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 3: Signature Policies

Revision: 1.9.5

Authors:

Germany: bremen online services

Norway: Difi

Italy: InfoCamere, InfoCert

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

Greece: University of Piraeus

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

Revision History

Revision	Date	Author	Organisation	Description
1.0	2009/02/11			Complete version for internal quality assurance.
1.1	2009/02/27			Submitted to PEPPOL project management, approved with comments at project management meeting 2009/03/27.
1.2	2009/04/30			For publication, updated according to comments.
1.3	2009/11/06			Formal update of D1.1 after EC approval.
1.8	2010/09/24			Complete D1.3 version edited from D1.1 part 3. For internal quality assurance.
1.9	2010/09/30			D1.3 submitted to PEPPOL project operating office (POO) for approval.
1.9.5	2010/11/05			D1.3 ready for publication, updated according to comments from POO. Uploaded for EC approval.
2.0	2010/xx/xx			Formal update after EC approval.

Statement of originality

This deliverable contains original unpublished work except where clearly indicated otherwise.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

Statement of copyright

Table of contents

1 Summary and Structure of Document

1.1 Scope and Structure of Deliverable D1.3

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

D1.3 consists of the following documents:

Part 1: Background and Scope

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

Part 3: Signature Policies

Part 4: Architecture and Trust Models

Part 5: XKMS v2 Interface Specification

Part 6: OASIS DSS Interface Specification

Part 7: eID and eSignature Quality Classification

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

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

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

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

1.2 Demonstrator Software Components and Documentation

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

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

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

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

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

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

1.3 Scope and Structure of this Document

This part of D1.3 defines a signature policy framework that enables description of requirements for use of signatures in public procurement processes – as well as other processes. The purpose of a signature policy is to clearly describe the requirements imposed on the actors with respect to the following issues:

- When and how to sign in a business process;
- Authorisation and commitment implied by a signature or a set of signatures;
- Signing policy defining the requirements that must be fulfilled by a signer;
- Signature verification policy defining requirements to be fulfilled by the relying party (the receiver).

Following signature policy definitions in chapter 2, the scope of such policies in PEPPOL is refined in chapter 3 and an introduction to the structure of the signature policy framework is given in 4. Policy elements to specify use of signatures in business processes are given in 6. Commitment rules are specified in 7. Signing policy elements are given in 8 and signature verification policy elements in 9.

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.

This document is almost entirely restructured and rewritten with respect to the version published in PEPPOL deliverable D1.1 part 3.

Further evolution of the signature policy framework must be expected in the course of the PEPPOL pilots as experience is gained from real use of the framework.

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

1.5 List of Contributors

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

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

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

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

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

2 Signature Policy Introduction

2.1 Signature Policy Definition

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

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

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

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

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

A unique reference for a signature policy may be in the form of an OID (Object Identifier) or URI.

2.2 Signatures in Business Protocols

A business process may be anything from a single message (e.g. an invoice) to a complex task involving multiple parties and sequences of messages. Along with the process (protocol) definition, use of signatures (which documents shall/should/may/shall not be signed at what steps of the process) may be defined. This can be considered the top level of the signature policy in force.

Use of signatures in business process may be guided by legislative or regulatory requirements, contractual obligations, or by risk management decisions by one or several parties.

A signature policy framework must support specification of use of signatures in business processes.

2.3 Commitment Rules

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

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

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

Examples of such extended business scenarios are:

- Two (or more) primary signatures, such as buyer and seller on a contract;
- A countersignature as “authorisation” or witnessing of a primary signature;
- Signatures which are applied as part of a document flow, i.e. which assume a responsibility for a defined part of a document or transactional process;

- A combination of signatures all of which may be signed by another party, e.g. a notarial signature.

A signature policy framework should enable expression of such signature requirements, although even a simpler framework may be useful to express simpler cases of commitment rules.

2.4 Signature Validation Policy

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

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

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

In the signature policy framework presented in this document, these elements are structured in a slightly different way:

- Signing policy – rules to be followed by the signer;
- Signature verification policy – rules to be followed by the verifier (relying party),
- Rules on AAs, to the extent covered, are filed under commitment rules,
- Other elements are filed under either signing policy or signature verification policy as appropriate.

2.5 Signature Policy Representation

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

[ETSI-102-041] suggests content of a signature policy. This can be used to form a template for the mandatory human readable policy. The technical reports [ETSI-102-038] and [ETSI-102-272] define signature policy elements in XML and ASN.1 format respectively.

[CROBIES5.1] gives recommendations in direction of signature policies for interoperability in Europe, including elements that are recommended to be included.

This document is a framework for a human readable signature policy. The framework does not specifically follow the references above but is clearly influenced by these documents. D1.3 specifies some machine processable elements, see D1.3 parts 4-7.

The XAdES/CAdES/PAdES signature formats all include EPES (Explicit Policy Electronic Signature) variants that may incorporate an explicit signature policy reference for the policy to be used when validating the signature.

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

2.6 Referring to a Signature Policy

A purpose of a signature policy is to make the purposes and commitments of signing clear to the parties. Furthermore, one may argue that the desired WYSIWYS (What You See Is What You Sign) property is not only about the content to be signed but also about awareness of the conditions for signing.

To avoid later disputes, in particular about commitments implied by a signature, it is necessary to link the signature to the signature policy (whether it is explicitly defined and identified or implicitly defined). Requirements for the strength of this linking may vary.

The strongest link is achieved when the signer uses the EPES format of XAdES/CAdES/PAdES and an explicit signature policy reference. Thus, the signer signs not only document content but also the signature policy identification. The problem (in the current situation) is that support for the EPES formats is missing in many signing software platforms. Furthermore, the process of fetching the unique policy reference to include in the signed data object (and not in the document that is signed) may be cumbersome to a person. This situation may change over time, and use of EPES may be a desired situation in the longer term.

> Slovak legislation requires use of the EPES-formats with explicit signature policy identification and requires for multiple signatures that all parties refer to the same signature policy. Reference signature policies are defined by the assigned Slovak authority.

Without explicit reference to the signature policy, the link between signature and signature policy must be proved by other means. As an example, for a public procurement tendering process the signature policy (requirements) can be clearly stated in connection with the invitation to tender. All signatures received are then assumed to be according to the signature policy even though the signature policy is not explicitly referred to in the signed data object. All actors are required to know and adhere to the signature policy.

It is assumed that such implicit/contextual reference to a signature policy is sufficient in most cases for public procurement but a requirement is imposed to ensure that policy requirements are clearly stated and readily available for all relevant parties.

3 Scope of Signature Policies in PEPPOL

3.1 State on Use of Signature Policies

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

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

Consequently, PEPPOL WP1 has decided to revitalise the signature policy concept.

3.2 Current Signature Policies for Public Procurement

The term signature policy is not used by today's public procurement systems and policies are not explicitly stated but some information can still be provided. The goal described in REC03 of the IDABC study [IDABC01] pinpoints the challenge of PEPPOL WP1:

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

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

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

Assuming that both alternatives use proper strength cryptography and otherwise offer sufficient quality, a first approach at quality requirements could be to distinguish only between these two. However, there is a need for interoperability and thus definitions of security/reliability levels also for signatures based on non-qualifies certificates.

Quality and approval requirements for signatures in e-procurement vary significantly across member states. End 2007, IDABC [IDABC01] found 15 countries with e-procurement services for tendering in operation, where 6 required qualified signatures, 7 required advanced signatures (sometimes with the additional requirement of a qualified eID), while two countries required only authentication. The services furthermore either listed one or a few eID issuers or were able to accept all domestic issuers and perhaps a few foreign issuers.

Correspondingly, CIDX (Chemical Industry Data Exchange) surveyed requirements for signatures on e-invoices [CIDX] in 2008, finding 11 countries requiring qualified signatures for e-invoices; the rest presumably then accepting other signatures although requirements are not explicitly stated.

[IDABC01] states that the national accreditation schemes that exist in many countries pose an obstacle to interoperability. These are strongly related to national laws and for this reason it is practically infeasible for eID issuers to declare conformance with specific national requirements in a lot of different countries. PEPPOL's recommendation is that such accreditations schemes are either abandoned or kept at a national level, with requirements not imposed on eID issuers registered in other countries.

3.3 PEPPOL's Pragmatic Approach

In PEPPOL WP1's view, differences in national legislation as well as different requirements for different e-procurement processes necessitate development of a framework to enable specification of the crucial elements of signature policies. The specification must provide non-discriminatory rules for acceptance of eIDs to replace present policies for national solutions, which refer to domestic issuers or national accreditation schemes.

With respect to the constituents of a signature policy as described in chapter 2, PEPPOL's approach for the pilots is:

- Policy rules for use of signatures in business protocols are to be specified in human readable form[4].
- Commitment rules and authorisations must be described in human readable form linked to the policy rules for business protocols.
- Signing policy – the set of conditions that must be fulfilled by the signer, such as quality of eID used and signature format – shall be defined in a human readable way and some of the policy elements are defined in a machine processable way.
- Signature verification policy – the set of conditions that is controlled entirely by the receiver (the relying party), such as recording of verification metadata – shall be specified in a human readable way and a machine readable representation is a local decision.
- A subset of the signature policy elements can be signalled over the interface to a validation service in order to have the properties assessed by the service, notably quality of eID used; these elements must be defined in a machine processable way.

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

One will usually measure all signatures from all parties towards the same signature policy; however signatures from time stamping authorities and issuers of certificates and attestations [Siemens] may need to be addressed separately; these cannot in general be qualified signatures since they are not applied by natural persons. Use of TTPs is at least partly covered by PEPPOL's signature policies but signature policies for the signatures applied by TTPs are not covered.

3.4 Policy Framework

This document specifies a framework of signature policy elements, possible values for these elements, and relationships between them. Specific signature policies may then be defined by picking the relevant elements for the case at hand and the appropriate values for each element.

In addition to the experience gained by the PEPPOL WP1 team in the course of the project, [CROBIES5.1] has been a valuable source of information.

3.5 Policies to Be Defined along with Pilot Scenarios

Rather that postulating specific policies, this leaves the selection of values to the pilot scenarios. However, scenarios are presented including examples of requirements from several Member States resulting from national legislation or business practices.

[4] For some protocols this may be defined along with a processable definition of the protocols. This may be further explored in PEPPOL in conjunction with development of CEN ISSS/BII protocol profiles (see 6.2).

PEPPOL should define signature policies for its pilots whenever signatures are used. This applies to both tendering pilots, where signatures are particularly important, and to signatures in post-award processes (order, order confirmation, catalogues, invoicing). PEPPOL WP1 will co-operate with the PEPPOL WPs responsible for the different processes.

3.6 Only Advanced Electronic Signatures Considered

The EU's e-signature Directive [EU01], implemented in national laws in all Member States, guarantees the legal value of a qualified signature but also states that other e-signatures should not unduly be denied legal value.

The requirements of the e-signature Directive are implemented differently in different Member States. Some Member States place a lot of emphasis on qualified signatures. Other Member States have decided to accept legal value of advanced, non-qualified e-signatures and even "simple" (not advanced) e-signatures; typically these Member States still define requirements for the eID to be used, e.g. "advanced signature using qualified eID" (which is not the same as a qualified signature).

> Note: A typical scenario for a "simple" e-signature is that the user logs on to a service, uploads or creates (e.g. fills in a form) documents and explicitly clicks "submit". Logs have to provide reliable traces of the authentication, actions, and information submitted. Quality requirements will be imposed on the eID used for authentication; this need not be a PKI-based eID.

PEPPOL signature policies are based on the following assumptions:

- Only advanced electronic signatures are considered.
- Special attention is given to the two variants "qualified electronic signature" and "advanced signature using qualified eID". The latter alternative does not mandate use of SSCD (Secure Signature Creation Device).
- Interoperability of advanced signatures using non-qualified eIDs shall also be addressed; two examples are personal eIDs at lower quality levels and corporate (non-personal) eIDs.

3.7 Legal Considerations

National laws have supreme value in national context. A process or transaction using an electronic signature may be subject to explicit legal requirements. It is important that all Member States ensure that legal requirements do not block cross-border interoperability.

Note that for public procurement (the scope of PEPPOL), transactions will usually be carried out referring to the Contracting Authority's (the buyer's) governing law.

PEPPOL cannot change legislation but will point out problems and suggest interpretations that can overcome such legal problems. In most cases, the problem will not be the law but rather regulations or other governing documents that may be simpler to change.

The following principles are stated by PEPPOL:

- The signature policy applied must comply with its referred legislation.
- The signature policy shall as far as possible be specified independently from legislation. In particular, the policy shall not refer to specific national approval/accreditation/supervision schemes, specifications, profiles or other elements that one cannot expect foreign eID issuers or users to comply with.
- Requirements shall as far as possible be stated in general terms that can be fulfilled by actors in other Member States. As an example, a policy rule may, based on national legislation, require a

qualified signature but in this case the policy shall not refer to particular requirements imposed on issuers of qualified eIDs in the particular Member State.

- The signature policy shall as far as possible avoid requirements that are likely to cause conflicts with legislations of other Member States.
- The signature policy shall as far as possible be non-discriminatory with respect to e-signatures from other Member States, i.e. it should be possible to fulfil the policy based on products and services that can reasonably be assumed to be available in any Member State.
- It is recognised that that there are limitations to the previous bullet point. E.g. qualified signature may be required by some Member States but products and services supporting qualified signature are not available in all Member States.

As a general principle, PEPPOL builds on the assumption that:

- The national approval status of an eID or e-signature in one Member State shall be accepted by other Member States.
- In particular: A qualified eID and e-signature from one Member State must be accepted as qualified in other Member States. Member State A shall not refuse to accept a qualified eID or e-signature from Member State B on the grounds that the eID would not have been accepted as qualified according to Member State A requirements. (In short: Qualified is Qualified, everywhere.)

3.8 Parties Involved, Trust Service Providers

The main parties involved in an electronic signature process are:

- The signer,
- The relying party,
- The Trust Service Providers (TSP).

The signer (or the signers in case of multiple signatures) generates the document signature.

The relying party is the entity that shall rely on the validity of the signature(s), and that needs to ensure that the signature(s) fulfil the stated signature policy requirements. There may be more than one relying party for a specific signature.

A signature policy may refer to various trusted services offered by Trust Service Providers (TSP). Usually, the service will be offered by a TSP that is an independent third party with respect to the (business) protocol in question but the service may, if accepted by the other parties, be offered by an actor that is not independent. A TSP actor may offer one or more trusted service(s).

Some TSPs offer services directly to signers or relying parties. The following services are identified:

- Certification Authority (CA), issuing eID certificates to signers,
- Validation Authority (VA), providing validation evidence to relying parties,
- Time-Stamp Authority (TSA), providing trusted time,
- Attribute Authority (AA), providing trusted attributes outside of those contained in the eID certificate of the signer.

In a business protocol context, other trusted services may also be defined, such as:

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

A CA issuing qualified certificates is regulated by the EU's e-signature Directive [EU01]. Depending on national interpretation of the Directive, other CAs and other roles may also be subject to regulations according to the Directive. TSPs may also be subject to other EU and/or national legislation, e.g. the TSA and Notary roles are defined in some Member States but not all.

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

- Supervision and accreditation body for TSPs, notably for CAs,
- Trust Status List (TSL) issuer,
- Root-CA provider, acting as trust anchor for processing of certificates from underlying CAs,
- Bridge-CA provider, to link different PKIs through cross-certification with the bridge-CA,
- Product certification body, notably for certification of SSCD,
- Policy owner, where certificate policy or signature policy is governed by another body than the one responsible for the operational trust service.

There are other TSP roles that may be defined, such as Registration Authority (RA) for identification and registration of entities before a CA issues a certificate. A signature policy is concerned with use of certificates rather than certificate issuing, and the RA role can thus in this context be viewed as a part of the CA provisioning.

TSPs are discussed as needed in appropriate sections of the rest of this document.

3.9 Receiver Requested or Sender Initiated Signatures

The selection of business protocol and related options is a matter between the parties. As one alternative, actors may state which protocols they are capable of fulfilling, and other actors may try to match these requirements. One party may select the protocol to use or the parties may negotiate or refer to a common (e.g. standard) specification.

For public procurement, the Contracting Authority will usually set protocol requirements but there may also be elements of negotiation.

In a protocol, signatures may be used because the receiver (relying party) requires other parties to sign or because the sender (signer) independently decides to sign, if allowed by the protocol.

In the first case – requiring other parties to sign – the receiver must clearly state the signature policy requirements (relevant elements, not necessarily a comprehensive policy) that shall be fulfilled.

In the second case, the sender may state the signature policy used when signing. E.g. the sender's legislation or normal business practices may require a signature, while the legislation and practices of the receiver do not.

As a rule, the receiver should accept such signatures but the receiver may deny use of signatures or decide signature policy rules according to "unsigned OK – if signed, the following policy applies". See 6.1.1 for some more information on this topic.

3.10 Conversion and Use of Signatures

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

There are four possible solutions:

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

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

3.11 A Note on Logging, Archival, Records Creation

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

In archive records, time stamps are associated to documents as metadata. Records may be used in the execution of a business process, or be created at a later stage based on logs and other information collected during the process. An example of a record structure is a signed data object (SDO) such as XAdES [ETSI-101-903], CAdES [ETSI-101-733] or PAdES [ETSI-102-778] archive formats.

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

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

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

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

Chemical Industry Data Exchange (CIDX) has surveyed requirements for e-invoicing [CIDX], summing up country specific archiving requirements in a table. This table indicates requirements across EU for

storage period (varies from 4/5 to 10 years – ultimately 20 years in Switzerland), format received or format issued to be archived (in some cases both, probably meaning that they should be the same), requirements to store signatures (all countries require this but details, refer alternatives 1 and 2 above, are not known), and requirements for full on-line access to archive (all but 8 countries).

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

Verification in retrospect of an archival SDO is usually done by verifying the outer (archival) signature only. This signature is then trusted to attest to the correctness of the other information in the SDO; that this information was checked and found to be correct at the time when the outer signature was made. In principle, all other information in the SDO may also be verified but the process may be more or less cumbersome. Several software products, e.g. the Governikus platform used in Germany, support processing of such SDOs.

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

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

4 Structuring the Signature Policy Framework

4.1 Top-Down Approach

A top-down approach is needed, starting from the signature needs of business protocols and business scenarios. At the topmost level of a signature policy, it must be possible to express use of signatures in business processes in a precise way. This use will pose requirements at the next levels.

At the second level is specification of the meaning (semantics) of signatures including commitments and authorisations implied by signing something.

Then, at the third and lowest level the technical elements of signing and signature verification policies must be expressed.

A comprehensive signature policy will consist of many elements with referrals indicating that selection of a value for an element at a higher level may guide values for lower level elements.

4.2 Reusable and independent Policy Elements

All policy elements must be defined in a reusable way, and in a way that allows as far as possible each single element to be used in isolation without reference to or from other elements. As stated in 3.3, PEPPOL does not necessarily define all-encompassing signature policies; in many cases only certain elements may have to be defined.

4.3 Signature Policy Elements and Relationships

The figure below shows how signature policy elements can be grouped into the categories:

- Signatures in business processes;
- Commitment rules and authorisations;
- Signature verification policy;
- Signing policy.

The latter two are a separation of signature validation policy into requirements to be fulfilled by the verifier and signer respectively.

Typical elements (not all elements) are shown for each category.

The “signatures in business processes” category may pose requirements on all other categories, e.g. legislative requirements for technical implementation of signatures. The “commitment rules and authorisations” category may pose requirements on how to sign or verify. “Signature verification policy” may only be fulfilled if elements of the “signing policy” are fulfilled.

These are only relationships at a coarse level. More detailed relationships may be specified between signature policy elements inside or across signature policy categories.

[CROBIES5.1] suggests a guidance model for e-signature implementation and signature policy design. The policy elements and structuring suggested in this document are rather similar to the approach of CROBIES although some deviations exist. This document specifies policy elements and values at a greater level of detail than CROBIES, at least for selected policy elements.

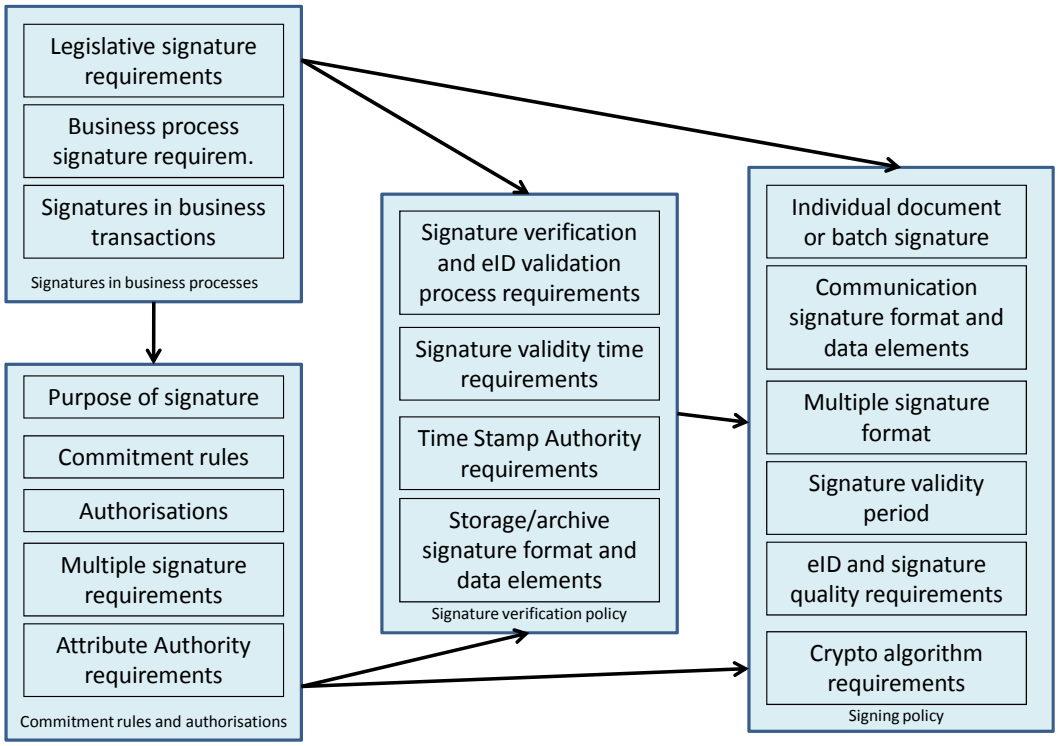

Figure 1: Signature policy categories, typical elements and relationships.

4.4 Signature Policy Development Process

[CROBIES5.1] suggests a phased approach to signature policy development:

- Phase 1: The Business Rules design phase describes the conditions under which signatures will be used within a business or application domain and process.
- Phase 2: The eSignature Implementation Rules design phase shall identify for each signature the associated management, procedural, operational and technical rules, including creation, validation and long-term aspects.
- Phase 3: The Signature Policy Documents design phase sums up all decisions into a human readable and, as far as relevant, machine processable forms.

As stated in 4.1, PEPPOL also envisages that a top-down approach will be used in most cases. The process is not formalised by PEPPOL (the CROBIES approach can be a good starting point). A signature policy for a pilot scenario in PEPPOL is outlined in chapter 10.

The process can be imagined as outlined below. In the context of PEPPOL, the actor developing the signature policy will be a public sector contracting authority, or perhaps rather a public sector agency developing a standardised set of policies on behalf of several or all contracting authorities in the given Member State. Service providers offering e-procurement services to public contracting authorities may also take a role in the development of signature policies.

1. Describe the process, e.g. a tendering process for public procurement.
2. Determine legal requirements for signatures in the process and add requirements resulting from risk analysis and other sources.

3. Map the requirements to signature requirements for each step of the business protocol, for each part (document) exchanged as a part of a step and whether or not a container signature can be used (e.g. signing a zip-file instead of signing each document).
4. State requirements for multiple signatures and their relationships.
5. For each signature required (or desired, or optional), state the commitment implied by the signature including authorisations needed.
6. Specify when, or for what period of time, an eID must remain valid.
7. Specify signing requirements, e.g. format requirements, eID and e-signature quality requirements and cryptographic algorithms or quality.
8. State the verification process that will be applied and describe requirements and solutions for archival, including archival format and later verification of an archive record.

5 Signature Policy Identification and Administration

5.1 Policy Element: Unique Signature Policy Identifier

As stated above, PEPPOL does not necessarily see the need to always define comprehensive, uniquely defined signature policies but the ability to assign an identifier must exist. An identifier may be an OID (Object Identifier) or a URI. Both may be specified for the same policy.

Unique signature policy identifier: OID or URI.

If several representations of a signature policy exist, they should use the same OID but may be referenced by different URIs. One representation must be declared as the authoritative version (could be done by a separate signature policy element but not included here).

To disambiguate between versions of a signature policy, new version should be assigned a new URI, thus enabling reference to older versions in contexts where this is relevant.

5.2 Policy Element: Signature Policy Version

Version number is needed, possibly also referring to previous versions of the policy.

Signature policy version: Version number, possibly revision history

5.3 Policy Element: Signature Policy Date of Issue

The date of issue for the policy is needed. Possibly, this can be amended by a “valid until” date if expiry or updating is scheduled.

Signature policy date of issue: Date of issuing of this version of the signature policy.

5.4 Policy Element: Signature Policy Hash

Using the URI alternative as an example, a relevant threat is that the content referenced by the URI is changed without notice; might even be due to a malicious action. To counter such situations, a hash value of the signature policy document should be used in addition to the unique identifier.

This approach is further specified for the EPES-variants of XAdES, CAdES and PAdES, see for example [ETSI-101-903] section 7.2.3.

The details of the hash computation are not specified here; note that hash algorithm and document to hash must be specified.

Signature policy hash: Hash value and algorithm identification.

5.5 Policy Element: Signature Policy Qualifier

See for example [ETSI-101-903] section 7.2.31 for a description of this element. Two qualifiers are at present identified: A URL where a copy of the policy may be obtained, a user notice text that should be displayed when the signature is verified.

Signature policy qualifier: URL to policy document or user notice text.

5.6 Policy Element: Signature Policy Issuer

This element identifies the party responsible for the signature policy. Contact information should be provided.

Signature policy issuer: Identification and contact information for responsible party.

5.7 Policy Element: Application Areas and Restrictions

If relevant, specific areas of application can be stated for the signature policy (e.g. tendering for public procurement) or restrictions can be specified if use of the policy for certain purposes or by certain actors shall be limited.

Application areas and restrictions: Specification of the areas and restrictions.

6 Signatures in Business Processes

6.1 Why sign?

6.1.1 Legislative Requirements

A main reason for use of signatures in a business process is that legislation in a particular Member State mandates use of an advanced or qualified electronic signature in order to complete the procedure at hand. The following should be noted:

- A particular business process may require an advanced signature in one country but not in another.
- For a cross-border process, the actors must select a legislation to refer to. For public procurement, the contracting authority's legislation will usually be referred to.
- Note that legislative requirements may extend to detailed technical requirements.
- Even if not mandated by the selected legislation, an actor may wish to use signatures in order to comply with his own, local legislation and the resulting normal business practices.

The last bullet point may pose a challenge. The public procurement Directives [EU-02] [EU-03] state that an actor shall not use signatures unless explicitly asked for, while the e-signature Directive [EU-01] states that at least a qualified signature should be accepted whenever electronic procedures are used. This may be explicitly clarified by a signature policy stating whether "may use signature" is acceptable, or alternatively "do not use" if signatures are not accepted.

6.1.2 Risk Management

Even if not mandated by legislation, a risk analysis may result in a decision by an actor to require signatures from counterparts or use signatures himself.

This may be particularly relevant in cross-border procurement where actors do not necessarily know or trust one another to a high degree in advance, and thus might want to opt for a strong commitment mechanism for non-repudiation purposes.

6.1.3 Contractual Obligation, Best Practices

Use of signatures may be decided by contractual obligations between the parties, e.g. for post-award processes according to a contract.

Best practice recommendations for a business process may state that signatures should be used, and actors may decide to adhere to a principle of following best practices.

6.2 Business Processes in PEPPOL

Business processes defined by PEPPOL are preferably standardised through CEN ISSS WS/BII[5]. These processes, realised as "business interoperability interfaces" are specified as profile descriptions focussing on organisational and semantic interoperability rather that the technical aspects. A profile description is defined [CEN-16073-1] as a technical specification describing:

[5] 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

- The choreography of the business process(es) covered, i.e. a detailed description of the way the business partners collaborate to play their respective roles and share responsibilities to achieve mutually agreed goals with the support of their respective information systems;
- The electronic business transactions exchanged as part of the business process and the sequence in which these transactions are exchanged;
- The business rules governing the execution of that business process(es), its business collaborations and business transactions, as well as any constraints on information elements used in the transaction data models;
- The information content of the electronic business transactions exchanged by pointing to a given data model for each of the business transactions.

With respect to signature policies, requirements for signatures may be part of the business process choreography on an overall level. The second and third bullet points are however more relevant: use of signatures in the business transactions and the role of signatures in the governing business rules.

> The specifications of CEN ISSS/BII should incorporate placeholders for specification of signature requirements and may give recommendations on use of signatures in business processes. In the time frame of the PEPPOL pilots, this will not be the case but signature policies may be defined as additional elements to the business protocol specifications.

The last bullet point is less relevant as the signature as a mechanism should be independent from the data model and information content actually signed. The technical BII profiles specify how to sign any BII XML business document by applying an XML DSIG [RFC3275] or XAdES BES [ETSI-101-903] signature.

Apart from this technical specification work, the current status of the BII profiles is that signatures are not covered; [CEN-16073-1] states that “e.g. signature of contract document is not supported by current BII profiles”. The results of this D1.3 part 3 may potentially add this aspect to the BII profiles.

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

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

6.3 Sources of Signature Requirements

6.3.1 Policy Element: Legislation

This signature policy element identifies the national legislation governing other elements of the signature policy and to be applied in case of disputes. Legislation will usually be determined by the actor initiating the business protocol, e.g. the contracting authority for public procurement.

> *Legislation: Select country and/or region if regional legislation applies.*

6.3.2 Policy Element: Legislative References

This signature policy element should list laws, regulations and other rule sets that govern use of signatures for the business process in question. References to paragraphs should be given, and in order for a foreign actor to understand requirements it is recommended that the requirements are explicitly stated.

> *Legislative references: List of laws, regulations, other rule sets with paragraphs and preferably explaining text.*

6.3.3 Policy Element: Risk Management References

If use of signatures in the business process is based on a risk management decision, a referral to this fact may be given:

> *Risk management references: Referral to or citation from risk management decision.*

6.3.4 Policy Element: Contractual, Best Practice, Other Reference

If use of signatures for the business process is covered by some contractual relationship, business best practice recommendations, references or statements to this effect should be made:

> *Contractual, best practice, other reference: Referral to or citation from contracts or other relevant documents.*

6.4 Signatures in Business Protocol Messages

6.4.1 Introduction, Including Multiple Signatures

A business protocol may on one hand be just one message/document sent from one party to another. At the other extreme, the protocol may also be a complex sequence of messages containing multiple documents exchanged between multiple parties.

The business protocol signature policy as specified by this document treats single steps of the business process assuming that only one side of the protocol signs for each step (might be multiple signatures internal to this actor); e.g. in a scenario where a contract is signed by two parties, the first party will sign in one protocol step, while the second protocol step would be the other party verifying the first signature and then applying the second signature, see next section and section 8.2.8.

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

Examples of such extended business scenarios are:

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

To this can be added that several signatures may be needed even for one actor (company) to represent the authorisations needed for the commitments represented by a document (see 6.4.3).

PEPPOL does not endeavour to outline highly complicated, multi-signature policies but it must be easy to cover at least simple cases such as primary signatures on a contract. Although many trusted roles are identified in 3.8, only a few of these (and their signatures) are considered in the current signature policy framework.

6.4.2 Policy Element: Content Previously Signed

This policy element is the minimum to indicate that multiple signatures shall or may be used (by different parties).

> *Content previously signed: Required, optional, not allowed.*

Required means that at least one other actor must have signed in advance, e.g. the other party signs the contract first. Optional may for example mean that the sequence of the signatures is irrelevant. Not allowed means that this actor signs first.

More elaborate policies defining sequences of signatures may be defined. Note that by applying commitment rules as defined in the next chapter to each signature, one should be able to define many rules applying to such sequences.

If previously signed, existing signatures shall be verified according to the signature policy in force before the signer adds his own signature.

The technical details on how to apply further signatures on a previously signed element are covered by the signing rules, see 8.2.8.

6.4.3 Policy Element: Multiple Signatures for same Actor

This policy element specifies whether an actor may apply more than one signature in order to represent the necessary authorisations implied by signing.

Multiple signatures for same actor: Required, optional, not allowed.

If required or optional, commitment rules should be applied individually to each signature. Further signature policy elements could be defined to this effect. Not allowed means that one signature (usually one person) must have sufficient privileges to sign alone.

6.4.4 Policy Element: Signature in Business Protocol Step

A requirement for use of signatures may be stated at an overall level for a business protocol step, defined as the transmission of a protocol message containing one or several parts.

Signature required: List of values: Shall, should, may, shall not be signed.

This may be posed as an overall requirement for a business protocol step. The overall requirement may also be omitted, referring to specification of signatures for individual parts of a multi-part protocol message (see next section).

If stated at this overall level, signing of a multi-part message is left unspecified. Therefore, use of signatures should be further detailed as in the next section.

> A default value should be assumed if no explicit statement is given. The default may, unless guided otherwise by signature requirements sources, be that a business protocol step MAY be signed.

The “shall not” part is needed. A protocol may specify that signatures shall not be used unless explicitly accepted by other parties.

A business protocol may be well-defined or ad hoc. For a well-defined protocol, the signature element should be part of the protocol specification. For ad hoc communication, the signature element may be signalled as part of a negotiation procedure. Unless explicitly instructed not to sign, a sender may independently decide to sign as part of a protocol step.

> One may argue that a qualified signature shall always be accepted even when the receiver has stated no need for signatures; however this may be interpreted differently in different Member States.

6.4.5 Policy Element: Signatures on Multi-Part Messages

For a multi-part message, the signature policy element in the previous section should be replicated for each part to indicate the need to sign each individual part. If not replicated for each part of the message, the default value (e.g. may) shall apply to each part.

Repeat for all parts of message:

Signature required: List of values: Shall, should, may, shall not be signed.

The policy element will usually refer to categories rather than specific document types but this depends on the protocol step.

As an example: A tendering document may consist of a cover letter and attachments. A signature policy may state that the cover letter shall be signed, while attachments may be signed.

6.4.6 Policy Element: Batch Signature Allowed

When several parts of a multi-part message are signed, there is a need to specify whether or not a batch signature shall or can be used. With a batch signature, several message elements are assembled into one signed data object. Examples of such assembly methods are:

- Signing a zip-file composed from message parts,
- Signing an EDIFACT exchange composed from several EDIFACT elements.

Batch signature allowed: List of values: Shall, should, may, shall not be used.

If not allowed, each part must be individually signed whenever signature is required.

German example: A dispute over a signed zip-file consisting of multiple parts was ruled to acceptance of the signature as a qualified signature on the documents of the zip-file.

Norwegian example: In the health care sector, messages may have to be signed individually by the medical practitioner. Messages (e.g. bills from a practitioner to the public authority responsible for paying) are frequently assembled into an exchange, which in turn is signed (mandatory) using a corporate eID of the practitioner's organisation.

The Norwegian example shows that batch signatures may be used in addition to signatures on individual parts. This can be handled as a multiple signature requirement.

6.5 Notes on Additional Policy Elements

Even at the business protocol level, format requirements may be posed. This could be document format, signature format or batch format for aggregating several parts into one container. These are not included in the signature policy, e.g. batch format is not considered, only whether or not signing such a container is allowed.

Requirements for multiple signatures are treated in the next chapter under commitment rules. One may argue that multiple signatures should be a business protocol requirement but one may also treat signing by several parties as separate steps of the business protocol, resulting in a requirement like:

In this step you shall verify the signature(s) already applied to the content, and only if verification is OK, you should also sign – specifying through multi-signature policy elements how this signing shall be done.

7 Commitment Signature Policy Elements

7.1 Introduction

Note: This chapter shows how commitment rules can be specified for an individual signature. If multiple signatures are used, the policy elements should be repeated and specified individually for each signature.

This signature policy framework does not at present contain elements to combine authorisations from several signatures; this must be specified by the business protocol rules.

With respect to commitment and authorisation, the usual requirement in Member States is that, when a signature is required, a personal signature from an authorised person is needed.

Since a signature binds to the name in the eID, and this usually is a person name only, the signature in itself gives no assurance about authorisations. The receiver may then need additional assurance that this signature also represents the signer's organisation and that the person has the required role and authorisations.

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

Information on binding of person identification to a company, roles and authorisations should be considered as claims about identity attributes that are additional to those included in the eID certificate. A signature policy should then make clear:

- The claims that are assumed by a signature, e.g. that a person is authorised to sign on behalf of the company for a given amount.
- The assurances that are required to support those claims.

In the signature policy definitions cited in chapter 2, use of attribute authorities is classified as a part of signature validation policies, indicating a more technical approach at attributes. In the context of public procurement, attributes are rather related to business roles and authorisations and thus handled in this chapter. Use of attribute *authorities* is not detailed but business registers and/or issuers of VCD (Virtual Company Dossier) as specified by PEPPOL WP2 are mentioned. Use of identity providers for additional attributes is a possibility but not explored by PEPPOL. The STORK pilot project[6] conducts work on trusted attributes.

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

The use of corporate, non-personal eIDs for signing (or sealing, which is the term used in some places for this kind of signature) and use of employee eIDs that also bind to company name may be used to attest that a signature represents a company. Use of such eIDs may be listed as alternatives in signature policies but such certificates cannot be assumed to be generally available.

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

7.2 Policy Element: Purpose of Signature

There may be a need to state the purpose of a particular signature. This can be stated by the receiver: “When I receive a signature on this message/transaction, I will consider it as a signed contract” or mediated by the sender: “This signature attests that I am the author of this document”. This must then be compared to the role and authorisation information about the signer; both signing for the correct purpose and possessing the authorisations that allow the person to sign that way.

A set of general statement may be defined plus it may be possible to extend by separate definitions or free text statements. An example of a starting point is the way this can be done for PDF signatures [PDF(v1.6)] by creating a set of commitment statements.

> *Signature purpose: List of statements to select one or more from, possibly also free form statement.*

Examples:

- This is a transport signature only (authentication and integrity protection),
- I am the author of this document,
- I attest to the correctness of this document,
- I approve the content,
- I attest to this signature (countersignature),
- I sign this contract,
- ... and so on.

7.3 Policy Element: Authorisation Statement

There may be a further need to specify authorisations necessary – like the ability to sign on behalf of the company for the sum implied by a contract.

> *Authorisation statement: List of statements to select from, possibly one or more statements that shall be included, possibly also free form statement.*

Examples:

- I am managing director for company NN,
- I am authorised to sign this contract on behalf of company NN,
- ... and so on.

This may point at a need for multiple signatures where the combination of authorisations attributed to different persons is needed to achieve the task.

7.4 Policy Element: Assurance Level for Company, Role, Authorisation Attributes

Additional attributes concerning company, roles and authorisations should be regarded as claims that in a given context may have to be supported by assertions of a given assurance level.

> *Assurance level for company, role, authorisations: Selection of alternatives.*

Appropriate assurance level can be specified in a number of ways, including use of external sources for attestations. As an example, six approaches for use of e-signatures in tendering are outlined below. The alternatives are:

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

7.4.1 Alternative 1: Accept Signed Documents

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

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

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

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

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

7.4.2 Alternative 2: Registration Procedure

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

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

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

Example Italian Approach (CONSIP eTender – Ministry of Economy and Finance)
Q. In which phases of the e-procurement process (e.g. notification, tendering, awarding, etc.) is there a need for signatures?

A. For the registration procedure and the final offering

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

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

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

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

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

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

7.4.3 Alternative 3: Attestations, Attribute Certificates, VCD

Registration is done through a trusted identity service provider.

In this alternative, independent proofs of roles and authorisations are required for all or parts of the information. This may be mediated using:

- An attribute certificate issued by a trusted actor and attesting to the information,
- Separate certificates and attestations, possibly assembled into a VCD,
- A Virtual Company Dossier (VCD) as studied by PEPPOL WP2,
- Reference to a trusted business register from which the information can be verified based on the person's name/identifier.

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

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

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

- Syntax and semantics of attributes representing roles and authorisations must be standardised and agreed among all users of a register.

- Roles and authorisations must be linked in the register to name used in the eID, or to a unique attribute of that name. National identifiers for persons are used to this effect but use of such identifiers across borders is not straightforward, and identifiers do not exist in all countries.

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

- The economic operator fetches the information from its local register, obtaining a data structure or document that should be signed by the register authority.
- The (tendering solution used by the) awarding authority requests the information, possibly through a chain of registers such as devised by the BRITE project[7]. In this case, authenticating the register (e.g. by use of the TSL protocol) should normally be sufficient; if the register is trusted, no signature is necessary (signature from register may still be an option).

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

It is also possible to register attributes at an identity provider and have the attributes conveyed e.g. in a SAML token when a user authenticates to the e-tendering service. This will not be tried in PEPPOL as the approach is too far from common practice to be useful in a pilot; such an approach is however piloted by STORK. In yet another approach, a company may itself make some of its internal directory information concerning names, authorisations and roles available to external parties, who in that case must be able to understand the information. This approach places too high requirements on economic operators and is not recommended.

7.4.4 Alternative 4: Employee eID Binding Person to Company

Within corporate PKIs, eIDs will usually identify the company in addition to the person. Such eIDs may also be issued by external eID issuers, if allowed by the company in question since the registration procedure must ensure not only that the name of the person is correct but also that the binding to the company is correct. The eID may even be at qualified level although most corporate PKIs are at a more modest quality level.

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

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

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

7.4.5 Alternative 5: Corporate eID without Person Name

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

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

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

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

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

7.4.6 Alternative 6: Combination Personal and Corporate Signature

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

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

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

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

7.5 Policy Element: Attribute Authority Requirement

Note that [ETSI-102-038] defines use of attribute authorities as a signature validation policy element. In the context of PEPPOL, and perhaps most other contexts as well, attributes are rather associated with (assurance of) claims about authorisations and roles.

Apart from the use of trusted business registers and VCD issuers discussed in the previous section, this signature policy framework does not cover the use of attribute authorities. In the VCD or business register cases, attributes are conveyed in separate documents.

> *Attribute authority requirement: Placeholder for signature policy element that may be a textual statement.*

Attributes may be issued in the form of X.509 attribute certificates, SAML tokens, XACML (eXtensible Access Control Markup Language) statements or otherwise. These elements may be included in signed data objects but will be separately signed.

As one example, STORK lists a set of personal attributes (no business context in STORK) such as name, address, age etc. that are usually not included in eID certificates but may be requested to be returned in the SAML token issued during an authentication process. The SAML issuer – in the user’s home country – will fetch the attribute values from trusted sources and act as the attribute authority upon issuing the SAML token.

7.6 Policy Element: Notary and Other TTP Requirement

The notary role is recognised and in common use in some Member States. Although it is potentially useful in some public procurement cases (e.g. contracts), the role is not discussed here and neither

are other possible TTP roles except for the TSA (Time Stamp Authority) role which is discussed in 9.3 below.

> *Notary and other TTP requirement: Placeholder for signature policy element that may be a textual statement.*

8 Signing Policy

8.1 Introduction

This part of the signature policy specifies the rules that must be adhered to by the signer. A signing policy as specified in this chapter is intended to be used by a receiver (relying party) of a signed document to explicitly request actions by the signer. The signer might also explicitly refer to these policy elements but in reality they will anyway be implicitly defined by the signature in this case.

8.2 Communication Signed Data Object (SDO) Requirements

8.2.1 Introduction

By applying one or more signatures, one creates a signed data object (SDO). The overall requirement is the format of this SDO, while more detailed requirements may specify information elements to include in an SDO. Probably, more elements than those included below could be specified, looking at possible elements defined by the various SDO formats.

There is a need to differentiate between signature formats for communication and storage. Upon signing a document, the sender creates as communication signature format. The receiver may add on information elements to this format to achieve a storage/archival format. E.g. XML DSIG or XAdES-BES may be used in the transfer of an XML document, while the receiver creates an XAdES-A object for archival. The list of formats (see next section) is the same but the signature policy will normally specify different selections for communication and storage formats.

8.2.2 Policy Element: Communication SDO Format

The first requirement to the signer is the SDO format to use, or (preferably) a list of allowed standard formats specified as references to standards plus possibly more detailed requirements related to options and profiles of the standards.

Communication signature format: Selection of allowed formats, alternatively restrictions.

List of formats:

- CMS [RFC5652]
- PKCS#7 [RFC2315]
- XML DSIG [RFC3275]
- PDF inline signature [PDF(v1.6)]
- XAdES with variants [ETSI-101-903]
- CAdES with variants [ETSI-101-733]
- PAdES with variants [ETSI-102-778]
- Others (e.g. S/MIME [RFC1847], Microsoft variants, EDIFACT signature etc.)

Some signature formats are closely tied to document formats, notably XML DSIG and PDF inline signature. However, document format requirements are not part of a signature policy. The general signature formats, which can be used with any document format, are CMS, PKCS#7, and CAdES.

An issue for a signature policy may thus be e.g.: I have a PDF document, shall I sign by a PDF signature or is a CMS signature allowed?

As a starting point, PEPPOL recommends placing few format requirements on the sender; the sender should be allowed to sign using the format supported by local software. This adds to the complexity on the receiving side, having to handle different formats.

In the longer term, the XAdES/CAdES/PAdES standards should be referred to. For communication, the simpler variants of these standards, such as BES, should be used. If signature policies are defined in a comprehensive and identifiable way, the EPES variant can be used.

Some signature policy requirements may implicitly restrict the selection of signature formats, e.g.:

- Signature type (wrapping, independent, embedded);
- Multiple signature modes;
- Use of TSA time-stamps.

Not all alternatives for such elements can be supported by all signature formats.

8.2.3 Policy Element: Signature Type

With respect to the document, a signature may be:

- Wrapping, i.e. the document is part of the signature; an example is a CMS signature that results in a “p7 object”.
- Embedded, i.e. the signature is part of the document; examples are PDF signatures and XML DSIG.
- Detached, i.e. the document remains the same while the signature object is independent but associated with the document; e.g. a CMS detached signature in a separate file.

Not all signature formats can support all signature types.

> *Signature type: List of: Wrapping, Embedded, Detached.*

Selection of signature type is primarily a matter of processing convenience. One cannot really say that different signature types imply different semantics for the meaning of the signature.

PEPPOL thus recommends not placing particular requirements for this policy element. An exception may be for use with multiple signatures, e.g.:

- A wrapping CMS signature may be cumbersome with respect to the WYSIWYS (What You See Is What You Sign) properties for multiple signatures, as the document content is not readily readable for the second signer.
- A detached CMS signature may be cumbersome if it is required that the next signature shall cover both document content and previous signatures.

8.2.4 Policy Element: Data to Be Signed

With some signature formats, the entire content is always signed, while for other formats (e.g. XML DSIG) one may sign only parts of the content. Additional elements may be included in the data to be signed, e.g. the signer’s certificate and the signing time.

If particular considerations exist, the signing policy should detail data to be signed requirements. Details are not discussed further in this document.

> *Data to be signed: Specification of elements that shall be included in the data set to be signed, or explicitly kept out of the data set.*

Keeping elements out of the data to be signed can be beneficial e.g. if some elements are to be changed by the receiver.

As a rule, PEPPOL WP1 assumes that the entire content is signed while other elements to include in the data to be signed are not specified.

8.2.5 Policy Element: Certificates and Certificate Path

For many signature formats, including the signer's certificate is optional, as well as including the path to a root-CA certificate. A signer certificate may be identified by a reference consisting of certificate serial number and name of CA.

This policy element states whether a certificate reference is allowed, signer certificate MUST be included, or path MUST be included with a signature. If a reference is allowed, the signer MAY still decide to include certificate or path, and if certificate is required, the signer MAY also decide to include path.

> *Certificate and Certificate Path: List of values: Certificate reference allowed, Signer certificate to be included, Certificate path to be included*

In PEPPOL's approach, the signer certificate *must* be included. Including the path is as a starting point optional since only CAs known in advance by the validation service (federation) can be handled. There may be however be national requirements to include path.

8.2.6 Policy Element: Revocation Information

Some signature formats allow revocation information in the form of a CRL and/or OCSP response valid at the time of signing to be included by the signer. A relying party may then only need to check this revocation information instead of performing its own call to a CRL or OCSP service.

Trusting revocation information supplied by the signer implies trust in the correspondence between the time of signing and the timeliness of the revocation information. In practice either:

1. The relying party must trust the signing time submitted by the signer (or require a TSA time-stamp), or
2. The delay from the sender fetching the revocation information until signature verification by the relying party must be small enough for the relying party to regard the revocation information as "fresh".

A signature format may allow only CRL, only OCSP, or both alternatives to be included. Thus, not all alternatives can be supported by all signature formats. Use of other revocation information formats such as SCVP or XKMS (e.g. from a PEPPOL validation service) is not considered.

> *Revocation information: List of values: Not to be included, Optional OCSP response, Optional CRL, Optional OCSP or CRL, OCSP to be included, CRL to be included, OCSP or CRL to be included, other values are possible (e.g. SCVP, XKMS).*

In the PEPPOL approach, the relying party shall always check revocation status by use of the VS. Thus, inclusion of signer side revocation information shall not be mandatory. There is however no need to pose a stricter requirement than: The signer *should not* include revocation information. If included, the relying party may simply discard the information. The only reason for denying revocation information submitted by the signer may be to avoid large CRLs in signed data objects.

> In Germany, the relying party is required to perform a check of the certificate path including revocation status. Revocation information submitted by the signer cannot be used.
>
> The Norwegian BankID system[8] has no publicly available revocation checking service. When a document is signed using BankID, an OCSP response is always included in the signed data object. A relying party outside of the BankID community must trust this OCSP response. (A

[8] https://www.bankid.no

solution to PEPPOL is to ensure that a VS covering Norway has access to the restricted BankID OCSP service; at the time of writing, use of BankID is not considered for PEPPOL pilots.)

Depending on the configuration of a validation service (VS) (this behaviour is not specified by the XKMS interface, D1.3 part 5), the VS may choose to return as much information as possible even though the information is not complete; e.g. the VS may verify the certificate path of a BankID certificate and return the fact that a Norwegian BankID is a qualified certificate, even if the VS cannot check revocation status. The relying party may then use the VS to assess certificate validity and quality and decide to trust the revocation information submitted by the signer.

8.2.7 Policy Element: Signing Time

Most signature formats can include signing time. Some signature formats can include also a time-stamp from a TSA. Unless a TSA is used, the signing time must be treated as a purported signing time. The relying party may decide to trust the signing time.

Include signing time: Not allowed, Optional, Mandatory, TSA time-stamp mandatory.

The latter option may not be desired but is included for completeness.

The need for inclusion of signing time depends on the relying party's selection of "verification time policy" (see 9.2). If "time of signing" is used, signing time is mandatory (and must be trusted, whether or not it is from a TSA); however this is not the recommended policy for PEPPOL.

PEPPOL suggests "optional" as a default policy for its pilots. There is no reason to discourage the inclusion of signing time but the practical value is in most cases limited.

8.2.8 Policy Element: Multiple Signature Format

Signing a document that is previously signed can be done in three ways:

- Parallel signature: The new signature covers document content but not previous signatures,
- Sequential signature: The new signature covers document content and previous signatures (the alternative that some, but not all, previous signatures are covered is not further considered here),
- Countersignature: The new signature covers one or more previous signatures but not document content.

It is clearly possible to assign different meaning (semantics) to the different variants, e.g. a countersignature attests to the correctness of a previous signature, not to the correctness of the document content. A sequential signature emphasises the ordering of the signatures.

Multiple signature format: Parallel, Sequential, Countersignature.

In the current state of the art in signature creation environments, including user friendliness and user understanding, PEPPOL suggests not placing too much emphasis on the possible semantics of multiple signature formats. A user cannot today be assumed to understand the differences between the alternatives.

PEPPOL's advice is to make the purpose of each signature clear by use of "commitment rules" policy elements (see chapter 7); e.g. if the purpose of the signature is "countersignature", but the signature is embodied as a sequential signature, this should be accepted.

Two probable exceptions are:

- A countersignature should not be used when the requirement is a signature on document content, even though the countersignature *may* be said to "indirectly" sign document content.

- A parallel signature should not be used when the requirement is a countersignature, although if signing time is included with signatures, the countersigning property *may* be deduced.

Note that multiple signature scenarios can be made almost arbitrary complex by mixing parallel, sequential and countersignatures using different SDO formats. A simple example is a PDF document signed first using an embedded PDF signature, and then wrapped in a CMS SDO for the second signature. Although SDO formats may be specified independently for each signature, a prudent advice is to try to avoid too complex scenarios.

8.3 Policy Element: Signature Validity Period

A signature validation policy may require that signatures remain valid for a period of time, e.g. until the end of a work process like public tendering. Such a requirement simplifies processing at the relying party side since signature verification until the specified time can always be done by checking that the signature is still valid (see 9.2).

It is not expected that a start time is necessary; a signature must be valid from the time of signing until the end of the validity period.

> *Signature validity period: Valid until time.*

Member State legislation may prohibit such a signature policy element to be used, e.g. require that a signature valid at the time of signing shall be considered to remain valid.

The signer can guarantee that the eID will not expire before the stated time but cannot guarantee that revocation will not happen. Backup procedures should be in place to ensure e.g. that a tender is not rejected because a signer had to ask for revocation of the eID during the (perhaps duration of months) tender processing at the contracting authority.

8.4 Certificate (eID) Requirements

8.4.1 Policy Element: Certificate Format Restrictions

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

> *Certificate format restrictions: Free text statement referring to profiles or other certificate information.*

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

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

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

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

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

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

8.4.2 Policy Element: Subject Name Restrictions

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

> *Subject name restrictions: Free text statement referring to profiles or other certificate information.*

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

A unique identifier in the subject name in a certificate may be defined in the context of:

- Country or application area, i.e. the identifier is assigned by an authority outside of the CA;
- The CA, i.e. the identifier is reused for all certificates for the same person;
- The certificate, i.e. the identifier may change between (generations of) certificates for the same person.

A particular issue is persistence of names. If the same name (identifier) must be used for an entire procurement process or even for subsequent processes involving the same actor, then in most cases the user must use the same eID certificate (e.g. instead of using the identifier from the subject name, the certificate serial number may be used). A further problem concerns identification over generations of eIDs even from the same CA. If the user must renew the eID, most solutions will guarantee reuse of name and identifier but exceptions exist (e.g. Germany) where the user may get a new identifier and thus will not be recognised as the same user.

8.4.3 Policy Element: eID Quality

Acceptance of a signature may require use of an eID of sufficient quality. This policy element corresponds to the *claimed quality* from certificate policy as described by D1.3 part 7 and XML definitions in D1.3 part 5.

> *eID quality: Level 0-7 as defined in D1.3 part 7, alternatively as in TSL: qualified eID, qualified signature.*

8.4.4 Policy Element: eID Assurance Level (and Approval Status)

This policy element corresponds to the assurance level as defined in D1.3 part 7 and XML definitions in D1.3 part 5; the assurance that the claimed quality is actually fulfilled by the CA. Notably, this *may* refer to national approval status (accreditation or supervision).

> *eID assurance level: Level 0-8 as defined in D1.3 part 7, alternatively as in TSL: supervised or accredited issuer (of qualified eID).*

Note: In PEPPOL's view, discriminating between an accreditation and a supervision model for qualified eIDs shall not be allowed.

8.5 Algorithm Requirements

8.5.1 Introduction

Requirements may be posed for strength of the cryptography used: hash algorithm and public key algorithm including key length. Alternatively, a list of accepted algorithms may be used, either separately for hash and public key crypto or combined as requirement for the crypto suite. However if algorithms are listed, care must be taken not to pose requirements that will exclude actors from other Member States.

8.5.2 Policy Element: Hash Algorithm Quality

Hash algorithm quality: 1-5 as specified in D1.3 part 7.

8.5.3 Policy Element: Hash Algorithms accepted

Hash algorithms accepted: List of hash algorithms.

8.5.4 Policy Element: Public Key Quality

Public key algorithm quality: 1-5 as defined in D1.3 part 7.

8.5.5 Policy Element: Public Key Algorithms accepted

Public key algorithms accepted: List of public key algorithms including key length.

8.5.6 Policy Element: Crypto Suites accepted

Crypto suites accepted: List of crypto suites (combinations of hash and public key algorithms).

9 Signature Verification Policy

9.1 Introduction

This part of the signature policy is in principle local to the relying party but there may still be a need to state the policy requirements towards other parties such as the signer.

9.2 Policy Element: Validity Time

A signature policy should specify at which time(s) in the work flow signatures must be valid. The alternatives are:

- Valid at time of signing; this can only be achieved if the relying party trusts the signing time supplied by the signer (or the signer supplies a TSA time stamp).
- Valid at time of first verification by relying party; e.g. the time of receiving a tender or the time of opening a tender. This alternative requires evidence of the verification process to be captured and stored at the time of verification. This alternative may be combined with use of the "signature validity period" policy element.
- Valid at time of verification; this implies that eID certificates must be valid (not expired nor revoked) until the end of the business process (e.g. tendering). This alternative should be combined with use of the "signature validity period" policy element (see 8.3).

Validity time: Time of signing, Time of first verification, Time of verification.

With respect to the first alternative: Note that the signature may be applied "a long time" before sending the document. For procurement processes, the time of delivery is of importance, not time of signing. Thus, the "valid at time of signing" alternative is in general not recommended by PEPPOL but Member State legislation may state that this shall be accepted.

With respect to the second alternative, a recommendation is to capture the necessary information in a standard format at the time of first verification, e.g. XAdES/CAdES-X variant like XAdES/CAdES-X-L. With PAdES, the signature creation application may have to make provision for the space necessary for insertion of a timestamp at the time of first verification. The verification information may also be captured in a proprietary format or by means of logs, databases and other information recording means.

Use of a revocation grace period, where signature/eID verification is delayed until after the next scheduled issuing of revocation information by the eID issuer, is considered a local policy decision. Note that national requirements for revocation grace period may exist. The specifications of PEPPOL D1.3 do not at present address revocation grace period.

9.3 Use of Time-Stamp Authority (TSA)

9.3.1 Introduction

A TSA may be used in different contexts and may itself be subject to detailed policies [ETSI-102-021]. PEPPOL *does not* address the problem of cross-border recognition of TSAs. PEPPOL's approach is the following:

- The receiver (relying party) may use a TSA as a local matter and in case will select a locally trusted TSA.

- The receiver should not request a TSA time stamp from the sender; since the TSA role is defined and services exist in only some Member States, this will restrict cross-border interoperability.
- If the sender independently decides to apply a TSA time stamp, the receiver should be able to process this but is not required to pay attention to the fact that the time stamp exists nor to the time indicated.

Thus, neither a detailed policy for use of a TSA nor a TSA policy is detailed in this document and use of a TSA is considered part of the signature verification policy (could also be specified by business process rules as well as signing policy).

9.3.2 Policy Element: Sending Side initiated Use of TSA

A TSA time-stamp may be used by the sending side (either initiated by the signer or at a later stage of the workflow on the sending side). The receiver (the relying party) may explicitly pose a requirement (required), or the sender may initiate TSA use at its own initiative (optional).

> *Sending side initiated use of TSA: Not allowed, optional, mandatory.*

PEPPOL strongly discourages posing a mandatory requirement on the signer for use of a TSA. The TSA role is only formalised in some European countries, and a sending side TSA time stamp creates a need for pan-European recognition of TSAs, including the quality of the TSA where relevant. TSAs may be included in TSLs but PEPPOL has still defined this interoperability problem as out of scope.

Correspondingly, this policy element is not further elaborated concerning possible semantics of time-stamps, quality requirements etc.

Usually, optional may be an appropriate policy setting in order to allow the signer to include a TSA time-stamp, e.g. if this is normal procedure in the signer's Member State or according to the signer's business practices. The relying party may in this case validate and make use of the time-stamp if possible or simply discard the time-stamp.

> In France, a public agency, upon receiving e.g. an electronic tender, is obliged to answer by a signed receipt including a TSA time-stamp. Thus, when participating in a tendering process in France, an economic operator will receive such time-stamped receipts.

9.3.3 Policy Element: Relying Party initiated Use of TSA

The receiver may independently or due to legislative requirements in its Member State use a TSA at appropriate steps of the workflow/process applied. As one example, this may be done to build an advanced signed data object for archival.

> *Relying party initiated use of TSA: Not allowed, Optional, Mandatory.*

In PEPPOL, such use of a TSA is considered a local matter to the receiver (e.g. the contracting authority). Correspondingly, this policy element is not further elaborated concerning possible semantics of time-stamps, quality requirements etc.

However, the receiver should state in its "verification time policy" whether a TSA is used in the signature verification process or not, by setting the signature policy element to "mandatory" if used.

The policy element could in theory be used by the sender to force the receiver to use a TSA. PEPPOL does not foresee a need for such a policy mechanism; one reason being the lack of cross-border recognition of the TSA role.

9.4 Policy Element: Storage SDO Format

As stated in 8.2.1, there is a need to differentiate between communication signature format and storage signature format. The latter will typically be created by the receiver by adding information to

the communication format. The need to add information may depend on validity time (see 9.2) and the needs for further archival or storage of the signed data object; if this is longer than the validity period of the eID certificates used, there is a need to store verification information.

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

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

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

Only alternative 1 is considered in this document. This alternative depends on recording of verification information as metadata in or associated with the SDO.

> *Storage signature format: Same list of formats as the communication signature format policy element, see 8.2.2.*

The recommended approach is to create storage signature formats as follows:

- XML DSIG or XAdES stored as XAdES-A or similar,
- PDF embedded signature or PAdES stored as PAdES-A or similar,
- CMS/PKCS#7 signatures or CAdES stored as CAdES-A or similar.

Further policy elements concerning which information to include in the storage format are considered local to the receiver and not detailed further here. Legislation in the particular Member State may mandate use of particular formats and inclusion of information like validation information and time-stamps.

Following the creation of a storage signature format, typically including a signature verification process and use of a TSA time-stamp, scenarios can be depicted where the resulting signed data object is in turn forwarded to further receivers. Such scenarios are not explicitly targeted by this document but it is noted that it should be possible by use of the policy framework of this document to create signature policies for such cases. E.g. the format of the signed data object must be allowed as “communication SDO format”, and the policy must set “sending side TSA” to optional or mandatory.

A use case is signing of a multi-part contract where each signer verifies the signature of the previous signer(s) and adds verification information and a time-stamp to the object before adding its own signature.

9.5 Signature Verification Process

9.5.1 Introduction and Steps of the Process

For each signature on a document, the signature verification process needs to perform:

- Cryptographic verification of the signature;
- Validation of the user eID certificate (see 9.6 below);

- Validation of the certificate of the CA issuing the user's certificate and possibly of further certificates in a path (see 9.6 below);
- Verification of Signature Policy adherence, i.e. a check that conditions stated in the signing policy (see chapter 8) are fulfilled.

9.5.2 Policy Element: Signature Verification Result

The output status of a verification process is:

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

Signature verification result: Valid, invalid, incomplete.

PEPPOL has proposed to add the following status:

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

NOTE: This status code is not supported by today's signature verification environments, meaning that the addition should only be envisaged in the longer term. In the short term, "invalid" should be used when a signature does not pass signature policy checks.

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

Output status should be indicated for each signature individually and as an aggregate value. If the "insufficient quality" status is included, the aggregate shall be in order of evaluation:

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

9.5.3 Policy Element: Signature Verification Status Code

In addition to the status, various reason codes can be used in particular in case of invalid results. This is described in D1.3 parts 5 and 6.

Signature verification status code: List of codes.

9.6 Certificate Validation Process

9.6.1 Introduction and Steps of the Process

The process to be done for complete validation of an eID certificate (relatively to the time of verification, verification of old signatures with verification metadata is not considered here) is as follows:

- Parsing and syntax checking of the certificate and its contents, including some semantic checking like use of certificate compared to allowed use (key usage settings) and presence of mandatory fields and critical extensions.

- Validation of the CA's signature on the certificate. This requires a trusted copy of the CA's own public key, either directly available, or obtained from further certificates in a certificate path.
- A check that the certificate is within its validity period, given by timestamps in the certificate.
- A check that the certificate is not revoked.
- Assessment of compliance with signature policy requirements, e.g. quality and approval status.
- Semantic processing of the certificate content, extracting information that shall be used either for presentation in a user interface or as parameters for further processing by programs. The name (or names) in the certificate and interpretation of naming attributes are particularly important.
- In the case of certificate paths, repeat this processing for each certificate in the path up to a trusted root-CA.

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

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

9.6.2 Policy Element: Certificate Validation Result

The overall result of the certificate validation needs to be represented. The commonly used result codes are:

Certificate validation result: Valid, Invalid, Incomplete

PEPPOL has proposed to add the following status:

- Insufficient quality – validation passed but signature policy rules are not fulfilled.

NOTE: This status code is not supported by today's signature verification environments, meaning that the addition should only be envisaged in the longer term. In the short term, "invalid" should be used when a signature does not pass signature policy checks.

9.6.3 Policy Element: Certificate Validation Status Code

In addition to the status, various reason codes can be used in particular in case of invalid results. This is described in D1.3 parts 5 and 6.

Certificate validation status code: List of codes.

9.6.4 Policy Element: Revocation Checking Requirement

This element is used to state revocation checking requirements for the relying party.

Revocation checking requirement: Mandatory using current information, mandatory using cached information, optional, signer supplied information accepted.

The last alternative points at the possibility for the signer to include revocation information in the SDO (see 8.2.6). Note that revocation grace period (delay verification until next issue of updated status information) is not covered by the present signature policy framework.

9.6.5 Policy Element: Revocation Checking Mechanism

This element may be used to state preferences or requirements for revocation checking mechanism. This may also guide a validation service in selection of mechanism. More than one alternative may be selected.

Revocation checking mechanism: OCSP, CRL, other (e.g. SCVP, XKMS).

9.6.6 Policy Element: Path Processing

A relying party may define a set of root-CAs that are accepted as trust anchors. However, such an approach, as well as merely a list of certificate-issuing CAs, is highly restrictive. There are many ways to construct hierarchies, and rules may even include elements such as bridge-CAs. Path construction is a potentially very hard problem.

The status for many CAs in Europe is that a “local” root-CA exists, and at the same time this root-CA may be certified by a “global actor” in order to ensure that certificates can be validated based on the list of root-CAs configured e.g. in Microsoft’s OSs.

Path processing: Required, optional, not allowed.

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

PEPPOL’s solution does not require the relying party to define trust anchors; rather non-discriminatory acceptance (signature policy) criteria are defined, and the VS is responsible for management of CA information.

Path processing is not allowed in Italy where a CA must provide its own root certificate.

Path processing is required in Germany up to a national root-CA operated by the accreditation authority for issuers of qualified certificates. How this requirement, which is valid for German CAs, shall be interpreted for a non-German CA is not specified.

9.7 Policy Element: Signature Verification Visualisation

Signature verification results may need to be presented to a human user, either directly in a user interface or in form of a human readable electronic document (e.g. recorded in PDF format). This must cover all signatures on a document as well as all associated eID certificates.

Signature verification visualisation: Required, optional, and specification of formatting and elements to include.

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

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

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

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

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

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

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

g) the identity code of the certificate;

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

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

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

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

10 Examples of Signature Policies

10.1 Tendering

In the time frame of PEPPOL, e-tendering is still assumed to be a manual process using human readable electronic documents (such as PDF format).

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

10.2 Post-Award Processes

For other procurement processes, a minimum requirement is that it must be possible to sign documents.

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

10.3 Phases of Public Procurement Procedures, Signatures

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

10.3.1 Tendering, Phases

The typical phases of a public e-tender are:

1. registration
2. tendering
3. awarding
4. contracting
5. possibly invoicing

10.3.2 Ordering, Phases

The typical phases of an e-order process are:

1. catalogue (by the seller)
2. order, choice of article from catalogue:
    a) direct choice of article in a catalogue (by the buyer)
    b) request for Quotation:
        i. offer (by the seller)
        ii. choice of best answer (by the buyer)

3. order confirmation (by the buyer)
4. invoicing (considered a separate step by PEPPOL)

10.3.3 Signatures in Tendering and Ordering

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

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

In the eTender registration phase (if applied, see 7.4.2) the economic operators, even when joining a consortium, register their data and link an eID to the roles played in the tender process, with the effects described. To create that link, the participant signs an agreement with the awarding authority.

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

Example Italian CONSIP eTender – Ministry of Economy and Finance

Q. Is there a registration procedure to verify the link between a person with a given eID and roles within companies?

A. The registration form is used to insert information and to upload documents that identify the person, the person's role in the company, and the company itself.

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

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

Example Italian CONSIP eTender – Ministry of Economy and Finance

Q. In which phases of the eProcurement process (e.g. notification, tendering, awarding, etc.) is there a need for signatures?

A. For the registration procedure and the final offering.

During tendering the bidder is required to insert a Personal Identification Number (PIN) to meet the non repudiation of data. The PIN is chosen by the bidder during registration. It is valid for 90 days and the bidder can renew it.

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

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

10.4 Example Signature Policy for Tendering

10.4.1 Responsibility for Signature Policy

The policy is set by the contracting authority. Elements are published and must be followed by the economic operator as seller/tenderer. Below, signature policy elements are cited and values suggested.

10.4.2 Business Process Rules

The following business process rules are suggested for the *"tendering" step* (see 10.3.1) of a tendering process (note: not for the entire tendering process). This step consists of the tenderer (economic operator) submitting the final documents of the tender, i.e. the offer that the contracting authority shall consider.

Legislation: Select country and/or region if regional legislation applies.

Legislation of contracting authority's home country is selected.

Legislative references: List of laws, regulations, other rule sets with paragraphs and preferably explaining text.

List compiled and published: "Public procurement legislation requires that tenders are signed using an advanced signature supported by a qualified eID." "Archival legislation requires that original, signed documents are archived for 10 years."

Risk management references: Referral to or citation from risk management decision.

No requirement.

Contractual, best practice, other reference: Referral to or citation from contracts or other relevant documents.

No requirement.

Content previously signed: Required, optional, not allowed.

Not allowed – the tender is signed unilaterally by the tenderer. Furthermore, the policy requires that the tender is signed by one responsible tenderer even if multiple parties may have formed a consortium for the tender.

Multiple signatures for same actor: Required, optional, not allowed.

Not allowed – one person shall sign possessing the required authorisations.

Signature required: List of values: Shall, should, may, shall not be signed.

Documents shall be signed at the tendering step of the tendering process.

Repeat for all parts of message:

Signature required: List of values: Shall, should, may, shall not be signed.

A tender usually consists of a cover letter and attachments. This policy requires all parts to be signed. The same commitment rules and signing policy shall be applied to all parts. The relying party will apply the same signature verification policy for all parts.

Batch signature allowed: List of values: Shall, should, may, shall not be used.

Shall not be used, i.e. all parts of the tender shall be signed individually.

10.4.3 Commitment Rules

As stated above, the same commitment rules are assumed for all parts of the tender. The following values are suggested.

Signature purpose: List of statements to select one or more from, possibly also free form statement.

The purpose “I approve the content of this document” is implied by the signature.

Authorisation statement: List of statements to select from, possibly one or more statements that shall be included, possibly also free form statement.

“I am authorised to sign this tender on behalf of the company” shall be implied by the signature.

Assurance level for company, role, authorisations: Selection of alternatives.

The tendering process requires that a registration process is completed at an earlier stage, listing the persons allowed to sign on behalf of the company.

The registration step is subject to a signature policy that may differ from the example for the tendering step; signature policy for registration is not outlined in this example. It may be assumed that the contracting authority performs background checks to verify that the persons listed are indeed authorised to sign.

Attribute authority requirement: Placeholder for signature policy element that may be a textual statement.

No requirement

Notary and other TTP requirement: Placeholder for signature policy element that may be a textual statement.

No requirement.

10.4.4 Signing Policy

The following requirements must be fulfilled by the tenderer upon signing the individual parts of the tender.

Communication signature format: Selection of allowed formats, alternatively restrictions.

In this example, the documents of the tender are required to be either PDF (humanly readable documents) or for some attachments XML. PDF documents shall be signed using a PDF embedded signature. XML documents shall be signed using XML DSIG.

Signature type: List of: Wrapping, Embedded, Detached.

No requirement, all modes are in principle accepted, although embedded in practice is implied by the requirement for use of PDF signature or XML DSIG.

Data to be signed: Specification of elements that shall be included in the data set to be signed, or explicitly kept out of the data set.

All content of a document shall be signed, no further requirements.

Certificate and Certificate Path: List of values: Certificate reference allowed, Signer certificate to be included, Certificate path to be included

Signer certificate shall be included, certificate path optional.

Revocation information: List of values: Not to be included, Optional OCSP response, Optional CRL, Optional OCSP or CRL, OCSP to be included, CRL to be included, OCSP or CRL to be included, other values are possible (e.g. SCVP, XKMS).

Not to be included. The contracting authority will check revocation status and will not use revocation information supplied by the signer.

Include signing time: Not allowed, Optional, Mandatory, TSA time-stamp mandatory.

Optional – signing time can be included but “time of first verification” is the essential time for validity of signatures.

Multiple signature format: Parallel, Sequential, Countersignature.

Not to be used, see business process requirements above. (If allowed, both parallel and sequential could be used.)

Signature validity period: Valid until time.

Signature (i.e. the eID used for signing) must be valid until published time for opening of the tender.

Certificate format restrictions: Free text statement referring to profiles or other certificate information.

No requirement.

Subject name restrictions: Free text statement referring to profiles or other certificate information.

No requirement but change of certificate for a person requires a new registration.

eID quality: Level 0-7 as defined in D1.3 part 7, alternatively as in TSL: qualified eID, qualified signature.

Qualified eID required – level 6 or above.

eID assurance level: Level 0-8 as defined in D1.3 part 7, alternatively as in TSL: supervised or accredited issuer (of qualified eID).

Supervised or accredited issuer as stated in TSL, level 7 or above.

Hash algorithm quality: Level 1-5 as specified in D1.3 part 7.

Hash algorithms accepted: List of hash algorithms.

SHA-2 shall be used, alternatively other hash algorithm of same strength, level 2 or above.

Public key algorithm quality: Level 1-5 as defined in D1.3 part 7.

Public key algorithms accepted: List of public key algorithms including key length.

RSA-2048 is required for the signer's key pair, alternatively other algorithm of same strength, level 2 or above..

Crypto suites accepted: List of crypto suites (combinations of hash and public key algorithms).

A crypto suite providing hash and public key crypto strength as specified above is required – level 2 or above for both hash and public key crypto.

10.4.5 Signature Verification Policy

When verifying the signatures, the contracting authority (the relying party) will apply the following signature verification policy rules.

Validity time: Time of signing, Time of first verification, Time of verification.

Signatures will be verified according to "time of first verification", which will be time of opening of the tenders.

Sending side initiated use of TSA: Not allowed, optional, mandatory.

Not allowed – the sender shall not supply a TSA time stamp as the contracting authority is not prepared to process such time stamps.

Relying party initiated use of TSA: Not allowed, Optional, Mandatory.

Mandatory – legislation requires that the contracting authority uses a TSA time-stamp when validity time is "time of first verification" as a part of the proof that the signature was valid at the time of opening of the tender.

Storage SDO format: Same list of formats as the communication signature format policy element.

The tender documents will be archived for 10 years according to the legislation. The original signed documents will be stored using PAdES-A for PDF documents and XAdES-A for XML documents.

Signature verification result: Valid, invalid, incomplete.

Signatures must be valid at time of first verification.

Signature verification status code: List of codes.

No stipulation.

Certificate validation result: Valid, Invalid, Incomplete

Certificates must be valid at time of first verification.

Certificate validation status code: List of codes.

No stipulation.

Revocation checking requirement: Mandatory using current information, mandatory using cached information, optional, signer supplied information accepted.

Revocation checking is mandatory at the time of first verification using current (not cached) status information.

Path processing: Required, optional, not allowed.

Certificate path processing is optional but shall be done if path is included by the signer.

Signature verification visualisation: Required, optional, and specification of formatting and elements to include.

Upon verification of the signatures, a PDF documents is created presenting the verification information for all documents.

11 References

[CEN-16073-1] CEN CWA 16703-1, Business Interoperability Interfaces for Public Procurement in Europe – Part 1: Profile Overview. January 2010, ftp://ftp.cenorm.be/PUBLIC/CWAs/BII/Final/2010_16073_1.pdf

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

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

[COMM-02] Commission of the European Communities, Action-Plan on e-Signatures and e-Identification to Facilitate the Provision of Cross-Border Public Services in the Single Market, Communication from the Commission to the Council, the European Parliament, the European Economic and Social Committee and the Committee of the Regions, November 2008, http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2008:0798:FIN:EN:PDF

[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

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

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

[ETSI-102-021] ETSI TS 102 023 V.1.2.1 (2003-01). Electronic Signatures and Infrastrutures (ESI) – Policy Requirements for Time-Stamping Authorities.

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

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

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

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

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

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

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

[EU01] EU: Community Framework for Electronic Signatures. Directive 1999/93/EC of the European Parliament and of the Council, 1999.

[EU02] EU: Coordination of Procedures for the Award of Public Works Contracts, Public Supply Contracts and Public Service Contracts. Directive 2004/18/EC of the European Parliament and of the Council, 2004.

[EU03] EU: Coordinating the Procurement Procedures of Entities Operating in the Water, Energy, Transport and Postal Services Sectors. Directive 2004/17/EC of the European Parliament and of the Council, 2004.

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

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

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

[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

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

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

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

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

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

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

[RFC5652] R. Housley. Cryptographic Message Syntax (CMS). RFC5652, 2009 http://datatracker.ietf.org/doc/rfc5652

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

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