PEPPOL
Pan-European Public Procurement Online

PEPPOL Deliverable D1.1
Requirements for Use of Signatures in Public Procurement Processes
Part 1: Background and Scope

Version 1.2

PEPPOL WP1 2009-04-30

Borderless eProcurement
Let's make it happen!

cip

Table of Contents

1 Summary and Structure of Document

1.1 Scope and Structure of Deliverable D1.1

This document is a part of the multi-part deliverable D1.1 "Requirements for Use of Signatures in the Procurement Processes" issued by the PEPPOL[1] (Pan-European Public Procurement On-Line) project. PEPPOL is a three-year (May 2008 – April 2011) large scale pilot under the CIP[2] (Competitiveness and Innovation Programme) initiative of the European Commission.

D1.1 consists of the following documents:

Part 1: Background and Scope

Part 2: E-tendering Pilot Specifications

Part 3: Signature Policies

Part 4: Architecture and Trust Models

Part 5: XKMS v2 Interface Specification

Part 6: OASIS DSS Interface Specification

Part 7: eID and eSignature Quality Classification

The D1.1 deliverable is the first version of **functional specifications** for cross-border interoperability of e-signatures in Europe. The specifications are specifically targeted at cross-border public procurement, the topic of PEPPOL. However, if the resulting solution is successful it is believed that it will be applicable also to other application areas in need of e-signature interoperability.

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

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

1.2 Scope and Structure of This Document

This document gives the background and scope of PEPPOL work on e-signatures and should be read before diving into the more technical content of D1.1 parts 2-7. Chapter 2 presents PEPPOL and some background. Chapter 3 sets the scope of PEPPOL's work on e-signatures. Chapter 4 presents some legal issues. Finally, chapter 5 gives information about other initiatives in PEPPOL's environment.

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

[2] http://ec.europa.eu/cip/index_en.htm

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 Background

2.1 The PEPPOL Project

PEPPOL[3] (Pan European Public Procurement On Line) is a three-year (1. May 2008 – 30. April 2011) pilot project under the European Commission's CIP (Competitiveness and Innovation Programme) initiative. 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.

Following a specification phase (project year 1) and a development phase (project year 2), PEPPOL will run real life pilots (project year 3) involving at least the countries that are partners of the project but possibly also other countries.

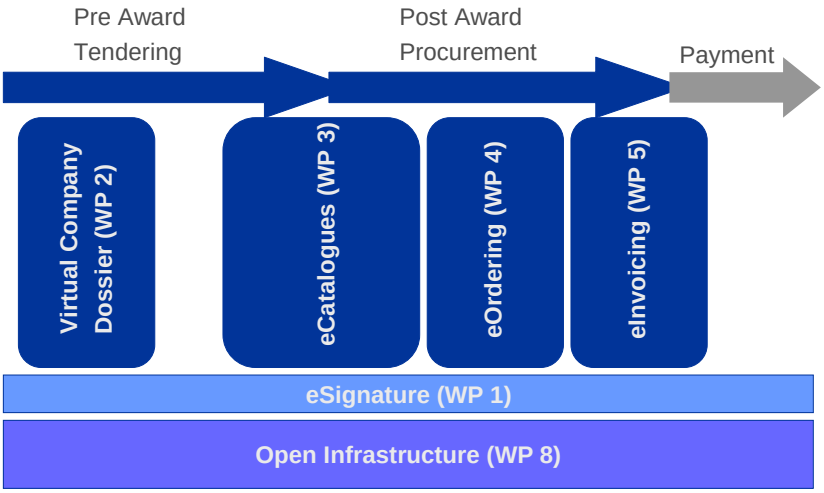

Figure 1: PEPPOL Work Packages.

The structure of the PEPPOL project is shown in Figure 1. In addition to the work packages (WP) shown in the figure, WP6 is project administration and WP7 results dissemination. Following invoicing, payment is the last step, which however is outside the scope of PEPPOL and assumed to be handled by existing payment systems.

E-procurement processes may be manual or automated, or combinations of the two. For example:

- Tendering (pre-award) is today typically manual processes:
  - Electronic documents are meant to be read by humans (e.g. PDF format).
  - Documents are submitted and read following manual work processes.

[3] For more information, see http://www.peppol.eu

  - More automated processes for e-tendering are envisaged but not within the timeframe of PEPPOL.

- Post-award (ordering, invoicing) may be automated or manual
  - In the manual case, electronic documents are sent by manual processes, addressed to an actor where a person will read the documents (e.g. a PDF format invoice).
  - In a fully automated case, the originating system will generate a structured document (typically XML) and ship this off to the receiver, where the document will be handled automatically by the receiver's system. Manual intervention may be kept at a minimum.

PEPPOL mainly addresses the automated case; it is a system integration project focussing on how to automatically exchange structured information between the IT systems of the actors involved.

Correspondingly, PEPPOL has no WP addressing tendering in general; only the aspects of VCD (virtual company dossier) and e-catalogues are covered. Since e-signatures are particularly important for tendering (see 2.3), the e-signature WP (WP1) has assumed responsibility for tendering pilots that are sufficiently advanced to show interoperability even in this phase.

Virtual company dossier (VCD) covers interoperable solutions for utilisation of company information (possibly including roles and authorisations) that is already registered, in order to reuse this information in electronic tendering processes across Europe. WP2 in PEPPOL will in particular focus on service interfaces and data structures for system integration towards the information sources, and to convey the information between the systems of the parties involved in the tendering process. Interactive, on-line solutions to business registers are not the main scope. Results from the EBR[4] and BRITE[5] projects will be utilised.

E-catalogues can be used in both tendering and for orders. WP3 in PEPPOL focuses on data structures and interfaces for catalogues suitable for automated exchange between systems, representing products, their specifications, and associated information such as price. PEPPOL will build on existing work in the area [EDYN]. Referral to standard product codes and other nomenclature and semantic information is necessary, although not specifically addressed by PEPPOL. E-catalogues intended for human use (such as PDF format brochures) are mainly out of scope.

WP4 and WP5 address ordering processes and invoicing respectively. For these WPs, automated transfer (interfaces, data structures) for system to system communication is the main focus. Electronic documents intended for human processing (such as a PDF format invoice) are mainly out of scope.

Catalogue, order, order confirmation, and invoice will in PEPPOL be based on the NES[6] profiles of UBL (Universal Business Language). PEPPOL contributes strongly to the ongoing standardisation work in CEN ISSS WS/BII[7]. This means that all business documents (at least for system to system communication) are XML-based.

The cross-cutting WP1 and WP8 handle e-signatures and transport infrastructure respectively. The PEPPOL transport infrastructure shall explicitly support system to system integration of procurement solutions across Europe. An actor that wants to participate in cross-border public procurement (buyer or seller side) shall integrate towards this infrastructure.

While the PEPPOL transport infrastructure provides transport security for e-procurement, e-signatures must work end-to-end between the actors that do business. Thus e-signature interoperability is

[4] European Business Register, http://www.ebr.org

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

[6] Northern European Subset of UBL, http://www.nesubl.eu

[7] CEN Workshop on 'Business Interoperability Interfaces on public procurement in Europe' (WS/BII), http://www.cen.eu/CENORM/businessdomains/businessdomains/isss/activity/ws_bii.asp

separated to the separate WP1. Other reasons for a separate e-signature WP are its importance (see 2.3 and 2.5) and the fact that e-signature work in PEPPOL has to address even the tendering phase, which is outside use of the PEPPOL transport infrastructure.

2.2 The PEPPOL Infrastructure

PEPPOL WP8 develops a pan-European transport infrastructure[8] for secure and reliable transport of business documents between the IT-systems used by the involved actors (awarding authorities and economic operators). IT-systems may belong to the actors themselves or they may be procurement services offered by service providers, e.g. national, public e-procurement solutions or commercial services.

The infrastructure is accessed by means of an Access Point (AP), which has one interface towards the IT-systems of the actors (this part is out of scope of PEPPOL) and another interface towards the common infrastructure. As shown in Figure 2, an AP will in many cases be implemented by components that are integrated directly in an Operator's system (Access Point Operator 2) but the AP may also be a service of its own (Access Point 1).

There will presumably be several thousand APs in Europe, showing the need for a PEPPOL Registry system (catalogue) to be able to locate the AP(s) associated with a particular actor. The registry system is not discussed further here.

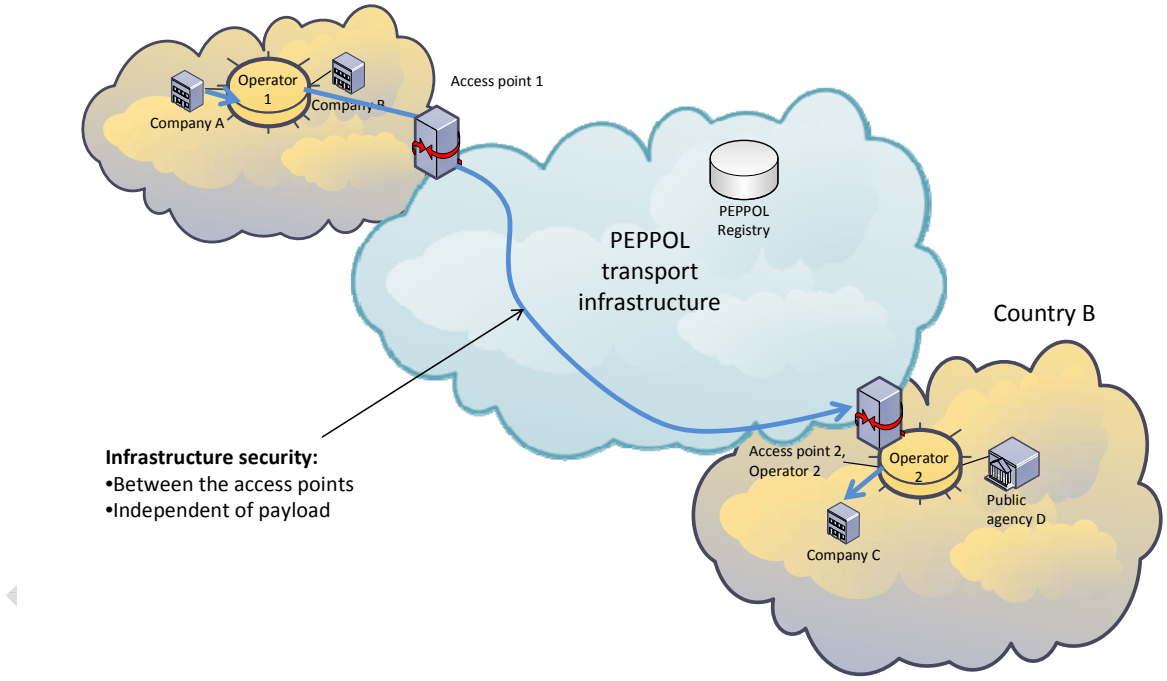

Figure 2: PEPPOL infrastructure and scope of security.

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

An AP interfaces to the PEPPOL infrastructure through a set of WS (Web Services) interfaces. The infrastructure provides reliable and secure transport of messages between APs. The PEPPOL infrastructure is agnostic about the content of the messages (i.e. the business documents) transported; any message is handled in the same way. Reliable means that actors will be informed in case of errors (e.g. addressing errors in message routing leading to delivery failure).

The relationship between the PEPPOL infrastructure and e-signature interoperability in PEPPOL is described in D1.1 part 4.

2.3 Public Procurement Directives, e-Signature Requirements for Tendering

The EU Directives on public procurement [EU02] [EU03] and the accompanying requirements document [COMM02] cover tendering (pre-award) only, According to these documents, awarding entities[9] may decide that communication and exchange of information with economic operators[10] shall be performed exclusively by electronic means or by a combination of electronic means and paper. Electronic communication must guarantee data integrity and confidentiality. Secure communication channels (such as provided by TLS/SSL) and/or advanced electronic signatures may be used to this effect. Traceability of processes must be guaranteed by storing the original version of all documents along with records of all exchanges carried out. Signatures may play a role in the traceability. Time stamping is required; by an independent time stamping authority or by other means that are considered sufficiently reliable.

Awarding entities are free (subject to national regulations) to choose the appropriate means of communication and to require a specific format and structure for tenders. Economic operators shall comply with these specifications (which must be readily available to all interested parties) in order to present a valid tender or request to participate.

The directives state that neither signatures nor encryption shall be used by economic operators unless they are invited to do so by the awarding entity. National legislation may establish mandatory requirements for use of signatures, which all awarding entities in this country must adhere to. In the absence of such legislation, the awarding entity can independently choose the level of signatures required for the particular case at hand.

Use of signatures shall be in accordance with the EU Directive on electronic signatures [EU01]. This directive explicitly states that a qualified signature shall be granted legal effect in the same manner as a handwritten signature, and that other electronic signatures shall not unduly be denied legal effect. The interpretation is that awarding entities are required to accept any qualified signature that has been legally produced in any EU Member State, and any other signature that fulfils the required level.

In repetitive procedures, e.g. tendering among economic operators that already have entered framework agreements, the public procurement directives allow signature requirements to be lowered since the actors are known a priori to one another.

Note that other pre-award documents, notably VCD and e-catalogues in the PEPPOL setting, and signatures for such documents are not covered by any directive.

[9] This term is used for the buying side of a public procurement process, i.e. a public agency.

[10] This term is used for the selling side of a public procurement process, usually a private company.

2.4 E-Signature Requirements for Post-Award Processes

The public procurement directives cover only the tendering (pre-award) phase of public procurement. Of the post-award processes, e-invoices are covered by the VAT directive [EU04]. Other post-award procedures, e.g. an order process, are not covered by EU directives.

According to [EU04] the primary mechanism to ensure authenticity and integrity of an e-invoice is an advanced e-signature. Alternatively, the so-called "EDI clause" of [EU04] states that unsigned invoices may be used provided that authenticity and integrity are otherwise guaranteed. The term "EDI clause" comes from the fact that such alternative solutions are usually provided by EDI service providers offering exchange of invoices (and other business documents) internally to a closed community of subscribers. Thus, referral to the EDI clause usually limits open exchange of e-invoices but it still seems like the prevailing practice in most countries is to refer to this clause and to not sign e-invoices. Lack of interoperability of e-signatures is one explicit reason for this situation.

In short: While e-signatures were intended as an enabler for e-invoices, in reality the lack of interoperability has made e-signatures an obstacle. If PEPPOL can make an impact on this situation, this will be an important result of the project.

Note that a revised version of the VAT Directive has recently (January 2009) been released. The changes in procedures are assumed to lead to less emphasis on e-signature as preferred mechanism but still it can be agreed that interoperable use of e-signature for e-invoicing should be in place.

Signatures for orders, order confirmations, and e-catalogues are at the discretion of the parties involved. If the e-invoice case is solved, the solution can be applied to other post-award documents as well, meaning that actors may pose requirements for signing of such documents and expect the requirements to be fulfilled, as opposed to the present situation where interoperability hinders use of signatures in such contexts.

2.5 E-Signatures as Blocking Factor for Public Procurement

The *Guidelines to Common Specifications for Cross Border use of Public eProcurement* [ICT-PSP] 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 document further identifies the following main obstacles:

1. Lack of consensus on critical concepts such as "advanced e-signature" and different levels of trust in e-signatures.
2. Legal hurdles due to different legislations in the EU Member States.
3. The acceptance of electronic solutions for signing documents by the public sector.
4. Limited support from service providers for development of interoperable solutions.

The fact that signature interoperability is perhaps the main obstacle to cross-border public procurement is a main reason for the establishment of a separate WP in PEPPOL to address the topic. It is specifically the task of WP1 in PEPPOL to overcome the obstacles identified above. These obstacles refer to tendering processes, which thus have to be addressed by PEPPOL WP1. To this must be added interoperability of e-signatures for other procurement processes, such as invoicing, where lack of signature interoperability also is identified as a blocking factor (see 2.4).

2.6 E-Signature Interoperability Requirements in General

The ultimate interoperability situation for e-signatures and any other use of eIDs can be stated as:

- An eID holder shall be able to use the eID to sign a document towards any counterpart, even internationally. The eID holder independently selects the eID to use.
- The receiver (relying party, RP) of a signed document shall be able to accept signatures from all counterparts, regardless of the eID used by the counterpart. In an open market, the RP has no influence on a counterpart's selection of eID.
- A third party, receiving a document signed by other parties, shall be able to verify the signatures no matter the eIDs used by the other parties. One does not know at the time of signing who may need to verify signatures.

The RP role is clearly the one facing the complexity. The eID holder has one trusted party to rely on: the eID issuer (CA – Certification Authority). Given today's predominant trust models in the PKI area, the RP however must rely independently on each and every CA used by its counterparts.

The interoperability challenges are thus best described from the viewpoint of an RP as the receiver of a digitally signed document. The RP must check all signatures, handling:

- The relevant signature formats (PKCS#7, CMS, XML DSIG etc.) including all necessary modes (enveloped, enveloping, and independent) for multiple signatures.
- All necessary hash and crypto algorithms.
- The eIDs of all signers.

Processing of an eID consists of the following steps:

- Parsing and syntax checking of the eID 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.
- Validation of the CA's signature on the eID 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.
- Checking that the eID is within its validity period, and that the eID is not revoked, i.e. declared invalid by the CA before the end of the validity period.
- Semantic processing of the eID content, extracting information that shall be used for presentation in a user interface or as parameters for further processing by programs. The name(s) in the eID and interpretation of naming attributes are particularly important.
- In the case of certificate paths, repeated processing for each certificate in the path.

Although the technical validation of signatures and eIDs has its challenges with respect to scaling, the real problem to the RP is:

- Assessment of the risk implied by accepting the signature (or an eID used for some other purpose), determined by the legal situation, the quality of the eID and the cryptography used, the liability situation, and the trustworthiness of the CA.

The acceptance criteria can (and shall according to the recommendations of this deliverable) be described as a signature policy (see D1.1 part 3). While current signature policies are frequently limited to a list of accepted CAs, signature policies for cross-border public procurement shall consist of open and non-discriminatory criteria.

3 Scope of e-Signature Work in PEPPOL

3.1 Commission Action Plan on eSignature and eIdentification

The Commission's *Action-Plan on e-Signatures and e-Identification to Facilitate the Provision of Cross-Border Public Services in the Single Market* [COMM-03] was launched November 2008 and PEPPOL's work on e-signatures must of course support and be aligned with this plan as far as possible. The following recommendations are noted.

A "quick win" is to utilise qualified signatures and advanced signatures using qualified eIDs since these are relatively well-defined. A trust list of supervised/accredited issuers of qualified eIDs shall be compiled by mid-2009. Guidelines for interoperability to be defined by end of 2009. PEPPOL will utilize such a trust list (see D1.1 part 4), while specification of the trust list concept is mainly done by the Services Directive expert group established by the Commission and IDABC.

Advanced (non-qualified) signature interoperability is more difficult. The action plan suggests a federation of validation services and definitions of quality levels. This is specifically the solutions that are treated by D1.1 part 4 (architecture and trust models) and part 7 (quality). Thus, PEPPOL should provide considerable input to this work.

E-identification (authentication) is not a topic of PEPPOL. Rather the action plan refers to the STORK[11] pilot to come up with solutions on this topic. PEPPOL WP1 has good liaisons to the STORK project in order to discuss common issues of interoperability.

3.2 Addressing Obstacles to Interoperability

Referring to the obstacles defined in the Guidelines to Common Specifications for Cross Border use of Public eProcurement [ICT-PSP] (see section 2.5), PEPPOL will attack all of these:

1. *Lack of consensus on critical concepts such as "advanced eSignature" and different levels of trust in eSignatures.* PEPPOL will address this by providing signature policy definitions and criteria to assess quality levels for advanced e-signatures and accompanying eIDs.
2. *Legal hurdles due to different legislations in the EU Member States.* PEPPOL is of course not in a position to change legislation but can only point at directions. The main observation is that recognition of a solution's compliance (e.g. acceptance of an eID as qualified) in one Member State must be accepted by other Member States. Particular national requirements cannot be imposed on actors outside of that particular country. Specifications must leave some flexibility in order to cater for different national requirements.
3. *The acceptance of electronic solutions for signing documents by the public sector.* This deliverable addresses signing by both sides of an eProcurement process: awarding entity and economic operator. Both must be provided with solutions for signing and verification; the verification challenge being mainly (due to the number of economic operators) on the awarding entity (public buying agency) side.
4. *Limited support from service providers for development of interoperable solutions.* This deliverable provides specifications that enables integration of the necessary (signing and) verification functionality at appropriate points in the workflow implementations. PEPPOL specifies a service-oriented approach with interfaces (D1.1 parts 5 and 6) based on the XKMS

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

[XKMS] and OASIS DSS [DSSCore] specifications. Validation services may provide functionality only, or they may be *authorities* where service providers not only obtain functionality but also reduced risk (see D1.1 part 4 for a discussion).

The IDABC *European Interoperability Framework for pan-European eGovernment Services* [IDABC03] refers to three interoperability layers: organizational, semantic, technical interoperability. To this may be added legal interoperability as there may be legal hurdles to cross-border use of e-signatures. The e-signature specifications in PEPPOL cover these aspects as discussed in the rest of this chapter.

3.3 Legal Interoperability

Conflicting legislation in different Member States will clearly hinder interoperability. EU Directives aim at alignment of the legislative environment (Public Procurement Directives, E-signature Directive, VAT Directive) but leave considerable freedom for implementation in national laws and regulations.

PEPPOL is not in a position to change legislation. The project can only identify issues and recommend measures. Some of this may be rather easily corrected. See chapter 4 below.

3.4 Organizational interoperability

3.4.1 Issues

This interoperability layer 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) in an e-procurement protocol/process?
- What shall these signatures imply in terms of commitment and authorization?
- Which signature acceptance criteria are applied to signatures and associated eIDs)?

These are all elements of signature policies and are detailed in D1.1 part 3.

3.4.2 Signatures in Business Processes, Roles and Authorizations

Use of signatures shall be defined as part of the definition of the business process (protocol, chain of transactions) between actors. The intention is not that requirements must be the same across all actors but that requirements must be transparent and non-discriminatory. PEPPOL WP1 will address this specifically for tendering processes and co-operate with other WPs for other processes.

A signature binds to the name in the eID, usually a person name only. The receiver needs assurance that this signature also represents the signer's organization and that the person has the required role and authorizations. This is addressed in D1.1 part 3.

3.4.3 Signature Acceptance Criteria

A signature policy defines a set of rules for the creation and validation of electronic signatures, under which a signature can be determined to be valid (signature acceptance). The receiver (the one accepting the signature) sets the policy, and the signer has to comply with the requirements. The main purpose of a signature policy is to define quality requirements (eID requirements, cryptographic requirements etc.). Additionally, the policy may set requirements for the signature format to be used and information to be included in the SDO (signed data object). Current signature policies mainly contain just a list of trusted (national) eID issuers, clearly not an interoperable solution. PEPPOL WP1 work on signature policies is documented in D1.1 part 3.

3.4.4 Risk Acceptance Criteria for Signatures

An eID issuer operates according to a certificate policy, which regulates use and acceptance of eIDs. A certificate policy will refer to the issuer's national legislation and may furthermore be written in the issuer's local language. This leaves the receiver of a signed document with a rather unpredictable risk picture in particular concerning liability and possibilities for claiming recourse in case of mistakes on the issuer's side. IDABC [IDABC01] cites this fact as another reason why national e-government services are reluctant to accept anything but eIDs from a few selected, and preferably domestic, issuers. At the core of this problem is an uncertain trust situation that must be handled through specification of (a set of) trust model(s) that explicitly identifies trusted actors and components. PEPPOL's signature and eID validation platform will explore solutions using service oriented architecture with services provided either as functionality only (local or remote software) or as trusted VA (Validation Authority) services [DNV01]. Trust status list distribution [ETSI01] [SEALED02] is an important aspect.

Note that "trust" in eID and e-signatures usually is interpreted as trust in correct technical processing (see "technical interoperability" below). In a business setting, this is not sufficient since liability and real possibilities to claim recourse (what happens if something goes wrong) are more important.

3.5 Semantic Interoperability

System to system exchange of procurement documents must rely on a common understanding (semantics) of the information exchanged. While this is not a core topic in PEPPOL, reliance on product codes and other nomenclature must be expected.

Specifically for signatures the main semantic issue is meaning of name attributes in eIDs. Experience shows major differences in content and encoding of names. Similar attributes (e.g. national identification numbers) may be placed in different attributes of names and have different semantics.

Additionally, encoding and semantics of roles and authorizations is an issue. To the extent addressed (see D1.1 part 3) this should be co-ordinated with PEPPOL WP2 work on VCD.

PEPPOL WP1 will not use many resources on semantic interoperability. There is a need for a common profile (or a limited set of profiles) for names in eID certificates in Europe; this is also addressed by the Commission's action plan [COMM-03]. An identity provider service may translate from different name formats into one common format to be used e.g. in SAML tokens issued. It is also possible to define an XML structure representing eID content in a normalized way. Mapping different eIDs into such formats requires detailed knowledge of the naming encoding and semantics of the relevant eIDs.

Consequently there is no chapter on semantic interoperability in D1.1.

3.6 Technical Interoperability

There is a tendency to focus too much on the technical interoperability problems although in reality these are not the most serious obstacles. PEPPOL will address the technical challenges.

One simplification for PEPPOL is that the project assumes that all actors are able to sign within their corporate infrastructure; thus interoperability of signing solutions (e.g. making your smart card work "everywhere") is largely out of the scope (but see D1.1 part 2 and in particular Appendix 1 to part 2). The STORK pilot[12] is assumed to do extensive work on this topic.

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

The receiver of a signed document must be technically able to process the signature format, including fields like time-stamps signed by some trusted TSP (time stamp provider), the necessary hash and cryptographic algorithms, and the eIDs, including verification of key usage and other extensions. The public keys of all relevant eID issuers must be reliably available, and it must be possible to check revocation status of eIDs. Estimates indicate that in the order of 100-200 eID issuers (the EU Action Plan [COMM-03] states 96 issuers of qualified certificates but even this number can be disputed) must be handled to cover relevant eIDs in the EU. Current state in technical standards [SEALED01] is that there are still some open issues adding to the scaling problems implied by the numbers cited above.

It is assumed that standard signature formats and signed data objects can be used for public procurement and that useful profiles exist that define e.g. how to sign an e-invoice.

Documents exchanged e.g. in a tendering process must be logged and retained for a period of time. The directives on public procurement and e-invoicing [EU02] [EU03] [EU04] all state that the original documents must be retained. The definition of “original” may however vary from country to country. PEPPOL pilots will not touch upon archival and records management but specifications must ensure that all information necessary for archival can be made available to the parties involved (see D1.1 part 3).

4 Legal Aspects

There are a few major issues (and probably a lot of minor ones, see 4.4 below) that cannot be solved by PEPPOL alone: requirements for qualified signatures, use of national accreditation schemes, and use of national identifiers for persons. These and other issues are identified and described by the IDABC study [IDABC01].

4.1 Qualified Signature Requirements

Qualified signature is a requirement that is imposed by some national authorities and contracting authorities. This is actually compliant with the intentions of the e-signature directive [EU01] and may be a realistic long-term goal. Products and services that offer qualified signature are available in most, but far from all, European countries, and in some countries the market penetration of such products is very limited. Thus, it can be discussed if a requirement for qualified signatures is not a non-discriminatory requirement today. PEPPOL will have to look at interoperability even of advanced e-signatures.

The status will be monitored by PEPPOL. If qualified e-signatures get increasingly used and available in more countries, it may be sufficient to devise interoperability of qualified signatures in Europe. However, “qualified” is a European term, so if interoperability on a global scale is addressed, either the qualified level is again non-discriminatory, or one will have to establish what can be considered as the equivalent term/solution in non-EU countries.

Alternatively, one must establish quality criteria and change policies into “either qualified (where applicable) or meeting these quality requirements”. The problem may be that qualified is more a legal term than a technical term, and thus non-qualified solutions may not carry the same legal value.

These issues are specifically addressed by D1.1 part 7.

4.2 National Accreditation Schemes for eID Solutions

The e-signature directive [EU01] is explicitly intended to enable cross-border use of e-signatures; however both the e-signature directive and the directives on public procurement have clauses that allow national authorities to introduce voluntary, national accreditation schemes for eID issuers, potentially recognizing only issuers that have obtained a national accreditation. The eID issuers then must declare conformance with national requirements that are additional to requirements for qualified eIDs (accreditation may be used for non-qualified eIDs as well). Since it will be practically infeasible for an eID issuer to declare conformance with national requirements in a lot of countries, and there may in fact be legal requirements on the contracting authority to accept only nationally accredited CAs, such accreditation systems may effectively block cross-border interoperability. This is identified by IDABC [IDABC01] as a major obstacle to cross-border use of e-signatures.

It is crucial that this is changed into a situation where a legal recognition in the eID issuer’s home country is accepted by other Member States. PEPPOL will work under the assumption that this is the case.

4.3 Use of National Identifiers for Persons

Many if not most countries in the EU have national identification number schemes for persons. When present, such numbers are usually directly (included in the eID) or indirectly (information in the eID can be used to look up the number) available in national eID solutions.

National applications using eID thus has a tendency to require the national identification number to be used to identify persons (even for public procurement), thus excluding foreign eIDs that cannot use this number. While there is no reason to stop using a national identification number when available, its presence cannot be made mandatory. Alternative solutions must be made to be able to accept other eIDs. PEPPOL does not rely on national identification numbers.

4.4 Miscellaneous

In addition to the major issues, there is with high probability a range of more minor issues relevant for individual or smaller groups of member states. This can be requirements for use of non-standard or "non-mainstream" solutions (national specifications), bundling of functionality (use of national identifiers being the most prominent example) or other peculiarities. Mapping all these issues is a too big task; rather PEPPOL will seek to handle them when they are encountered.

One example of such an issue is the German decision to abandon use of the SHA-1 hash algorithm and RSA key length of 1024 bits by end of 2008. SHA-1 is in Germany no longer accepted to sign qualified eIDs and qualified signatures, and RSA-1024 is no longer accepted for subject public key in qualified eIDs. At the same time the majority of issuers of qualified eIDs in Europe still use SHA-1 to sign eID certificates and RSA-1024 for the subjects' keys. Most signing software will as default select SHA-1 when signing documents. Most countries plan to abandon SHA-1 only by end of 2010. If Germany enforces this requirement strictly on foreign eIDs and signatures, interoperability will be very difficult at least in the short term.

5 European Initiatives on e-Signature Interoperability

5.1 Introduction and Disclaimer

There are several projects in Europe and globally that address the topic of e-signature interoperability from different angles of view. A close monitoring of such projects and liaison to selected projects is reasonable to avoid double work and to profit from each others experiences and results.

A disclaimer is necessary for this chapter: The descriptions below include only the projects and programmes "closest to" PEPPOL WP1. There are numerous other projects that we are aware of and that could have been mentioned; and probably several initiatives that we do not even know to a sufficient degree. The intention is not to provide a complete mapping – that would require too many resources and could warrant a report of its own – but rather to place PEPPOL WP1 within its closest surroundings. See also [i2010-HIS] for some additional information sources and reference documents.

5.2 CIP Pilots

PEPPOL is one of a series of pilots under the CIP Programme of the EU Commission. All these pilots are to some extent concerned with e-signature and eID interoperability. Notably:

- STORK focuses on eID interoperability for authentication but also addresses other aspects of interoperability;
- SPOCKS (Services Directive pilot) notably works on national Single Point of Access, including cross-border use of eID and e-signature in this context;
- PEPPOL focuses on eID and e-signature validation as the main issues to public procurement;
- epSOS specifically works on the health sector, with requirements for use of eID and e-signatures.

PEPPOL needs close liaisons with all the other pilots.

STORK aims at an interoperable solution for electronic identity (eID) based on a distributed architecture that will pave the way towards full integration of EU e-services while taking into account specifications and infrastructures currently existing in EU Member States. The project will result in the implementation of an EU wide interoperable system for recognition of eID and authentication that will enable businesses, citizens and government employees to use their national electronic identities in any member state. Note that STORK does not primarily focus on e-signatures although this is not entirely out of scope; authentication and identity are the main topics.

5.3 IDABC

IDABC[13] stands for Interoperable Delivery of European eGovernment Services to public Administrations, Businesses and Citizens. It uses the opportunities offered by information and communication technologies to encourage and support the delivery of cross-border public sector services to citizens and enterprises in Europe. IDABC issues recommendations, develops solutions and provides services that enable national and European administrations to communicate electronically while offering modern public services to businesses and citizens in Europe. Under the IDABC programme a lot of work is done in the field of eSignature and eProcurement, and this material has been crucial as background to the specifications in D1.1.

[13] http://europa.eu.int/idabc

5.4 PROCURE

The eTEN PROCURE project aims at enabling electronic bids for public procurement procedure through safe and intuitive web services for SMEs, across 5 pilot regions in the EU. This project is funded by the European Union via the eTEN programme. This programme is designed to contribute to the deployment of trans-European e-services in the public interest.

5.5 Standardization activities

In response to the demand for the standardization of eSignatures in Europe the European ICT Standards Board (ICTSB), with the support of the European Commission has been supporting an initiative that brings together the industry and public authorities under the European Electronic Signature Standardization Initiative (EESSI). EESSI sought to identify under a common approach the needs for standardization activities in support of the requirements of the eProcurement Directive. A significant part of the work of EESSI has been tackled with the support of the European Telecommunications Standards Institute (ETSI) and the European Standardization Committee (CEN). ETSI and CEN have provided several standards, workshop agreements, guidelines related to eSignatures. These outputs have been considered in the specification.

5.6 EUROCHAMBRES

EUROCHAMBRES[14] is the European Association of Chambers of Commerce and Industry and forms one of the key pillars of business representation to the European institutions.

The chambers of commerce have business registers as the primary focus. However, many leading CAs in Europe are run by chambers of commerce, and EUROCHAMBERS has established an initiative at interoperability between these eID solutions, ChamberSign[15]. PEPPOL WP1 has conducted meetings with EUROCHAMBERS and ChamberSign and intends to continue co-operation with these actors.

5.7 European Commission:

The *i2010 – A European Information Society for growth and employment* initiative was launched by the Commission on 1st June 2005 as a framework for addressing the main challenges and developments in the information society and media sectors up to 2010. It promotes an open and competitive digital economy and emphasises ICT as a driver of inclusion and quality of life. The initiative contains a range of EU policy instruments to encourage the development of the digital economy such as regulatory instruments, research and partnerships with stakeholders. One of the focus areas is eGovernment. In 2005, during the Manchester Ministerial eGovernment Conference, the path towards "Transforming Public Services" was set in. PEPPOL D1.1 is seen as a contribution to transforming public services through gaining interoperability in the field of eSignatures.

Public procurement is identified as a “high impact service” for the European Information Society [i2010-HIS].

[14] http://www.eurochambres.be

[15] http://www.chambersign.com

5.8 Excursus European Bridge CA

European Bridge CA[16] was founded in 2000 with the aim of facilitating **secure e-mail communication** between companies and public authorities without any need to conclude n-fold bilateral contracts. European Bridge CA is sponsored and operated by TeleTrusT Deutschland e.V., a German non-profit association which provides central infrastructural components on behalf of members and root certificates for the root authority. European Bridge CA is focusing only on software certificates, in particular for e-mail based communication. Qualified electronic signatures are not supported, only advanced electronic signatures.

European Bridge CA is a non-commercial network consisting of public key infrastructures of the members – companies and public authorities. The members are at the moment only German (one Austrian) companies and public authorities.

A liaison between PEPPOL and European Bridge CA is set up to exchange information on a regular basis. The aim of this liaison is also to avoid double work and that PEPPOL participates in the lessons learned of European Bridge CA.

5.9 European Bridge CA Pilot

In 2004 IDABC started a pilot for a European Bridge CA[17]. The scope was to create an intermediate structure to guarantee the reliability and interoperability of different national CA certificates, in the well known contexts of mail exchange (electronic signature, encryption) and client authentication to online web services, for the use among civil servants; advanced/qualified e-signatures were not the main focus area.

The model is based on a centralized administrative structure and a trust list distribution model based on a Trust-service Status List compliant to [ETSI01]. Although the name of the pilot included “bridge CA”, no real bridge was established (a bridge is defined as a central hub-CA, were other CAs can cross-certify at an appropriate policy level).

The tests run during the pilot have shown a high level of interoperability among MS certificates and the possibility to implement and easily maintain centralized TSLs. The work on TSL has been re-initiated by the Commission’s action plan [COMM-03], by the expert group established by the Commission and IDABC for the Services Directive, and even by PEPPOL (see D1.1 part 4).

A particular issue for the pilot is that the list distribution service assumed liability for the information in the list. Thus, the list distribution service was an authority according to definitions and discussions in part 4 of D1.1.

[16] https://www.bridge-ca.org

[17] http://europa.eu.int/idabc/en/document/2318

6 References

[COMM-01] Commission of the European Communities, Action Plan for the Implementation of the Legal Framework for Electronic Public Procurement. Communication from the Commission to the Council, the European Parliament, the European Economic and Social Committee and the European Committee of the Regions, December 2004, http://ec.europa.eu/internal_market/publicprocurement/docs/eprocurement/actionplan/actionplan_en.pdf

[COMM-02] 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 SEC(2005) 959 , July 2005, http://ec.europa.eu/internal_market/publicprocurement/docs/eprocurement/sec2005-959_en.pdf

[COMM-03] Commission of the European Communities, Action-Plan on e-Signatures and e-Identification to Facilitate the Provision of Cross-Border Public Services in the Single Market, Communication from the Commission to the Council, the European Parliament, the European Economic and Social Committee and the Committee of the Regions, November 2008, http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2008:0798:FIN:EN:PDF

[DNV01] Ølnes, Jon et al.: Making Digital Signatures Work across National Borders. ISSE Conference, Warszawa, 2007.

[DSSCore] S.Drees et al., Digital Signature Service Core Protocols and Elements OASIS, February 2007, http://docs.oasis-open.org/dss/v1.0/oasis-dss-core-spec-v1.0-os.html

[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

[ETSI01] ETSI: Electronic Signatures and Infrastructures; Provision of Harmonized Trust Service Provider Information. ETSI TS 102 231 v2.1.1,2006.

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

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

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

[EU04] EU, Amending Directive 77/388/EEC with a View to Simplifying, Modernising and Harmonising the Conditions Laid down for Invoicing in Respect to Value Added Tax. Council Directive 2001/115/EC, 2001.

[ICT-PSP] ICT Policy Support Programme (PSP), Guidelines to Common Specifications for Cross-border Use of Public Procurement, April 2007, http://ec.europa.eu/information_society/activities/ict_psp/documents/guidelines_common_specs_eproc.pdf

[IDABC-01] Siemens, Time.lex: Preliminary Study on Mutual Recognition of eSignatures for eGovernment Applications (Final Study and 29 Country Profiles). IDABC, July 2008, http://ec.europa.eu/idabc/en/document/6485

[IDABC-02] e-Procurement specification (Functional Requirements for conducting electronic public procurement under the EU framework), IDABC, 2005.

[IDABC-03] European Interoperability Framework for pan-European eGovernment Services, IDABC, 2004. http://ec.europa.eu/idabc/servlets/Doc?id=19528

[i2010-HIS] 12010 eGovernment Action Plan, High Impact Services, Information Sources Relevant for the Definition of Common Specifications for Cross-Border Use of Public eProcurement, Version 1.0, May 2007, http://ec.europa.eu/information_society/activities/ict_psp/documents/information_sources_guidelines_eproc.pdf

[SEALED01] Sealed, DLA Piper, Across, Study on the Standardisation Aspects of Esignature, Study for European Commission (DG Information Society and Media), November 2007, http://ec.europa.eu/information_society/eeurope/i2010/docs/esignatures/e_signatures_standardisation.pdf

[SEALED02] 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, 28 June 2005, http://www.w3.org/TR/2005/REC-xkms2-20050628/