Draft EN 119 172-1 V0.0.4 (2013-11)

Electronic Signatures and Infrastructures (ESI);

Part 1: Signature Policies

STABLE DRAFT FOR PUBLIC REVIEW UNTIL 15 JANUARY 2014

Download the template for comments:

http://docbox.etsi.org/ESI/Open/Latest_Drafts/Template-for-comments.doc

Send comments to E-SIGNATURES_COMMENTS@LIST.ETSI.ORG

Reference
DEN/ESI-0019172-1

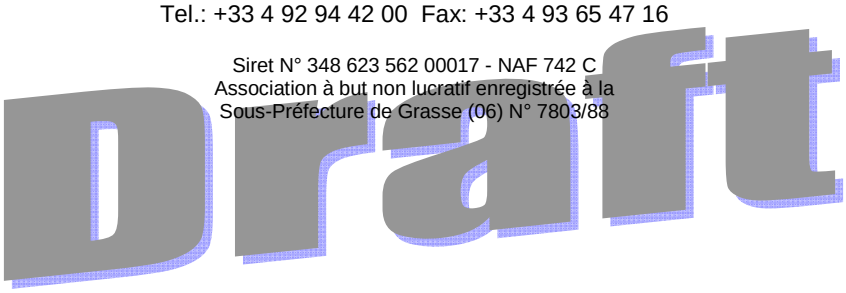
Keywords
e-Signatures, e-commerce, trust service

ETSI

650 Route des Lucioles
F-06921 Sophia Antipolis Cedex - FRANCE

Tel.: +33 4 92 94 42 00 Fax: +33 4 93 65 47 16

Siret N° 348 623 562 00017 - NAF 742 C
Association à but non lucratif enregistrée à la
Sous-Préfecture de Grasse (06) N° 7803/88



Contents

Intellectual Property Rights

IPRs essential or potentially essential to the present document may have been declared to ETSI. The information pertaining to these essential IPRs, if any, is publicly available for **ETSI members and non-members**, and can be found in ETSI SR 000 314: *"Intellectual Property Rights (IPRs); Essential, or potentially Essential, IPRs notified to ETSI in respect of ETSI standards"*, which is available from the ETSI Secretariat. Latest updates are available on the ETSI Web server (http://ipr.etsi.org).

Pursuant to the ETSI IPR Policy, no investigation, including IPR searches, has been carried out by ETSI. No guarantee can be given as to the existence of other IPRs not referenced in ETSI SR 000 314 (or the updates on the ETSI Web server) which are, or may be, or may become, essential to the present document.

Foreword

This draft European Standard (EN) has been produced by ETSI Technical Committee Electronic Signatures and Infrastructures (ESI) and is now submitted for the xxx phase of the ETSI standards EN Approval Procedure.

The present document is part 1 of a multi-part deliverable.

Proposed national transposition dates	
Date of latest announcement of this EN (doa):	3 months after ETSI publication
Date of latest publication of new National Standard or endorsement of this EN (dop/e):	6 months after doa
Date of withdrawal of any conflicting National Standard (dow):	6 months after doa

Introduction

Implementing electronic signatures into a business process very often requires considering more than one signature to give legal validity to one or several documents or to make a transaction effective. These may be parallel independent signatures, such as those of a buyer and seller on a contract; or embedded, countersignatures, where the countersignature is applied on top of a primary signature, such as a witness's signature, or the signature of a superior validating the signature of a subordinate.

A signature policy may be a useful tool for specifying the means for the creation and verification of ***all*** the typical qualities of an electronic signature. A signature policy should be drafted by reference to a specific business application. It does not ignore the fact that there is probably an existing business need for guidance or a set of rules which could be specified by two parties with no previous relationship who want to sign a once only contract electronically.

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.

1 Scope

This document provides a standardised table of contents for signature policy documents.

It additionally provides a standardised signature validation policy, the so-called "European Signature Validation Policy for advanced electronic signatures (AdES) supported by a qualified certificate and qualified electronic signatures against EU Member States Trusted Lists", aiming to describe the requirements imposed on the actors with respect to the application of electronic signatures to documents and data in order for these signatures to be considered as valid (technical) AdES, AdES supported by a Qualified Certificate ($AdES_{QC}$) or Qualified electronic Signature (QES), with all certificates and their related chains supporting the signatures are validated against the EU Member State Trusted Lists (this includes signer's certificate and certificates used to validate certificate validity status services - either based on CRLs or OCSP).

2 References

References are either specific (identified by date of publication and/or edition number or version number) or non-specific. For specific references, only the cited version applies. For non-specific references, the latest version of the referenced document (including any amendments) applies.

Referenced documents which are not found to be publicly available in the expected location might be found at http://docbox.etsi.org/Reference.

NOTE: While any hyperlinks included in this clause were valid at the time of publication ETSI cannot guarantee their long term validity.

2.1 Normative references

The following referenced documents are necessary for the application of the present document.

Not applicable.

2.2 Informative references

The following referenced documents are not necessary for the application of the present document but they assist the user with regard to a particular subject area.

[i 1] ETSI TR 119 000: “Rationalised Framework for Electronic Signature Standardisation”.

[i.2] Not used.

[i.3] Not used.

[i.4] Not used.

[i.5] Not used.

[i.6] Not used.

[i.7] ETSI EN 319 102: “Procedures for Signature Creation and Validation”.

[i.8] ETSI TS 119 101: "Policy and security requirements for signature creation and validation".

[i.9] ETSI EN 319 602: “Trust Service Status Lists Format”.

[i.10] ETSI EN 319 612: “Trusted Lists Format”.

[i.11] Not used.

[i.12] Not used.

[i.13] Not used.

[i.14] Not used.

[i.15] Not used.

[i.16] Not used.

[i.17] ETSI TR 119 100: "Business driven guidance for signature creation and signature validation".

[i.18] Directive 1999/93 Directive 1999/93/EC of the European Parliament and of the Council of 13 December 1999 on a Community framework for electronic signatures.

[i.19] Commission Decision 2009/767/EC of 16 October 2009 setting out measures facilitating the use of procedures by electronic means through the 'points of single contact' under Directive 2006/123/EC of the European Parliament and of the Council on services in the internal market. OJ L 274, 20.10.2009, p. 36.

[i.20] Commission Decision 2011/130/EU of 25 February 2011 establishing minimum requirements for the cross-border processing of documents signed electronically by competent authorities under Directive 2006/123/EC of the European Parliament and of the Council on services in the internal market

[i.21] Not used.

[i.22] ETSI TS 119 001: "Electronic Signature Infrastructure; Definitions and abbreviations."

[i.23] ETSI TS 119 312: "Electronic Signature Infrastructure; Cryptographic suites.

[i.24] IETF RFC 5280: "internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile.

[i.25] IETF RFC 6960: "X.509 Internet Public Key Infrastructure Online Certificate Status Protocol - OCSP".

[i.26] ETSI EN 319 411-1

[i.27] ETSI EN 319 411-2

[i.28] ETSI EN 319 411-3

[i.29] ETSI EN 319 412-5

3 Definitions, symbols and abbreviations

3.1 Definitions

For the purposes of the present document, definitions in TR 119 001 [i.22] apply with in particular the following definitions being imported in the present document for the sake of reader's convenience:

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.

NOTE 1: When validated against a signature policy X, the validity of an electronic signature is a relative concept and will be determined against the rules defined by such a policy. The same signature can be determined as valid against signature policy X while being invalid against

signature policy Y. 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 in a specific context (e.g. business process, a specific application), their potential legal effect and value will be driven by the applicable laws and/or contractual relationships between the parties involved and concerned by the signatures. Closed user group domains of application should be clearly distinguished from a purely open context to which generally applicable laws may address.

NOTE 2: A Signature Policy may cover the three following aspects related to the management of each of the considered electronic signature(s):

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.

3.3 Abbreviations

AdES	Advanced Electronic Signature
$AdES_{QC}$	Advanced Electronic Signature supported by a Qualified Certificate
ASiC	Associated Signature Containers
B2B	Business to Business
B2C	Business to Consumer
BPMN	Business Process Modelling Notation
CAdES	CMS Advanced Electronic Signature
CRL	Certificate Revocation List
DOTBS	Data Object To Be Signed
DTBSR	Data To Be Signed Representation
EN	European Norm
EU	European Union
Gov2B	Government to Business
Gov2C	Government to Consumer
LTV	Long Term Validation
OCSP	Online Certificate Status Protocol
OID	Object Identifier
PAdES	PDF Advanced Electronic Signature
QES	Qualified Electronic Signature
RF	Rationalised Framework
SAP	Signature Application Practices
SAPS	Signature Application Practices Statements
SCA	Signature Creation Application
SCDev	Signature Creation Device
SVA	Signature Validation Application
TL	Trusted List
ToC	Table of Content
TR	Technical Report
TS	Technical Specifications
TSL	Trust Service Status List
TSP	Trust Service provider
UML	Unified Modelling Language
XAdES	XML Advanced Electronic Signature

4 Implementing electronic signatures

4.1 Overview of the ETSI business driven guidance for implementing electronic signatures

For stakeholders (e.g. businesses, governments, service providers) wanting to implement a Signature Creation or Validation solution, the starting point should be ETSI TR 119 100 ("Business Driven Guidance for implementation of Signature Creation and Validation") [i.17]. Information from that document should be used to start an analysis of the business application context in which the eSignature should be implemented. This analysis should include a risk assessment and should lead to a set of security, policy and legal requirements, control objectives and controls to implement. ETSI TS 119 101[i.8] provides a selection of control objectives and controls which should be considered during the analysis. They are separated into five main categories:

- Legal driven policy requirements,
- Information security (management system) requirements,
- Signature Creation and Signature Validation processes requirements,
- Development & coding policy requirements,
- General requirements.

This policy & security requirements and controls document [i.8] helps to make declaration and statements on practices that are used or to be used by applications implementing electronic signatures in a specific context. However under the same set of practices, applications may still use or follow different set of rules to create different types of electronic signatures.

Starting from their model, stakeholders are guided by ETSI TR 119 100 :

- for properly specifying all the relevant parameters (hereafter “business scoping parameters” - BSP) regarding the creation and the validation of electronic signatures for the specific addressed application / business processes, and
- for making the best choice among the wide offer of standards from the Rationalised Framework of European Standards for Electronic Signatures (RF) [i.1] in order to ensure the best implementation of electronic signatures within the addressed application / business processes.

The guided implementation process proposed by TR 119 100 [i.17] is defined in a way that ensures to stakeholders a proper and consistent treatment of all essential business scoping parameters, including:

- parameters directly dependant on the specific application or business electronic processes,
- parameters derived from the regulatory/legal framework where the business must be conducted,
- parameters inherent to the different types of signing entities, as well as
- other aspects that do not fall within the above three listed categories but are important to be addressed when implementing electronic signatures.

A signature policy document is a declaration of the practices and rules (to be) used when creating, preserving and validating electronic signatures in a specific context (e.g. business process) and is usually a document resulting from the execution of the implementation process described in the present document.

The present document that specifies a standardised table of contents can be used to document the various decisions taken while executing the business driven electronic signature implementation process for which guidance is provided in ETSI TR 119 100 [i.17]. At the end of this iterative process, this will help to finalise and formalise the declaration of the practices and rules (to be) used when creating, preserving and validating electronic signatures in the concerned specific context (e.g. business process) into such a standardised signature policy document.

4.2 Importance of the signature policy

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.

When validated against a signature policy X, the validity of an electronic signature is a relative concept and will be determined against the rules defined by such a policy. The same signature can be determined as valid against signature policy X while being invalid against signature policy Y. 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 in a specific context (e.g. business electronic process, a specific application), their potential legal effect and value will be driven by the applicable laws and/or contractual relationships between the parties involved and concerned by the signatures. Closed user group domains of application should be clearly distinguished from a purely open context to which generally applicable laws may address.

A Signature Policy may cover the three following aspects related to the management of each of the considered electronic signature(s):

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

A signature policy may cover several electronic signatures being part of a group of electronic signatures implemented in the context of a specific business or application process. It is not unusual that a business process requires the implementation of several signatures being either multiple signatures applied to the same data object(s) or to different data objects being signed by the same or different entities at different moments alongside the workflow of events and need for evidences covered by the considered workflow. Hence a signature policy and in particular a signature policy document may cover a set of several signature policies that will define the set of rules applicable to one or several signatures to which the same set of rules apply.

As part of the rules covered by a signature policy, or closely associated to them a set of rules applicable to the application and/or its environment implementing the creation, the upgrade and/or the validation of electronic signatures. In particular this covers rules with regards to the practices used by the application and its environment to properly implement the generation, upgrade and/or validation of electronic signatures. A community of users may define as part of a signature policy the applicable requirements with regards to those practices any application will have to meet in order to comply with the community signature policy. A signature policy may also refer to an external set of practices statements that describes the practices used by an application or an application provider that generate/validate electronic signatures according to several signature policies defined several communities of users. A signature policy may also be defined in the context of a specific legal context and define a set of rules to create or validate a signature meeting specific legal requirements (e.g. a qualified electronic signature as defined in the applicable European legislation framework) including specific requirements on signature creation applications (SCAs) and signature validation applications (SVAs) and their environments.

A document stating such signature application practices (SAPs) defining requirements or making statements on the way signature applications are meeting application level policy and security requirements when creating or validating electronic signatures, whatever and independently of the type of signature and of the set of requirements ruling the creation or validation of a type of signature (i.e. the applied signature policy), might be compared to a signature policy as a Certification Practice Statement can be compared to a Certificate Policy.

4.3 Structure of the present document

Section 5 provides a standardised table of contents for signature policy documents.

Section 6 provides a standardised signature validation policy, the so-called "European Signature Validation Policy for $AdES_{QC}$ and QES against EU Member States Trusted Lists", aiming to describe the requirements imposed on the actors with respect to the application of electronic signatures to documents and data in order for these signatures to be considered as valid (technical) AdES, AdES supported by a Qualified Certificate ($AdES_{QC}$) or Qualified electronic Signature (QES), with all certificates and their related chains supporting the signatures are validated against the EU Member State Trusted Lists (this includes signer's certificate and certificates used to validate certificate validity status services - CRLs, OCSP).

5 Standardised table of content for signature policies

The present clause defines the standardised table of content (ToC) for signature policies conformant to the present document. The numbering of the components of the standardised ToC is on purpose provided as it shall appear in the signature policy document instantiating the standardised ToC. The provided text specifies the expected content of each component.

1. Introduction

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 it describes and to the specific business or application context it applies. When no text is provided, no additional specific requirement applies.

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 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.

1.2.1 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).

1.2.2 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.

1.2.3 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.

1.3 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.

1.3.1 Signature Policy name(s)

1.3.2 Signature Policy identifier(s)

The signature policy document **should** allocate a distinct identifier to the signature policy (document) itself and to each of the set of rules applicable to a specific set of signatures (could be a single signature) to distinguish several sets of such rules applicable to the various types of signatures concerned in the applicable electronic business process.

The signature policy document may also derive from the signature policy document OID used as a root, several leaf OIDs to identify such sets of rules applicable to the various types of signatures (e.g. a signature policy document having identifier 1.3.777.1.1 could further identify three sets of rules applicable to three types of signatures in the concerned workflow of the business process via the respective 1.3.777.1.1.**1**, 1.3.777.1.1.**2**, and 1.3.777.1.1.**3** OIDs).

1.3.3 Signature Policy conformance rules

1.3.4 Signature Policy distribution points

1.4 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.

1.5 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 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 **shall** 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 **shall** also include the procedures by which this determination is made.

1.5.1 Organisation administering the document

1.5.2 Contact person

1.6 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. Signature creation/validation application practices statements

As part of the rules covered by a signature policy, or closely associated to them a set of rules applicable to the application and/or its environment implementing the creation, the upgrade and/or the validation of electronic signatures. In particular this covers rules with regards to the practices used by the application and its environment to properly implement the generation, upgrade and/or validation of electronic signatures. A community of users may define as part of a signature policy the applicable requirements with regards to those practices any application will have to meet in order to comply with the community signature policy. A signature policy may also refer to an external set of practices statements that describes the practices used by an application or an application provider that generate/validate electronic signatures according to several signature policies defined several communities of users. A signature policy may also be defined in the context of a specific legal context and define a set of rules to create or validate a signature meeting specific legal requirements (e.g. a qualified electronic signature as defined in the applicable European legislation framework) including specific requirements on signature creation applications (SCAs) and signature validation applications (SVAs) and their environments.

A document stating such signature application practices (SAPs) defining requirements or making statements on the way signature applications are meeting application level policy and security requirements when creating or validating electronic signatures, whatever and independently of the type of signature and of the set of requirements ruling the creation or validation of a type of signature (i.e. the applied signature policy), might be compared to a signature policy as a Certification Practice Statement can be compared to a Certificate Policy.

The present component **shall** either include by reference or explicitly the set of (policy and security) practices requirements that the SCA/SVA will have to meet when generating, upgrading and/or validating electronic signatures in compliance with the applicable signature policy.

With regards to its content and sub-components, the present component **shall** make use of the structure defined from the structure of the ETSI TS 119 101 ("Policy and security requirements for signature creation and validation") [i.8] that specifies policy and security requirements that must be considered when creating and validating signature in a trustworthy manner. The analysis of the business application context in which the eSignature should be implemented should include a risk assessment and should lead to a set of security, policy and legal requirements, control objectives and controls to implement with regards to the SCA/SVA. ETSI TS 119 101[i.8] provides a selection of control objectives and controls which should be considered during the analysis. They are separated into five main categories:

- Legal driven policy requirements,
- Information security (management system) requirements,
- Signature Creation and Signature Validation processes requirements,
- Development & coding policy requirements,
- General requirements.

NOTE: When the signature policy document is referring to such practices requirements or is claiming compliance with practices statements provided as external document(s), those external documents consisting in declarations of signature application practices statements (SAPS) should be structured according to the ToC provided in ETSI TS 119 101 [i.8].

2.1 Legal driven policy requirements

This component **shall** contain requirements, control objectives and controls in connection with:

1. the processing of personal data,
2. the significance of digital signatures, and
3. the business continuity.

See ETSI TS 119 101[i.8] for further guidance on, or referencing of, potentially applicable controls.

2.2 Information security (management system) requirements

This component shall contain requirements, control objectives and controls in connection with information security and information security management systems, and in particular:

1. security policy(ies),
2. network protection,
3. information system protection,
4. software integrity of the application,
5. data storage security,
6. risk assessment, and
7. audit trail security.

See ETSI TS 119 101[i.8] for further guidance on, or referencing of, potentially applicable controls.

2.3 Signature Creation and Signature Validation processes requirements

This component **shall** contain requirements, control objectives and controls in connection with:

1. signature creation process and systems, and in particular:
    a. data content type management,
    b. signature attribute viewer,
    c. timing and sequencing enforcement,
    d. signature invocation,

e. selection of the level of signature longevity,

f. signer's authentication procedure (& access control management),

g. DOTBS preparation,

h. Data To Be Signed Representation (DTBSR),

i. signature creation device management,

j. protection of the communication between Signature Creation Device (SCDev) and SCA,

k. robustness of signature cryptographic suites,

l. community adaptability,

m. bulk signing operation

2. signature validation process and systems, and in particular:

   a. validation process rules enforcement,

   b. validation user interface

   c. validation input/output relative conformance (correctness of the implemented validation procedure).

See ETSI TS 119 101[i.8] for further guidance on, or referencing of, potentially applicable controls.

2.4 Development & coding policy requirements

This component **shall** contain requirements, control objectives and controls in connection with the development and coding policies, in particular with:

1. the secure development methods,
2. the security of the application, and
3. testing compliance and interoperability.

See ETSI TS 119 101[i.8] for further guidance on, or referencing of, potentially applicable controls.

2.5 General requirements

This component **shall** contain other general requirements, control objectives and controls in connection with:

1. the user interface,
2. the interface to external trust service providers, and
3. general security measures.

See ETSI TS 119 101[i.8] for further guidance on, or referencing of, potentially applicable controls.

3. Business scoping parameters

The purpose of a signature policy is to describe, as clearly as possible, the requirements imposed on or committing the involved actors (signers, verifiers and potentially one or more trust service providers) with respect to the application of electronic signatures to documents and data that should be signed in a particular context, transaction, process, business or application domain (see component 1.2) in order for these signatures to be considered as valid signatures under this signature policy.

These requirements are organised against so-called business scoping parameters (BSPs) of which we can distinguish:

- Parameters mainly related to the application and/or business process for which implementation of electronic signature(s) is required;
- Parameters mainly influenced by legal provisions associated to the application and/or business context in which the business process takes place;
- Parameters related to the actors involved in the creation/validation of electronic signatures; and
- Other signature parameters.

The sub-components (described hereafter) of this component **shall** each include the description of the applicable BSP provisions not only in terms of business language but also the counterpart technical choices and specifications.

3.1 BSPs mainly related to the concerned application/business process

3.1.1 BSP (a): Workflow (sequencing and timing) of electronic signatures

This component **shall** be used to describe and specify whether the business electronic process and hence the signature policy address a single signature or a set of signatures. In this latter case it **shall** describe and specify the workflow and in particular the sequencing and the cardinality of the concerned signatures and whether the concerned workflow is made of:

- parallel (or independent) signatures (i.e. signatures applied exactly to the same data object(s)); or
- serial signatures (i.e. signatures applied to different data object(s) and serialised); or
- counter signatures (i.e. signatures successively applied to the same original data object(s) and to the set of previous signatures); or
- a combination of such signatures.

This component **shall** include illustration of the business scenario use cases implementing electronic signature(s) and the associated eSignature(s) flow. Such use cases **should** be produced using the Unified Modelling Language (UML), the Business Process Modelling Notation (BPMN - a standard for modelling business processes and web service processes, as put forth by the Business Process Management Initiative – www.bpmi.org) 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 (mutually independent signatures for which the ordering of the signatures is not important), or sequential (signature for which the ordering is important), 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 business signing role (primary signature versus countersignature) defining the relationship between each actor's signature and any other required signature.
d. For each data object to be signed, what sequence of signature(s) do apply (e.g. single; multiple parallel; counter signatures; sequential; or a combination)

This component **shall** indicate whether and which signature is required to be validated before generating the next signature in the workflow.

This component **shall** indicate whether the time when a signature is generated or validated is relevant or not (e.g. in order to be legally enforceable) and in particular the timing constraints apply to the generation or validation of electronic signatures (e.g. whether a specific signature must be generated before a certain deadline, whether a set of parallel signatures must be generated within a certain timeframe, whether the elapsed time between two serial or counter signatures must be greater, equal or smaller than a certain duration, etc.). 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.

This component **shall** indicate the cardinality of signatures involved in the concerned business process and in particular whether mass signing is applicable, i.e. a significant number of serial signatures like signing a significant number of documents per day, as this may have an impact on, for example, requirements for use of signing devices designed for mass signing (e.g. hardware security modules).

3.1.2 BSP (b): Data object(s) to be signed

For each signature identified and for each element (data object) to be signed as identified in the concerned workflow (see BSP(a)):

This component **shall** be used to describe and specify all the relevant aspects concerning to the data object(s) that have to be signed and the related technology, i.e. the type of technological environment in which those data objects are managed. These aspects include:

1. **The nature and the format of the data to be signed** (e.g. binary, structured data, xml, PDF document, editable documents such as Word or ODF, multimedia packages, images, etc.). The type of format for the DOTBS may also be influenced by business risks or legal provisions, for example, when a specific provision is imposed on the formalities of signing (e.g. what you see is what you sign, see BSP(i)).

   NOTE: At present electronic signatures may be generated following XML, ASN.1 or PDF syntax. It is quite obvious to conclude that where the data to be signed are specified in one of the aforementioned syntaxes, a reasonable initial choice would be to select the electronic signature defined for that syntax, unless other business parameters clearly recommend to use another one.

2. In those cases where the data object involved in a signing process is structured, this component **should** identify whether the whole data object or only certain part(s) have to be signed.

3.1.3 BSP (c): The relationship between signed data object(s) and signature(s)

For each signature identified and for each element (data object) to be signed as identified in the concerned workflow (see BSP(a)):

This component **shall** be used to describe and specify the type of relationship between the signed data and the signatures. In particular, this component **shall** address:

1. The need for signed data referencing mechanisms and in particular the use or relevance of bulk signatures, i.e. when one signature has to sign different data objects (e.g. through the implementation of signature on several document references consisting in hashes of the referenced documents).

2. The number of the data objects that one signature actually signs.

3. The relative position of the signed data object and its signature (e.g. associated, encapsulated, encapsulating, enveloped, enveloping, detached).

4. The signature format (including levels) to be used.

3.1.4 BSP (d): Targeted community

For each signature identified and for each element (data object) to be signed as identified in the concerned workflow (see BSP(a)):

This component **shall** be used to identify and describe the community each signed data object(s) (e.g. documents) and its (their) signature(s) is (are) addressed to. This component **shall** identify any specific community rules in place. These rules could, for instance, state the conditions under which a certain signature may be relied upon, or include provisions relating to the intended effectiveness of signatures, where multiple signatures are required. These rules could greatly impact not only the formats of the signatures and their relationships with the signed documents, but also the specific standards and/or profiles to be used.

3.1.5 BSP (e): Allocation of responsibility of signatures validation and upgrade

For each signature identified and for each element (data object) to be signed as identified in the concerned workflow (see BSP(a)):

This component **shall** be used to describe and specify the allocation of the responsibility of validating and/or upgrading such electronic signatures in particular among the following entities, according to the specificities of the business process:

1. Party relying on the signature, being either the signer or any other appropriate relying party.

2. Electronic Signature Validation Trusted Services, on request of either the signer or any other appropriate relying party.

3. Business processes where countersignatures are generated, could require that counter-signing parties are required to perform a validation of the signature(s) to be counter-signed before actually countersigning them, as part of the data flow.

These three types of allocations are not necessarily exclusive, being it possible that some of them coexist within complex business processes.

Upgrading electronic signatures is a co-lateral process to the validation of electronic signatures, namely the process by which certain material (e.g. time-stamps, validation data and even archival-related material) is incorporated to the electronic signatures for making them more resilient to change or for enlarging their longevity. This component should, in consequence, also identify requirements for upgrading electronic signatures as they are validated and progress in the business process data flow.

3.2 BSPs mainly influenced by the legal/regulatory provisions associated to the concerned application/business process

The following BSPs may not strictly be influenced by legal provisions only but may also be driven by business considerations inherent to the concerned business process and its expectations with regards to the type of evidences resulting from the implementation of electronic signatures.

3.2.1 BSP (f): Legal level of the signatures

For each signature identified in the concerned workflow (see BSP(a)):

This component **shall** be used to describe and specify the signature legal level required in the context of the business process and the associated legal requirements. This parameter has an impact on the level of assurance on the authentication (i.e. the certification of the identification) of the actor generating an electronic signature, on the class and policy requirements on the TSP providing such level of assurance, on the class of signature creation device used by such actors, on the use of a specific trust model for TSP issuing certificates (e.g. trusted lists, specific trust anchors in PKI hierarchy, use of certification authority certificate stores).

NOTE: The following levels are identified in accordance with Directive 1999/93/EC [i.18], CD 2009/767/EC [i.19] and CD 2011/130/EU [i.20]: qualified electronic signatures (QES), advanced electronic signatures supported by a qualified certificate ($AdES_{QC}$), and advanced electronic signatures (AdES).

3.2.2 BSP (g): Commitment assumed by the signer

For each signature identified in the concerned workflow (see BSP(a)):

This component **shall** be used to describe and specify the expected purpose of the signature and hence the expected meaning and the precise nature of the responsibility assumed by the signer when generating the concerned signature, i.e. the type of commitment associated to the signature.

The explicit description of such electronic signature commitments 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 and relying on the implicit contextual information may be hazardous.

In particular, there may be a need to be able to distinguish between:

- electronic signatures intended for data authentication purposes only

  NOTE: It should be noted that the generation of "data in electronic form which are attached to or logically associated with other electronic data to ensure the origin and the integrity of the associated data" are defined as the generation of electronic seals when such data are generated by legal persons as defined in COM(2012)238final regulation proposal [i.21]. The generation of electronic signature for which the expression of the intention to sign is limited to ensure the authentication of the data to which it is associated (signed data object(s)) will serve the same purpose towards natural person signers while being electronic signatures in essence.

- electronic seals generated by legal persons,
- electronic signatures intended for entity authentication purposes only,
- electronic signatures created with the intention to sign the associated data (signed data object(s)):
  - as a draft,
  - as an acknowledgement of receipt,
  - as an intermediate approval as part of a decision process,
  - to indicate authorship or responsibility for a document (signed data),
  - to indicate having reviewed a document (signed data),
  - to certify that a document is an authentic copy,
  - to indicate witnessing of someone else signature on the same document (signed data)
  - having read, approving and being bound accordingly to the content of the data object that is signed
  - etc.

  and being bound accordingly to the data object that is signed.

NOTE: Indication of commitment types may assist in the management and validation of multiple signatures under a signature policy.

3.2.3 BSP (h): Level of assurance on timing evidences

For each signature identified in the concerned workflow (see BSP(a)):

This component shall be used to describe and specify the requirement on the level of assurance on the required timing evidences. This component is closely related to the components BSP(a), (j) and (k). It should be distinguished between claimed assertions with regards to time information, trusted time-stamps provided by trust service providers issuing time-stamp tokens, the requirements and level of assurance associated respectively to the time-stamp tokens and the providers, on which type of information the time-stamp tokens are generated (e.g. time information only, signed data object(s), signature(s), signature(s) and validation data, etc.).

3.2.3 BSP (i): Formalities of signing

For each signature identified in the concerned workflow (see BSP(a)):

This component **shall** be used to describe and specify the way evidences are built with regards to the expression of will or intention of the signer to sign and in particular the requirements related to the way the attention of the signer is drawn to the significance of the commitment he is undertaking by performing the act of signing. This aims to ensure as far as this is possible, a proper and valid legal signature environment.

In particular this component **shall** identify and specify:

1. requirement for having a WYSIWYS environment;
2. requirements for providing the actor generating/ validating electronic signatures with:
    i. proper advice and information on the application's signature process,
    ii. proper advice and information on legal consequences,
    iii. a user interface guaranteeing, to the extent possible, a valid legal signature environment.
3. requirements for designing the user interface:
    i. guaranteeing the above requirements
    ii. allowing and demonstrating clear expression of a will to sign and the user's intention to be bound by the signature;
    iii. allowing and demonstrating an informed consent;
    iv. ensuring 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)
4. requirements for providing the relying party (including the signatory) with correct procedures for the validation and the archival of the electronic signature and the validation data.

This may impact the selection of appropriate protection profiles and conformity assessment schemes against which the signature creation and validation application will be designed and assessed.

3.2.4 BSP (j): Longevity and resilience to change

For each signature identified in the concerned workflow (see BSP(a)):

This component **shall** be used to describe and specify the expected longevity and resilience to change of the electronic signature such that it is verifiable after a given period of time, such as short term (transaction lifetime up to 1 day), medium term (up to the remaining time before expiration of the signing certificate, long term (up to min_of{6years; max_of{guarantee-given-by-$TST_{T\text{-}Level}$;weakest-robustness-of-signatures-on-Validation-Data}}), or very long term (up to min_of{10years;guarantee-given-by-the-TST_A-or-the-successive-application-of-TST_A's}).

NOTE : Such requirements will have a impact on the adequate form of the signature technical format. For creation of electronic signatures with a preservation need for:

- short term (If no expiredCertRevocationInfo Then Min_of{expiration of the certificate,revocation of certificate, 1year} Else Min_of{revocation of certificate,

1year}), the related type of signature "form" is B-Level specified in Baseline Profile for CAdES, XAdES and PAdES, respectively.

- medium term (up to min_of{3years; max_of{guarantee-given-by-$TST_{T\text{-}Level}$;weakest-robustness-of-signatures-on-Validation-Data}}), the related type of signature "form" is T-Level specified in Baseline profiles for CAdES, XAdES and PAdES (and associated requirements for time-stamp services);
- long term (up to min_of{6years; max_of{guarantee-given-by-$TST_{T\text{-}Level}$;weakest-robustness-of-signatures-on-Validation-Data}}), the related type of signature "form" is LT-Level specified in Baseline Profiles for CAdES, XAdES and PAdES (and associated requirements for time-stamp services);
- very long term (up to min_of{10years;guarantee-given-by-the-TST_A-or-the-successive-application-of-TST_A's}), the related type of signature "form" is LTA-Level specified in Baseline Profiles for CAdES, XAdES and PAdES (and associated requirements for time-stamp services);

The key length is determined by the TSP having issued the signing certificate; however BSP(p) recommendations shall be followed according to the expected term of validity of the signature.

3.2.5 BSP (k): Archival

For each signature identified in the concerned workflow (see BSP(a)):

This component **shall** be used to describe and specify archival requirements.

3.3 BSPs mainly related to the actors involved in creating/validating electronic signatures

3.3.1 BSP (l): Identity (and roles/attributes) of the signers

For each signature identified in the concerned workflow (see BSP(a)):

This component **shall** be used to describe and specify requirements on:

1. the identification of the proposed signers,
2. the associated signer identification rules,
3. if any, the rules applicable to the roles and/or attributes of the signers, as well as
4. if any the associated proof of authority.

This component **shall**, in consequence, identify and describe 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 is the required identification element (identity attributes) for each type of signer. For instance 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.

In some business scenarios, the role or attributes of a signer are at least as important as his identity. In this sub-component, when applicable, “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, when present, **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.

This "associated proof of authority" sub-component, when present, **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.

3.3.2 BSP (m): Level of assurance required for the authentication of the signer

For each signature identified in the concerned workflow (see BSP(a)):

This component **shall** be used to describe and specify the level of assurance required for the authentication of the signer, in particular what are the expectations in terms of trust on the signatory identification (e.g. quality level of certificate). For instance, certificates may be required to 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.

3.3.3 BSP (n): Signature Creation Devices

For each signature identified in the concerned workflow (see BSP(a)):

This component **shall** be used to describe and specify requirements on the signature creation devices that will be used for generating the signatures within the business process, in order to ensure their fulfilment.

3.4 Other BSPs

3.4.1 BSP (o): Other information to be associated with the signature

For each signature identified in the concerned workflow (see BSP(a)):

This component **shall** be used to describe and specify, when applicable, any other information to be associated with the signature, such as: signature policy reference, geographic location at which the signature takes place, the time of signing, content time-stamp, content related information, signer claimed or certified attributes, etc.

This may have an impact on the use of additional signature attributes that will be added to the DTBS when creating the signature and hence an impact on the implementation of the selected signature format.

3.4.2 BSP (p): Cryptographic suites

For each signature identified in the concerned workflow (see BSP(a)):

This component **shall** be used to describe and specify requirements on the robustness of cryptographic suites used to generate or upgrade electronic signatures. It is recommended to use the following table to express such requirements:

Quality Level	Expected resistance	X/C/PAdES Baseline Level	Entry name of signature suite	Min. key size
Low Level	If no expiredCertRevocationInfo Then Min_of{expiration of the certificate,revocation of certificate, 1year} Else Min_of{revocation of certificate, 1year}	B-Level	• sha256-with-rsa RSASSA-PSS with mgf1SHA224Identifier RSASSA-PSS with mgf1SHA256Identifier • sha224-with-ecdsa sha256-with-ecdsa	• [1024] 1536 • 224 256
Medium Level	Up to min_of{3years; max_of{guarantee-given-by-$TST_{T\text{-}Level}$; weakest-robustness-of-signatures-on-Validation-Data)	T-Level	• sha256-with-rsa RSASSA-PSS with mgf1SHA224Identifier RSASSA-PSS with mgf1SHA256Identifier • sha224-with-ecdsa sha256-with-ecdsa	• 2048 • 224 256
Standard Level	Up to min_of{6years; max_of{guarantee-given-by-$TST_{T\text{-}Level}$; weakest-robustness-of-signatures-on-Validation-Data)	LT-Level		• 2048 • 224 256
Strongest level	Up to min_of{10 years; guarantee-given-by-the-TST_A-or-the successive-application-of-TST_A's}	LTA-Level	• RSASSA-PSS with mgf1SHA256Identifier • sha256-with-ecdsa	• 3072 • 256

Table 1: crytographic suites recommendations

NOTE: This table is based on guidance provided in ETSI TS 119 312 [i.23] or TS 119 100 [i.17].

3.4.3 BSP (q): Technological environment

This component should identify the type of technology in which the data objects to be signed and the signatures are managed as this may have an impact on the signature format to be used. In particular it should identify whether it is required (or even could be required in the future) allowing the generation and/or validation of certain signatures applied to certain document to be done not only in classical environments but also within mobile environments. In case this latter requirement exists, this component should clearly identify which type(s) of document(s) and which signatures within them, need to also be managed within mobile environments. This is extremely relevant, as the mobility aspect may require to make use of specific services for supporting these tasks, and in consequence, to use specific sets of standards.

4. Requirements / statements on technical mechanisms and standards implementation

4.1 Technical counterparts of BSPs - Statement summary

For each signature identified in the concerned workflow (as defined in section 3.1.1 - BSP(a)), this component **shall** summarise the requirements related to the BSPs specified in the previous components, and specify the counterpart statements or requirements on the technical mechanisms and standards to be implemented by signature creation/validation applications conformant to the signature policy.

In particular it **shall** specify the selected signature format(s) (e.g. XAdES, CAdES, PAdES and/or their baseline profile) including details on the format of the signed data object(s), the relative placement of the signature and

the signed data object(s) (e.g. enveloped, enveloping, detached), the relevance of use of a container to package the signature(s) together with signed data object(s) (e.g. ASiC and or its baseline profile), the specific attributes (signed or unsigned) of the signature, and the form level of selected signature format.

This component **should** make use of the following signature policy disclosure statement sheet, one sheet being produced per each signature identified in the concerned workflow. One single sheet may however be used when the same set of requirements/statements are applicable to a group of signatures.

Identifier of the concerned signature policy : .....

Identifier of the concerned signature(s) in the concerned signature workflow: .....

BSP	BSP title	Business statement summary	Technical statement counterpart
(a)	Workflow (sequencing & timing)		
(b)	DOTBS		
(c)	DOTBS vs Signature		
(d)	Targeted community		
(e)	Validation & upgrade responsibility		
(f)	Legal level		
(g)	Commitment type		
(h)	LoA on timing		
(i)	Formalities of signing		
(j)	Longevity & resilience		
(k)	Archival		
(l)	Identity of signers		
(m)	LoA on signers authentication		
(n)	Signature Creation Devices		
(o)	Signature attributes		
(p)	Cryptographic suites		
(q)	Technological environment		

Summary of the selected signature format(s) (e.g. XAdES, CAdES, PAdES and/or their baseline profile) including details on the format of the signed data object(s), the relative placement of the signature and the signed data object(s) (e.g. enveloped, enveloping, detached), the relevance of use of a container to package the signature(s) together with signed data object(s) (e.g. ASiC and or its baseline profile), the specific attributes (signed or unsigned) of the signature, and the form level of selected signature format:

4.2 Constraints for signature creation and validation procedures

This component **shall** specify the requirements, derived from the BSPs applicable to each signature covered in the policy, on the input/output of the signature creation procedure, the signature upgrade (extension) procedure and/or the signature validation procedure respectively. To this respect, this component **should** make use of the following sheets in particular when implementing the standard ETSI EN 319 102 ("Procedures for signature creation and validation") [i.7].

4.2.1 Input constraints to be used when generating, validating or upgrading electronic signatures in the context of the identified signature policy

Editorial note: Part of those constraints are identified in Annex A of ETSI EN 319 102 [i.7]. Definition, specification and of use of these constraints in [1.7] and in the present document will still require some fine-tuning and alignment.

The table below aims to facilitate deriving respectively signature creation constraints, signature validation constraints and signature upgrading constraints from applicable BSPs statements when considering the set of rules applicable to one or more signatures of the same type to which the same set of rules apply. These set of constraints and their values will then condition the respective creation, validation and upgrading procedures implemented at the Signature Creation Application (SCA) level or Signature Validation Application (SVA) level, and/or even at the Driving Application level.

Identifier of the concerned signature policy : ..... **Identifier of the concerned signature(s) in the concerned signature workflow: .....**							
BSP	**BSP title**	**Business statement summary**	**Technical statement counterpart**	**Constraint(s)**	**Creation** [yes/no]**.** **Validation** [yes/no]**.** **Upgrading** [yes/no]	**SCA** [yes/no]**.** **SVA** [yes/no]**.** **DA** [yes/no]	**Value**
(a)	Workflow (sequencing & timing)			**(a)1. OrderInSequence**: This constraints indicate requirements on the sequencing order of the applicable signature in the workflow. This may be expressed as "n" out of "m", where "m" is the number of signature (types) considered in the workflow, and last position in the sequence.	any.any.any	any.any.yes	
				(a)2. SequencingNature: This constraints indicate the characteristic of the signature with regards to sequencing. A possible syntax/semantic for a set of requirement values used to express such requirements is	any.any.any	any.any.yes	

BSP	BSP title	Business statement summary	Technical statement counterpart	Constraint(s)	**Creation** [yes/no]. **Validation** [yes/no]. **Upgrading** [yes/no]	**SCA** [yes/no]. **SVA** [yes/no]. **DA** [yes/no]	Value
				defined as follows: **(a)2.1 Mandated-independent** [Editorial note: or parallel]: independent signatures are defined as signatures applied to exactly the same data object(s). This constraint indicates that the signature is mandated to be an independent signature. **(a)2.2 Mandated-serial**: serial signatures are defined as signatures applied to different data object(s) and serialised. This constraint indicates that the signature is mandated to be a serial signature. **(a)2.3 MandatedUnsignedQProperties-counter-signature**: counter-signatures are defined as signatures successively applied to the same original data object(s) and to the set of previous signatures. This constraint indicates that the corresponding unsigned qualifying property is mandated to be present in the signature. Editorial note: there is so far no unsigned qualifying property to express the fact that a signature is a serial or independent signature.			
				(a)3. TimingRelevance: **(a)3.1 TimingRelevanceOnSequencing**: This constraints indicate the required relevance of timing with regards to the sequencing of the signatures. A possible syntax/semantic for a set of requirement values used to express such requirements is defined as follows: o before a certain deadline (date) o within a certain timeframe (not before /not after) o elapsed time against max.duration (<, ≤ , =, ≥, >) **(a)3.2 TimingRelevanceOnEvidence**: This constraint indicates the required timing evidence under the form of signed or unsigned qualifying properties that are mandated to be present in the signature. This includes:	any.any.any any.any.any	any.any.yes any.any.any	

BSP	BSP title	Business statement summary	Technical statement counterpart	Constraint(s)	**Creation** [yes/no]. **Validation** [yes/no]. **Upgrading** [yes/no]	**SCA** [yes/no]. **SVA** [yes/no]. **DA** [yes/no]	Value
				○ **(a)3.2.1 MandatedSignedQProperties-signing-time** to require from the signer a signed claimed time indication on when the signature has been generated. ○ **(a)3.2.2 MandatedSignedQProperties-content-time-stamp** to require a content-time-stamp being signed by the signer as part of the signed qualifying properties. ○ **(a)3.2.3 MandatedUnsignedQProperties-signature-time-stamp** (e.g. AdES-T, AdES T-level) to require a time-stamp on the signature ○ **(a)3.2.4 MandatedUnsignedQProperties-archival-form** (e.g. AdES-A, AdES LTA-level) to require an archival time-stamp			
				(a)4. MassSigningAcceptable (yes/no): This constraints indicate whether mass signing is acceptable with regards to the concerned type of signature. This may be expressed as a boolean.	any.any.any	any.any.any	
(b)	DOTBS			**(b)1. ConstraintOnNatureAndFormatOfTheContent** (DTBS): This constraint indicate requirements on the nature and format of the data (content) to be signed by the signer ("content" here is not taking into account any additional information or properties that may be signed together with the "content")	any.any.any	any.any.yes	
				(b)2. ContentRelatedConstraintsAsPartOfSignatureElements: This set of constraints indicate the required content related information elements under the form of signed or unsigned qualifying properties that are mandated to be present in the signature. This includes: **(b)2.1 MandatedSignedQProperties-DataObjetFormat** to require a specific format for the content being signed by the signer. **(b)2.2 MandatedSignedQProperties-content-hints** to	any.any.any	any.any.any	

BSP	BSP title	Business statement summary	Technical statement counterpart	Constraint(s)	**Creation** [yes/no]. **Validation** [yes/no]. **Upgrading** [yes/no]	**SCA** [yes/no]. **SVA** [yes/no]. **DA** [yes/no]	Value
				require specific information that describes the innermost signed content of a multi-layer message where one content is encapsulated in anotherfor the content being signed by the signer. **(b)2.3 MandatedSignedQProperties-content-reference** to require {incorporation of information on the way to link request and reply messages in an exchange between two parties, the way such link has to be done, etc.}. **(b)2.4 MandatedSignedQProperties-content-identifier** to require {the presence, a specific value for} an identifier that may be used later on in the signed qualifying property "content-reference" attribute.			
				(b)3. DOTBSAsAWholeOrInParts: This constraints indicate whether the whole data object or only certain part(s) have to be signed. A possible syntax/semantic for a set of requirement values used to express such requirements is defined as follows: o **whole**: the whole data object has to be signed; o **parts**: only certain part(s) of the data object have to be signed. In this case additional information should be used to express which parts have to be signed.	any.any.any	any.any.any	
(c)	Relationship between DOTBS and Signature			**(c)1. BulkSigningRelevance**: This constraint indicates the requirement for signed data referencing mechanisms and in particular for bulk signatures, i.e. when one signature has to sign different data objects (e.g. through the implementation of signature on several document references consisting in hashes of the referenced documents) or on the contrary its prohibition. A possible syntax/semantic for a set of requirement values used to express such requirements is defined as follows: **(c)1.1 mandatedBulkSigning**; **(c)1.2 prohibitedBulkSigning**.	any.any.any	any.any.yes	

BSP	BSP title	Business statement summary	Technical statement counterpart	Constraint(s)	**Creation** [yes/no]. **Validation** [yes/no]. **Upgrading** [yes/no]	**SCA** [yes/no]. **SVA** [yes/no]. **DA** [yes/no]	Value
				(c)2. ConstraintsOnTheNumberOfDOTBS: This constraints indicate the requirement on the number of data objects that one signature actually may sign. A possible syntax/semantic for a set of requirement values used to express such requirements is defined as follows: minValue {<, ≤ , =} x {=, ≥, >} maxValue	any.any.any	any.any.yes	
				(c)3. SignatureRelativePosition: This constraints indicates the requirement with regards to the relative position of the signed data object(s) and the signature. A possible syntax/semantic for a set of requirement values used to express such requirements is defined as follows: o associated; o encapsulated; o enveloped; o enveloping; o detached.	any.any.any	any.any.any	
				(c)4. MandatedSignatureFormat: This constraint indicates the required signature format. A possible syntax/semantic for a set of requirement values used to express such requirements is defined as follows: o **format**: ▪ XAdES ▪ CAdES ▪ PAdES o **level**: (note: values here below clearly distinguish between core or baseline specifications of the selected format ▪ BES; ▪ EPES;	any.any.any	any.any.any	

BSP	BSP title	Business statement summary	Technical statement counterpart	Constraint(s)	**Creation** [yes/no]. **Validation** [yes/no]. **Upgrading** [yes/no]	**SCA** [yes/no]. **SVA** [yes/no]. **DA** [yes/no]	Value
				▪ T; ▪ T-level; ▪ C; ▪ {X1,X2}; ▪ X-L; ▪ LT-level; ▪ A; ▪ LTA-level ▪ LTV.			
(d)	Targeted community			**(d)1. TargetedCommunityConstraints**	any.any.any	no.no.yes	
(e)	Allocation of responsibility for validation & upgrade			**(e)1. ValidationRequiredBeforeUpgrading**: This constraint indicates whether validation is required before upgrading a signature to a upper level. This can be expressed as a boolean (1=true; 0=false).	no.any.any	no.any.any	
				(e)2. UpgradeToLevel: This constraint indicates the level of the signature format to be reached after upgrading a (received) signature. A possible syntax/semantic for a set of requirement values used to express such requirements is defined as follows: ○ **level**: (note: values here below clearly distinguish between core or baseline specifications of the selected format ▪ BES; ▪ EPES; ▪ T; ▪ T-level; ▪ C;	no.any.any	no.any.any	

BSP	BSP title	Business statement summary	Technical statement counterpart	Constraint(s)	**Creation** [yes/no]. **Validation** [yes/no]. **Upgrading** [yes/no]	**SCA** [yes/no]. **SVA** [yes/no]. **DA** [yes/no]	Value
				▪ {X1,X2}; ▪ X-L; ▪ LT-level; ▪ A; ▪ LTA-level ▪ LTV.			
(f)	Legal level			**(f)1. ConstraintsOnCertificateMetadata**: This set of constraints indicate requirements on specific certificate metadata (see Annex B for further details on certificate metadata). A possible syntax/semantic for a set of requirement values used to express such requirements is defined as follows: **(f)1.1. QualifiedCertificateRequired**: This constraint indicates that the signer's certificate used in validating the signature is required to be a qualified certificate as defined in the applicable EU legislation. This can be expressed as a boolean (1=true; 0=false). **(f)1.2. SSCDRequired**: This constraint indicates that the private key corresponding to the public key in the signer's certificate used in validating the signature is required to reside in an SSCD as defined in the applicable EU legislation. This can be expressed as a boolean (1=true; 0=false). **(f)1.3. LegalPersonSignerRequired**: This constraint indicates that the subject entity identified in the signer's certificate used in validating the signature is required to be a legal person. This can be expressed as a boolean (1=true; 0=false). **(f)1.4. LegalPersonSignerAllowed**: This constraint indicates that the subject entity identified in the signer's certificate used in validating the signature is allowed to be	any.any.any	any.any.any	

BSP	BSP title	Business statement summary	Technical statement counterpart	Constraint(s)	**Creation** [yes/no]. **Validation** [yes/no]. **Upgrading** [yes/no]	**SCA** [yes/no]. **SVA** [yes/no]. **DA** [yes/no]	Value
				a legal person. This can be expressed as a boolean (1=true; 0=false). **(f)1.5. AdESRequired**: This constraint indicates that the signature is required to be an advanced electronic signature as defined in the applicable EU legislation. This can be expressed as a boolean (1=true; 0=false). It is possible to combine the use of the above set of constraints to require the signature to be an Advanced Electronic Signature (AdES), an Advanced Electronic Signature supported by a qualified certificate ($AdES_{QC}$), or a Qualified Electronic Signature (QES).			
(g)	Commitment type			**(g)1. CommitmentTypesRequired**: This set of constraints indicate the required (possible) values for the commitment to be expressed by the signer and whether this expression is required to be part of the signed qualifying properties. A possible syntax/semantic for a set of requirement values used to express such requirements is defined as follows: **(g)1.1. MandatedSignedQProperties-commitment-type-indication**: This constraint indicates whether the expression of the commitment by the signer is required to be part of the signed qualifying properties. This can be expressed as a boolean (1=true; 0=false). **(g)1.2. MandatedCommitmentTypeValues**: This constraint indicates the required (possible) values for the commitment type to be expressed by the signer. A possible syntax/semantic for a set of requirement values used to express such requirements is defined as follows: ▪ **MatchingValuesIndicator**: An indication on the way the commitment type value(s) in the signature must be matched against the required (possible) commitment type values. This matching values indicator that can have the following values:	any.any.no	any.any.any	

BSP	BSP title	Business statement summary	Technical statement counterpart	Constraint(s)	**Creation** [yes/no]. **Validation** [yes/no]. **Upgrading** [yes/no]	**SCA** [yes/no]. **SVA** [yes/no]. **DA** [yes/no]	Value
				○ "all" if all of the values shall be met; ○ "atLeastOne" if at least one of the values shall be met; or ○ "none" if all the values shall not be met ▪ **CommitmentTypeValues:** A non-empty sequence of commitment type values amongst the following: ○ **Proof-of-origin** indicates that the signer recognizes to have created, approved, and sent the message. ○ **Proof-of-receipt** indicates that signer recognizes to have received the content of the message. ○ **Proof-of-delivery** indicates that the TSP providing that indication has delivered a message in a local store accessible to the recipient of the message. ○ **Proof-of-sender** indicates that the entity providing that indication has sent the message (but not necessarily created it). ○ **Proof-of-approval** indicates that the signer has approved the content of the message. ○ **Proof-of-creation** indicates that the signer has created the message (but not necessarily approved, nor sent it).			
(h)	LoA on timing evidences			**(h)1. LoAOnTimingEvidences**: This set of constraints indicate the required level of assurance (LoA) on the required timing evidence(s). A possible syntax/semantic for a set of requirement values used to express such requirements is	any.any.any	any.any.no	

BSP	BSP title	Business statement summary	Technical statement counterpart	Constraint(s)	**Creation** [yes/no]. **Validation** [yes/no]. **Upgrading** [yes/no]	**SCA** [yes/no]. **SVA** [yes/no]. **DA** [yes/no]	Value
				defined as follows: **(g)1.1. LoA-on-signing-time**: This constraint indicates the required LoA on the signing time expressed in the corresponding signed qualifying property. **(g)1.2. LoA-on-content-time-stamp**: This constraint indicates the required LoA on the content time-stamp expressed in the corresponding signed qualifying property. **(g)1.3. LoA-on-signature-time-stamp**: This constraint indicates the required LoA on the signature time-stamp expressed in the corresponding un-signed qualifying property. **(g)1.4. LoA-on-archival-time-stamp**: This constraint indicates the required LoA on the archival time-stamp expressed in the corresponding un-signed qualifying property. **(g)1.5. LoA-on-time-in-OCSP-response**: This constraint indicates the required LoA on the time expressed in the OCSP response used to support validation of the signer's certificate. **(g)1.6. LoA-on-time-in-CRL**: This constraint indicates the required LoA on the time expressed in the CRL used to support validation of the signer's certificate. The possible values used to express the above requirements are {1,2,3,4,Q}. Four levels are defined as levels of assurance (i.e. 1: LoA-1, low or no assurance; 2: LoA-2, medium assurance; 3: LoA-3, high assurance; 4: LoA-4, very high level of assurance; Q: LoA-Q, qualified level of assurance}. LoA-Q is not expected to be interpreted as a 5th LoA denoting a higher level of assurance than LoA-4 but rather to be associated to one of the four other levels and bear some legal constraints as defined in the applicable EU legislation.			

BSP	BSP title	Business statement summary	Technical statement counterpart	Constraint(s)	**Creation** [yes/no]. **Validation** [yes/no]. **Upgrading** [yes/no]	**SCA** [yes/no]. **SVA** [yes/no]. **DA** [yes/no]	Value
(i)	Formalities of signing			**(i)1. WYSIWYSRequired**: This constraint indicates the requirement for having a "what you see is what you sign" environment. This can be expressed as a boolean (1=true; 0=false).	any.no.any	any.any.yes	
				(i)2. WYSIWHBSRequired: This constraint indicates the requirement for having a "what you see is what has been signed" environment. This can be expressed as a boolean (1=true; 0=false).	no.any.any	any.any.yes	
				(i)3. ProperAdviceAndInformationRequired: This constraint indicates whether it is required providing the user (signer or verifier) with proper advice and information on the application's signature process and on the legal consequences, as well as a user interface guaranteeing, to the extent possible, a valid legal signature environment. This can be expressed as a boolean (1=true; 0=false).	any.any.any	any.any.yes	
				(i)4. UserInterfaceDesignConstraints: This constraint indicates whether it is required designing the user interface to guarantee requirements expressed in section 3.2.3.(3) - BSP(i) as described in clause 5 of the present document. This can be expressed as a boolean (1=true; 0=false).	any.any.any	any.any.yes	
				(i)5. CorrectValidationAndArchivalProcedures: This constraint indicates whether it is required for providing the relying party (including the signatory) with correct procedures for the validation and the archival of the electronic signature and the associated validation data. This can be expressed as a boolean (1=true; 0=false).	no.any.no	any.any.yes	
(j)	Longevity & resilience			**(j)1. LoAOnLongevityAndResilience**: This constraint indicates the required LoA on the longevity and resilience to change expected to apply to the evidence provided by the signature. The possible values used to express such a requirement are {1,2,3,4,Q}. Four levels are defined as levels of assurance (i.e. 1: LoA-1, low or no assurance; 2: LoA-2, medium assurance; 3: LoA-3, high assurance; 4: LoA-4, very	any.any.any	any.any.any	

BSP	BSP title	Business statement summary	Technical statement counterpart	Constraint(s)	**Creation** [yes/no]. **Validation** [yes/no]. **Upgrading** [yes/no]	**SCA** [yes/no]. **SVA** [yes/no]. **DA** [yes/no]	Value
				high level of assurance; Q: LoA-Q, qualified level of assurance}. LoA-Q is not expected to be interpreted as a 5th LoA denoting a higher level of assurance than LoA-4 but rather to be associated to one of the four other levels and bear some legal constraints as defined in the applicable EU legislation.			
(k)	Archival			**(k)1. ArchivalConstraints**: This constraint indicates the requirements with regards to the archival of the signature and the associated validation data.	any.any.any	any.any.yes	
(l)	Identity and role attributes of the signer			**(l)1. ConstraintsOnCertificateMetadata-LegalPersonSignerRequired**: see (f)1.3			
				(l)2. ConstraintsOnCertificateMetadata-LegalPersonSignerAllowed: see (f)1.4			
				(l)3. MandatedSignedQProperties-signer-attributes: This constraint indicates whether the signed qualifying property signer-attribute is required and the associated constraints on the required attributes. This can be expressed as a tuple made of a boolean (1=true;0=false) associated with a sequence of identifiers expressing constraints on the required attributes of the signer. Such constraints on signer's attributes or roles can cover: ▪ which roles/attributes are mandated ▪ how such roles/attributes are certified ▪ constraints on the type of roles/attributes ▪ constraints on the values of roles/attributes			
				(l)4. NameConstraints: These constraints indicate requirements on the distinguished names (DN) for issued certificates (e.g. to signer, CAs, OCSP responders, CRL Issuers, Time-Stamping Units) as defined in RFC 5280 [i.24].			
				(l)5. ProofOfAuthorityConstraints: This constraint indicates whether a proof of authority is required and what are the			

BSP	BSP title	Business statement summary	Technical statement counterpart	Constraint(s)	**Creation** [yes/no]. **Validation** [yes/no]. **Upgrading** [yes/no]	**SCA** [yes/no]. **SVA** [yes/no]. **DA** [yes/no]	Value
				associated requirements when required. This can be expressed as a boolean together with a list of qualifiers when boolean is set.			
(m)	LoA on signer authentication			**(m)1. X509CertificateValidationConstraints**: This set of constraints indicate requirements for use in the certificate path validation process as defined in RFC 5280 [i.24]. These constraints may be different for different certificate types (e.g. certificates issued to signer, to CAs, to OCSP responders, to CRL Issuers, to Time-Stamping Units). A possible syntax/semantic for a set of requirement values used to express such requirements is defined as follows: • **(m)1.1. SetOfTrustAnchors**: This constraint indicates a set of acceptable trust anchors (TAs) as a constraint for the validation process. Such TAs are recommended to be provided in the form of (self-signed) certificates and a time until when these trust anchors were considered reliable. The set of TAs may be provided under the form of : – Trust points specified in signature validation policies; – Sets of trusted CAs, e.g. represented by their root certificates stored in the environment (like certificate trust store or list); – Trust Service Status Lists as defined in [i.9] – LOTL and/or Trusted Lists as defined in [i.10], such as EC LOTL and EU MS Trusted Lists as defined in [i.19]; • **(m)1.2. CertificationPath**: This constraint indicates a certification path of length 'n' from the trust anchor (TA) down to the certificate used in validating a signed object (e.g. the signer's certificate or a time stamping certificate). The given certification path has to be used by the SVA for validation of the signature. This can be provided directly or by considering the path provided in	no.yes.any	no.yes.no	

BSP	BSP title	Business statement summary	Technical statement counterpart	Constraint(s)	**Creation** [yes/no]. **Validation** [yes/no]. **Upgrading** [yes/no]	**SCA** [yes/no]. **SVA** [yes/no]. **DA** [yes/no]	Value
				the signature if any. • **(m)1.3. user-initial-policy-set**: This constraint indicates *"a set of certificate policy identifiers naming the policies that are acceptable to the DA. The user-initial-policy-set contains the special value any-policy when not concerned about certificate policy"* [i.24]. • **(m)1.4. initial-policy-mapping-inhibit**: This constraint indicates *"if policy mapping is allowed in the certification path"* [i.24]. • **(m)1.5. initial-explicit-policy**: This constraint indicates *"if the path must be valid for at least one of the certificate policies in the user-initial-policy-set"* [i.24]. • **(m)1.6. initial-any-policy-inhibit**: This constraint indicates *"whether the anyPolicy OID should be processed if it is included in a certificate"* [i.24]. • **(m)1.7. initial-permitted-subtrees**: This constraint indicates *"for each name type (e.g. X.500 distinguished names, email addresses, or IP addresses) a set of subtrees within which all subject names in every certificate in the certification path MUST fall"* [i.24]. • **(m)1.8. initial-excluded-subtrees**: This constraint indicates *"for each name type (e.g. X.500 distinguished names, email addresses, or IP addresses) a set of subtrees within which no subject name in any certificate in the certification path may fall"* [i.24]. • **(m)1.9. path-length-constraints**: This constraint indicates restrictions on the number of CA certificates in a certification path [i.24]. This may need to define initial values for this or to handle such constraint differently (e.g. ignore it). • **(m)1.10. policy-constraints**: This constraint indicates requirements for certificate policies referenced in the certificates [i.24]. This may need to define initial values for this or to handle such constraint differently (e.g. ignore it). This should also allows the ability to require a			

BSP	BSP title	Business statement summary	Technical statement counterpart	Constraint(s)	**Creation** [yes/no]. **Validation** [yes/no]. **Upgrading** [yes/no]	**SCA** [yes/no]. **SVA** [yes/no]. **DA** [yes/no]	Value
				(possible set of) specific certificate policy extension value(s) in end-entity certificates (without requiring such values appearing in certificate of authorities in the certification path). The values to be considered in a all/atLeastOne/none mode are the QCP, QCP+, NCP, NCP+, LCP policies as defined in [i.27] and [i.28], other policies identified by an OID.			
				(m)2. RevocationConstraints: This set of constraints indicate requirements for use when verifying the certificate validity status of the certificates during the certificate path validation process [i.24]. These constraints may be different for different certificate types (e.g. certificates issued to signer, to CAs, to OCSP responders, to CRL Issuers, to Time-Stamping Units). A possible syntax/semantic for a set of requirement values used to express such requirements is defined as follows: • **(m)2.1. RevocationCheckingConstraints**: This constraint indicates requirements for checking certificate revocation. Such constraints may specify if revocation checking is required or not and if OCSP responses or CRLs have to be used. A possible syntax/semantic for a set of requirement values used to express such requirements is defined as follows: – "**clrCheck:** Checks shall be made against current CRLs (or ARLs); – **ocspCheck:** The revocation status shall be checked using OCSP RFC 6960 [i.25]; – **bothCheck:** Both OCSP and CRL checks shall be carried out; – **eitherCheck:** Either OCSP or CRL checks shall be carried out; – **noCheck:** No check is mandated. • **(m)2.2. RevocationFreshnessConstraints**: This constraint indicates time requirements on revocation	no.yes.any	no.yes.no	

BSP	BSP title	Business statement summary	Technical statement counterpart	Constraint(s)	**Creation** [yes/no]. **Validation** [yes/no]. **Upgrading** [yes/no]	**SCA** [yes/no]. **SVA** [yes/no]. **DA** [yes/no]	Value
				information. The constraints may indicate the maximum accepted difference between the issuance date of the revocation status information of a certificate and the time of validation (see clause 4.5 of [i.7]) or require the SVA to only accept revocation information issued a certain time after the signature has been created. • **(m)2.3. RevocationInfoOnExpiredCerts**: This constraint mandates the signer's certificate used in validating the signature to be issued by a certification authority that keeps revocation notices for revoked certificates even after they have expired for a period exceeding a given lower bound.			
				(m)3. LoAOnTSPPractices: This constraint indicates the required LoA on the practices implemented by the TSP having issued the certificates validated during the certificate path validation process [i.24]. The possible values used to express such a requirement are {1,2,3,4,Q}. Four levels are defined as levels of assurance (i.e. 1: LoA-1, low or no assurance; 2: LoA-2, medium assurance; 3: LoA-3, high assurance; 4: LoA-4, very high level of assurance; Q: LoA-Q, qualified level of assurance}. LoA-Q is not expected to be interpreted as a 5th LoA denoting a higher level of assurance than LoA-4 but rather to be associated to one of the four other levels and bear some legal constraints as defined in the applicable EU legislation.	any.yes.any	any.yes.no	
(n)	Signature Creation Devices			**(n)1. LoAOnSCD**: This constraint indicates the required LoA on the Signature Creation Device in which resides the private key corresponding to the certificates validated during the certificate path validation process [i.24]. The possible values used to express such a requirement are {1,2,3,4,Q/SSCD}. Four levels are defined as levels of assurance (i.e. 1: LoA-1, low or no assurance; 2: LoA-2, medium assurance; 3: LoA-3, high assurance; 4: LoA-4, very high level of assurance; Q/SSCD: LoA-Q/SSCD, qualified level of assurance}. LoA-	any.any.any	any.any.any	

BSP	BSP title	Business statement summary	Technical statement counterpart	Constraint(s)	**Creation** [yes/no]. **Validation** [yes/no]. **Upgrading** [yes/no]	**SCA** [yes/no]. **SVA** [yes/no]. **DA** [yes/no]	Value
				Q/SSCD is not expected to be interpreted as a 5th LoA denoting a higher level of assurance than LoA-4 but rather to be associated to one of the four other levels and bear some legal constraints as defined in the applicable EU legislation.			
(o)	Other information to be associated with signatures			**(o)1. MandatedSignedQProperties-signer-location**: This constraint indicate that the signer location is required to be expressed as a signed qualifying property and may additionally expressed constraints on the value.	any.any.any	any.any.any	
				(o)2. MandatedUnsignedQProperties-signature-policy-extension: This constraint indicate that the signature policy extension is required as an unsigned qualifying property and may additionally expressed constraints on the values.	any.any.any	any.any.any	
				(o)3. MandatedUnsignedQProperties-signature-policy-inclusion-in-archival-form: This constraint indicate that the requirement to include the signature policy as part of the corresponding unsigned qualifying property.	any.any.any	any.any.any	
(p)	Cryptographic suites			**(p)1. CryptographicSuitesConstraints**: This constraint indicates requirements on algorithms and parameters used when creating signatures or used when validating signed objects included in the validation or upgrading process (e.g. signature, certificates, CRLs, OCSP responses, time-stamps). They will be typically be represented by a list of entries as in the table below	any.any.any	any.any.any	

(p)1. Cryptographic-constraints				
Type of signature	**Algorithm identifiers**	**Minimum signature key size**	**Minimum length of hash value**	**Expiration date**

Signature to be validated				
Signer's certificate				
CA certificate in a valid chain				
Time-Stamp Token				
OCSP response				
CRLs				

(q)	Technological environment			**(q)1. TechnologicalEnvironmentConstraints**: This contraint indicates the requirements on the technological environment in which signatures are processed.	any.any.any	any.any.any	
Summary of the selected signature format(s) (e.g. XAdES, CAdES, PAdES and/or their baseline profile) including details on the format of the signed data object(s), the relative placement of the signature and the signed data object(s) (e.g. enveloped, enveloping, detached), the relevance of use of a container to package the signature(s) together with signed data object(s) (e.g. ASiC and or its baseline profile), the specific attributes (signed or unsigned) of the signature, and the form level of selected signature format:							

4.2.2 Output constraints to be used when validating electronic signatures in the context of the identified signature policy

Constraints to be used as output for validating electronic signatures in the context of the identified signature policy	
Identifier of the concerned signature policy : ..... **Identifier of the concerned signature(s) in the concerned signature workflow: .....**	
A. ... title ...	
General constraints	**Signature policy values**
...	

Editorial note: Specifications work is to be continued once concepts provided in TR 119 100, TS 119 101, EN 319 102 and in the present document are validated.

4.2.4 Output constraints to be used for generating/upgrading electronic signatures in the context of the identified signature policy

Constraints to be used as input for generating/upgrading electronic signatures in the context of the identified signature policy	
Identifier of the concerned signature policy : ..... **Identifier of the concerned signature(s) in the concerned signature workflow: .....**	
A. ... title ...	
General constraints	**Signature policy values**
...	

Editorial note: Specifications work is to be continued. It should be linked to the specification work to be done in EN 319 102.

5. Other business and legal matters

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.

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

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. 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.
c. Applicable fees
d. Financial Responsibility
e. Confidentiality of Business Information
f. Privacy of Personal Information
g. Intellectual Property Rights
h. Representations and Warranties
i. Disclaimers of Warranties
j. Limitations of Liability
k. Indemnities
l. Term and Termination
m. Individual notices and communications with participants
n. Amendments
o. Dispute Resolution Procedures
p. Governing Law
q. Compliance with Applicable Law
r. Miscellaneous Provisions (e.g. entire agreement, assignment, severability, enforcement, force majeure)
s. Other Provisions

6. 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.

6 European Signature Validation Policy for $AdES_{QC}$ and QES against EU MS Trusted Lists

This section provides a standardised signature validation policy, the so-called "European Signature Validation Policy for AdESQC and QES against EU Member States Trusted Lists", aiming to describe the requirements imposed on the actors with respect to the application of electronic signatures to documents and data in order for these signatures to be considered as valid (technical) AdES, AdES supported by a Qualified Certificate (AdESQC) or Qualified electronic Signature (QES), with all certificates and their related chains supporting the signatures are validated against the EU Member State Trusted Lists (this includes signer's certificate and certificates used to validate certificate validity status services - CRLs, OCSP).

As per CD 2009/767/EC [i.19], a certificate claimed to be a qualified certificate (QC) by including either a QcCompliance statement [i.29] or a QCP or QCP+ certificate policy OID [i.27] is confirmed to be a qualified certificate by a Trusted List of the Member State in which the issuer of the certificate is established, if a certificate path can be found from this certificate to the public key of a listed CA/QC service (i.e. being considered as TA in this context) and when no Qualifications Service information (Sie:Q) extension [i.10]] of such a listed service does contradict such a claim. This of course subject to the status of the CA/QC matching listed service with regards to the reference in time when the certificate is assessed to be qualified.

As per CD 2009/767/EC [i.19], a certificate which is not claimed to be a qualified certificate (QC)through the inclusion of either a QcCompliance statement [i.29] or a QCP or QCP+ certificate policy OID [i.27], is to be considered as a QC when a certificate path can be found from this certificate to the public key of a listed CA/QC service (i.e. being considered as TA in this context) in the Trusted List of the Member State in which the issuer of the certificate is established and when an ad hoc Sie:Q extension of such a listed service explicitly indicates this certificate to be considered as qualified. This of course subject to the status of the CA/QC matching listed service with regards to the reference in time when the certificate is assessed to be qualified.

As per CD 2009/767/EC [i.19], a certificate for which it is claimed that the corresponding private key resides in an SSCD by inclusion in the certificate of a QcSSCD statement [i.29] or QCP+ certificate policy OID [i.27], is confirmed to be supported by an SSCD by the Trusted List of the Member State in which the issuer of the certificate is established, if a certificate path can be found from this certificate to the public key of a listed CA/QC service (i.e. being considered as TA in this context) and when no Sie:Q extension of such a listed service does contradict such a claim. This of course subject to the status of the CA/QC matching listed service with regards to the reference in time when the certificate is assessed to be supported by an SSCD.

As per CD 2009/767/EC [i.19], a certificate which is not claimed to be supported by an SSCD through the inclusion of either a QcSSCD statement [i.29] or a QCP+ certificate policy OID [i.27], is to be considered as a supported by an SSCD when a certificate path can be found from this certificate to the public key of a listed CA/QC service (i.e. being considered as TA in this context) in the Trusted List of the Member State in which the issuer of the certificate is established and when an ad hoc Sie:Q extension of such a listed service explicitly indicates this certificate to be supported by an SSCD. This of course subject to the status of the CA/QC matching listed service with regards to the reference in time when the certificate is assessed to be supported by an SSCD.

The following table describes the expected conclusions of the validation algorithm with regards to the indication of the QES and $AdES_{QC}$ status of the validated signature:

Certificate content / Trusted List content	QCP only	QCP + QcC	QCP + QcC +QcSSCD	QCP+ only	QCP+ + QcC	QCP+ + QcC +QcSSCD	QcC only	QcSSCD only	QcC + QcSSCD	No machine processable info (+)
Cert covered by CA/QC (no Sie:Q extension)	2	2	1	1	1	1	2	3	1	3
Cert covered by CA/QC + Sie:Q:QCWithSSCD	1	1	1	1	1	1	1	3	1	3
Cert covered by CA/QC + Sie:Q:QCNoSSCD	2	2	2	2	2	2	2	3	2	3
Cert covered by CA/QC + Sie:Q:QCSSCDAsInCert	2	2	1	1	1	1	2	3	1	3
Cert covered by CA/QC + Sie:Q:QCForLegalPerson	2	2	1	1	1	1	2	3	1	3
Cert covered by CA/QC + Sie:Q:QCWithSSCD + Sie:Q:QCStatement	1	1	1	1	1	1	1	1	1	1
Cert covered by CA/QC + Sie:Q:QCNoSSCD + Sie:Q:QCStatement	2	2	2	2	2	2	2	2	2	2
Cert covered by CA/QC + Sie:Q:QCSSCDAsInCert + Sie:Q:QCStatement	2	2	1	1	1	1	2	1	1	2
Cert covered by CA/QC + Sie:Q:QCForLegalPerson + Sie:Q:QCStatement	2	2	1	1	1	1	2	1	1	2
Cert not covered by CA/QC	2*	2*	1*	1*	1*	1*	2*	3*	1*	3
Trusted List not available	2**	2**	1**	1**	1**	1**	2**	3**	1**	3**
TL available but not signed or TL validation certificate not in LOTL	2***	2***	1***	1***	1***	1***	2***	3***	1***	3***

indicates a conflict between certificate content and Trusted List content and overruling by TL

Strictly speaking a cert with QcSSCD only (no QcC statement set) should not be considered as a QC

(+) None of the QCP, QCP+, QcC or QcSSCD machine processable statement is present in the certificate.

Legend (*/**/*** indicate a warning message):
1 = QES ; 2 = $AdES_{QC}$; 3 = AdES
* = no TL confirmation from MS where TSP is established
** = no TL confirmation as MS TL where TSP is established is not available
*** = TL confirmation but TL not signed or TL verification cert not in LOTL

In the above Table, the meaning of the cell values and special cases mentioned by a number or a number and one or several asterisks make reference to the legend whose references must be combined (e.g. "2**" means that the signature should be considered as an "$AdES_{QC}$ but for which the warning that no TL confirmation could be obtained as the TL of the MS where the TSP is established is not available").

The following tables describes the applicable requirements expressed using the tables specified in clause 4 of the present document:

Identifier of the concerned signature policy : *< an OID could be given to such a policy >*			
BSP	**BSP title**	**Business statement summary**	**Technical statement counterpart**
(a)	Workflow (sequencing & timing)	No specific requirement	
(b)	DOTBS (& technology)	No specific requirement	
(c)	DOTBS vs Signature	ETSI standards on X/C/PAdES, ASiC, in particular their Baseline Profiles, are recommended to be used for signature generation formats. No specific requirement on relationship between the signed data and the signature (e.g. enveloping, enveloped, detached)..	
(d)	Targeted community	No specific requirement	
(e)	Validation & upgrade responsibility	Validation of electronic signatures: validation of electronic signatures should be performed according to the "Signature Validation Procedures" ETSI EN 319102. The final conclusion of the validation report of the signature validation must determine whether or not the end-entity certificate is a QC, supported or not by an SSCD and hence whether the signature is an AdES, an $AdES_{QC}$ or a QES. Extension of electronic signatures: When preservation of received signatures is an issue, received signatures may be extended to X/C/PAdES -X-L/LTV level or to X/C/PAdES Baseline Profile LT level at a minimum, when they do not reach this level.	
(f)	Legal level	The signature shall be either AdES, AdESQC or QES	

(g)	Commitment type	REG: The intention to sign and the potential expression of the commitment shall be expressed alongside the signature, either implicitly or explicitly.	REG: No specific technical requirement. ETSI: Explicit use of commitment type to be used as foreseen in AdES formats..
(h)	LoA on timing	Signature time-stamp is recommended. Time Stamping Authority services issuing time-stamps used in this context should be either [qualified trust service providers providing time-stamping services] included in a Trusted List or known and trusted by the relying party.	
(i)	Formalities of signing	The signature environment either selected and used by the signer or provided to the signer must provide a valid legal signature environment, with WYSIWYS features to the greatest extent possible, and providing appropriate advice and information on the application's signature generation and validation processes and their legal consequences. Signers and relying parties should be provided with correct procedures and facilities: • to validate the signatures and obtain validation results data, • to allow archival of signed documents/data and associated signatures.	
(j)	Longevity & resilience	Electronic signatures must be verifiable up to a date which is relevant to the application domain being concerned.	ETSI : In line with Figure 3of the present document (or Table 14 of ETSI TS 119 132 when this one will be available and maintained there).
(k)	Archival	No specific requirement	
(l)	Identity of signers	A set of data unambiguously representing the signatory to whom the certificate is issued including at least the name of the signatory (natural person) or a pseudonym, which shall be identified as such	ETSI: As per ETSI EN 319 412.
(m)	LoA on signers authentication	Signer's certificate, and all other certificates supporting the validation of the signature being validated, shall be validated against the MS Trusted Lists accessed through the EC List Of The Lists (LOTL).	Validation against TL. ETSI: Certificates as per ETSI 319 412.
(n)	Signature Creation Devices	For QES, the private key of the signer must reside in an SSCD. This must be confirmed by the applicable MS Trusted List when this is not stated in the signer's certificate. No specifications on SCD for other types of electronic signatures.	Validation against TL. ETSI: Certificates as per ETSI 319 412 with regards to the claimed support by an SSCD.
(o)	Signature attributes	Time of signing is required by CD 2011/130/EU and by ETSI Baseline Profiles for X/C/PAdES. Signer's certificate is required as part of the signed properties by ETSI Baseline profiles.	
(p)	Cryptographic suites	Refer to national rules or to Figure 3of the present document (or Table 14 of ETSI TS 119 132 when this one will be available and maintained there).	
(q)	Technological environment	No specific requirement	
Summary of the selected signature format(s) (e.g. XAdES, CAdES, PAdES and/or their baseline profile) including details on the format of the signed data object(s), the relative placement of the signature and the signed data object(s) (e.g. enveloped, enveloping, detached), the relevance of use of a container to package the signature(s) together with signed data object(s) (e.g. ASiC and or its baseline profile), the specific attributes (signed or unsigned) of the signature,			

and the form level of selected signature format:

CD 2011/130/EU refers to XAdES, CAdES, PAdES and/or their baseline profiles.

Identifier of the concerned signature policy : .....
Identifier of the concerned signature(s) in the concerned signature workflow: .....

BSP	BSP title	Constraint(s)	Value
(a)	Workflow (sequencing & timing)	**(a)1. OrderInSequence**:	(a)1. Not specified (any).
		(a)2. SequencingNature: **(a)2.1 Mandated-independent** **(a)2.2 Mandated-serial** **(a)2.3 MandatedUnsignedQProperties-counter-signature**	(a)2.x Not specified (any).
		(a)3. TimingRelevance: **(a)3.1 TimingRelevanceOnSequencing**: **(a)3.2 TimingRelevanceOnEvidence**: o **(a)3.2.1 MandatedSignedQProperties-signing-time** o **(a)3.2.2 MandatedSignedQProperties-content-time-stamp** o **(a)3.2.3 MandatedUnsignedQProperties-signature-time-stamp** o **(a)3.2.4 MandatedUnsignedQProperties-archival-form**	(a)3.1 Not specified (any). (a)3.2.x Not specified (any). except **(a)3.2.1 set.**
		(a)4. MassSigningAcceptable	Not specified (any).
(b)	DOTBS	**(b)1. ConstraintOnNatureAndFormatOfTheContent**	Not specified (any).
		(b)2.ContentRelatedConstraintsAsPartOfSignatureElements: **(b)2.1 MandatedSignedQProperties-DataObjetFormat** **(b)2.2MandatedSignedQProperties-content-hints** **(b)2.3 MandatedSignedQProperties-content-reference** **(b)2.4 MandatedSignedQProperties-content-identifier**	Not specified (any).
		(b)3. DOTBSAsAWholeOrInParts:	Not specified (any).
(c)	Relationship between DOTBS and Signature	**(c)1. BulkSigningRelevance**: **(c)1.1 BulkSigningRelevance-mandatedBulkSigning** **(c)1.2 prohibitedBulkSigning**.	Not specified (any).
		(c)2. ConstraintsOnTheNumberOfDOTBS: minValue {<, ≤, =} x {=, ≥, >} maxValue	Not specified (any).
		(c)3. SignatureRelativePosition	Not specified (any).
		(c)4. MandatedSignatureFormat	Not specified (any).
(d)	Targeted community	**(d)1. TargetedCommunityConstraints**	Not specified (any).
(e)	Allocation of responsibility for validation & upgrade	**(e)1. ValidationRequiredBeforeUpgrading**	Not specified (any).
		(e)2. UpgradeToLevel	Not specified (any).
(f)	Legal level	**(f)1. ConstraintsOnCertificateMetadata**: **(f)1.1. QualifiedCertificateRequired**	(f)1.1 and (f)1.5 required for QES and $AdES_{QC}$.

BSP	BSP title	Constraint(s)	Value
		(f)1.2. SSCDRequired **(f)1.3. LegalPersonSignerRequired** **(f)1.4. LegalPersonSignerAllowed** **(f)1.5. AdESRequired**	(f)1.2 Required for QES not for $AdES_{QC}$. Both must be confirmed by Trusted List when not stated in certificate. (f)1.3 & (f)1.4 not specified.
(g)	Commitment type	**(g)1. CommitmentTypesRequired** **(g)1.1. MandatedSignedQProperties-commitment-type-indication** **(g)1.2. MandatedCommitmentTypeValues** ▪ **MatchingValuesIndicator** ▪ **CommitmentTypeValues**	Not specified (any).
(h)	LoA on timing evidences	**(h)1. LoAOnTimingEvidences**: **(g)1.1. LoA-on-signing-time** **(g)1.2. LoA-on-content-time-stamp** **(g)1.3. LoA-on-signature-time-stamp** **(g)1.4. LoA-on-archival-time-stamp** **(g)1.5. LoA-on-time-in-OCSP-response** **(g)1.6. LoA-on-time-in-CRL**	Not specified (any).
(i)	Formalities of signing	**(i)1. WYSIWYSRequired**	Not specified (any).
		(i)2. WYSIWHBSRequired	Not specified (any).
		(i)3. ProperAdviceAndInformationRequired	Not specified (any).
		(i)4. UserInterfaceDesignConstraints	Not specified (any).
		(i)5. CorrectValidationAndArchivalProcedures	Not specified (any).
(j)	Longevity & resilience	**(j)1. LoAOnLongevityAndResilience**	Not specified (any).
(k)	Archival	**(k)1. ArchivalConstraints**	Not specified (any).
(l)	Identity and role attributes of the signer	**(l)1. ConstraintsOnCertificateMetadata-LegalPersonSignerRequired**: see (f)1.3	Not specified (any).
		(l)2. ConstraintsOnCertificateMetadata-LegalPersonSignerAllowed: see (f)1.4	Not specified (any).
		(l)3. MandatedSignedQProperties-signer-attributes	Not specified (any).
		(l)4. NameConstraints	Not specified (any).
		(l)5. ProofOfAuthorityConstraints	Not specified (any).
(m)	LoA on signer authentication	**(m)1. X509CertificateValidationConstraints** • **(m)1.1. SetOfTrustAnchors** • **(m)1.2. CertificationPath** • **(m)1.3. user-initial-policy-set** • **(m)1.4. initial-policy-mapping-inhibit** • **(m)1.5. initial-explicit-policy** • **(m)1.6. initial-any-policy-inhibit** • **(m)1.7. initial-permitted-subtrees** • **(m)1.8. initial-excluded-subtrees** • **(m)1.9. path-length-constraints** • **(m)1.10. policy-constraints**	(m)1.1 EC LOTL (m)1.2 Not applied (m)1.3 Any policy (m)1.4 Not allowed (m)1.5 No (m)1.6 Not applied (m)1.7 Not applied (m)1.8 Not applied (m)1.9 Not applied (m)1.10 Not applied
		(m)2. RevocationConstraints: • **(m)2.1. RevocationCheckingConstraints** • **(m)2.2. RevocationFreshnessConstraints** • **(m)2.3. RevocationInfoOnExpiredCerts**	(m)2.1 eitherCheck (OSCP responses and CRLs to be signed and their

BSP	BSP title	Constraint(s)	Value
			signature certificates to be validated with a valid chain up to Trust Anchors in Trusted Lists) (m)2.2 Not applied (m)2.3 Not applied
		(m)3. LoAOnTSPPractices	LoA-Q (Qualified) - Supervised for issuance of QC (CA/QC)
(n)	Signature Creation Devices	**(n)1. LoAOnSCD**	LoA-Q/SSCD for QES
(o)	Other information to be associated with signatures	**(o)1. MandatedSignedQProperties-signer-location**	Not specified(any)
		(o)2. MandatedUnsignedQProperties-signature-policy-extension	Not specified(any)
		(o)3. MandatedUnsignedQProperties-signature-policy-inclusion-in-archival-form	Not specified(any)
(p)	Cryptographic suites	**(p)1. CryptographicSuitesConstraints**	Not specified(any) Compliance with TS 119 312 [i.23] recommended.

(p)1. Cryptographic-constraints				
Type of signature	**Algorithm identifiers**	**Minimum signature key size**	**Minimum length of hash value**	**Expiration date**
Signature to be validated				
Signer's certificate				
CA certificate in a valid chain				
Time-Stamp Token				
OCSP response				
CRLs				

(q)	Technological environment	**(q)1. TechnologicalEnvironmentConstraints**:	Not specified(any)

Constraints on validation report:

Editorial note: Specifications work is to be continued once concepts provided in TR 119 100, TS 119 101, EN 319 102 and in the present document are validated.

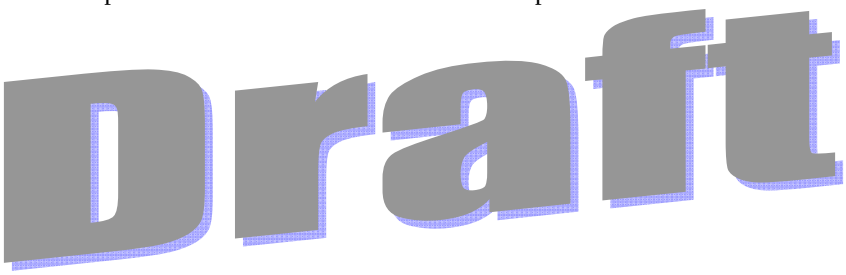
The signature validation report in the context of the "European Signature Validation Policy for AdESQC and QES against EU Member States Trusted Lists" shall include the following elements that shall be presented in a legible way to the verifier when this verifier is a natural person:

- Making clear that the Signature Validation Policy that has been used for validation of the signature is the "European Signature Validation Policy for AdESQC and QES against EU Member States Trusted Lists" by using the following text:

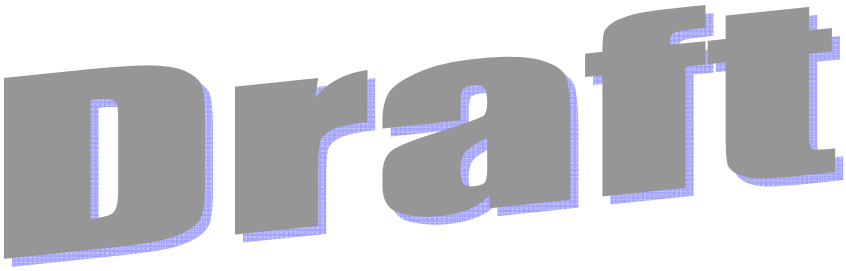
European Signature Validation Policy for $AdES_{QC}$ and QES against EU Member States Trusted Lists

*Validates electronic signatures and indicates whether they are Advanced electronic Signatures (AdES), AdES supported by a Qualified Certificate (AdES$_{QC}$) or a Qualified electronic Signature (QES). All certificates and their related chains supporting the signatures are validated against the **EU Member State Trusted Lists** (this includes signer's certificate and certificates used to validate certificate validity status services - CRLs, OCSP, and time-stamps)*

- Presenting the identification information about the signer (based on the signer's certificate Subject Distinguished Name).
- Presenting the time reference against the signature validation results are provided.
- Making available the presentation of the data that has been covered by the signature (signed data). This can be done by using a SD Presentation Components (see clause 4.3.2 of ETSI EN 319 102 [i.7]).
- Presenting any signature attributes that have been included in the signature and make clear which attributes were signed and which were unsigned.
- Presenting the overall status of the signature validation (VALID, INVALID, INDETERMINATE)
- In case of INVALID: Highlight the reasons having led to such a result.
- In case of INDETERMINATE: Highlight the parts of the validation report that indicates steps to be taken to potentially get to a determinate result.
- Making available the presentation of the detailed validation report.



Annex <A>:
Void



Annex <B>:
Bibliography

- CROBIES WP 5-1: "Guidelines and guidance for cross-border and interoperable implementation of electronic signatures. WP 5-1".

  Editorial note: It is not expected that this document should be referenced in the present document. However the present document is largely inspired and derived from this report of the CROBIES study. This fact should be mentioned in the IPR section or foreword section.

- ETSI TR 102 045: “Signature Policy for extended business model”.

  Editorial note: This document should be deprecated and hence not be referenced in the present document. Any interesting part should be updated and integrated in the appropriate document(s) of the rationalised framework.

History

Document history		
<Version>	<Date>	<Milestone>
0.0.1	09/09/2013	Early draft for public review" submitted to ESI#40 for comments.
0.0.2	30/09/2013	Updated early draft to align with changes made in TR 119 100.
0.0.3	11/11/2013	Draft of the "stable draft" version of the document as submitted to ESI#41.
0.0.4	30/11/2013	Stable draft submitted for public review.