DELIVERABLE

Project Acronym: PEPPOL

Grant Agreement number: 224974

Project Title: Pan-European Public Procurement Online

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

Part 1: Background and Scope

Revision: 2.2

Authors:

Germany: bremen online services

Norway: Difi

Italy: InfoCamere, InfoCert

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

Greece: University of Piraeus

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

Revision History

Revision	Date	Author	Organisation	Description
1.0	2009/02/11			Complete version of D1.1 for internal quality assurance.
1.1	2009/02/27			D1.1 submitted to PEPPOL project management, approved with comments at project management meeting 2009/03/27.
1.2	2009/04/30			D1.1 for publication, updated according to comments.
1.3	2009/11/06			Formal update of D1.1 after EC approval
1.8	2010/09/22			Complete D1.3 version edited from D1.1 part 1. For internal quality assurance.
1.9	2010/09/30			D1.3 submitted to PEPPOL project operating office (POO) for approval.
1.9.5	2010/11/05			D1.3 ready for publication, updated according to comments from POO. Uploaded for EC approval.
2.0	2010/07/15			Formal update after EC approval.
2.1	2011/08/30			Implementation of EC recommendations.
2.2	2012/04/25			Sharpening terms “TSL” and “TL” and finalising for hand over

Statement of originality

This deliverable contains original unpublished work except where clearly indicated otherwise.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

Statement of copyright

Table of Contents

1 Summary and Structure of Document

1.1 Scope and Structure of Deliverable D1.3

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

D1.3 consists of the following documents:

Part 1: Background and Scope

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

Part 3: Signature Policies

Part 4: Architecture and Trust Models

Part 5: XKMS v2 Interface Specification

Part 6: OASIS DSS Interface Specification

Part 7: eID and eSignature Quality Classification

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

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

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

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

1.2 Demonstrator Software Components and Documentation

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

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

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

- PEPPOL XKMS responder component (server side component) according to the specifications of D1.3 part 5 is provided as open source. The software component, source code and documentation are available on Joinup[3],
- A free to use client side component for signature validation, available as a standalone version and a version for integration into other software applications.
- Open source software components for own development (XKMS requester, Report Agent, Verify Agent, Hashing API, System Configuration API)

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

1.3 Scope and Structure of this Document

This document gives the background and scope of PEPPOL's work on e-signatures and should be read before diving into the more technical content of D1.3 parts 3-7. 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.

1.4 Evolution of this Document and Changes from D1.1

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

No further revision of part 1 of D1.3 is planned. This part of D1.3 provides an overview of the European e-signature interoperability scene at the time of writing.

The notable changes since the version published as [PEPPOL-D1.1] part 1 are:

- Added sections on IDABC's EVFS (European Federated Validation Services) study and CROBIES.
- References updated throughout and all sections brought up to date incorporating developments since the writing of D1.1; in particular this applies to chapter 5.
- Updated and corrected information in some other sections, notably background on the PEPPOL project.

1.5 List of Contributors

The following organisations, in alphabetical order, have contributed to Deliverable D1.3:

- **ADETEF, France** http://www.adetef.fr
- **ANSSI, French Network and Information Security Agency, France** http://www.ssi.gouv.fr
- **bos, bremen online services, Germany,** http://www.bos-bremen.de
- **Difi, Agency for Public Management and eGovernment, Norway** http://www.difi.no

[3] Open source software, semantic assets and other interoperability solutions for public administrations, https://joinup.ec.europa.eu/.

- **DILA, Direction de l'Administration Légale et Administrative Of French Prime Minister Office, France** http://www.dila.premier-ministre.gouv.fr
- **Esteral Consulting, France** http://www.esteralconsulting.com
- **InfoCamere, Italy** http://www.infocamere.it
- **InfoCert, Italy** http://www.infocert.it
- **Lex Persona, France** http://www.lex-persona.com
- **University of Piraeus, Greece** http://www.unipi.gr

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

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

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

2 Background

2.1 The PEPPOL Project

PEPPOL[4] (Pan European Public Procurement On Line) is a 4-year (1st May 2008 – 30th April 2012) pilot project under the European Commission's CIP ICT PSP (Competitiveness and Innovation Programme, ICT Policy Support Programme) initiative[5]. 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), a development phase (project year 2), and a testing phase (beginning of May – end October 2010), PEPPOL will run real life pilots during the last 18 months of the project involving at least the countries that are partners of the project but possibly also other countries.

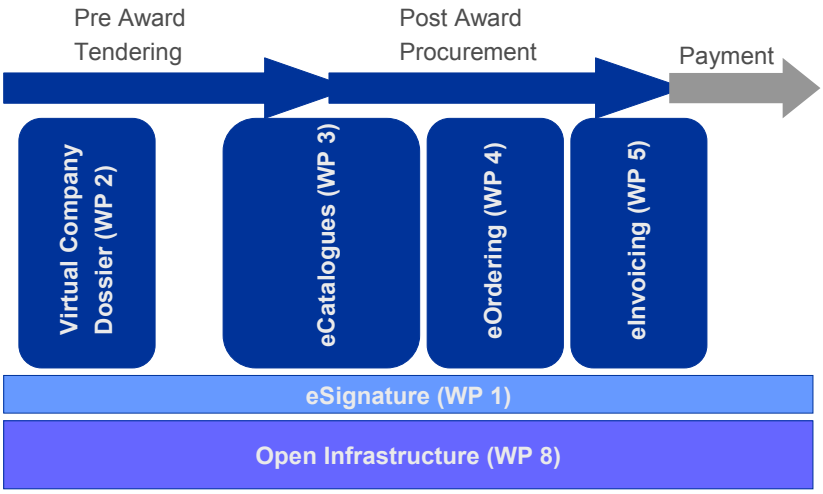

Figure 1: PEPPOL Work Packages

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 a manual process:
  - Electronic documents are meant to be read by humans (e.g. PDF format).
  - Documents are submitted and read following manual work processes.

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

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

  - 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 an 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.

PEPPOL has no separate WP addressing tendering in general but WP2 and WP3 cover the aspects of VCD (Virtual Company Dossier) and e-catalogues respectively. However, a co-ordinator role has been established in PEPPOL in order to enable tendering pilots.

E-signatures are particularly important for tendering (see section 2.3). Thus, the e-signature WP (WP1) will focus on tendering pilots that are sufficiently advanced to show e-signature interoperability; however use of e-signatures for post-award processes is surely within scope as can be seen from the horizontal illustration of WP1 in Figure 1.

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 in particular focuses 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[6] and BRITE[7] projects are 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 builds 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 are in PEPPOL based on structured specifications of message content and business processes. The specifications are standardised by CEN ISSS WS/BII[8] in alignment with UBL 2.0 (OASIS Universal Business Language). This means that all business documents (at least for system to system communication) are XML-based.

The cross-cutting WP8 handles transport infrastructure. WP8 has produced specifications and software to support secure and reliable transport of business documents (see section 2.2). The

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

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

[8] 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

specifications are named BusDoX[9] (Business Documents Exchange Network) and standardisation through OASIS is sought. BusDoX specifies access to the infrastructure, routing of messages, and protection of messages between the access points to the infrastructure. End-to-end protection is not guaranteed; this also depends on the communication means used before entering the access point.

E-signature on business documents must work end-to-end between the communicating parties and thus cannot be handled as part of the transport infrastructure. Thus, e-signature interoperability is separated to the separate WP1. Another reason for a separate e-signature WP is the importance of the topic (see 2.3 and 2.5).

2.2 The PEPPOL Transport Infrastructure

Based on the BusDoX specifications, PEPPOL WP8 develops a pan-European transport infrastructure 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.

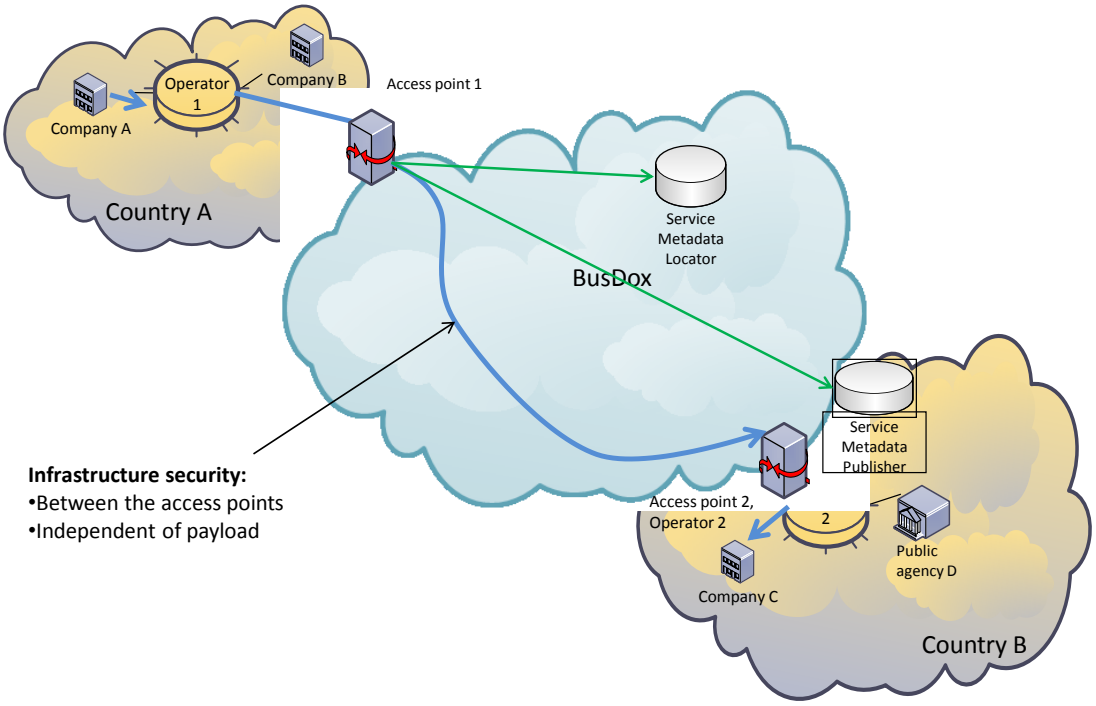

Figure 2: PEPPOL infrastructure and scope

The infrastructure is accessed by means of an Access Point (AP), which has one interface towards the IT-systems of the actors and another interface towards the common infrastructure. As shown in Figure

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

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).

The START protocol (Secure Trusted Asynchronous Reliable Transport) is specified for communication between APs and must also be supported by an AP for access from operators. An alternative protocol, LIME (Lightweight Message Exchange Profile) is defined as a low-cost alternative to access business documents directly in an AP.

Routing of documents is done by the initiating AP accessing a central Service Metadata Locator within the BusDoX infrastructure using identification of the receiving organisation as a lookup key. The return information is a pointer to the Service Metadata Publisher holding information about the receiver. The Service Metadata Publishers are associated with APs although there need not be a one-to-one correspondence. The AP serving the receiver is located.

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 to the destination AP leading to delivery failure. The reliability of the delivery chain before the originating AP and behind the destination AP is out of scope of the BusDoX specification. This may be settled by means of a mutual agreement between of the sender's and the recipient's infrastructures.

Reliable messaging infrastructures are made available at a national level in quite a few countries. The bulk of this work is based on the REM (Registered Electronic Mail) standards [ETSI-102-640].

The SPOCS project[10] has specified a solution to bridge these national infrastructures to enable end-to-end reliable messaging from an endpoint in one national infrastructure to an endpoint in another national infrastructure. It is noted that the BusDoX infrastructure could be used in a similar way by interfacing the national messaging infrastructures to BusDoX Access Points; however this is at present out of scope of PEPPOL.

The relationship between the PEPPOL infrastructure and e-signature interoperability in PEPPOL is described in D1.3 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[11] may decide that communication and exchange of information with economic operators[12] 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.

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

[11] This term is used for the buying side of a public procurement process, i.e. a public agency. The term contracting authority may also be used for the same actor.

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

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 signature requirements for such documents are not covered by any directive.

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. However, [EU04] also states that: “Invoices may, however, be sent or made available by other electronic means, subject to acceptance by the Member States concerned”.

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.

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.

Lack of signature interoperability as *the main* obstacle to cross-border public procurement can be argued but not that the lack of such interoperability is *a major* obstacle. This fact is a main reason for the establishment of a separate WP in PEPPOL to address the topic. It follows that a specific task of WP1 in PEPPOL is to overcome the obstacles identified above (this is further discussed in 3.2). 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 is also 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, advanced signature formats 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 D1.3 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 eSignature 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. The main actions are:

- Establish a system of TLs (Trusted List) of supervised/accredited issuers of qualified eIDs; this system is utilised by PEPPOL as described in D1.3 part 4.
- Enable cross-border recognition of not only qualified signatures but also advanced signatures using qualified eID; e.g. [COMM-05] on electronic procedures for the Services Directive, Article 1, states this explicitly (although acceptance shall be based on a risk analysis, which of course for some Member States may conclude that only qualified signatures are acceptable).
- Improve the standardisation situation by a restructuring of the standards landscape [COMM-04], see also section 5.2); but it is acknowledged that bringing all solutions up to new versions of standards and profiles will by necessity require some time.

Interoperability even of non-qualified, advanced signatures even using non-qualified eIDs is desired. A study on federated validation services has been conducted as briefly discussed below in section 5.4.4. Furthermore, the action plan [COMM-03] explicitly points to PEPPOL for testing of the approach of federated validation services. This is well aligned with the plans of PEPPOL; although it is not clear to what extent non-qualified eID will in practice be used in PEPPOL demonstrators, the solutions are specified to handle this.

E-identification (authentication) is not a topic of PEPPOL. Rather the action plan refers to the STORK[13] 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 (D1.3 parts 3 and 7).
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

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

in order to cater for different national requirements. Some recommendations are given in D1.3 part 3, see also section 4 below.

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 enable integration of the necessary (signing and) verification functionality at appropriate points in the workflow implementations. PEPPOL specifies a service-oriented approach with interfaces (D1.3 parts 5 and 6) based on the XKMS [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][14] refers to three interoperability layers: organisational, 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 Organisational 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 authorisation?
- Which signature acceptance criteria are applied to signatures and associated eIDs)?

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

3.4.2 Signatures in Business Processes, Roles and Authorisations

Use of signatures should 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

[14] A European Interoperability Strategy is under development in the ISA programme, see http://ec.europa.eu/isa

actors but that requirements must be transparent and non-discriminatory. PEPPOL WP1 will address this in co-operation with other WPs of PEPPOL.

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 organisation and that the person has the required role and authorisations. This is addressed in D1.3 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 usual situation is that 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's work on signature policies is documented in D1.3 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 [Olnes]. Trust status list distribution [ETSI-102-231] [CROBIES2.1] 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 authorisations is an issue. To the extent addressed (see D1.3 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] and CROBIES [CROBIES3]. 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 be possible to define an XML structure representing eID content in a

normalised way. Mapping different eIDs into such formats requires detailed knowledge of the naming encoding and semantics of the relevant eIDs.

Consequently there is no section or chapter on semantic interoperability in D1.3.

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. Some work was carried out in the context of [PEPPOL-D1.1] (see Appendix 1 to D1.1 part 2); this work has not been continued in D1.3. The STORK pilot[15] addresses the topic.

The receiver of a signed document must be technically able to process the signature format, including fields like time-stamps signed by some trusted TSA (Time Stamp Authority), 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 and the number of issuers covered by the EU's TL system is slightly above 100. Current state in technical standards [SEALED] 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. This is covered by the CEN ISSS WS/BII specifications by reference to use of [XMLDSIG].

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 D1.3 part 3).

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

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 a discriminatory requirement today. PEPPOL anyway considers interoperability of other advanced e-signatures.

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 discriminatory, or one will have to establish equivalent terms/solutions in non-EU countries.

The problem has been recognised by the EU advising interoperability to be extended at least to advanced (non-qualified) signatures using qualified eIDs [COMM-03] [COMM-05], see also 3.1.

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 D1.3 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 recognising 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, for qualified as well as non-qualified solutions.

4.3 Use of National Identifiers for Persons

Most countries in the EU have national identification number schemes for persons, either in the form of a single identifier used across all government sectors or in the form of separate identifiers for separate sectors of government. 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 have 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 available in order 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 many issuers of qualified eIDs in Europe still (towards the end of 2010) use SHA-1 to sign eID certificates and RSA-1024 for the subjects' keys. Most signing software as default selects SHA-1 when signing documents (this selection is not governed by the eID used).

The recommendation is to abandon SHA-1 by end of 2010 but many solutions will not comply. If Germany enforces its requirements strictly on foreign eIDs and signatures, acceptance of foreign signatures in Germany will be restricted 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.

The EU is at the core of the interoperability efforts and numerous policy documents and decisions could have been referenced as relevant for e-signature interoperability. Mapping such requirements is another exercise that is not taken on in this document.

5.2 Standardisation

Several standards bodies are active in the e-signature area. In Europe, particular emphasis has been placed on CEN and ETSI, which through a concentrated effort have produced a bulk of standards in the area. Studies such as [SEALED] have still revealed a need for a revision of the standards landscape.

In response to these identified challenges, a new mandate was issued to the standards bodies end of 2009 [COMM-04]. A survey of relevant standards and ongoing and future standardisation activities has not been conducted in this document but relevant standards are identified and referred to throughout this deliverable D1.3.

Internet specifications published by IETF are also important to the work in PEPPOL, and important base standards are published by W3C (e.g. [XKMS]) and OASIS (e.g. [DSSCore]).

5.3 CIP ICT PSP Pilots

PEPPOL is one of a series of pilots under the European Commission's CIP ICT PSP (Competitiveness and Innovation Programme, ICT Policy Support Programme) initiative[16]. All these pilots are to some extent concerned with e-signature and eID interoperability. The other pilots are:

- STORK[17] focuses on eID interoperability for authentication but also addresses other aspects of interoperability including some work on e-signatures. STORK is a 3-year project ending end of May 2011.
- SPOCS (Simple Procedures Online for Cross-border Services) addresses electronic procedures for setting up a business in another Member State in the context of the EU's Services Directive. SPOCS reuses results from STORK and PEPPOL, notably also PEPPOL's e-signature solutions as specified in this deliverable D1.3, SPOCS started 1st May 2009 and lasts for three years.

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

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

- epSOS (European Patients Smart Open Services) pilots electronic prescriptions and patient summary across Europe. epSOS may also reuse results from STORK and PEPPOL and adds aspects of identity management that may be of interest to the other pilots. epSOS is a 3-year project that started 1st July 2008.
- A new pilot on cross-border legal services is about to start towards the end of 2010.

PEPPOL maintains close liaisons with all the other pilots.

5.4 The ISA Programme and IDABC

5.4.1 About the Programmes

IDABC[18] is Interoperable Delivery of European eGovernment Services to public Administrations, Businesses and Citizens. This programme ended 2009 and has been succeeded by the ISA[19] (Interoperability Solutions for European Public Administrations) programme.

ISA and previously IDABC aim to support the delivery of cross-border public sector services to citizens and enterprises in Europe. IDABC has issued recommendations, developed solutions and provided services to enable national and European administrations to communicate electronically. ISA inherits this bulk of work and continues the effort.

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 D1.3. In addition to those explicitly mentioned below, the interoperability framework [IDABC-03] and the e-procurement specifications [IDABC-02] are important.

5.4.2 European Bridge CA Pilot

In 2004 IDABC started a pilot for a European Bridge CA[20]. 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 centralised administrative structure and a trust list distribution model based on a Trust-service Status List compliant to (an older version of) [ETSI-102-231]. 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 were the first to document the possibility to implement and easily maintain centralised TLs. The work on Trusted Lists was re-initiated by the Commission’s action plan [COMM-03] and has now been implemented by the EU.

A particular issue is that the list distribution service for the European Bridge CA 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 D1.3.

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

[19] http://ec.europa.eu/isa

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

5.4.3 Study on eSignatures for eGovernment Applications

The *Preliminary Study on Mutual Recognition of eSignatures for eGovernment Applications* [IDABC-01] was conducted by IDABC and published mid-2008. The issues identified by this study is at the core of identification of the issues that PEPPOL needs to address for e-signature interoperability, as documented in many sections of this part of D1.3.

5.4.4 The EFVS Study

The European Federated Validation Service study [IDABC-04] profiled existing validation services and solutions in Europe, made an assessment report, and concluded on a common solution model. There were close liaisons between the EFVS team and PEPPOL WP1 during the work, and [PEPPOL-D1.1] is one of the solution profiles presented.

The study identifies a number of challenges that validation solutions must address; hopefully PEPPOL is able to advance the state of the art in these areas. One conclusion of this study and other studies is that the e-signature Directive [EU01] should be expanded to cover more trusted services than merely eID issuers.

5.5 CROBIES

CROBIES (Study on Cross-Border Interoperability of eSignatures) was launched to support the action plan on e-signature and e-identification [COMM-03]. CROBIES started August 2008 and ended June 2010. There was close contact between the CROBIES team and PEPPOL WP1 during the work.

CROBIES' work on TL (Trusted Lists) [CROBIES2.1] has guided the TL system implemented by the EU, utilised by PEPPOL as described in D1.3 parts 4 and 7.

CROBIES' quality classification system [CROBIES5.2] is inspired by but somewhat different from the one presented in D1.3 part 7. PEPPOL has decided to not adopt this part of CROBIES' recommendation at this stage.

CROBIES' work on guidelines for interoperable implementation of electronic signatures [CROBIES5.1] is a major source of information for PEPPOL's work on signature policies, D1.3 part 3.

Additionally, CROBIES addresses some issues that are outside the scope of PEPPOL, such as common supervision model for issuers of qualified eIDs, interoperable qualified certificate profile [CROBIES3], and cross-border recognition of SSCDs (Secure Signature Creation Device).

5.6 EUROCHAMBRES

EUROCHAMBRES[21] 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[22].

InfoCamere (and InfoCert) from Italy are members of both EUROCHAMBRES and PEPPOL WP1 and maintains the relations.

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

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

5.7 Excursus European Bridge CA

European Bridge CA[23] 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 from the European Bridge CA.

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

6 Conclusion – PEPPOL Impact on European e-Signature Interoperability

PEPPOL aims to progress interoperability to a level where e-signatures can be recognised, verified and assessed cross-border in Europe for any purpose. In this, PEPPOL results may be used as a foundation for both EU policies and practical solutions for cross-border use of e-signatures. PEPPOL's topic of public procurement is the case study and proof of concept for the interoperability solutions.

The challenges of e-signature interoperability are primarily faced by the receiver (the relying party) of a signed document. Thus, PEPPOL focuses on solution to enable verification and acceptance of signatures at the receiving side. PEPPOL provides the following solution elements:

- A signature policy framework suitable for formalising the conditions for use of signatures (where such conditions are not implicit from the context) in a practical way. The signature policy framework allows expression of policies at several levels:
    - Use of signatures in (business) processes/protocols;
    - Commitments implied by a signature;
    - Technical conditions for signing, such as eID and signature quality and formats;
    - Signature verification and archival requirements.
- A quality classification system to assess eIDs and e-signatures towards requirements for quality and (national) approval status.
- Interface specifications for validation services that the receiver of a signed document can use to assess validity and quality of any eID and e-signature.
- Open source software implementation of a validation service and client software for integration to a validation service.
- Instantiation of validation services both based on the open source software and based on commercial services in the market.

Several service providers already support the PEPPOL XKMS interface, and the open source code provided by PEPPOL enables instantiation of such services when needed. Integration towards validation services is simple given the client side components provided. Thus, PEPPOL solutions can be used in any context, not only for public procurement.

Not all e-signature interoperability challenges are solved by PEPPOL. Note in particular the following:

- Signing in a user interface (e.g. of an e-tendering service) is not addressed. Solving this in a general way, i.e. any eID may be used for signing, is a separate, big challenge that is out of scope of PEPPOL. PEPPOL assumes that all actors are able to sign locally and that (e-procure¬ment) systems allow uploading of signed documents.
- Legal requirements in one country may be incompatible with products and services offered in another country. E.g. qualified signature is a mandatory requirement in some countries but in other countries products and services for qualified signature are not available.

7 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

[COMM-04] European Commission, Enterprise and Industry Directorate General: Standardisation Mandate to the European Standardisation Organisations CEN, CENELEC and ETSI in the Field of Information and Communication Technologies Applied to Electronic Signatures. December 2009, http://ec.europa.eu/information_society/policy/esignature/docs/standardisation/mandate/m460_en.pdf

[COMM-05] Commission of the European Communities: Commission Decision of 16 October 2009 setting out measures facilitating the use of procedures by electronic means through the 'points of single contact' under Directive 2006/123/EC of the European Parliament and of the Council on services in the internal market. Commission Decision 2009/767/EC, October 2009, http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2009:299:0018:0054:EN:PDF

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

[CROBIES3] Sealed, time.lex, Siemens: Study on Cross-Border Interoperability of eSignatures (CROBIES), Interoperable Qualified Certificate Profiles. CROBIES deliverable 3, July 2010, http://ec.europa.eu/information_society/policy/esignature/docs/crobies_deliverables/crobiesd3.pdf

[CROBIES5.1] Sealed, time.lex, Siemens: Study on Cross-Border Interoperability of eSignatures (CROBIES), Guidelines and Guidance for Cross-Border and Interoperable Implementation of Electronic Signatures. CROBIES deliverable 5.1, July 2010, http://ec.europa.eu/information_society/policy/esignature/docs/crobies_deliverables/crobiesd5.1.pdf

[CROBIES5.2] Sealed, time.lex, Siemens: Study on Cross-Border Interoperability of eSignatures (CROBIES), Quality Classification Scheme for eSignature Elements. CROBIES deliverable 5.2, July 2010, http://ec.europa.eu/information_society/policy/esignature/docs/crobies_deliverables/crobiesd5.2.pdf

[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

[ETSI-102-231]ETSI: Electronic Signatures and Infrastructures; Provision of Harmonised Trust Service Provider Information. ETSI TS 102 231 v3.1.2, 2009.

[ETSI-102-640] ETSI: Electronic Signature and Infrastructures; Registered Electronic Mail (REM) parts 1-5. ETSI TS 102 640 v2.1.1. 2010.

[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, On the Common System of Value Added Tax. Council Directive 2006/112/EC, 2006, http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2006:347:0001:0118:en:PDF

[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

[IDABC-04] European Federated Validation Service (Common Solution Model, Analysis and Assessment of the Solutions, 22 Solution Profiles). IDABC, March 2010, http://ec.europa.eu/idabc/en/document/7764

[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

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

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

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

[SEALED] 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

[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/

[XMLDSIG] World Wide Web Consortium. XML-Signature Syntax and Processing (Second Edition), W3C Recommendation, 10 June 2008; http://www.w3.org/TR/xmldsig-core