service Directive expert group it is emerged that the most adopted or accepted signature formats are:

- XAdES – ETSI TS 101 903
- CAdES – ETSI TS 101 733
- PDF embedded signature – RFC 3778
- PKCS#7 – v.1.5 – RFC 2315
- CMS – RFC 3852
- XMLDSig – RFC 3275

It is quite important to distinguish between "adopted" and "accepted", because the first declares an effective use of the standard, whilst the second could only represent a "moral/legal" obligation without an effective use. The Service Directive expert group is still arguing on what will be the official standard for cross-border purposes. In the meantime PEPPOL will accept all formats in the list even though for the first (a probably for the second too) is foreseen a limited support, mostly if in advanced format (i.e. X, C, or A), due to the known interoperability lack issues [12].

REQ.12. The allowed electronic signature formats are: PDF embedded signature (RFC 3778), PKCS#7 v.1.5 (RFC2315), XMLDSig (RFC3275), CMS (RFC 3852). XAdES (ETSI 101 903) and CAdES (101 733) are accepted but limited supported.

When the Service Directive expert group will have decided a standard format, the PEPPOL policy will be updated recommending that standard.

If necessary, it is allowed the use of multiple signatures (when foreseen in the signature format):

- Sequential - a signature of a previous signed document

- Parallel - a signature of the same data set as the previous signature(s)
- Countersignature - a signature of the previous signature

REQ.13. Multiple signatures (Sequential, Parallel and Countersiganture) are allowed if created following the standard ETSI TS 101 903, ETSI TS 101 733, RFC 3778, RFC 2315, RFC 3275 and RFC 3852.

9.10 References

[1] ETSI TS 101 456 V1.4.3 (2007-05) Electronic Signatures and Infrastructures (ESI): Policy requirements for certification authorities issuing qualified certificates

[2] Directive 1999/93/EC of the European Parliament and of the Council of 13 December 1999 on a Community framework for electronic signatures

[3] Guidelines to Common Specifications for Cross Border use of Public eProcurement . May 2007

[4] DIRECTIVE 2006/123/EC OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 12 December 2006 on services in the internal market

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

[7] Service Directive Questionnaire – May 2008

[8] Cryptographic Algorithms and Key Sizes for Personal Identity Verification – NIST August 2007

[9] Federal Information Processing Standard 180-2, Secure Hash Standard

[10] PKCS #1: RSA Cryptography Standard

[11] Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile

[12] http://www.ecom.jp/LongTermStorage/en/testhistory.html

10 Appendix 2: Signature Formats

10.1 Introduction

Signature formats can roughly be divided into two levels:

- Low-level-signatures
  Low-level Signature formats specify how data or a hash-value of this data has to be handled by an application. The format itself depends mainly on the cryptographic algorithm used (e.g. RSA, DSA, ECDSA)
- High-level-signatures
  High-level-signature formats include the raw signature data as it is given by the low-level format plus some additional information such as the timestamp for the signature creation and the certificate needed for the validation process.

High-level signatures may in turn be embedded into signed data objects containing essential metadata such as validation information and time stamps. SDOs are particularly important for signed documents that need to survive over time.

While a signature based upon the low-level format can only be validated mathematically (proof of integrity), a signature of a high-level-format can usually be validated not only mathematically but also in terms of authenticity of the issuer. Low-level-formats are therefore not appropriate for e-procurement.

There are three high-level signature formats (four if S/MIME is considered a format of its own) that are widely used. They are described in the following paragraphs.

10.2 Cryptographic Message Syntax / PKCS#7

The Cryptographic Message Syntax (CMS) [RFC3852] is based upon PKCS#7 Standard [RFC2315]. It is currently probably the most widely adopted signature standard for electronic documents.

The specification of CMS defines containers in which data is stored. Each container has a distinct type, specified in [RFC3852]

There are two types of signatures possible with CMS:

- Enveloping Signature
  The message is encoded according to ASN.1 and put into the eContent-field of the signedData-structure. There is only one file containing both the signature and the message.
- Detached Signature
  Otherwise the eContent-field stays empty and the message is put into a separate file. In this case the term “detached signature” is used. Optional the filename of the message file can be put as an attribute within the signature to ease the mapping of both files.

Both types of signatures have pros and cons:

Since enveloping signatures include both message and signature there are no problems in terms of mapping. On the other hand the message is only accessible using a CMS-capable application. This is problematic in many cases. Therefore the detached signature is used more commonly. To facilitate the mapping between a detached signature and its message file, usually the signature file is named the same as the message file, appended with “.p7s”. However, while this is common practice – it is not standardized in any official way.

While in widespread use, the main disadvantage of CMS alone is that it changes or adds formats and thus needs separate software to process and display. This opposed to a signed XML document, which is still an XML document, or a signed PDF, which is still a PDF. In particular enveloping signatures renders the content in a format that cannot be displayed or processed without removal of the signatures to get to the “real” document format.

10.3 S/MIME

Secure Multipurpose Internet Mail Extensions (S/MIME) was initially developed by RSA Security Inc and is based on PKCS#7/CMS. Nowadays it is standardized by the IETF in [RFC2632, RFC2633]. It is targeted for signature and encryption of eMails and eMail-Attachments (MIME-Format [RFC1521]).

Two variants are possible:

- application/pkcs7-mime with SignedData
  In this case the transfered message consists of a SMS-sructure of type SignedDate which is transported within a MIME-message of type application/pkcs7-mime.
  The message is transformed to a canonical form (e.g. it is ensured that each line ends with a (CR)/(LF) (Carriage Return and Line Feed)). This data is then encoded by base64 or quoted-printable to ensure the correct handling even if a mail-relay only supports 7bit-character sets. The encoded data is then put into a CMS structure which is then embedded into a MIME-type "application/pkcs7-mime”
- multipart/signed
  The multipart/signed-variant is defined in [RFC1847]. The S/MIME-message consists of two parts, which are each encoded as MIME-messages. The first part is the message to be signed; the second is the according signature. The signature is a CMS-structure with an empty eContent-field. Again the messaged to be signed is transferred into its canonical form. Both parts are encoded for transport, too.

As the signed message can be read with eMail-clients without support for S/MIME using the multipart/signed-variant, this variant should be preferred over application/pkcs7-mime with SignedData.

10.4 XML Digital Signature

For signature of XML-files a specific signature format was specified by W3C. It is described in [RFC3275]. In comparison to the cryptographic message syntax-signature format it offers a higher degree of flexibility, which is needed to leverage the full potential of the extensible mark-up language.

While the cms-format only supports enveloping and detached signatures, the signature can be embedded within the message using the xml-format [RFC3275]. This approach is somewhat similar to the embedding of a cms-signature into a PDF-document (see below).

With an xml-signature you can sign arbitrary document formats (of course including XML documents) as well as only parts of an xml-document. Using XPath-Transformations [XPath] it is posible to exclude certain parts of a message from the signature. These fields can change its contents without invalidating the signature. This feature can be used to create enveloped signatures. Using XSL-Transformation [XSLT] the data of an xml-document can be to a certain layout [XSL] prior to the signature and validation of a document.

10.5 Embedding of Signatures in PDF-Documents

As stated it is not possible to embed CMS-signatures in a standardized way into electronic documents in every case. An exception of this are PDF-documents [PDF(v1.6)]. CMS-Signatures can be embedded to pdf-documents as a signature directory.

Signatures can be made visible by signature fields in the PDF document, including statements about the purpose of this particular signature. For electronic documents meant to be read by humans this is an appealing solution as PDF provides good WYSIWYS (What You See Is What You Sign) properties and good visualization if signature properties and validity to the receiver.

It is claimed that future versions of both the PDF document format and PDF-signatures will be based on XML (and XML-DSIG). This may even make PDF documents suitable for automated processing.