Study on Cross-Border Interoperability of eSignatures

(CROBIES)

Guidelines and guidance for cross-border and interoperable implementation of electronic signatures

A report to the European Commission

from SEALED, time.lex and Siemens

FINAL REPORT

Editing company: SEALED sprl,
VAT: BE 0876.866.142 – RPM: Tournai
12, rue de la Paix, B-7500 Tournai
olivier.delos@sealed.be, sylvie.lacroix@sealed.be

Date: 31/07/2010
Version: 1.0

Document information

Title:	CROBIES Work Package 5-1 Guidelines and guidance for cross-border and interoperable implementation of electronic signatures
Project reference:	CROBIES
Document archival code:	INFSO-CROBIES-FINALREPORT-WP5-1-SEALED-31072010_v1.0

Version control

Version	Date	Description / Status	Responsible
V0.1	29/05/2010	Draft Final Report	ODO, SLR
V1.0	31/07/2010	Final Report	ODO, SLR

References

Reference	Title
[1]	The European Directive 1999/93/EC of the European Parliament and the Council of the 13 December 1999 on a Community framework for electronic signatures. O.J. L 13, 19.1.200, p.12.
[2]	Study on the standardisation aspects of eSignature. A study for the European Commission (DG Information Society and Media) by SEALED, DLA Piper and Across communications, 22/11/2007.
[3]	Commission Decision 2003/511/EC "on the publication of reference numbers of generally recognised standards for electronic signature products in accordance with Directive 1999/93/EC of the EP and the Council". OJ L 175 15.7.2003, p.45.
[4]	Services Directive 2006/123/EC of the European Parliament and of the Council of 12 December 2006 on services in the internal market. OJ L 376, 27.12.2006, p. 36.
[5]	Commission Decision 2010/425/EU of 28 July 2010 amending Decision 2009/767/EC as regards the establishment, maintenance and publication of trusted lists of certification service providers supervised/accredited by Member States (OJ L 199 of 31.07.2010).
[6]	European Data Protection Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regards to the processing of personal data and on the free movement of such data.
[7]	Mandate M460, Standardisation Mandate to the European Standardisation Organisations CEN, CENELEC and ETSI in the field of Information and Communication Technologies applied to electronic signatures, 7 January 2010.

Definitions and Acronyms

Please refer to the Head Document for definitions and acronyms used throughout the present report.

Table of Contents

Guidelines and guidance for cross-border and interoperable implementation of electronic signatures

1 Introduction

1.1 CROBIES

The CROBIES study looks at eSignature interoperability in general, but specifically in the context of cross-border use. While considering a consistent global and long term approach in proposed improvements at the legal, technical and trust levels, CROBIES is also focusing on quick wins that could substantially improve the interoperability of electronic signatures.

The CROBIES Study concentrates in particular on the following aspects through related work packages and their associated reports:

WP1. The proposal for a common model for supervision and accreditation systems of certification service providers (CSPs) issuing QCs (and other services ancillary to electronic signatures);

WP2. The establishment of a "Trusted List of supervised/accredited Certification Service Providers" (in particular issuing QCs);

WP3. Interoperable profiles of qualified certificates issued by supervised/accredited CSPs in Member States;

WP4. A proposed framework for interoperable Secure Signature Creation Devices (SSCDs); and

WP5. A proposed model for providing guidelines and guidance for cross-border and interoperable implementation of electronic signatures.

The global overview of the CROBIES study and of its approach is to be found in the "Head Document" of the study. The study is part of the *Action Plan on e-signatures and e-identification to facilitate the provision of cross-border public services in the Single Market* adopted by the European Commission on 28.11.2008[1] which aims at facilitating the provision of cross-border public services in an electronic environment. Readers are suggested to read this Head Document prior to reading the present report.

1.2 Target audience

The present report is addressed to stakeholders willing to implement electronic signatures in the context of electronic business processes. The present report provides the basis for a methodology allowing stakeholder to address consistently the process of implementing eSignatures into electronic business process in the context of a specific application or business domain.

The present report is also addressed to the ESO's to support their work in the context of the eSignature Mandate M460 [7]. Recommendations are specifically made with regards to rationalisation and improvements of existing eSignature standards and standardisation

[1] COM(2008) 798, http://ec.europa.eu/information_society/policy/esignature/action_plan/index_en.htm

framework, in particular within the scope of signature creation and verification products and services, related guidelines and procedures.

1.3 Executive Summary

Moving from paper to electronic world and transposing paper based business processes into electronic equivalent may require the use of electronic signatures. Evidently there may be a business need to transpose all the features of a handwritten signature into the virtual world, and to develop an equivalent trust in electronic signatures, particularly where they indicate a legally binding commitment. Directive 1999/93/EC [1] provides for the equivalence to handwritten signatures where an electronic signature is supported by enhanced technical security measures (article 5.1). Electronic signatures do play a significant role of catalyst for secure transactions and communications as they can provide to an electronic business process the right level of security, authenticity and legal effect as required by the business process and associated risk assessment. However, there are many aspects of "real world" characteristics of signatures which are not provided for in the Directive and moreover a business process is likely to be more complex than involving only one single signature but multiple signatures, each of which being likely associated with different level of security, and various legal or business purpose requirements.

When attempting to implement electronic signatures and before arriving to a consensus on clear and detailed rules to be followed by both signers and verifiers of such electronic signatures identified in an electronic business process, the task can be really hard to find its way:

- Between the applicable legal frameworks and requirements with regards to eSignatures, including but not limited to consideration of long term validity requirements,
- Between the different levels of legal or technical electronic signatures (e.g. quality and security levels), their legal effect and their adequacy to the business needs and to the associated risk assessment requirements,
- Between the standards related to electronic signatures, which eSignature standard for which type of document to be signed,
- In the technical implementation of those standards which are often too academic and lacking clear practical guidelines,
- Amongst identifying best practices when considering implementation of electronic signatures.

The task can be even more complex when considering the fact that business processes or transactions may usually be quite complex and involve a flow of multiple signatures whether sequential or parallel, or even a combination of sequential and or parallel signatures. Those signatures can furthermore be applied on static or evolving documents for which part or all of the contained signed information should be machine processable in order to be treated in an automated way.

Facing the inherent complexity of eSignatures underlying technologies, the lack of global guidance on addressing business, legal and technical requirements, and focusing on measures facilitating the interoperability and cross-border usage of eSignatures, the European Commission included in its COM(2008) 798 Action Plan on e-signatures and e-identification[2] an action related on the aim to *"establish guidelines and guidance on common requirements to help stakeholders implement QES or AdES based on QC in an interoperable*

[2] http://ec.europa.eu/information_society/policy/esignature/action_plan/index_en.htm

way". In support to the EC Action Plan on e-signatures, the present WP5 deliverable of the CROBIES study fulfils this action point.

When considering setting-up or trying to define rules for managing, creating and validating electronic signatures in an electronic communication or transaction process, whatever the "business" or application domain (e.g. ebusiness, egov, etc.), ETSI ESI has created the concept of "Signature Policy"[3] which is defined as *a set of rules for the creation and validation of an electronic signature, under which the signature can be determined to be valid*.

The purpose of the present document is not to re-invent the concept of Signature Policy as defined by ETSI ESI but to further extend the work initiated in this area by improving the guidance for eSignature stakeholders in implementing electronic signatures in a business process. Establishing the specifications of the rules to be applied for the implementation of eSignatures, i.e. not only the creation and verification processes but also the (long term) management of generated electronic signatures, can be a very complex process.

The present document provides the basis for a guidance model on eSignature implementation supporting electronic signature stakeholders attempting to implement electronic signatures. The proposed guidance model relies on a methodology that allows stakeholders willing to implement electronic signatures in a dematerialised business process to be guided through the whole process of implementing electronic signatures. This methodology follows a three-step approach guiding the stakeholder in first defining from the applicable business, policy and legal requirements, the business rules applying to the considered eSignatures flow. It then gives guidance on defining the technical implementation rules associated to the identified business rules. Finally those business and technical implementations rules are formalised in both a human readable and a machine processable signature policy.

The proposed guidelines should be enriched by:

- Effective procedure for technical creation and verification of electronic signatures
- Minimal requirements for interoperable and cross-border electronic signatures
- A to be defined and standardised "Quality Classification Scheme for electronic signature elements".

The proposed methodology would ideally result in a guided drafting and design of a Signature Policy on the basis of a formal and standardised, table of contents for such Signature Policy documents (for both human readable and machine processable forms).

The report provides recommendations to ESOs for further standardisation work in the context of Signature Policies and ancillary topics or tools.

[3] Signature Policy [ETSI TS 101 733] : set of rules for the creation and validation of an electronic signature that defines the technical and procedural requirements for electronic signature creation and validation, in order to meet a particular business need, and under which the signature can be determined to be valid. Further information on Signature Policies is provided in:

- ETSI TR 102 041 ("Signature Policies Report") and TR 102 045 ("Signature policy for extended business model");
- ETSI TS 101 733 ("CAdES") and TR 102 272 ("ASN.1 format for signature policies");
- ETSI TS 101 903 ("XAdES") and TR 102 038 ("XML format for signature policies");
- IETF RFC 3125 ("Electronic signature policies");
- CWA 14171 ("General guidelines for electronic signature verification").

1.4 Definition

Throughout the remaining part of the document the following definitions will be used:

Signature Policy: Set of rules for the creation and validation of one (or more interrelated) electronic signature(s) that defines the technical and procedural requirements for creation, validation and (long term) management of this (those) electronic signature(s), in order to meet a particular business need, and under which the signature(s) can be determined to be valid[4].

Note: A Signature Policy covers the three following aspects related to the management of each of the considered electronic signature(s)[5]:

1. a ***Signature Creation Policy***: part of the Signature Policy, which specifies the technical and procedural requirements on the signer in creating a signature;

2. a ***Signature Validation Policy***: part of the Signature Policy, which specifies the technical and procedural requirements on the verifier when validating a signature; and

3. a ***Signature (LTV) Management Policy***: part of the Signature Policy, which specifies the technical and procedural requirements on the long term management and preservation of a signature.

The present document focuses on QES and on AdES based on Qualified Certificates (QC).

2 The proposed Guidance Model

As illustrated in Figure 1 below, the proposed guidance model is based on a three-phase methodology providing electronic signature stakeholders with guidance when addressing implementation of electronic signatures in a business process. The completion of this methodology would result in the writing of a corresponding Signature Policy for which a proposed table of content is provided in Annex 1 of the present document and will be used to support the implementation of the methodology by electronic signature stakeholders willing to implement electronic signatures. The CROBIES Study Team recommends that such a table of contents would be further standardised.

[4] The notion of Signature Policy here should be clearly dissociated from a legal purpose document. While the Signature Policy is expected to further precise the context in which the underlying signatures are to be considered as valid, their legal effect and value will be driven by Directive 1999/93/EC and its implementation in national laws. Closed user group domains of application should be clearly distinguished from a purely open context to which Directive 1999/93/EC addresses.

[5] Those definition (above and below) slightly differ from but further precise the definitions provided in ETSI related standards.

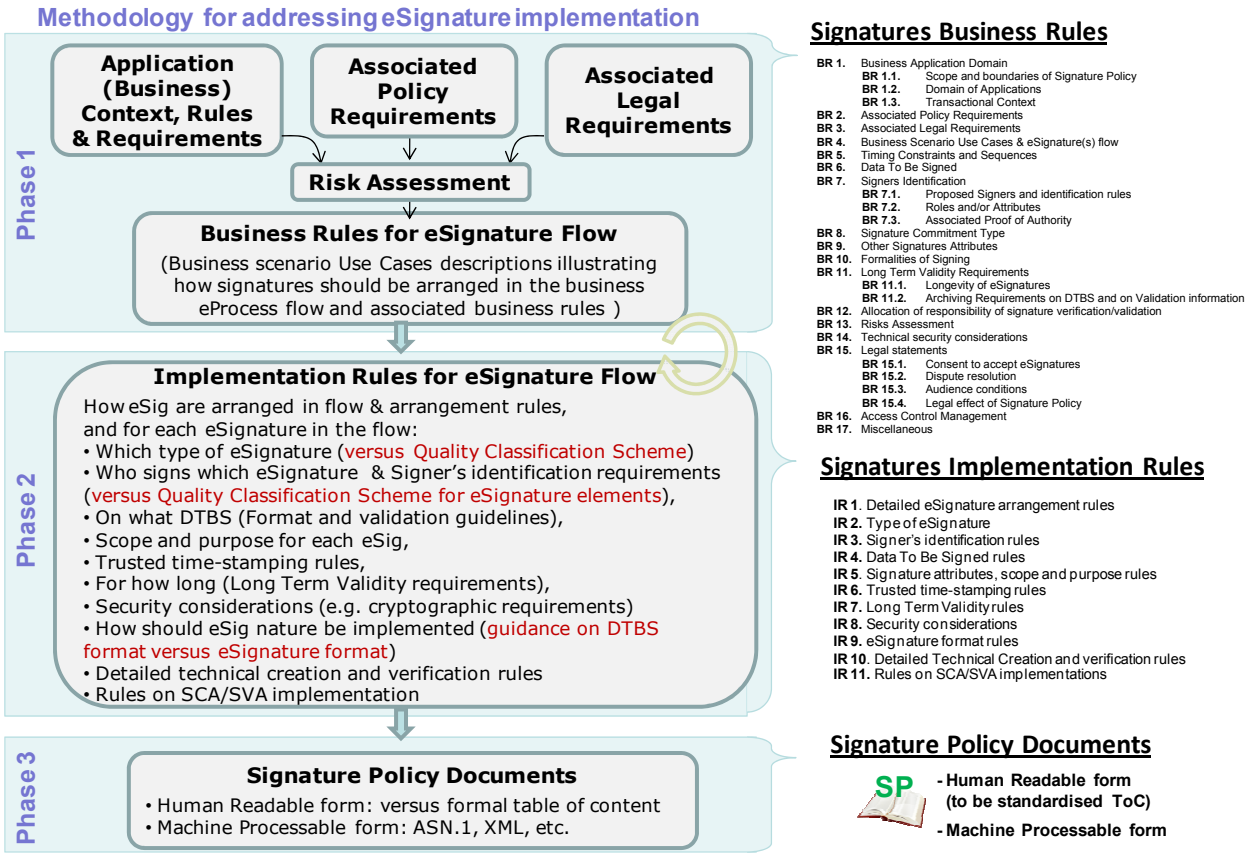

Figure 1: Guidance model for eSignature implementation and Signature Policy design

Those design phases, each subordinate phase deriving its parameters from the higher one, are namely:

1. The **Business Rules** design phase: This first phase of Signature Policy design aims to describe at high level the conditions under which electronic signatures will be used within a business or application domain and process, as well as to identify the resulting eSignatures flow that has to be considered in the context of:
    - A specific business application domain and/or process, with its own context and requirements,
    - Its associated set of policies (e.g. corporate IT and security policies) including any existing signature policy to which the to be designed signature policy is subordinate,
    - Its associated legal requirements, and of course,
    - The associated risk assessment identifying risks for which electronic signatures can be a mitigation tool but also risks induced by the use of electronic signatures themselves in the business or application process.

    The "output" of this first phase when designing a Signature policy consists in the description of the business scenario use cases illustrating how signatures should be arranged in the considered business electronic process, together with the associated business, policy and legal rules under which they will be (deemed to be) accepted as valid.

2. The **eSignature Implementation Rules** design phase: The risk assessment conducted on the basis of the outputs of the previous phase also aims to further

identify for each eSignature involved in the eSignature flow, the associated management, procedural, operational, and technical rules, describing how electronic signatures will be created, validated and their (long term) validity managed, addressing in particular the following:

- ***Detailed eSignature arrangement rules***: Which place does each signature have in the eSignature flow, i.e. how can multiple signatures in the identified flow be arranged and what are the rules to determine whether the expected arrangement has been respected;
- ***And for each eSignature to be considered in the flow***:
  - Which **type of eSignature** is to be considered (a *Quality Classification Scheme for eSignature elements* is proposed to be associated to such considerations) (see CROBIES Deliverable 5.2);
  - **Signer's identification rules**: Who is to sign which eSignature (determination of the signer(s)) and what are the requirements on signers' identification rules, (i.e. helping to determine which type of electronic identity certificate is required – the Quality Classification Scheme is here likely to be supportive as well);
  - **Data To Be Signed (DTBS) rules**: What should be signed (i.e. rules and requirements on the format and on validation guidelines with regards to data to be signed);
  - **Scope and purpose rules**: What is the scope, purpose and commitment level for each signature in the eSignature flow;
  - **Trusted time-stamping rules**: How business timing constraints will be implemented for each eSignature;
  - **Long Term Validity (LTV) rules**: For how long should each signature's validity be maintained once initially validated (i.e. what are the LTV requirements for each eSignature) and how this will be ensured;
  - **Security considerations**: Rules should be defined with regards to the strength of the technical solution used to implement the ruled level of electronic signatures, e.g. authorised eSignature and hashing function algorithms, key size and other relevant security parameters (*best practices should be provided*) (see also CROBIES Deliverables 5.2 and 5.3);
  - **eSignature format rules**: How eSignatures should be formatted (*guidance on mapping between DTBS versus eSignature format, topology and packaging should be provided*), which eSignature format or profile should be used with which set of minimal requirements for ensuring interoperability and cross-border use when applicable (*best practices* and *guidance on interoperability minimal requirements should be provided*);
  - **Detailed technical creation and verification rules**: specifying for each signature the applicable technical requirements on the signer in creating it and on the verifier when validating it;
  - **Rules on Signature Creation Application (SCA) and on Signature Verification Application (SVA) implementations**.

3. The **Signature Policy Documents** design phase: This level formalizes the results of the previous phases into a standardized table of content based document that should be available in two forms:
   - ***Human Readable Signature Policy document***: A formalized and standardized table of content should be made available for such a document, in a similar way as what RFC 3647 is providing as Table of contents with

regards to Certification Practice Statement and Certificate Policies (a proposal for such a table of contents is provided in Annex 1);

- ***Machine Processable form***: Signature Policies are likely to be more effective when they are available in a machine processable form, allowing them to be implemented by automated means. A signature policy may be written using a formal notation like ASN.1 (see ETSI TR 102 272:"ASN.1 format for signature policies") or XML (see ETSI TR 102 038:"XML format for signature policies"). However it should be noted that those standards should be updated, e.g. to take into consideration signature flows involving multiple signatures and Trusted Lists based trust models.

Both Human Readable and Machine Processable forms should of course cover the three parts of a signature policy, namely the signature creation policy, signature validation policy and the signature (long term) management policy.

The present document will not discuss the legal effect and value of a Signature Policy document and of its usage either in an explicit or implicit manner, or even in an open or closed environment.

3 Business Rules level – Signature Policy Design Phase 1

At the first phase of the Signature Policy design one has to determine the Business Rules, i.e. a set of business rules describing at a high level the conditions under which eSignatures will be used within a business application domain and in particular within determined application processes, and the conditions under which they will be considered as valid.

These business rules and actually the scope of a signature policy as a whole may be applicable to a wide range of different applications, from a purely internal process or set of processes, a multi-party trading network whose parties may negotiate and agree on the applicable terms and rules as part of a contract or as being referenced by more general terms or policies, up to nationwide rules governing the use of electronic signatures in eGovernment and eBusiness processes.

An organization (public or private) may have several sets of such rules depending on the context in which electronic signatures are to be used. Those different sets of rules can be part of one single signature policy or being part of separate signature policies.

Those **Business Rules** are roughly analogous to a policy statement, i.e. they state **what** has to be achieved, while the second level, the **eSignature Implementation Rules**, should implement the business rules and be considered as roughly equivalent to a practice statement, in that it should state **how** electronic signatures are to be created and validated under the policy.

It is suggested that the business rules should address and contain the following information and be structured as follows[6] (besides an introductory part covering e.g. Title/identification of Signature Policy, Signature Policy Issuer details, Policy administration, Definitions and Acronyms, and other parts related to compliance audit and other assessments, as well as other business and legal matters):

BR 1. Business Application Domain
BR 1.1. Scope and boundaries of Signature Policy

[6] This list extends and structures the list provided in clause 10.4.1 of ETSI TS 102 045 ("Signature policy for extended business model").

- **BR 1.2.** Domain of Applications
- **BR 1.3.** Transactional Context
- **BR 2.** Associated Policy Requirements
- **BR 3.** Associated Legal Requirements
- **BR 4.** Business Scenario Use Cases & eSignature(s) flow
- **BR 5.** Timing Constraints and Sequences
- **BR 6.** Data To Be Signed
- **BR 7.** Signers Identification
  - **BR 7.1.** Proposed Signers and identification rules
  - **BR 7.2.** Roles and/or Attributes
  - **BR 7.3.** Associated Proof of Authority
- **BR 8.** Signature Commitment Type
- **BR 9.** Other Signatures Attributes
- **BR 10.** Formalities of Signing
- **BR 11.** Long Term Validity Requirements
  - **BR 11.1.** Longevity of eSignatures
  - **BR 11.2.** Archiving Requirements on DTBS and on Validation information
- **BR 12.** Allocation of responsibility of signature verification/validation
- **BR 13.** Risks Assessment
- **BR 14.** Technical security considerations
- **BR 15.** Legal statements
  - **BR 15.1.** Consent to accept eSignatures
  - **BR 15.2.** Dispute resolution
  - **BR 15.3.** Audience conditions
  - **BR 15.4.** Legal effect of Signature Policy
- **BR 16.** Access Control Management
- **BR 17.** Miscellaneous

The next sections will describe each item of the above listed expected information as part of the Business Rules level of a Signature Policy.

3.1 Business Application Domain

Stakeholders willing to implement electronic signatures in a business process (here after denoted as the "Implementers") should describe the business (application) domain in which the signature policy is suitable for use. The business (application) domain should be understood as any business or commercial transaction process(es), which may involve several actors/participants and/or multiple actions in its process(es) and which may require one or multiple signatures to give it effect. This "Business Application Domain" component of the Business Rules should be made of the following three sub-components.

The "***Scope and boundaries of Signature Policy***" sub-component should describe the scope and boundaries of the business (application) domain in which the signature policy is suitable for use. This can range from a purely corporate internal process or set of processes, through a multi-party trading network whose parties may negotiate and agree on the applicable terms and rules, up to nationwide rules governing the use of electronic signatures in eGovernment and eBusiness processes. The signature policy may be applicable to one or several domains of applications (e.g. B2B, B2C, Gov2B, Gov2C, contractual, financial, medical/health, consumer transactions, e-notary services, etc.), whether mono-organisation, corporate or cross-organisations, nationwide or cross-borders, horizontal or vertical (e.g. eProcurement, eInvoice, eHealth, eJustice, etc.). When applicable, the hierarchy of signature policies included in a Signature Policy should be detailed, illustrated and be consistently identified (e.g. through the allocation of sub-OIDs subordinated to OID of the main Signature Policy).

The "***Domain of Applications***" sub-component should further describe each domain of applications that is considered and for which the usage of electronic signatures is ruled by the signature policy.

The "***Transactional Context***" sub-component should provide additional information about the transactional context, e.g. Request for Proposal, any form of offer, exchange of documents of certain specific types, draft of contractual terms and nature of those terms (e.g. contract, Non Disclosure Agreement, etc.), approval, any type of acknowledgement (e.g. of receipt, of delivery, of sending, etc.), documents requiring specific types of authorisation (e.g. because of value, because of applicable law or legal requirements, etc.), etc.

3.2 Associated Policy Requirements

Implementer should identify the applicable policies and policy requirements on the use of electronic signatures or any related information security requirements with regards to the applicable Business Application Domain. Any applicable policy and applicable policy requirements with regards to e.g. data authentication, data origin authentication, data originator identification, data integrity, expression of will, of intent of any action related to data, data privacy and/or confidentiality, and/or any other type of information security policy requirements ancillary to electronic signatures should be identified and associated to each covered business application.

3.3 Associated Legal Requirements

Implementers should identify the applicable laws, and legal requirements on the use of electronic signatures or any related information security requirements with regards to the applicable Business Application Domain. Any applicable law and applicable legal requirements with regards to e.g. data authentication, data origin authentication, data originator identification, data integrity, expression of will, of intent of any action related to data, data privacy and/or confidentiality, and/or any other type of information security requirements ancillary to electronic signatures should be identified and associated to each covered business application.

As additional guidance to the consideration of the applicable legal requirements, a set of best practices should be provided together with the standardised Table of Contents tool for designing a Signature Policy. This should include the following aspects:

- From a legal point of view, the following two elements need to be incorporated to an electronic signature implementation in particular when it is intended to be the equivalent of a handwritten signature but not necessarily limited to this case or especially to be unambiguously distinguished from such a case:[7]
  - The intention to express and the **expression** itself **of a commitment**;
  - The intention to create a signature often referred to as the ***formality of signing***.

- Processing of personal data: it must be made sure that personal data are processed fairly and lawfully in accordance with applicable personal data protection legislation and in particular the European Data Protection Directive 95/46/EC [6] and its implementation in Member State's laws.[8]
- Treatment of the signature: Application users (in particular signers) should be provided with proper advice and information on the application's signature process and legal consequences; user interface should be designed in such a way to guarantee, to the extent possible, a valid legal signature environment; relying parties

[7] See Note 2 of clause 4.2 of ETSI TS 102 045.

[8] See "Best Practices for Applications using the electronic Identity Card (eID)". DIS Authors (SEALED et al) February 2008 (ISBN: 978-2-9600761-0-3. www.sealed.be) for further detailed best practices and controls recommendations with regards to this topic.

should be provided with correct procedures for the verification and the archival of the electronic signature and verification data.[8]

3.4 Business Scenario Use Cases & eSignature(s) flow

Implementers should identify and describe the business scenario use cases for electronic signature and the associated eSignature(s) flow. It is recommended that such use cases are produced using the Unified Modelling Language (UML) or any similar standard notation in order to provide continuity into the development and use of electronic signatures.[9]

Uses cases should be used to describe and specify:

a. What is the sequence flow of data exchanges between those actors in the considered business scenario;

b. How electronic signatures should be arranged within the application process, i.e. what is the use case for electronic signature(s) use in the considered business scenario? This should reflect the potential usage of multiple signatures, whether parallel (mutually independent signatures for which the ordering of the signatures is not important), or sequential (signature for which the ordering is important), or embedded signatures or countersignatures (where one signature is applied to another) or a combination of those; individual transaction signatures versus bloc transactions signatures, signature of a multi-screen transaction.

c. What are the actors *(e.g. customer, bank agent, merchant, application server, mass-signing server, etc.)* and their signing role (primary signature versus countersignature) defining the relationship between each actor's signature and any other required signature.

d. For each Data To Be Signed (DTBS), what sequence of signature(s) do apply (e.g. Single; Multiple parallel; Counter signatures; Sequential; a Combination)

3.5 Timing Constraints and Sequences

Implementers should identify constraints on the timing and sequence of signatures as it may have relevance within the considered business scenario or transaction, in that one action must take place in a certain sequence or time frame e.g. in order to be legally enforceable. In some business scenarios, sequence and timing may not just relate to signatures on a single document, but on multiple documents or signatures which may all form part of a single process or transaction. In some circumstances, the validity or acceptance of an agreement/authorization etc may be contingent upon certain steps or approvals having been taken within given timeframes.

For example:

- *where the signature of an actor (e.g. a superior company officer) is required to authorize or "sign off" a piece of work, it is obvious that that signature should come after the primary signature of the actor (e.g. the employee) who has performed the work.*

[9] Refer to ETSI TS 102 045 Annex A for examples of use cases illustrations using UML.

- *In some case, the counter signature may not be allowed to occur after a certain delay (e.g. must occur within a few hours after the initial signature), or not before a certain delay.*

3.6 Data To Be Signed

Implementers should identify and specify:

a. For each element to be signed as identified in the workflow, what are the data to be actually signed (*e.g. the whole document, specific parts in the document);*

b. For each data to be signed the nature and format of the data to be signed (*e.g. PDF, office documents, images, XML)*.

3.7 Signers Identification

Implementers should identify and specify which are the proposed signers, the associated signer identification rules, as well as rules applicable to the roles and/or attributes of the signers, and the potential requirements on associated proof of authority.

3.7.1 Proposed Signer and identification rules

Implementers should identify and describe:

a. What are the necessary elements to ensure that a signature is that of a specified individual (i.e. whether a physical or legal person, a business or transactional functional entity, a machine, an application or server, etc.), i.e. what are the required identification element (identity attributes) for each type of signer.

E.g. where a contract names an individual as a party to be bound by its terms, what is required as signer identification elements; names, date of birth, unique identification number, etc.

b. What are the expectations in terms of trust on the signatory identification (e.g. quality level of digital certificate)

E.g. certificates must be qualified certificates and/or issued by an accredited, supervised, certified, or audited certification authority, or be issued according to a specific Certificate Policy, etc.

3.7.2 Signer Roles and/or Attributes

In some business scenarios, the role or attributes of a signer are at least as important as his identity. In this component, “signer role” does not refer to the “signing role” played by the signer in the electronic signature supported business process (e.g. primary signature, countersignature) but relates to roles such as “official representative of a legal person” or “sales director”, which may be claimed or certified, but which implies some attribute(s) associated with the signer. Implementers should identify and describe the set of attributes, authorities and responsibilities which are associated with each signatory, his access rights, or authority to sign, to act on behalf of the organization he purports to represent, etc.

3.7.3 Associated Proof of Authority

Implementers should identify and specify the type of proof of authority to sign which is acceptable. Where the parties have already established communications, and there is ostensible authority to enter into the proposed transaction, an identity certificate may be considered sufficient. In some cases, additional proof may be appropriate, an attribute certificate, or certified attribute information from a reliable source. This may include proof that an employee or representative is authorized to enter into transactions over a specified value. This may also include a statement about whether authority to sign may be delegated.

3.8 Signature Commitment Type

Implementers should identify and describe the meaning and the precise nature of the responsibility assumed by signing or in other words the type of commitment for each electronic signature in the considered business scenario and identified eSignature(s) flow. The description of such eSignature commitment types may be useful for avoiding potential ambiguity due to the fact that electronic signatures may not provide equivalent contextual information as in the paper world leading to uncertainty about the signer's intention.

Examples of common types of commitment are:

- *signing a draft (e.g. a contract) to identify the status/integrity of the draft under discussion, but no intention to be legally bound by the draft contract;*
- *indicate an intention to be legally bound by the content of signed document (e.g. signing a contract, commitment on an offer, to accept terms and conditions);*
- *an acknowledgement (proof) of receipt;*
- *author or reviewer of a document:*
- *certify that a document is an authentic copy;*
- *indication of an approval and what kind of approval when applicable;*
- *witness another person's signature;*
- *etc.*

We recommend further standardising most used and relevant commitment types and associating them with specific and unique identifiers.

In particular there may be a need to distinguish between electronic signatures intended for authentication purposes (e.g. data origin authentication only), those which are evidence of an intention to assume a legal commitment, or those intended for any other purpose to be defined in an as unambiguous way as possible.

Furthermore indication of commitment types may assist in the management and validation of multiple signatures under a signature policy.

3.9 Other Signatures Attributes

Implementers should identify and describe any other applicable signature attributes. Geographic location where the signature was created may be an example of such a specific signature attribute as location or jurisdiction, in which the signature was made, may have legal consequences in the event of a dispute, in determining where the dispute should be heard/subject to the laws of which jurisdiction.

3.10 Formalities of Signing

Implementers should identify and specify the need for any type of evidence of the will or intention to sign that would have an influence on the manner the electronic signature is

created and the act of signing is presented to the signer in order to draw attention to the signer to the significance of the commitment he is undertaking under the electronic signing process.

Such requirements are likely to require the signer interface to be designed in a way to guarantee, to the extent possible, a valid legal signature environment, including the implementation of the following controls:

1. Provide users with proper advice and information on the application's signature process and legal consequences.

2. Design the user interface in a way to guarantee, to the extent possible, a valid legal signature environment, including:

- Consistence between the use of the appropriate signature creation and verification data, signature creation device, the data to be signed and the expected scope and purpose of the signature (or the act of signing);
- Provision to the user of clear information about the application's signature process and legal consequences;
- Implementation allowing and demonstrating clear expression of a will to sign and the user's intention to be bound by the signature;
- Implementation allowing and demonstrating an informed consent, and
- Non-repudiation.

3. Provide the relying party (including the signatory) with correct procedures for the verification and the archival of the electronic signature and the verification data.

3.11 Long Term Validity Requirements

Implementers should identify requirements related to the longevity of electronic signatures and archiving requirements on Data To Be Signed (DTBS) and on validation information.

In particular:

a. ***Longevity of eSignatures***: What are the requirements in term of longevity of the signatures? Are there circumstances in which it may become necessary to re-verify the signature, for example in the event of litigation, or allegations of fraud or compromise of the electronic signature itself?

b. ***Archiving Requirements on DTBS and on Validation information***: Are there particular validation data that need to be kept together with the signed document and its signature (e.g. in order to sustain the longevity of eSignatures)? *E.g. revocation lists, timestamp, proof of any kinds…*

3.12 Allocation of responsibility of signature verification/validation

It should not be assumed that in every instance, it will be the party relying on a signature which will be responsible for its validation as this, in some cases, may turn out to be impractical. It is possible that one or more parties to a transaction may be nominated to perform this task, or that it will be undertaken by a trusted independent party. Alternatively, signatures may be validated by counter signers as part of a data flow. Implementers should identify and describe the rules applicable in that matter for each signature in the considered flow and it may also include an obligation to capture and archive validation data.

3.13 Risk Assessment

It is strongly recommended that a risk assessment shall be done in the context of the usage of electronic signatures as part of a business process scenario. Implementers should identify the relevant outputs of such a risk assessment to be considered in establishing the present business rules. Mitigation measures should be identified and reflected in the business rules.

3.14 Technical Security Considerations

Implementers should identify (at high level) requirements relating to technical security or "trust" issues such as "trust model" related to the digital certificate quality and the independent assurance level on this quality, or strength and quality level of cryptographic tools eligible for electronic signatures.

3.15 Legal Statements

Implementers should identify and specify the conditions relating to the following legal statements:

a. ***Consent to accept eSignatures***: Indication whether the parties' consent to accept electronic signature is actual or deemed. *E.g. consent may be required by the laws of some jurisdictions, and may be revoked on notice to the other party.*

b. ***Dispute resolution***: Indication of the applicable dispute resolution rules and procedures. *E.g. falling under a certain jurisdiction, within pre-agreed terms, …*

c. ***Audience conditions***: Indication of the conditions under which a signature may be relied upon. *E.g. the signature is only valid in a specified jurisdiction, or where laws exist which recognize the legal validity of signatures created under conditions as specified in the policy, etc.*

3.16 Access Control Management

Implementers should identify and describe rules about who may access data, and under what circumstances. This is not the same as a privacy or data processing notice, but may, for example, provide rules for controlling access to, and use of data which is protected by law, business custom or contractual obligations.

3.17 Miscellaneous

Implementers should identify and describe any other element that would not fit in the previous sections while being of importance for the specifications and policy description of eSignature use in the considered business process scenario.

4 eSignature Implementation Rules level – Signature Policy Design Phase 2

The risk assessment conducted on the basis of the outputs of the previous level will also aim to further identify for each eSignature involved in the eSignature flow both the requirements and associated management and operational rules as well as the technical rules describing how electronic signatures will be created, validated and their (long term) validity managed.

The "eSignature Implementation Rules" should implement the "Business Rules" elaborated in the context of the first phase of the design of a Signature Policy. If the business rules are

roughly analogous to a policy statement, i.e. what is to be achieved; then Implementation Rules might be considered roughly equivalent to a practice statement, in that it should set out how (multiple) signatures are to be created and validated under the policy.

It is suggested that the eSignature Implementation Rules should contain the following information and be structured as follows[10]:

IR 1. Detailed eSignatures arrangement rules
IR 2. Type of eSignatures
IR 3. Signer's identification rules
IR 4. Data To Be Signed rules
IR 5. Scope and purpose rules
IR 6. Trusted time-stamping rules
IR 7. Long Term Validity rules
IR 8. Security considerations
IR 9. eSignature format rules
IR 10. Detailed Technical Creation and verification rules
IR 11. Rules on Signature Creation Application / Signature Verification Application implementations

The next sections will describe the expected information for each item of the above listed.

4.1 Detailed eSignatures arrangement rules

Implementers should identify and describe in further details the business scenario (e.g. UML) use cases for electronic signatures and the associated eSignature(s) flow as a more technical update of the version identified in section 3.4 (BR4). In particular it will illustrate, taking into account all the relevant previously defined business rules (e.g. in particular BR4 to BR12), which place each signature in the eSignature flow has, how the multiple signatures in the identified flow are arranged and what the rules are to determine whether the expected arrangement has been respected.

4.2 Type of eSignatures

Implementers should identify and specify the requirements with regards to the technical type of eSignature that is to be considered per eSignature in the considered flow. *E.g. QES based on QCP+ certificates, AdES based on QCP, NCP+, NCP, or LCP certificates, use of signature creation tokens (e.g. SSCD or Secure User Device or software based tokens).*

On this point we refer to the CROBIES proposal for a "Quality Classification Scheme for eSignature elements" that is further described in Work Package 5-2 report of the CROBIES Study. This classification scheme uses a so-called Quality Identifier (QID) notation made of seven identifiers, namely "**a.b.c.d.e.f.g**" for which each identifier can have a value from "1" to "5" which corresponds to the identification of the quality level of respectively:

a) The Signing Device;
b) The Certificate Provision;
c) The Independent Assurance on (b);
d) The Signature Cryptographic Suite;
e) The Long Term Validity (LTV) solutions;
f) The Signature Application; and
g) The Independent Assurance on (f).

[10] This list extends and structures the list provided in clause 10.4.2 of ETSI TS 102 045 ("Signature policy for extended business model").

4.3 Signer's identification rules

Implementers should translate the signer's identification rules into technical rules relating to who signs which eSignature (determination of the signer(s)) and what are the requirements on signers' identification rules (including statement on the trust model)

E.g.:

- *which type of electronic identity certificate (provision) is required (e.g. QCP, QCP+, NCP, NCP+, LCP and/or conform to a more specific Certificate Policy identified by a specific OID)*
- *what are the requirements, if any, in terms of certification of signer's attribute information related to the signer's identity/role?*
- *what are the requirements, if applicable and if any, on the entity which certifies or guarantees such attribute(s)*

On this point we refer to the classification scheme for "Certificate Provision" quality and "Independent Assurance" quality on such certificate provision as part of the CROBIES proposal for a "Quality Classification Scheme for eSignature elements" that is further described in Work Package 5-2 report of the CROBIES Study.

4.4 Data To Be Signed rules

Implementers should identify and specify technical details about the nature of DTBS, i.e. what should (technically) be signed, including what are the rules and requirements on the format, packaging convention and on validation guidelines with regards to data to be signed? This should cover each signature as part of a flow, in particular when the flow implements multiple signatures (e.g. countersignatures).

4.5 eSignature scope and purpose rules

Implementers should identify and specify how the scope, purpose and commitment level for each signature in the eSignature flow are implemented.

It is recommended that the signature creation process makes appropriate use of signature attributes, in particular the signed attributes, in accordance with the business, policy and legal requirements. Signed signature attributes (or Signed Properties) are pieces of information that support the electronic signature and which are covered by the signature together with the Data To Be Signed (DTBS). In particular the following signed signature attributes should be considered for use in accordance with the business, policy and legal requirements: signer's certificate identifier, signature policy reference when applicable, data content type, commitment type indication, and potentially other signed attributes like role assumed by the signer, location of the signer's signature creation, signing time, etc.

4.6 Trusted time-stamping rules

Implementers should identify and specify:

a. How business timing constraints are implemented for each eSignature, and

b. What the technical requirements on time-stamping authorities and provided time-stamping services are.

4.7 Long Term Validity rules

Implementers should identify and specify how each signature's validity is to be maintained once initially validated, i.e. how the LTV business requirements for each eSignature have to be ensured.

4.8 Security considerations

Implementers should identify and specify implementation rules with regards to the strength of the technical solution used to implement the electronic signatures.
E.g.:

- *Authorised eSignature algorithms and relevant parameters*
- *Hashing functions algorithms,*
- *Key size requirements,*
- *and any other relevant security requirement.*

On this point we refer to the CROBIES proposal for a "Quality Classification Scheme for eSignature elements" that is further described in Work Package 5-2 report of the CROBIES Study.

For information purposes and considering the D.SPA.13 ECRYPT2 report[11], the ECRYPT2 recommendations for signature suites eligible for electronic signatures are summarised in WP5-2 report.

4.9 eSignature format rules

Implementers should identify and specify how eSignatures are to be formatted, i.e.:

- which eSignature formats, topology, signature-DTBS packaging and packaging convention are authorised,
- which set of minimal requirements for ensuring interoperability and cross-border use are applicable

4.10 Detailed technical creation and verification rules

Implementers should identify and specify for each signature the applicable technical requirements on the signer in creating it and on the verifier when validating it.

This includes providing:

- Requirements on how multiple (e.g. countersignatures) should be created;
- Indication which eSignature(s) should or must be time stamped by a TSA;
- The requirements on the verifier with regards to what should be checked and how this should be checked;
- The description of how each signature validation process should occur with regards to certificate validation data (e.g. OCSP responses for each certificate in the chain supporting the signer's certificate) and trust model related information (e.g. use of Trusted Lists);
- The requirements on how validation results should be presented to the verifier;
- The description of what should be archived and preserved for medium or long term and how this should be implemented.

[11] D.SPA.13 ECRYPT2 Yearly Report on Algorithms and Key sizes (2009-2010), dated 30 March 2010 (http://www.ecrypt.eu.org/documents/D.SPA.13.pdf).

4.11 Rules on Signature Creation Application (SCA) and Signature Verification Application (SVA) implementations

This component describes and specifies SCA and on SVA implementations including in particular:

a. The requirements on security measures the application should or must provide to the signer. *E.g. a secure display interface insuring that what the signatory sees is really what he's signing, a trusted path between the Human Interface and the (S)SCD, is the application audited against IT security criteria ?…*

b. The requirements on security measures the application should or must provide to the verifier. *E.g. what are the rules for certification path construction/validation, including the validation of the trust model requirements, the rules for the revocation status validation (whether the grace period should be considered), the security measures undertaken for long term validity (e.g. re-timestamping), is the application audited against IT security criteria …*

5 Signature Policy Documents – Design Phase 3

The last phase in the design process of a Signature Policy is to formalise rules and requirements established in the two previous phases into a standardized table of content based document that should be available in two forms:

- ***Human Readable Signature Policy document***: A formalized and to be standardized table of content for such a document should be made available in a roughly similar way as what RFC 3647 is providing as Table of contents with regards to Certification Practice Statement and Certificate Policies (a proposal for such a table of contents is provided in Annex 1);

- ***Machine Processable form***: A signature policy may be written using a formal notation like ASN.1 (see ETSI TR 102 272:"ASN.1 format for signature policies") or XML (see ETSI TR 102 038:"XML format for signature policies"). However it should be noted that those standards should be updated, e.g. to take into consideration signature flows involving multiple signatures and Trusted Lists based trust models.

Both Human Readable and Machine Processable forms should of course cover the three parts of a signature policy, namely the signature creation policy, signature validation policy and the signature (long term) management policy.

6 Conclusions and recommendations

Signature policies can cover a wide range of aspects related to electronic signatures, business, legal and technical and can act as a useful tool to specify the conditions under which electronic signatures will be implemented, accepted by or on behalf of a relying party, and maintained, as well as the means by which the "formality of signing" may be accomplished.

It is obviously not possible to write a single, generic, signature policy which is capable of applying to all types of business or application models, nor for handling all situation in which multiple signatures may be used. However, the design process of a signature policy, when

covering not only the signature creation policy, the signature verification policy but also the signature (long term) management policy, can be an excellent basis for developing "guidelines and guidance on common requirements to help stakeholders implement QES or AES based on QC in an interoperable way" as defined in the related action item of the COM(2008)798 EC Action Plan on e-signatures and e-identification[12], and more generally to support implementation of advanced electronic signatures.

The following **recommendations** are made by the CROBIES Study Team:

1. The standardisation work done so far in the context of Signature Policies should be further developed in order to extend it further towards guidance and guidelines for implementation of electronic signatures (in particular QES and $AdES_{QC}$), including the standardisation of a Guidance Model for assisting eSignature stakeholders when they are willing to implement electronic signatures, and supported by a standardised table of content for human readable forms of Signature Policies as based from the one proposed in the present report.

2. This should also include further work on the standardisation aspects of Signature Policies as the current standardisation framework in this matter is quite incomplete. In particular the following aspects should be considered:

    - Taking into account signature flows involving multiples signatures and modelling mechanisms for both human readable and machine processable signature policies;
    - Taking into account trust models based on Trusted Lists[13] and other Trust Service Status Lists;
    - Allow hierarchical (and or nested) use of signature policies;
    - The relationship and mapping between human readable and machine processable signature policies.

3. The standardisation of a "Quality Classification Scheme for eSignature elements"[14];

4. The standardisation of requirements with regards to signature creation processes and Signature Creation Applications as well as with regards to signature verification processes and Signature Verification Applications. This should include appropriate Protection Profiles and related Conformity Assessment Guidance. Inputs for such standardisation efforts are the existing CWA 14170, CWA 14171, ETSI TS 102 869, the draft ETSI TS 102 853, and private or industry initiatives like DIS Book[15] and QuEST[16] amongst others.

5. The baseline profiling of extended, self-sustainable and long-term validity (verification) forms of electronic signature formats like XAdES, CAdES and PAdES (i.e. X/CAdES –A forms and PAdES-LTV) ensuring maximal interoperability and cross-border use of electronic signatures implemented according to those profiles. Rather than looking for an academic comprehensiveness, options in standardization

[12] http://ec.europa.eu/information_society/policy/esignature/action_plan/index_en.htm
[13] See [5].
[14] See CROBIES Work Package 5-2 report.
[15] "Best Practices for Applications using the electronic Identity Card (eID)". DIS Authors (SEALED et al) February 2008 (ISBN: 978-2-9600761-0-3. www.sealed.be)
[16] Qualified Electronic Signature Tutorial: http://www.microsoft.com/downloads/details.aspx?displaylang=en&FamilyID=0b3c55f6-11d4-4f46-8a37-0ba004e14dcf

deliverables should be reduced as much as possible to what is really needed for an application and in particular for the verification of an electronic signature.

These recommendations and the present report should be considered as input to the execution of mandate M460 [7] for the rationalisation of the EU eSignature standardisation framework.

It may also be advised, in the context of a recast of the eSignature legal framework, adding some legal provisions related to the use of signature policies, e.g. stating presumption of legal compliance to a recast (and in this particular case reinforced) Directive 1999/93/EC Annex IV and to (a further developed) art. 5.2 when a signature creation and validation process implementation follows a given standardised signature policy.

Annex 1 – Proposed table of contents and component specifications for a Human Readable Signature Policy Document

1 Introduction

Within the present document the key words "MUST", "MUST NOT", "REQUIRED", "SHALL", "SHALL NOT", "SHOULD", "SHOULD NOT", "RECOMMENDED", "MAY", and "OPTIONAL" are to be interpreted as described in RFC 2119[17].

A signature Policy is a set of rules for the creation and validation of one (or more interrelated) electronic signatures that defines the technical and procedural requirements for creation, validation and (long term) management of this (those) electronic signature(s), in order to meet a particular business need, and under which the signature(s) can be determined to be valid.

This component SHOULD provide a general introduction to the signature policy.

1.1 Overview

This component SHALL be used to provide a general introduction to the document being written. It SHALL be used to provide a synopsis of the business or application domain and the specific business or application process to which the signature policy applies. Depending on the complexity and scope of the particular business or application process implementing electronic signatures, a diagrammatic representation MAY be useful here.

1.2 Signature Policy name, identification and conformance rules

This component SHALL be used to provide information:

- *About any applicable names for the Signature Policy;*
- *About any applicable other identifiers for the Signature Policy (e.g. unique identifier, OIDs);*
- *About conformance rules;*
- *About where the signature policy is available (e.g. a URL or by email) and how a paper/hard copy can be made available.*

1.2.1 Signature Policy name

1.2.2 Signature Policy identifier(s)

1.2.3 Signature Policy conformance rules

1.2.4 Signature Policy distribution points

1.3 Signature Policy Issuer

This component SHALL include the name of the organization that is issuing the Signature Policy. It SHALL also provide information identifying the digital certificate used by the Signature Policy Issuer to electronically sign the Signature Policy.

1.4 Signature Policy Administration

This component SHALL include the name and mailing address of the organization that is responsible for the drafting, registering, maintaining, and updating of the Signature Policy. It SHALL also include the name, electronic mail address, telephone number, and fax number of a contact person. As an alternative to naming an actual person, the document MAY name a title or role, an e-mail alias, and other generalised contact information. In some cases, the organisation MAY state that its contact person, alone or in combination with others, is available to answer questions about the document.

Moreover, when a formal or informal policy authority is responsible for determining whether one or more separate signature policies should be allowed to be subordinated, included in or include another

[17] IETF RFC 2119: "Key words for use in RFCs to indicate Requirements Levels".

Signature Policy, it MAY wish to approve the separate signature policy(ies) as being suitable for the policy authority's Signature Policy. If so, this component MUST include the name or title, electronic mail address (or alias), telephone number, fax number, and other generalized information of the entity in charge of making such a determination. Finally, in this case, this subcomponent MUST also include the procedures by which this determination is made.

1.4.1 Organisation administering the document

1.4.2 Contact person

1.5 Definitions and Acronyms

This component SHALL contain a list or a reference to a list of definitions for defined terms used within the document, as well as a list or a reference to a list of acronyms in the document and their meanings.

2 eSignatures Flow Business Rules

2.1 Business Application Domain

This component SHALL describe the business (application) domain in which the signature policy is suitable for use. The business (application) domain should be understood as any business or commercial transaction process(es), which may involve several actors/participants and/or multiple actions in its process(es) and which may require one or multiple signatures to give it effect.

2.1.1 Scope and boundaries of Signature Policy

This sub-component SHOULD describe the scope and boundaries of the business (application) domain in which the signature policy is suitable for use. This can range from a purely corporate internal process or set of processes, through a multi-party trading network whose parties may negotiate and agree on the applicable terms and rules, up to nationwide rules governing the use of electronic signatures in eGovernment and eBusiness processes. The signature policy MAY be applicable to one or several domains of applications (e.g. B2B, B2C, Gov2B, Gov2C, contractual, financial, medical/health, consumer transactions, e-notary services, etc.), whether mono-organisation, corporate or cross-organisations, nationwide or cross-borders, horizontal or vertical (e.g. eProcurement, eInvoice, eHealth, eJustice, etc.). When applicable the hierarchy of signature policies included in a Signature Policy SHOULD be detailed, illustrated and be consistently identified (e.g. through the allocation of sub-OIDs subordinated to OID of the main Signature Policy).

2.1.2 Domain of Applications

This sub-component SHOULD further describe each domain of applications that is considered and for which the usage of electronic signatures is ruled by the signature policy.

2.1.3 Transactional Context

This sub-component SHOULD provide additional information about the transactional context, e.g. Request for Proposal, any form of offer, exchange of documents of certain specific types, draft of contractual terms and nature of those terms (e.g. contract, Non Disclosure Agreement, etc.), approval, any type of acknowledgement (e.g. of receipt, of delivery, of sending, etc.), documents requiring specific types of authorisation (e.g. because of value, because of applicable law or legal requirements, etc.), etc.

2.2 Associated Policy Requirements

This component SHALL contain information about the applicable policies and policy requirements on the use of electronic signatures or any related information security requirements with regards to the applicable Business Application Domain. Any applicable policy and applicable policy requirements with regards to e.g. data authentication, data origin authentication, data originator identification, data integrity, expression of will, of intent of any action related to data, data privacy and/or confidentiality, and/or any other type of information security policy requirements ancillary to electronic signatures SHOULD be identified and associated to each covered business application.

2.3 Associated Legal Requirements

This component SHALL contain information about the applicable laws, and legal requirements on the use of electronic signatures or any related information security requirements with regards to the applicable business application domain. Any applicable law and applicable legal requirements with regards to e.g. data authentication, data origin authentication, data originator identification, data integrity, expression of will, of intent of any action related to data, data privacy and/or confidentiality, and/or any other type of information security requirements ancillary to electronic signatures SHOULD be identified and associated to each covered business application.

As best practices this should include the following aspects:

- *From a legal point of view, the following two elements need to be incorporated to an electronic signature implementation in particular when it is intended to be the equivalent of a handwritten signature but not necessarily limited to this case or especially to be unambiguously distinguished from such a case:*[18]
  - *The intention to express and the **expression** itself **of a commitment**;*
  - *The intention to create a signature often referred to as the **formality of signing**.*

- *Processing of personal data: it must be made sure that personal data are processed fairly and lawfully in accordance with applicable personal data protection legislation and in particular the European Data Protection Directive 95/46/EC [6] and its implementation in Member State's laws.*[19]
- *Treatment of the signature: Application users (in particular signers) should be provided with proper advice and information on the application's signature process and legal consequences; user interface should be designed in such a way to guarantee, to the extent possible, a valid legal signature environment; relying parties should be provided with correct procedures for the verification and the archival of the electronic signature and verification data.*[8]

2.4 Business Scenario Use Cases & eSignature(s) flow

This component SHALL be used to illustrate the business scenario use cases implementing electronic signature(s) and the associated eSignature(s) flow. It is RECOMMENDED that such use cases are produced using the Unified Modelling Language (UML) or any similar standard notation in order to provide continuity into the development and use of electronic signatures.

Uses cases SHALL be used to describe and specify:

a. *What is the sequence flow of data exchanges between those actors in the considered business scenario and application process;*

b. *How electronic signatures should be arranged within the application process, i.e. what is the use case for electronic signature(s) use in this application process in the considered business scenario? This should reflect the potential usage of multiple signatures, whether parallel*

[18] See Note 2 of clause 4.2 of ETSI TS 102 045.

[19] See "Best Practices for Applications using the electronic Identity Card (eID)". DIS Authors (SEALED et al) February 2008 (ISBN: 978-2-9600761-0-3. www.sealed.be) for further detailed best practices and controls recommendations with regards to this topic.

(mutually independent signatures for which the ordering of the signatures is not important), or sequential (signature for which the ordering is important), or embedded signatures or countersignatures (where one signature is applied to another) or a combination of those usages; individual transaction signatures versus bloc transactions signatures, signature of a multi-screen transaction.

c. *What are the actors (e.g. customer, bank agent, merchant, application server, mass-signing server, legal person) and their signing role (primary signature versus countersignature) defining the relationship between each actor's signature and any other required signature.*

d. *For each Data To Be Signed (DTBS), what sequence of signature(s) do apply (e.g. Single; Multiple parallel; Counter signatures; Sequential; a Combination)*

2.5 Timing Constraints and Sequences

This component SHOULD express constraints on the timing and sequence of signatures as it MAY have relevance within the considered business scenario or transaction, in that one action must take place in a certain sequence or time frame e.g. in order to be legally enforceable. In some business scenarios, sequence and timing may not just relate to signatures on a single document, but on multiple documents or signatures which may all form part of a single process or transaction. In some circumstances, the validity or acceptance of an agreement/authorization etc. may be contingent upon certain steps or approvals having been taken within given timeframes.

For example:

- *Where the signature of an actor (e.g. a superior company officer) is required to authorize or "sign off" a piece of work, it is obvious that this signature should come after the primary signature of the actor (e.g. the employee) who has performed the work.*

- *In some case, the counter signature may not be allowed to occur after a certain delay (e.g. must occur within a few hours after the initial signature), or not before a certain delay.*

2.6 Data To Be Signed

This component SHALL describe and specify:

a. *For each element to be signed as identified in the workflow, what are the data to be actually signed (e.g. the whole document, specific parts in the document);*

b. *For each data to be signed the nature and format of the data to be signed (e.g. PDF, office documents, images, XML).*

2.7 Signers Identification

This component SHALL describe and specify which are the proposed signers, the associated signer identification rules, as well as rules applicable to the roles and/or attributes of the signers, and the potential requirements on associated proof of authority.

2.7.1 Proposed Signer and identification rules

This subcomponent describes:

a. *What are the necessary elements to ensure that a signature is that of a specified individual (i.e. whether a physical or legal person, a business or transactional functional entity, a machine, an application or server, etc.), i.e. what are the required identification element (identity attributes) for each type of signer.*

E.g. where a contract names an individual as a party to be bound by its terms, what is required as signer identification elements; names, date of birth, unique identification number, etc.

b. *What are the expectations in terms of trust on the signatory identification (e.g. quality level of digital certificate)*

E.g. certificates must be qualified certificates and/or issued by an accredited, supervised, certified, or audited certification authority, or be issued according to a specific Certificate Policy, etc.

2.7.2 Signer Roles and/or Attributes

In some business scenarios, the role or attributes of a signer are at least as important as his identity. In this component, "signer role" does not refer to the "signing" role played by the signer in the electronic signature supported business process (e.g. primary signature, countersignature) but relates to roles such as "official representative of a legal person" or "sales director", which may be claimed or certified, but which implies some attribute(s) associated with the signer. This subcomponent SHOULD describe the set of attributes, authorities and responsibilities which are associated with each signatory, his access rights, or authority to sign, to act on behalf of the organization he purports to represent, etc.

2.7.3 Associated Proof of Authority

This subcomponent SHOULD state the type of proof of authority to sign which is acceptable. Where the parties have already established communications, and there is ostensible authority to enter into the proposed transaction, an identity certificate may be considered sufficient. In some cases, additional proof may be appropriate, an attribute certificate, or certified attribute information from a reliable source. This may include proof that an employee or representative is authorized to enter into transactions over a specified value. This clause may also include a statement about whether authority to sign may be delegated. Where the document or transaction is to be notarized, this clause MAY be superfluous.

2.8 Signature Commitment Type

This component SHALL be used to describe and specify the meaning and precise nature of the responsibility assumed by signing or in other words the type of commitment for each electronic signature in the considered business scenario and identified eSignature(s) flow. The description of such eSignature commitment types may be useful for avoiding potential ambiguity due to the fact that electronic signatures may not provide equivalent contextual information as in the paper world leading to uncertainty about the signer's intention.

Examples of common types of commitment are:

- *signing a draft (e.g. a contract) to identify the status/integrity of the draft under discussion, but no intention to be legally bound by the draft contract;*
- *indicate an intention to be legally bound by the content of signed document (e.g. signing a contract, commitment on an offer, to accept terms and conditions);*
- *an acknowledgement (proof) of receipt;*
- *author or reviewer of a document:*
- *certify that a document is an authentic copy;*
- *indication of an approval and what kind of approval when applicable;*
- *witness another person's signature;*
- *data authentication (i.e. corroboration of the origin and integrity of the signed data)*
- *entity authentication (e.g. when implementing a signature mechanism to attest the identity of the signer usually for the purpose of authorising access to protected data, area, or services).*
- *etc.*

Furthermore indication of commitment types may assist in the management and validation of multiple signatures under a signature policy.

In particular it SHALL be distinguished between (i) electronic signatures intended for authentication purposes (i.e. data authentication, or entity authentication), (ii) those which are evidence of an intention to assume a legal commitment, and (iii) those intended for any other purpose to be defined in an as unambiguous way as possible.

2.9 Other Signatures Attributes

This component SHOULD indicate any other applicable signature attributes. Geographic location where the signature was created may be an example of such a specific signature attribute as location or jurisdiction, in which the signature was made, may have legal consequences in the event of a dispute, in determining where the dispute should be heard/subject to the laws of which jurisdiction. Other examples of applicable signature attributes MAY be signing time (which is only to be considered as a claim and should not be considered as trusted unless time is provided as a trusted time service from a Trusted Time-stamping Service Provider), content time-stamp, content related information, signer claimed or certified attributes.

2.10 Formalities of Signing

This component SHALL describe and specify the need for any type of evidence of the will or intention to sign that would have an influence on the manner the electronic signature is created and the act of signing is presented to the signer in order to draw attention to the signer to the significance of the commitment he is undertaking under the electronic signing process.

The signer/signature interface SHALL be designed in a way to guarantee, to the extent possible, a valid legal signature environment and taking into account the requirements related to the formalities of signing expressed in the applicable signature policy(ies).

2.11 Long Term Validity Requirements

This component SHALL address requirements related to the longevity of electronic signatures and archiving requirements on Data To Be Signed (DTBS) and on validation information.

In particular:

c. ***Longevity of eSignatures**: What are the requirements in term of longevity of the signatures? Are there circumstances in which it may become necessary to re-verify the signature, for example in the event of litigation, or allegations of fraud or compromise of the electronic signature itself?*

d. ***Archiving Requirements on DTBS and on Validation information**: Are there particular validation data that need to be kept together with the signed document and its signature (e.g. in order to sustain the longevity of eSignatures)? E.g. revocation lists, timestamp, proof of any kinds…*

Application Owners implementing electronic signatures are RECOMMENDED to respect the prerequisites of electronic archiving from the early stages of the design of new developments and when integrating electronic signature solutions in current products. This aims to ensure proper implementation of electronic archiving once electronic archiving will be legally recognized and facilitate compliance with future regulations applicable in matter of electronic archiving.

2.12 Allocation of responsibility of signature verification/validation

It should not be assumed that in every instance, it will be the party relying on a signature which will be responsible for its validation as this, in some cases, may turn out to be impractical. It is possible that one the parties to a transaction may be nominated to perform this task, or that it will be undertaken by a trusted independent party. Alternatively, signatures may be validated by counter signers as part of a data flow. This component SHALL describe the rules applicable in that matter for each signature in the considered flow and it MAY also include an obligation to capture and archive validation data.

2.13 Risk Assessment

A risk assessment SHALL be done in the context of the usage of electronic signatures as part of a business process scenario. This component SHALL provide the relevant outputs of such a risk assessment to be considered in establishing the present business rules. Mitigation measures SHOULD be reflected in the business rules.

2.14 Technical Security Considerations

This component SHOULD deal (at high level) with requirements relating to technical security or "trust" issues such as "trust model" related to the digital certificate quality and the independent assurance level on this quality, or strength and quality level of cryptographic tools eligible for electronic signatures.

2.15 Legal Statements

This component SHALL address the conditions relating to the following legal statements:

a. ***Consent to accept eSignatures**: Indication whether the parties' consent to accept electronic signature is actual or deemed. E.g. consent may be required by the laws of some jurisdictions, and may be revoked on notice to the other party.*

b. ***Dispute resolution**: Indication of the applicable dispute resolution rules and procedures. E.g. falling under a certain jurisdiction, within pre-agreed terms, …*

c. ***Audience conditions**: Indication of the conditions under which a signature may be relied upon. E.g. the signature is only valid in a specified jurisdiction, or where laws exist which recognize the legal validity of signatures created under conditions as specified in the policy, etc.*

2.16 Access Control Management

This component SHOULD provide rules about who may access data, and under what circumstances. This is not the same as privacy or data processing notice, but MAY, for example, provide rules for controlling access to, and use of data which is protected by law, business custom or contractual obligations.

2.17 Miscellaneous

This component MAY be used to provide any other element that would not fit in the previous sections while being of importance for the specifications and policy description of eSignature use in the considered business process scenario.

3 eSignature Implementation Rules

3.1 Detailed eSignature arrangement rules

This component SHALL describe in further details the business scenario (UML-based) use cases for electronic signatures and the associated eSignature(s) flow as a more technical update of the version identified in section 2.4. In particular it will illustrate, taking into account all the relevant previously defined business rules (e.g. in particular as defined in sections 2.4 to 2.12) at which place each signature in the eSignature flow has, how the multiple signatures in the identified flow are arranged and what the rules are to determine whether the expected arrangement has been respected.

3.2 Type of eSignature

This component states the requirements with regards to the technical type of eSignature that is to be considered per eSignature in the considered flow. E.g. QES based on QCP+ certificates, AdES based on QCP, NCP+, NCP, or LCP certificates, use of signature creation tokens (e.g. SSCD or Secure User Device or software based tokens).

*On this point we refer to the CROBIES proposal for "Quality Classification Scheme of eSignature elements" that is further described in Work Package 5-2 report of the CROBIES Study. The classification scheme uses a so-called Quality Identifier (QID) notation made of seven identifiers, namely "**a.b.c.d.e.f.g.**" for which each identifier can have a value from "1" to "5" and correspond to the identification of the quality level of respectively:*

a) The Signing Device;
b) The Certificate Provision;
c) The Independent Assurance on (b);
d) The Signature Cryptographic Suite;
e) The Long Term Validity (LTV) solutions;
f) The Signature Application; and
g) The Independent Assurance on (f).

3.3 Signer's identification rules

This component SHALL translate the signer's identification rules into technical rules relating to who signs which eSignature (determination of the signer(s)) and what are the requirements on signers' identification rules (including statement on the trust model)
E.g.:

- *which type of electronic identity certificate (provision) is required (e.g. QCP, QCP+, NCP, NCP+, LCP and/or conform to a more specific Certificate Policy identified by a specific OID)*
- *what are the requirements, if any, in terms of certification of signer's attribute information related to the signer's identity/role?*
- *what are the requirements, if applicable and if any, on the entity which certifies or guarantees such attribute(s)*

On this point we refer to the CROBIES proposal for "Quality Classification Scheme for eSignature elements" that is further described in Work Package 5-2 report of the CROBIES Study.

3.4 Data To Be Signed rules

This component SHALL describe and specify technical details about the nature of DTBS, i.e. what should (technically) be signed, including what are the rules and requirements on the format, packaging convention and on validation guidelines with regards to data to be signed? This SHOULD cover each signature as part of a flow, in particular when the flow implements multiple signatures (e.g. countersignatures).

3.5 eSignature attributes, scope and purpose rules

This component SHALL describe and specify how the attributes, scope, purpose and commitment level for each signature in the eSignature flow are implemented.

The signature creation process SHALL make appropriate use of signature attributes, in particular the signed attributes, in accordance with the business, policy and legal requirements.[20]

Signed signature attributes (or Signed Properties) are pieces of information that support the electronic signature and which are covered by the signature together with the Data To Be Signed (DTBS). Signed signature attributes SHOULD be used in accordance with the business, policy and legal requirements, in particular:

1. *Signer's Certificate Identifier SHALL be used (Signing Certificate). It is the identifier of, or a reference to, the certificate holding the Signature Verification Data corresponding to the Signature Creation Data that the signer uses to create the electronic signature. It is required to avoid certificate substitution attacks and to indicate the correct signature verification data to the verifier.*

2. *Signature Policy reference SHOULD be used when applicable. It is the identifier of, or a reference to, the correct Signature (Validation) Policy to be used during the verification process.*

3. *Data Content Type attribute SHALL be used. The Signature Creation Application (SCA) SHALL make use of the "Data Content Type" signature attribute for correct specifications on DTBS presentation. Through this signed attribute implementation, the DTBS presentation format of the data is always indicated within the electronic signature and that information is thus protected by the digital signature from the signer.*

4. *Commitment Type indication SHALL be used. This is an indication by the signer of the precise meaning of the electronic signature in the context of the Signature Policy selected by (or imposed to) the signer. It SHALL be selected, approved and explicitly displayed to/by the signer.*
The concept of CommitmentTypeIndication is also closely related to the usage of a Signature Policy. In any case, the usage of such indication of the type of commitment claimed and signed by the signer MUST be consistent with the Signature Policy. It is also REQUIRED to have a signer interface through which the signer can select the appropriate commitment type indication according to the signature context and in compliance with the Signature Policy.

5. *Other signed attributes like role assumed by Signer, location of the Signer signature creation, signing time, etc., SHOULD be considered for use when applicable.*

Note: *Like any other signed attribute, the "signing time" attribute only represents a claim from the signer. When this attribute needs to be demonstrated to a third party, it is RECOMMENDED to the verifier (or the signer) to request a proof-of-existence for the signature at (or more precisely before) a certain point in time (e.g., under the form of a Time Stamp obtained from a Time Stamping Authority see also section 3.6). The notion of time related to implementation of electronic signature is further illustrated below:*

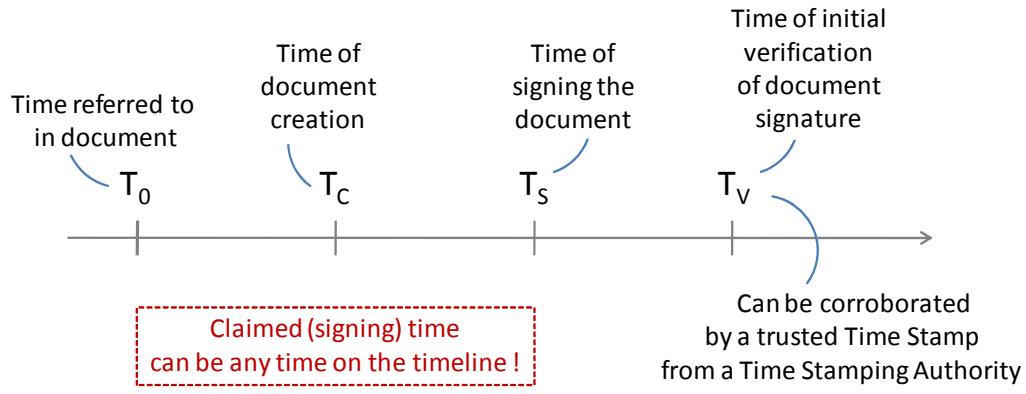

Figure 2

[20] Credits are given to [7].

Those T_0, T_C, T_S, and T_V times are logically represented as sequential in the above timeline in Figure 2. However such time indications including the value in the signed "Signing Time" attribute could be claimed as any time on the timeline by the signer. The time of initial verification of the document signature (T_V) SHOULD however be corroborated by a trusted Time Stamp obtained from a Time Stamping Authority. This can be initiated either by the verifier of the signature or by the signer who has interest in obtaining such type of proof.

3.6 Trusted time-stamping rules

This component SHALL describe and specify:

a. *How business timing constraints are implemented for each eSignature, and*

b. *What the technical requirements on time-stamping authorities and provided time-stamping services are.*

3.7 Long Term Validity rules

This component describes and specifies how each signature's validity is to be maintained once initially validated, i.e. how the LTV business requirements for each eSignature have to be ensured.

On this point we refer to the CROBIES proposal for "Quality Classification Scheme for eSignature elements" that is further described in Work Package 5-2 report of the CROBIES Study.

3.8 Security considerations

This component describes and specifies implementation rules with regards to the strength of the technical solution used to implement the electronic signatures.
E.g.:

- *Authorised eSignature algorithms and relevant parameters*
- *Hashing functions algorithms,*
- *Key size requirements,*
- *and any other relevant security requirement.*

On this point we refer to the CROBIES proposal for "Quality Classification Scheme for eSignature elements" that is further described in Work Package 5-2 report of the CROBIES Study.

It is also referred to the CROBIES Work Package 5-3 report of the CROBIES Study

3.9 eSignature format rules

This component SHALL describe and specify how eSignatures are to be formatted, i.e.:

- *which eSignature formats, topology, signature-DTBS packaging and packaging convention are authorised,*
- *which set of minimal requirements for ensuring interoperability and cross-border use are applicable*

3.10 Detailed technical creation and verification rules

This component SHALL describe and specify for each signature the applicable requirements on the signer in creating it and on the verifier when validating it.

This SHALL include providing:

- *Requirements on how multiple (e.g. countersignatures) should be created;*
- *Indication which eSignature(s) should or must be time stamped by a TSA;*
- *The requirements on the verifier with regards to what should be checked and how this should*

be checked;

- *The description of how each signature validation process should occur with regards to certificate validation data (e.g. OCSP responses for each certificate in the chain supporting the signer's certificate) and trust model related information (e.g. use of Trusted Lists);*
- *The requirements on how validation results should be presented to the verifier;*
- *The description of what should be archived and preserved for medium or long term and how this should be implemented.*

3.11 Rules on Signature Creation Application (SCA) and Signature Verification Application (SVA) implementations

This component SHALL describe and specify SCA and on SVA implementations including in particular:

a. *The requirements on security measures the application should or must provide to the signer. E.g. a secure display interface insuring that what the signatory sees is really what he's signing, a trusted path between the Human Interface and the (S)SCD, is the application audited against IT security criteria ?…*

b. *The requirements on security measures the application should or must provide to the verifier. E.g. what are the rules for certification path construction/validation, including the validation of the trust model requirements, the rules for the revocation status validation (whether the grace period should be considered), the security measures undertaken for long term validity (e.g. re-timestamping), is the application audited against IT security criteria …*

References should be included to applicable standards with regards to requirements on SCA and SVA (e.g. CWA 14170, CWA 14171 or their successors in the context of the execution of Mandate M460 [7]).

3.12 Signature Policy Documents

The last phase in the design process of a Signature Policy MUST formalise rules and requirements established in the two previous phases into a standardized table of content based document that should be available in two forms:

- ***Human Readable Signature Policy document**: A formalized and standardized table of content for such a document should be standardised and made available in a similar way as RFC 3647 is providing with regards to Certification Practice Statement and Certificate Policies;*

- ***Machine Processable form**: Signature Policies are likely to be more effective when they are available in a machine processable form, allowing them to be implemented by automated means. A signature policy may be written using a formal notation like ASN.1 (see ETSI TR 102 272:"ASN.1 format for signature policies") or XML (see ETSI TR 102 038:"XML format for signature policies").*

Both Human Readable and Machine Processable forms SHOULD of course cover the three parts of a signature policy, namely the signature creation policy, signature validation policy and the signature (long term) management policy.

This component SHALL state requirements with regards to the availability and use of machine processable forms for the Signature Policy.

4 Compliance Audit and Other Assessments

This component SHALL describe and specify the following:

- *The list of topics covered by the assessment and/or the assessment methodology used to perform the assessment;*
- *Frequency of compliance audit or other assessment:*
    - *for each subordinate Signature Policy that must be assessed pursuant to a Signature Policy, or the circumstances that will trigger such an assessment;*
    - *for each Application that must be assessed pursuant to the Signature Policy or a compliant (subordinate) Signature Policy, or the circumstances that will trigger such an assessment.*

  Possibilities include an annual audit, pre-operational assessment as a condition of allowing an entity to be operational, or investigation following a possible or actual compromise of security.
- *The identity and/or qualifications of the personnel performing the audit or other assessment.*
- *The relationship between the assessor and the entity being assessed, including the degree of independence of the assessor.*
- *Actions taken as a result of deficiencies found during the assessment; examples include a temporary suspension of operations until deficiencies are corrected, changes in personnel, triggering special investigations or more frequent subsequent compliance assessments, and claims for damages against the assessed entity.*
- *Who is entitled to see results of an assessment (e.g., assessed entity, other participants, the general public), who provides them (e.g., the assessor or the assessed entity), and how they are communicated.*

5 Other Business and Legal Matters

This component SHALL describe and specify general business and legal matters not covered yet by the previous sections of the present document, such as:

- *Applicable fees*
- *Financial Responsibility*
- *Confidentiality of Business Information*
- *Privacy of Personal Information*
- *Intellectual Property Rights*
- *Representations and Warranties*
- *Disclaimers of Warranties*
- *Limitations of Liability*
- *Indemnities*
- *Term and Termination*
- *Individual notices and communications with participants*
- *Amendments*
- *Dispute Resolution Procedures*
- *Governing Law*
- *Compliance with Applicable Law*
- *Miscellaneous Provisions (e.g. entire agreement, assignment, severability, enforcement, force majeure)*
- *Other Provisions*