ETSI TS 119 172-1 V1.1.1 (2015-07)

Electronic Signatures and Infrastructures (ESI);
Signature Policies;
Part 1: Building blocks and table of contents for human readable signature policy documents

Reference
DTS/ESI-0019172-1

Keywords
electronic signature, e-commerce,
trust services

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 5
Foreword 5
Modal verbs terminology 5
Introduction 5
1 Scope 7
2 References 7
2.1 Normative references 7
2.2 Informative references 7
3 Definitions and abbreviations 9
3.1 Definitions 9
3.2 Abbreviations 11
4 Signature policies and signature policy document 12
Annex A (normative): Table of contents for signature policies expressed as human readable documents 14
A.1 Introduction 14
A.1.1 Overview 14
A.1.2 Business or Application Domain 14
A.1.2.1 Scope and boundaries of signature policy 14
A.1.2.2 Domain of applications 14
A.1.2.3 Transactional context 14
A.1.3 Document and policy(ies) names, identification and conformance rules 15
A.1.3.1 Signature policy document and signature policy(ies) names 15
A.1.3.2 Signature policy document and signature policy(ies) identifier(s) 15
A.1.3.3 Conformance rules 15
A.1.3.4 Distribution points 15
A.1.4 Signature policy document administration 15
A.1.4.1 Signature policy authority 15
A.1.4.2 Contact person 16
A.1.4.3 Approval procedures 16
A.1.5 Definitions and Acronyms 16
A.2. Signature application practices statements 16
A.3 Business scoping parameters 16
A.3.1 BSPs mainly related to the concerned application/business process 16
A.3.1.1 BSP (a): Workflow (sequencing and timing) of signatures 16
A.3.1.2 BSP (b): Data to be signed 17
A.3.1.3 BSP (c): The relationship between signed data and signature(s) 18
A.3.1.4 BSP (d): Targeted community 18
A.3.1.5 BSP (e): Allocation of responsibility for signature validation and augmentation 18
A.3.2 BSPs mainly influenced by the legal/regulatory provisions associated to the concerned application/business process 19
A.3.2.1 BSP (f): Legal type of the signatures 19
A.3.2.2 BSP (g): Commitment assumed by the signer 19
A.3.2.3 BSP (h): Level of assurance on timing evidences 20
A.3.2.4 BSP (i): Formalities of signing 20
A.3.2.5 BSP (j): Longevity and resilience to change 21
A.3.2.6 BSP (k): Archival 21
A.3.3 BSPs mainly related to the actors involved in creating/augmenting/validating signatures 21
A.3.3.1 BSP (l): Identity (and roles/attributes) of the signers 21
A.3.3.2 BSP (m): Level of assurance required for the authentication of the signer 22
A.3.3.3 BSP (n): Signature creation devices 22
A.3.4 Other BSPs 22

A.3.4.1 BSP (o): Other information to be associated with the signature 22
A.3.4.2 BSP (p): Cryptographic suites 22
A.3.4.3 BSP (q): Technological environment 23

A.4 Requirements / statements on technical mechanisms and standards implementation 23
A.4.1 Technical counterparts of BSPs - Statement summary 23
A.4.2 Input and output constraints for signature creation, augmentation and validation procedures 25
A.4.2.1 Input constraints to be used when generating, augmenting and/or validating signatures in the context of the identified signature policy 25
A.4.2.2 Output constraints to be used when validating signatures in the context of the identified signature policy 36
A.4.2.3 Output constraints to be used for generating/augmenting signatures in the context of the identified signature policy 36

A.5 Other business and legal matters 38

A.6 Compliance audit and other assessments 39

Annex B (normative): Commitment types 40

Annex C (normative): Constraints in the context of EU legislation 41

Annex D (normative): Signature application practices statements 42

D.1 General requirements 42

D.2 Signature application practices statements 42
D.2.1 Legal driven policy requirements 42
D.2.2 Information security (management system) requirements 42
D.2.3 Signature Creation and Signature Validation processes requirements 43
D.2.4 Development & coding policy requirements 43
D.2.5 General requirements 44

History 45

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 Technical Specification (TS) has been produced by ETSI Technical Committee Electronic Signatures and Infrastructures (ESI).

The present document is part 1 of a multi-part deliverable specifying Signature Policies as identified below:

Part 1: "Building blocks and table of contents for human readable signature policy documents";

Part 2: "XML Format for signature policies";

Part 3: "ASN.1 Format for signature policies";

Part 4: "Signature validation policy for European qualified electronic signatures/seals using trusted lists".

Modal verbs terminology

In the present document "**shall**", "**shall not**", "**should**", "**should not**", "**may**", "**need not**", "**will**", "**will not**", "**can**" and "**cannot**" are to be interpreted as described in clause 3.2 of the ETSI Drafting Rules (Verbal forms for the expression of provisions).

"**must**" and "**must not**" are **NOT** allowed in ETSI deliverables except when used in direct citation.

Introduction

A digital signature is always used in a context, either implicit or explicit, e.g. as part of a business process.

That context can impose various types of requirements such as requirements related to the application and/or the business process for which implementation of a digital signature is required (e.g. which document(s)/data, in which steps of the business process one would need to sign and how):

- requirements influenced by legal provisions associated to the application and/or business context in which the business process takes place (e.g. the level of assurance on evidences and the longevity of such evidences);
- requirements on the actors involved in the creation/validation of signatures; and/or
- requirements linked to the technological environment in which the process takes place.

NOTE 1: Regulation (EU) No 910/2014 [i.1] defines the terms electronic signature, advanced electronic signature, qualified electronic signature, electronic seal, advanced electronic seal and qualified electronic seal. These electronic signatures and seals can be created using digital signature technology.

NOTE 2: When not stated otherwise in the present document, "signature" denotes "digital signature".

Implementing digital signatures into a business process very often implies considering more than one signature to make a transaction effective or to give legal validity to one or several documents. Those signatures can be parallel and independent over the content (e.g. such as those of a buyer and seller on a contract); or enveloping countersignatures where each countersignature covers both content and all previous signature(s); or not-enveloping countersignatures where each countersignature covers previous signature(s) but not the previously signed content; or a mix of such signatures. Since very complex situations can arise when considering multiple signatures, specific requirements on their sequencing and respective scope in terms of data to be signed needs to be considered to ensure their correct implementation into the concerned work-flow.

There needs to be some way of expressing all applicable requirements into rules for creating, augmenting, and validating a single signature or a set of signatures in the context in which that(these) signature(s) have been applied so that the concerned parties, signers and relying parties, can abide by the applicable rules.

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

The establishment of such rules into a signature policy results from the need:

- to document the decisions resulting from an analysis driven by a business or application context on how the concerned signature(s) needs to be implemented to meet the needs of the specific business application or electronic process it(they) support; and

- to specify the means for the creation, augmentation or long term management and verification of ***all*** the features of the concerned signature(s).

1 Scope

The present document defines the building blocks of signature policy and specifies a table of contents for human readable signature policy documents.

2 References

2.1 Normative 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 reference 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.

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

[1] ETSI EN 319 142-1: "Electronic Signatures and Infrastructures (ESI); PAdES digital signatures; Part 1: Building blocks and PAdES baseline signatures".

[2] ISO 19005-2:2011: "Document management - Electronic document file format for long-term preservation - Part 2: Use of ISO 32000-1 (PDF/A-2)".

[3] ETSI TS 103 172: "Electronic Signatures and Infrastructures (ESI); PAdES Baseline Profile".

2.2 Informative 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 reference document (including any amendments) applies.

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

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] Regulation (EU) No 910/2014 of the European Parliament and of the Council on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC.

[i.2] ETSI TR 119 001: "Electronic Signatures and Infrastructures (ESI); The framework for standardisation of signatures; Definitions and abbreviations".

[i.3] ETSI TR 119 100: "Electronic Signatures and Infrastructures (ESI); Business Driven Guidance for Signature Creation and Validation".

[i.4] ETSI EN 319 102-1: "Electronic Signatures and Infrastructures (ESI); Procedures for Signature Creation and Validation of AdES Digital Signatures; Part 1: Creation and Validation".

[i.5] ETSI TS 119 312: "Electronic Signatures and Infrastructures (ESI); Cryptographic Suites".

[i.6] ISO/IEC 27001: "Information technology -- Security techniques -- Information security management systems -- Requirements".

[i.7] ISO/IEC 27002: "Information technology -- Security techniques -- Code of practice for information security management".

[i.8] ETSI TS 103 173: "Electronic Signatures and Infrastructures (ESI); CAdES Baseline Profile".

[i.9] ETSI TS 103 171: "Electronic Signatures and Infrastructures (ESI); XAdES Baseline Profile".

[i.10] Unified Modelling Language.

NOTE: Available at http://www.uml.org/#UML2.0.

[i.11] ETSI TS 102 231: "Electronic Signatures and Infrastructures (ESI); Provision of harmonized Trust-service status information".

[i.12] ETSI TS 119 612 (V1.1.1): "Electronic Signatures and Infrastructures (ESI); Trusted Lists".

[i.13] IETF RFC 5280: "internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile".

[i.14] IETF RFC 6960: "X.509 Internet Public Key Infrastructure Online Certificate Status Protocol - OCSP".

[i.15] Directive 1999/93/EC of the European Parliament and of the Council of 13 December 1999 on a Community framework for electronic signatures.

[i.16] 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.

[i.17] Commission Decision 2013/662/EU of 14 October 2013 amending Decision 2009/767/EC as regards the establishment, maintenance and publication of trusted lists of certification service providers supervised/accredited by Member States.

[i.18] 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.19] Business Process Modelling Notation: "A standard for modelling business processes and web service processes, as put forth by the Business Process Management Initiative".

NOTE: Available at www.bpmi.org.

[i.20] ETSI EN 319 122-1: "Electronic Signatures and Infrastructures (ESI); CAdES digital signatures; Part 1: Building blocks and CAdES baseline signatures".

[i.21] ETSI EN 319 132-1: "Electronic Signatures and Infrastructures (ESI); XAdES digital signatures; Part 1: Building blocks and XAdES baseline signatures".

[i.22] ETSI EN 319 122-2: "Electronic Signatures and Infrastructures (ESI); CAdES digital signatures; Part 2: Extended CAdES signatures".

[i.23] ETSI EN 319 132-2: "Electronic Signatures and Infrastructures (ESI); XAdES digital signatures; Part 2: Extended XAdES signatures".

[i.24] IETF RFC 3647: "Internet X.509 Public Key Infrastructure Certificate Policy and Certification Practices Framework".

[i.25] ETSI EN 319 142-2: "Electronic Signatures and Infrastructures (ESI); PAdES digital signatures; Part 2: Additional PAdES signatures profiles".

[i.26] ETSI EN 319 162-1: "Electronic Signatures and Infrastructures (ESI); Associated Signature Containers (ASiC); Part 1: Building blocks and ASiC Baseline containers".

[i.27] ETSI EN 319 162-2: "Electronic Signatures and Infrastructures (ESI); Associated Signature Containers (ASiC); Part 2: Extended Containers".

[i.28] ETSI TS 102 918: "Electronic Signatures and Infrastructures (ESI); Associated Signature Containers (ASiC)".

[i.29] Commission Implementing Decision 2014/148/EU of 17 March 2014 amending Decision 2011/130/EU 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.30] ETSI TS 119 172-2: "Electronic Signature Infrastructure; Signature Policies; Part 2: XML format for signature policies".

[i.31] ETSI TS 119 172-3: "Electronic Signature Infrastructure; Signature Policies; Part 3: ASN.1 format for signature policies".

[i.32] Commission Decision 2010/425/EU of 28 July 2010 amending Decision 2009/767/EC as regards the establishment, maintenance and publication of trusted lists of certification service providers supervised/accredited by Member States.

[i.33] ETSI TS 101 733: "Electronic Signatures and Infrastructures (ESI); CMS Advanced Electronic Signatures (CAdES)".

[i.34] ETSI TS 101 903: "Electronic Signatures and Infrastructures (ESI); XML Advanced Electronic Signatures (XAdES)".

[i.35] ETSI TS 102 778: "Electronic Signatures and Infrastructures (ESI); PDF Advanced Electronic Signature Profiles; CMS Profile based on ISO 32000-1".

[i.36] Recommendation CCITT X.800 (1991): "Security Architecture for Open Systems Interconnection for CCITT applications. ISO 7498-2:1989, Information processing systems - Open Systems Interconnection - Basic Reference Model - Part 2: Security Architecture".

[i.37] Recommendation ITU-T X.1252 (2010): "Cyberspace security - Identity management - Baseline identity management terms and definitions".

[i.38] Recommendation ITU-T X.509 | ISO/IEC 9594-8: "Information technology - Open systems interconnection - The Directory: Public-key and attribute certificate frameworks".

3 Definitions and abbreviations

3.1 Definitions

For the purposes of the present document, the following terms and definitions apply:

CA-certificate: public-key certificate for one CA issued by another CA or by the same CA

NOTE: As defined in Recommendation ITU-T X.509 | ISO/IEC 9594-8 [i.38].

certification authority (CA)**:** authority trusted by one or more users to create and assign public-key certificates. Optionally the certification authority may create the subjects' keys

NOTE: As defined in Recommendation ITU-T X.509 | ISO/IEC 9594-8 [i.38].

certification path: ordered list of one or more public-key certificates, starting with a public-key certificate signed by the trust anchor, and ending with the public key certificate to be validated

NOTE 1: All intermediate public-key certificates, if any, are CA-certificates in which the subject of the preceding certificate is the issuer of the following certificate.

NOTE 2: As defined in Recommendation ITU-T X.509 | ISO/IEC 9594-8 [i.38].

certificate validation: process of verifying and confirming that a certificate is valid

cryptographic system: collection of transformations, normally defined by a mathematical algorithm, from plain text into cipher text and vice versa, the particular transformation(s) to be used being selected by (private or public) keys

NOTE: As defined in Recommendation ITU-T X.509 | ISO/IEC 9594-8 [i.38].

data integrity: property that data has not been altered or destroyed in an unauthorized manner

NOTE: As defined in ITU-TRecommendation X.800 | ISO 7498-2 [i.36].

data origin authentication: corroboration that the source of data received is as claimed

NOTE: As defined in ITU-TRecommendation X.800 | ISO 7498-2 [i.36].

digital signature: data appended to, or a cryptographic transformation (see cryptography) of a data unit that allows a recipient of the data unit to prove the source and integrity of the data unit and protect against forgery e.g. by the recipient.

NOTE: As defined in ITU-TRecommendation X.800 | ISO 7498-2 [i.36].

private key: in a public key cryptographic system, that key of an entity's key pair which is known only by that entity

NOTE: As defined in Recommendation ITU-T X.509 | ISO/IEC 9594-8 [i.38].

public key: in a public key cryptographic system, that key of an entity's key pair which is publicly known.

NOTE: As defined in Recommendation ITU-T X.509 | ISO/IEC 9594-8 [i.38].

public key certificate: public key of an entity, together with some other information, rendered unforgeable by digital signature with the private key of the certification authority which issued it

NOTE: As defined in Recommendation ITU-T X.509 | ISO/IEC 9594-8 [i.38].

public key infrastructure: infrastructure able to support the management of public keys able to support authentication, encryption, integrity or non-repudiation services

NOTE: As defined in Recommendation ITU-T X.509 | ISO/IEC 9594-8 [i.38].

repudiation: denial by one of the entities involved in a communication of having participated in all or part of the communication

NOTE: As defined in ITU-TRecommendation X.800 | ISO 7498-2 [i.36].

signature augmentation: process of incorporating to a digital signature information aiming to maintain the validity of that signature over the long term

NOTE: Augmenting signatures is a co-lateral process to the validation of signatures, namely the process by which certain material (e.g. time stamps, validation data and even archival-related material) is incorporated to the signatures for making them more resilient to change or for enlarging their longevity.

signature augmentation policy: set of rules, applicable to one or more digital signatures, that defines the technical and procedural requirements for their augmentation, in order to meet a particular business need, and under which the digital signature(s) can be determined to be conformant

NOTE: This covers collection of information and creation of new structures that allows performing, on the long term, validations of a signature.

signature creation device: configured software or hardware used to create a digital signature

signature creation policy: set of rules, applicable to one or more digital signatures, that defines the technical and procedural requirements for their creation, in order to meet a particular business need, and under which the digital signature(s) can be determined to be conformant

signature policy: signature creation policy, signature augmentation policy, signature validation policy or any combination thereof, applicable to the same signature or set of signatures

signature policy authority: entity responsible for the drafting, registering, maintaining, issuing and updating of a signature policy

signature policy document: document expressing one or more signature policies in a human readable form

signature validation: process of verifying and confirming that a digital signature is valid

signature validation policy: set of rules, applicable to one or more digital signatures, that defines the technical and procedural requirements for their validation, in order to meet a particular business need, and under which the digital signature(s) can be determined to be valid

trust: firm belief in the reliability and truth of information or in the ability and disposition of an entity to act appropriately, within a specified context

NOTE: As defined in Recommendation ITU-T X.1252 [i.37].

Trust Anchor (TA): entity that is trusted by a relying party and used for validating certificates in certification paths

NOTE: As defined in Recommendation ITU-T X.509 | ISO/IEC 9594-8 [i.38].

Trust Anchor information: at least the: distinguished name of the Trust Anchor, associated public key, algorithm identifier, public key parameters (if applicable), and any constrains on its use including a validity period

NOTE: As defined in Recommendation ITU-T X.509 | ISO/IEC 9594-8 [i.38].

validation data: data that is used to validate a digital signature

3.2 Abbreviations

For the purposes of the present document, the following abbreviations apply:

ASiC	Associated Signature Container
ASN	Abstract Syntax Notation
B2B	Business to Business
B2C	Business to Consumer
BPMN	Business Process Modelling Notation
BSP	Business Scoping Parameter
CA	Certification Authority
CD	Commission Decision
CRL	Certificate Revocation List
DA	Driving Application
DTBS	Data To Be Signed
EC	European Commission
EN	European Standard
EU	European Union
IP	Internet Protocol
Gov2B	Government to Business
Gov2C	Government to Consumer
LoA	Level of Assurance
OCSP	Online Certificate Status Protocol
OID	Object IDentifier
PKI	Public Key Infrastructure
SCA	Signature Creation Application
SVA	Signature Validation Application
TA	Trust Anchor
ToC	Table of Content
TR	Technical Report
TS	Technical Specification
TSP	Trust Service provider
TST_A	Time-Stamp Token applied in an archive level of CAdES signature or XAdES signature
$TST_{T\text{-}Level}$	Time-Stamp Token applied in a T-Level of CAdES signature or XAdES signature
UML	Unified Modelling Language
URI	Uniform Resource Identifier
URL	Uniform Resource Locator
UK	United Kingdom
XML	eXtensible Markup Language
WYSIWYS	What You See IS What You Sign

4 Signature policies and signature policy document

A signature policy should be derived from the analysis of the requirements applicable to the implementation of digital signatures into a specific business electronic process or application domain.

That requirement analysis should be done according to the process described in ETSI TR 119 100 [i.3].

The resulting rules related to the creation, augmentation and/or validation of one or more signatures to which the same set of rules apply shall be documented in a signature policy.

A signature policy shall cover at least one of the three following aspects related to the management of the signatures to which it applies:

1) a signature creation policy;

2) a signature augmentation policy; or

3) a signature validation policy.

When there is a need for expressing a signature policy in a human readable form, the table of content (ToC) specified in annex A shall be followed to establish the corresponding signature policy document, or the signature policy shall be expressed under the form of a signature policy statement summary established on the basis of table A.1 from annex A.

The numbering of the clauses of the table of content is provided in annex A as it shall appear in the signature policy document by removing the starting "A.". Each clause shall appear. If the clause does not apply, "not applicable" shall be written after the clause title. The text provided in each clause of annex A specifies the expected content of each clause. This text shall not be copied in the signature policy document.

Where applicable, the sub-clauses of the signature policy document may identify separate provisions for each signature policy addressed by the signature policy document and for each of them may identify separate provisions for the creation, augmentation and validation by using the following labels to start dedicated clauses on creation, augmentation, or validation aspects, respectively:

- [CREATION]
- [AUGMENTATION]
- [VALIDATION]

The provisions expressed in each clause may be texted explicitly or incorporated by reference to other sources of provisions, in particular to abide by, endorse, inherit or enforce requirements from other signature policies.

Clause A.3 covers the rules or requirements set by a signature policy organized against business scoping parameters (BSPs) which are:

- parameters mainly related to the application and/or business process for which implementation of 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 signatures; and
- other signature parameters.

The sub-clauses of clause A.3 shall each include the description of the applicable BSP provisions in terms of business language and shall indicate separately the corresponding requirements on signers, entities augmenting signatures and/or relying parties validating signatures covered by each signature policy addressed by the signature policy document.

When a specific business or application process involves several groups of signatures addressed by different signature policies, a single signature policy document may be used to express those signature policies.

EXAMPLE: Multiple signatures applied to the same data or to different (sets of) data being signed by the same or different entities at different moments alongside the workflow of events with a need for evidences covered by the considered workflow.

NOTE: A signature policy document can cover a group of several signature policies, in which case each signature policy defines the set of rules applicable to one or several signatures to which the same set of rules applies.

The signature policy document shall at least be provided in the form of a PDF/A-2 document according to ISO 19005-2 [2]. It shall be digitally signed according to PAdES baseline signatures ETSI TS 103 172 [3] or ETSI EN 319 142-1 [1].

Annex A (normative): Table of contents for signature policies expressed as human readable documents

Notwithstanding the provisions of the copyright clause related to the text of the present document, ETSI grants that users of the present document may freely reproduce the signature policy document table of content proforma in annex A so that it can be used for its intended purposes and may further publish the completed signature policy document.

A.1 Introduction

A.1.1 Overview

This clause shall provide a general introduction to the document being written. It shall provide a synopsis of the business or application domain and the specific business or application process to which the expressed signature policy(ies) applies(apply). Depending on the complexity and scope of the particular business or application process implementing signatures, a diagrammatic representation may be useful here.

A.1.2 Business or Application Domain

A.1.2.1 Scope and boundaries of signature policy

This clause shall describe the scope and boundaries of the business (application) domain in which the signature policy(ies) is(are) suitable for use.

NOTE: The business (application) domain is any business or commercial transaction process(es), which can involve several actors/participants and/or multiple actions and which can require one or multiple signatures to give it effect.

EXAMPLE: This can range from a purely corporate internal process or set of processes, through a multi-party trading network whose parties can 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(ies) 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-organization, corporate or cross-organizations, nationwide or cross-borders, horizontal or vertical (e.g. eProcurement, eInvoice, eHealth, eJustice, etc.).

When applicable the hierarchy of signature policies included in the signature policy document shall be detailed, illustrated and be consistently identified (see clause A.1.3.2).

A.1.2.2 Domain of applications

When applicable and when not sufficiently described by clause A.1.1, this clause shall further describe each domain of applications that is considered and for which the usage of signatures is ruled by the signature policy document.

A.1.2.3 Transactional context

This clause shall provide additional information about the transactional context, when applicable.

EXAMPLE: 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 authorization (e.g. because of value, because of applicable law or legal requirements, etc.), etc.

A.1.3 Document and policy(ies) names, identification and conformance rules

A.1.3.1 Signature policy document and signature policy(ies) names

This clause shall provide information about any applicable name for the signature policy document and about any applicable name(s) for the signature policy(ies) covered by the signature policy document.

A.1.3.2 Signature policy document and signature policy(ies) identifier(s)

This clause shall provide information about any other applicable identifiers for the signature policy document and for the signature policy(ies) it covers.

EXAMPLE 1: Unique identifier, OIDs.

When applicable, the hierarchy of signature policies included in a signature policy shall be identified, in such a way that at least one distinct unique identifier shall be allocated to the signature policy document itself and to each signature policy it covers. When OIDs are used, the OID for each set of rules may be derived from the OID of the signature policy document.

EXAMPLE 2: This can be done through the allocation of sub-OIDs subordinated to OID of the main signature policy. A signature policy document has identifier 1.3.777.1.1; three sets of rules applicable to three types of signatures in the concerned workflow of the business process can be identified via the respective 1.3.777.1.1.1, 1.3.777.1.1.2, and 1.3.777.1.1.3 OIDs.

A.1.3.3 Conformance rules

This clause shall provide information about conformance rules.

A.1.3.4 Distribution points

This clause shall provide information about where the signature policy document is available (e.g. a URL or by email) under electronic format (e.g. PDF) and, when applicable, how a paper/hard copy can be made available.

It may also provide information about whether and where the signature policy(ies) covered by the signature policy document are available under one or more machine processable formats (e.g. [i.30] and [i.31]).

A.1.4 Signature policy document administration

A.1.4.1 Signature policy authority

This clause shall include the name of the signature policy authority responsible for the signature policy document and the policy(ies) it covers, together with its country of establishment, its postal or electronic address and where applicable its registration number as stated in the official records of the country of establishment.

It shall also provide information identifying the public key certificate corresponding to the private key used by the signature policy issuer to digitally sign the signature policy document.

When the policy authority is responsible for determining whether one or more separate signature policies are allowed to be subordinated, included in or include a signature policy defined in the signature policy document, this clause shall include:

- the name or title of the entity in charge of making such a determination;
- its electronic mail address or alias;
- its telephone number;
- its fax number; and
- other generalized information.

In this case, this clause shall also include, either by reference or explicitly, the procedures by which that determination is made.

A.1.4.2 Contact person

When the contact point is a natural person, this clause shall include the:

a) name;

b) electronic mail address; and

c) telephone number.

In other cases, it shall include:

a) a title or role;

b) an electronic mail alias; and

c) other generalized contact information.

This clause may state that the contact person, alone or in combination with others, is available to answer questions about the document.

A.1.4.3 Approval procedures

This clause shall include the procedures by which the approval of the signature policy document is made.

A.1.5 Definitions and Acronyms

This clause shall contain a list or a reference to a list of definitions for defined terms used within the signature policy document, as well as a list or a reference to a list of acronyms and their meanings.

A.2. Signature application practices statements

This clause shall include, either by reference or explicitly, the set of policy and security practices requirements that the driving application (DA), the signature creation application (SCA) and/or the signature validation application (SVA) shall meet when creating, augmenting and/or validating signatures in accordance with the signature policy document.

When the policy and security practices requirements applicable to SCA and/or SVA are included explicitly in this clause, the table of content of this clause shall conform to the structure defined in annex D of the present document.

A.3 Business scoping parameters

A.3.1 BSPs mainly related to the concerned application/business process

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

This clause shall describe and specify whether the business electronic process and hence the signature policy address a single signature or a set of signatures.

When the signature policy addresses a set of signatures, this clause shall describe and specify the workflow.

The workflow should be produced using the Unified Modelling Language (UML) [i.10], the Business Process Modelling Notation (BPMN) [i.19] or any similar standard notation in order to provide continuity into the development and use of signatures.

The workflow shall indicate:

a) The sequence flow of data exchanges between those actors in the considered business scenario or application process and the use cases involving generation, augmentation and/or validation of signature(s) in this application process in the considered business scenario.

b) 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);
- serial signatures (i.e. signatures applied to different data and serialized);
- counter signatures (i.e. signatures successively applied to the set of previous signatures, and optionally to the same original data); or
- a combination of such signatures.

c) Whether the signatures apply on individual transaction, or apply on a block of transactions.

d) What the actors are (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.

e) For each data to be signed, what sequence of signature(s) applies (e.g. single; multiple parallel; counter signatures; sequential; or a combination).

f) Whether and which signature is required to be validated before generating the next signature in the workflow.

This clause shall indicate whether the time when a signature is generated is relevant or not. It shall indicate the timing constraints applying to the generation of signatures.

NOTE 1: The time at which the signature was generated can be relevant when legally enforceable.

EXAMPLE: Signature to be generated before a certain deadline, set of parallel signatures to be generated within a certain timeframe, elapsed time between two serial or counter signatures to be greater, equal or smaller than a certain duration, etc.

This clause shall indicate whether the time when a signature is validated is relevant or not. It shall indicate the timing constraints applying to the validation of signatures.

NOTE 2: In some business scenarios, sequence and timing relate to signatures on multiple documents or signatures which all form part of a single process or transaction. In some circumstances, the validity or acceptance of an agreement/authorization, etc. is contingent upon certain steps or approvals having been taken within given timeframes, e.g.:

- Where the signature of superior company officer is required to authorize or "sign off" a piece of work, this signature comes after the primary signature of the employee who has performed the work.
- The counter signature is not allowed to occur after a certain delay or not before a certain delay.

This clause shall indicate whether mass signing is applicable (e.g. a significant number of signatures signing a significant number of documents per day), as this can have an impact on, for example, requirements for use of signing devices designed for mass signing (e.g. hardware security modules).

A.3.1.2 BSP (b): Data to be signed

For each signature identified and for each data to be signed (DTBS) as identified in the concerned workflow (see BSP(a)), this clause shall describe and specify all the relevant aspects concerning the data that have to be signed and the related technology, i.e. the type of technological environment in which those data are managed. These aspects shall include:

1) the format of the data to be signed; and

2) where that data to be signed is structured, indication whether the whole data or only certain part(s) will be signed.

EXAMPLE: Binary, structured data, xml, PDF document, editable documents such as word processor made, multimedia packages, images, etc.

NOTE 1: The type of format for the DTBS can 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 2: Signatures can be generated following XML, ASN.1 or PDF syntax. Where the data to be signed is specified in one of the aforementioned syntaxes, the initial choice is to select the signature defined for that syntax, unless other business parameters clearly recommend using another one.

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

For each signature identified and for each data to be signed as identified in the concerned workflow (see BSP(a)), this clause shall describe and specify the type of relationship between the signed data and the signatures. These aspects shall include:

1) The need for signed data referencing mechanisms.

EXAMPLE: The use or relevance of bulk signatures, i.e. when one signature will sign different data (e.g. through the implementation of signature on several document references consisting in hashes of the referenced documents).

2) The number of data that one signature actually signs.

3) The relative position of the signature and its signed data (e.g. associated within an ASiC container, enveloped signature, enveloping signature, detached signature).

4) The signature format and levels to be used.

NOTE: Levels of signatures as defined in ETSI standards on signature formats (e.g. [3], [i.8], [i.9], [i.20] to [i.23], [i.25] to [i.28], [i.33] to [i.35]) address incremental (augmenting) requirements to maintain the validity of the signatures over the long term, in a way that a certain level always addresses all the requirements addressed at levels that are below it.

A.3.1.4 BSP (d): Targeted community

For each signature identified and for each data to be signed as identified in the concerned workflow (see BSP(a)), this clause shall identify and describe:

1) the addressed community; and

2) any specific community rules in place.

EXAMPLE: These rules can state the conditions under which a certain signature is relied upon, or include provisions relating to the intended effectiveness of signatures, where multiple signatures are required.

NOTE: These rules can impact not only the formats of the signatures and their relationships with the signed documents, but also the specific standards and/or levels to be used.

A.3.1.5 BSP (e): Allocation of responsibility for signature validation and augmentation

For each signature identified and for each data to be signed as identified in the concerned workflow (see BSP(a)), this clause shall describe and specify the allocation of the responsibility of validating and/or augmenting such 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) Signature validation trust services, on request of either the signer or any other appropriate relying party; or

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

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

This clause should also identify requirements for augmenting signatures as they are validated and progressed in the business process data flow.

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

A.3.2.1 BSP (f): Legal type of the signatures

For each signature identified in the concerned workflow (see BSP(a)) this clause shall describe and specify the signature legal type required in the context of the business process and the associated legal requirements.

NOTE 1: This parameter has an impact on the level of assurance on the authentication (i.e. the certification of the identification) of the actor generating a 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, and 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 2: In Europe, the following levels are identified

a) In accordance with Directive 1999/93/EC [i.15], CD 2009/767/EC [i.16] as amended by CD 2010/425/EU [i.32] and by CD 2013/662/EU [i.17] and CD 2011/130/EU [i.18] as amended by CD 2014/148/EU [i.29]: qualified electronic signatures, advanced electronic signatures supported by a qualified certificate, and advanced electronic signatures.

b) In accordance with Regulation (EU) No 910/2014 [i.1]: qualified electronic signatures, advanced electronic signatures supported by a qualified certificate, advanced electronic signatures, qualified electronic seals, advanced electronic seals supported by a qualified certificate, advanced electronic seals.

A.3.2.2 BSP (g): Commitment assumed by the signer

For each signature identified in the concerned workflow (see BSP(a)) this clause shall specify the authorized types of commitment associated to the signature.

NOTE 1: A commitment type associated to a signature is the representation of the expected purpose and meaning of the signature and of the precise nature of the responsibility assumed by the signer when generating the concerned signature.

NOTE 2: The explicit description of such signature commitments avoids potential ambiguity when signatures do not provide equivalent contextual information as in the paper world leading to uncertainty about the signer's intention; relying on the implicit contextual information is hazardous.

NOTE 3: Indication of commitment types assists in the management and validation of multiple signatures under a signature policy.

A commitment type shall be expressed as a unique identifier (OID or URI), associated to a description of the commitment type in a language that is understandable by the signer and at least in UK English.

EXAMPLE: The commitment types can be a representation of the fact that:

- the signature is intended for data authentication purposes only;
- the signature is intended for entity authentication purposes only; or
- the signature is created with the intention to sign the associated data (signed data):
  - 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's signature on the same document (signed data) having read, approving and being bound accordingly to the content of the data that is signed;
- etc.

▪ etc.

and being bound accordingly to the data that is signed.

The commitment types defined in annex B may be used.

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

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

1) This clause shall describe and specify the requirements on the level of assurance on the required timing evidences.

2) This clause should address:

   a) whether and on which type of data a timing evidence is required to be generated (e.g. a mere signing time indication claimed by the signer, or time evidences on signed data, on signature(s), on signature(s) and validation data, etc.); and

   b) for each required timing evidence:

      i) whether claimed assertions with regards to time information are allowed; or

      ii) whether time stamps provided by trust service providers are required, and in this case what the requirements and level of assurance associated respectively to the time stamps and the providers are.

NOTE: This clause is closely related to the clauses BSP(a), (j) and (k).

A.3.2.4 BSP (i): Formalities of signing

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

1) This clause shall 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.

NOTE 1: This aims at requiring that signing systems are built in a way that satisfy, as much as possible, legal requirements on expression of will or intentions by the signers.

2) This clause shall identify and specify:

   a) requirement for having a WYSIWYS environment;

   b) requirements for providing the actor generating/ validating signatures with:

      i) proper advice and information on the application's signature process;

      ii) proper advice and information on legal consequences; and

      iii) a user interface satisfying legal requirements on expression of will or intentions by the signers.

c) requirements on the user interface:

iv) guaranteeing the above requirements;

v) allowing and demonstrating clear expression of a will to sign and the user's intention to be bound by the signature;

vi) allowing and demonstrating an informed consent; and

vii) ensuring consistence between the use of the appropriate signature creation and validation data, signature creation device, the data to be signed and the expected scope and purpose of the signature (or the act of signing); and

d) requirements for providing the relying parties (including the signer) with correct procedures for the validation and the archival of the signature and the validation data.

NOTE 2: Addressing formalities of signing can impact the selection of appropriate protection profiles and conformity assessment schemes against which the signature creation application and/or signature validation application will be designed and assessed.

A.3.2.5 BSP (j): Longevity and resilience to change

For each signature identified in the concerned workflow (see BSP(a)), this clause shall describe and specify the expected longevity and resilience to change of the signature such that it is verifiable up to a given period of time.

EXAMPLE: Such period of time can be defined 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 (guarantee-given-by-the-TST_A-or-the-successive-application-of-TST_A's).

NOTE: Such requirements can have an impact on the adequate level of the signature (see [3], [i.8], [i.9], [i.20] to [i.23], [i.25] to [i.28], [i.33] to [i.35]), on the adequate key length (usually determined by the TSP having issued the signing certificate) of the signature private key, and on the selection of the cryptographic suites. To this extent BSP(p) recommendations can be followed according to the expected resistance of the signature.

A.3.2.6 BSP (k): Archival

For each signature identified in the concerned workflow (see BSP(a)), this clause shall describe and specify archival requirements.

A.3.3 BSPs mainly related to the actors involved in creating/augmenting/validating signatures

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

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

1) This clause shall describe and specify requirements on:

a) the nature/type and identification of the proposed signers;

b) the associated signer identification rules;

c) if any, the rules applicable to the roles and/or attributes of the signers; and

d) if any, the associated proof of authority and the type of proof of authority to sign that is acceptable and whether authority to sign can be delegated.

2) This clause shall, in consequence, identify and describe:

   a) what the necessary components are to ensure that a signature is that of a specified individual (e.g. whether a natural or legal person, a business or transactional functional entity, a machine, an application or server, etc.); and

   b) what the required identification components (identity attributes) are for each type of signer.

EXAMPLE: 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.

NOTE 1: In some business scenarios, the role or attributes of a signer are at least as important as his identity. "Signer role" does not refer here to the "signing" role played by the signer in the 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 can be claimed or certified, and which imply some attribute(s) being associated with the signer.
This clause aims to describe the set of attributes, authorities and responsibilities which are associated with each signer, his access rights, or authority to sign, to act on behalf of the organization he purports to represent, etc.

NOTE 2: Where parties have already established communications, and there is ostensible authority to enter into the proposed transaction, an identity certificate can be considered sufficient. In some cases, additional proof can be appropriate, an attribute certificate issued by a trust service provider, signed assertions or attested attribute information issued by a reliable source. This can include proof that an employee or representative is authorized to enter into transactions over a specified value.

A.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 clause shall describe and specify the level of assurance required for the authentication of the signer, in particular what the expectations are in terms of trust on the signer's identification (e.g. assurance or quality level of the certification policy under which a certificate has been issued and of the device used to protect the private key).

EXAMPLE: Certificates can be required to be legally recognized certificates and/or issued by an accredited, supervised, certified, or audited certification authority, or be issued according to a specific certificate policy, etc.

A.3.3.3 BSP (n): Signature creation devices

For each signature identified in the concerned workflow (see BSP(a)), this clause shall describe and specify requirements on the signature creation devices that will be used for generating the signatures within the business process.

A.3.4 Other BSPs

A.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 clause shall describe and specify, when applicable, any requirement to associate other information with the signature and any requirement on such information.

EXAMPLE: Such information can be signature policy reference, geographic location at which the signature takes place, content related information, etc.

NOTE: This can 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 techniques to be selected among those offered by the selected signature format.

A.3.4.2 BSP (p): Cryptographic suites

For each signature identified in the concerned workflow (see BSP(a)), this clause shall describe and specify requirements on the robustness of cryptographic suites used to generate or augment electronic signatures.

Guidance provided in ETSI TS 119 312 [i.5], in particular its table 12, should be taken into account.

A.3.4.3 BSP (q): Technological environment

This clause shall identify the constraints on technologies for the signature creation and signature validation applications and the environments they are used.

EXAMPLE: Operating system, programming language, protocols, etc.

A.4 Requirements / statements on technical mechanisms and standards implementation

A.4.1 Technical counterparts of BSPs - Statement summary

For each signature identified in the concerned workflow (as defined in clause A.3.1.1 - BSP(a)), this clause shall summarize the requirements related to the BSPs specified in the previous clauses, and shall specify the corresponding technical mechanisms and standards (counterpart statements) to be implemented by signature creation/validation applications conformant to the applicable signature policy.

It shall specify the selected signature format(s) (see [3], [i.8], [i.9], [i.20] to [i.23], [i.25] to [i.28], [i.33] to [i.35]) including details on the format of the signed data, the relative placement of the signature and the signed data (i.e. enveloped, enveloping, detached), the relevance of use of a container to package the signature(s) together with signed data (i.e. ASiC), the specific attributes (signed or unsigned) of the signature, and the expected level of the selected signature format.

This clause should use the following signature policy statement summary table, one table being produced per signature identified in the concerned workflow. One single table may however be used when the same set of requirements/statements are applicable to a group of signatures (i.e. the same signature policy applies).

Table A.1: Signature policy statement summary

Name and identifier of the signature policy authority: ..... **Name and identifier of the 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) of signatures		
(b)	Data to be signed (DTBS)		
(c)	Relationship between DTBS & signature(s)		
(d)	Targeted community		
(e)	Allocation of responsibility for signature validation and augmentation		
(f)	Legal type of signature		
(g)	Commitment assumed by the signer		
(h)	Level of assurance on timing evidences		
(i)	Formalities of signing		
(j)	Longevity & resilience to change		
(k)	Archival		
(l)	Identity of signers		
(m)	Level of assurance required for the authentication of the signer		
(n)	Signature creation devices		
(o)	Other information to be associated with the signature		
(p)	Cryptographic suites		
(q)	Technological environment		
Signature creation/validation application practices statements			
Summary of the selected signature format(s) (e.g. [3], [i.8], [i.9], [i.20] to [i.23], [i.25] to [i.28], [i.33] to [i.35]) including details on the format of the signed data, the relative placement of the signature and the signed data (i.e. enveloped, enveloping, detached), the relevance of use of a container to package the signature(s) together with signed data (i.e. ASiC), the specific attributes (signed or unsigned) of the signature, and the expected level of the selected signature format:			

A.4.2 Input and output constraints for signature creation, augmentation and validation procedures

A.4.2.1 Input constraints to be used when generating, augmenting and/or validating signatures in the context of the identified signature policy

This clause shall specify the requirements, derived from the BSPs applicable to each signature covered in the policy, on the input of the signature creation procedure, the signature augmentation procedure and/or the signature validation procedure respectively. To this respect, this clause should use table A.2 per concerned signature.

NOTE: Table A.2 aims to facilitate deriving respectively signature creation constraints, signature augmentation constraints and signature validation 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 constraints and their values will then condition the respective creation, augmentation and validation procedures implemented at the signature creation application (SCA) level or signature validation application (SVA) level, and/or even at the driving application (DA) level as they are defined in [i.4].

Table A.2 corresponds to one or more signatures to which the same rules apply in the context of the concerned signature policy. The header provides the identifier of such a set of signatures and of the signature policy.

The first column ("**BSP**") identifies the applicable BSP.

The second column ("**BSP Title**") identifies the BSP title.

The third column ("**Business statement summary**") and the fourth ("**Technical counterpart statement**") column summarize respectively the business statements and the counterpart technical statements applicable to the respective BSP.

The fifth column ("**Constraint(s)**") identifies the constraints that can be parameterized with regards to the respective BSP.

The sixth column ("**Constraint value at signature creation (SCA or DA)**") provides, when applicable, the value of the constraints at the level of signature creation (clarifying whether at SCA or DA level).

The seventh column ("**Constraint value at signature augmentation (SCA, SVA or DA)**") provides, when applicable, the value of the constraints at the level of signature augmentation (clarifying whether at SCA, SVA or DA level).

The eighth column ("**Constraint value at signature validation (SVA or DA)**") provides, when applicable, the value of the constraints at the level of signature validation (clarifying whether at SVA or DA level).

Table A.2

Name and identifier of the signature policy authority: ..... **Name and identifier of the signature policy: .....** **Identifier of the concerned signature(s) in the concerned signature workflow: .....**							
BSP	**BSP title**	**Business statement summary**	**Technical counterpart statement**	**Constraint(s)**	**Constraint value at signature creation** (SCA or DA)	**Constraint value at signature augmentation** (SCA, SVA or DA)	**Constraint value at signature validation** (SVA or DA)
(a)	Workflow (sequencing & timing)			**(a)1. OrderInSequence:** This constraint indicates 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.			
				(a)2. SequencingNature: This constraint indicates the characteristic of the signature with regards to sequencing. Semantic for a possible set of requirement values used to express such requirements is defined as follows: **(a)2.1 Mandated-independent:** independent signatures are defined as signatures applied to exactly the same data. 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 and serialized. 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 set of previous signatures, and optionally to the same original data. This constraint indicates that the corresponding unsigned qualifying property is mandated to be present in the signature.			

BSP	BSP title	Business statement summary	Technical counterpart statement	Constraint(s)	Constraint value at signature creation (SCA or DA)	Constraint value at signature augmentation (SCA, SVA or DA)	Constraint value at signature validation (SVA or DA)
				(a)3. TimingRelevance: **(a)3.1 TimingRelevanceOnSequencing:** This constraint indicates the required relevance of timing with regards to the sequencing of the signatures. Semantic for a possible set of requirement values used to express such requirements is defined as follows: • [not] before a certain date • [not] after a certain date • [not] before a certain amount of time • in exactly a certain amount of time • [not] after a certain amount of time **(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: • **(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 time-stamp(s) over the signed data as a whole or over a subset of that data as part of the signed qualifying properties. • **(a)3.2.3 MandatedUnsignedQProperties-signature-time-stamp** to require a time-stamp on the signature. • **(a)3.2.4 MandatedUnsignedQProperties-archival-form** to require an archival time-stamp.			
				(a)4. MassSigningAcceptable (yes/no): This constraint indicates whether mass signing is acceptable with regards to the concerned type of signature, expressed as a boolean.			

BSP	BSP title	Business statement summary	Technical counterpart statement	Constraint(s)	Constraint value at signature creation (SCA or DA)	Constraint value at signature augmentation (SCA, SVA or DA)	Constraint value at signature validation (SVA or DA)
(b)	DTBS			**(b)1. ConstraintOnDTBS:** This constraint indicates requirements on the type of the data to be signed by the signer.			
				(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 require specific information that describes the innermost signed content of a multi-layer message where one content is encapsulated in another for the content being signed by the signer. **(b)2.3 MandatedSignedQProperties-content-reference** to require the incorporation of information on the way to link request and reply messages in an exchange between two parties, or the way such link has to be done, etc. **(b)2.4 MandatedSignedQProperties-content-identifier** to require the presence of, and optionally a specific value for, an identifier that can be used later on in the signed qualifying property "content-reference" attribute.			
				(b)3. DOTBSAsAWholeOrInParts: This constraint indicates whether the whole data or only certain part(s) of it have to be signed. Semantic for a possible set of requirement values used to express such requirements is defined as follows: • **whole**: the whole data has to be signed; • **parts**: only certain part(s) of the data have to be signed. In this case additional information should be used to express which parts have to be signed.			

BSP	BSP title	Business statement summary	Technical counterpart statement	Constraint(s)	Constraint value at signature creation (SCA or DA)	Constraint value at signature augmentation (SCA, SVA or DA)	Constraint value at signature validation (SVA or DA)
(c)	Relationship between DTBS 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 (e.g. through the implementation of signature on several document references consisting in hashes of the referenced documents) or on the contrary its prohibition. Semantic for a possible set of requirement values used to express such requirements is defined as follows: **(c)1.1 mandatedBulkSigning;** **(c)1.2 prohibitedBulkSigning.**			
				(c)2. ConstraintsOnTheNumberOfDOTBS: This constraint indicates the requirement on the number of data that one signature can sign. Semantic for a possible set of requirement values used to express such requirements is defined as follows: minValue {<, ≤ , =} x {=, ≥, >} maxValue			
				(c)3. SignatureRelativePosition: This constraint indicates the requirement with regards to the relative position of the signature and the signed data. Semantic for a possible set of requirement values used to express such requirements is defined as follows: • associated; • enveloped; • enveloping; • detached.			
				(c)4. MandatedSignatureFormat: This constraint indicates the required signature format and level (see note of clause A.3.1.3).			
(d)	Targeted community			**(d)1. TargetedCommunityConstraints:** This set of constraints identifies the community to which each document and its (their) signature(s) is (are) addressed and indicates the applicable requirements on that community. It can be used to identify any specific community rules in place. EXAMPLE: These rules could, for instance, state the conditions under which a certain signature can 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.			

BSP	BSP title	Business statement summary	Technical counterpart statement	Constraint(s)	Constraint value at signature creation (SCA or DA)	Constraint value at signature augmentation (SCA, SVA or DA)	Constraint value at signature validation (SVA or DA)
(e)	Allocation of responsibility for validation & augmentation			**(e)1. ValidationRequiredBeforeAugmenting:** This constraint indicates whether validation is required before augmenting a signature to an upper level, expressed as a boolean.			
				(e)2. AugmentToLevel: This constraint indicates the level of the signature format to be reached after augmenting a (received) signature.			
(f)	Legal type			**(f)1. ConstraintsOnCertificateMetadata:** This set of constraints indicates requirements on specific certificate metadata. Semantic for a possible set of requirement values used to express such requirements is defined as follows: **(f)1.1. 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; expressed as a boolean. **(f)1.2. LegalPersonSignerAllowed:** This constraint indicates that the subject entity identified in the signer's certificate used in validating the signature is allowed to be a legal person; expressed as a boolean. Constraints defined in annex C may be used to indicate requirements on specific certificate metadata whose semantic applies in the context of the EU legislation.			
(g)	Commitment type			**(g)1. CommitmentTypesRequired:** This set of constraints indicates 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. Semantic for a possible 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; expressed as a boolean. **(g)1.2. MandatedCommitmentTypeValues:** This constraint indicates the required (possible) values for the commitment type to be expressed by the signer. Semantic for a possible set of requirement values used to express such requirements is defined as follows: • **MatchingValuesIndicator:** An indication of the requirement on the way the commitment type value(s) in the signature are matched against the required (possible) commitment type values. This matching values indicator may have the following values: – "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.			

BSP	BSP title	Business statement summary	Technical counterpart statement	Constraint(s)	Constraint value at signature creation (SCA or DA)	Constraint value at signature augmentation (SCA, SVA or DA)	Constraint value at signature validation (SVA or DA)
				• **CommitmentTypeValues:** A non-empty sequence of commitment type identifiers (OIDs or URIs), associated to their multilingual description.			
(h)	LoA on timing evidences			**(h)1. LoAOnTimingEvidences:** This set of constraints indicates the required level of assurance (LoA) on the required timing evidence(s). Semantic for a possible set of requirement values used to express such requirements is defined as follows: **(h)1.1. LoA-on-signing-time:** This constraint indicates the required LoA on the signing time expressed in the corresponding signed qualifying property. **(h)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. **(h)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. **(h)1.4. LoA-on-archival-time-stamp:** This constraint indicates the required LoA on the archival time-stamp expressed in the corresponding unsigned qualifying property. **(h)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. **(h)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.			
(i)	Formalities of signing			**(i)1. WYSIWYSRequired:** This constraint indicates the requirement for having a "what you see is what you sign" environment; expressed as a boolean.			
				(i)2. WYSIWHBSRequired: This constraint indicates the requirement for having a "what you see is what has been signed" environment; expressed as a boolean.			
				(i)3. ProperAdviceAndInformationRequired: This constraint indicates whether it is required providing the user (signer or verifier) with proper advice and information on the signature creation application process and on the legal consequences, as well as a user interface guaranteeing, to the extent possible, a valid legal signature environment; expressed as a boolean.			
				(i)4. UserInterfaceDesignConstraints: This constraint indicates whether it is required designing the user interface to guarantee requirements expressed in clause A.3.2.4.(3) - BSP(i) of the present document; expressed as a boolean.			

BSP	BSP title	Business statement summary	Technical counterpart statement	Constraint(s)	Constraint value at signature creation (SCA or DA)	Constraint value at signature augmentation (SCA, SVA or DA)	Constraint value at signature validation (SVA or DA)
				(i)5. CorrectValidationAndArchivalProcedures: This constraint indicates whether the SCA and SVA are required to provide (e.g. for display) the relying party (including the signer) with correct procedures for the validation and the archival of the signature and the associated validation data; expressed as a tuple made of a Boolean and an optional character string.			
(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.			
(k)	Archival			**(k)1. ArchivalConstraints:** This constraint indicates the requirements with regards to the archival of the signature and the associated validation data.			
(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 associated with a sequence of identifiers expressing constraints on the required attributes of the signer. Such constraints on signer's attributes or roles may cover: • which roles/attributes are mandated; • identification of those roles/attributes that need to be certified or be present within signed assertions; • constraints on the type of roles/attributes; and • constraints on the values of roles/attributes. This constraint may be used to express whether a proof of authority is required and the associated requirements when required.			
				(l)4. NameConstraints: These constraints indicate requirements on the distinguished names for issued certificates (e.g. to signer, CAs, OCSP responders, CRL Issuers, Time-Stamping Units) as defined in IETF RFC 5280 [i.13].			

BSP	BSP title	Business statement summary	Technical counterpart statement	Constraint(s)	Constraint value at signature creation (SCA or DA)	Constraint value at signature augmentation (SCA, SVA or DA)	Constraint value at signature validation (SVA or DA)
(m)	LoA on signer authentication			**(m)1. X509CertificateValidationConstraints:** This set of constraints indicates requirements for use in the certificate path validation process as defined in IETF RFC 5280 [i.13]. 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). Semantic for a possible 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 should be provided in the form of (self-signed) certificates (see clause 6.1.1 of IETF RFC 5280 [i.13] on how to treat such certificates as conveyor of TA information) and a time until when these trust anchors were considered reliable. EXAMPLE: The set of TAs can 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.11]; – Trusted Lists as defined in [i.12]; • **(m)1.2. CertificationPath:** This constraint indicates a certification path required to be used by the SVA for validation of the signature. The certificate path is 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). This constraint can include the path to be considered or indicate the need for considering the path provided in the signature if any. • **(m)1.3. user-initial-policy-set:** This constraint is as described in IETF RFC 5280 clause 6.1.1 item (c) [i.13]. • **(m)1.4. initial-policy-mapping-inhibit:** This constraint is as described in IETF RFC 5280 clause 6.1.1 item (e) [i.13]. • **(m)1.5. initial-explicit-policy:** This constraint is as described in IETF RFC 5280 clause 6.1.1 item (f) [i.13]. • **(m)1.6. initial-any-policy-inhibit:** This constraint is as described in IETF RFC 5280 clause 6.1.1 item (g) [i.13]. • **(m)1.7. initial-permitted-subtrees:** This constraint is as described in IETF RFC 5280 clause 6.1.1 item (h) [i.13]. • **(m)1.8. initial-excluded-subtrees:** This constraint is as described in IETF RFC 5280 clause 6.1.1 item (i) [i.13]. • **(m)1.9. path-length-constraints:** This constraint indicates restrictions on the number of CA certificates in a certification path [i.13]. This may need to define initial values for this or to handle such constraint differently (e.g. ignore it).			

BSP	BSP title	Business statement summary	Technical counterpart statement	Constraint(s)	Constraint value at signature creation (SCA or DA)	Constraint value at signature augmentation (SCA, SVA or DA)	Constraint value at signature validation (SVA or DA)
				• **(m)1.10. policy-constraints:** This constraint indicates requirements for certificate policies referenced in the certificates [i.13]. This may need to define initial values for this or to handle such constraint differently (e.g. ignore it). This should also allow the ability to require a (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).			
				(m)2. RevocationConstraints: This set of constraints indicates requirements applicable when verifying the certificate validity status of the certificates during the certificate path validation process [i.13]. 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). Semantic for a possible 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. Semantic for a possible set of requirement values used to express such requirements is defined as follows: – **clrCheck:** Checks shall be made against current CRLs (or Authority Revocation Lists); – **ocspCheck:** The revocation status shall be checked using OCSP IETF RFC 6960 [i.14]; – **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 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 [i.4]) 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.			

BSP	BSP title	Business statement summary	Technical counterpart statement	Constraint(s)	Constraint value at signature creation (SCA or DA)	Constraint value at signature augmentation (SCA, SVA or DA)	Constraint value at signature validation (SVA or DA)
				(m)3. LoAOnTSPPractices: This constraint indicates the required LoA on the practices implemented by the TSP(s) having issued the certificates to be validated during the certificate path validation process [i.13], i.e. the certificates present in the certificate path of the signer's certificate, and optionally those present in all or some of the other certificate chains validated during the signature validation process.			
(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.13], i.e. the certificates present in the certificate path of the signer's certificate, and optionally those certificates present in all or some of the other certificate chains validated during the signature validation process.			
(o)	Other information to be associated with signatures			**(o)1. MandatedSignedQProperties-signer-location:** This constraint indicates that the signer location is required to be expressed as a signed qualifying property and may additionally express constraints on the value.			
				(o)2. MandatedUnsignedQProperties-signature-policy-extension: This constraint indicates that the signature policy extension is required as an unsigned qualifying property and may additionally express constraints on the values.			
				(o)3. MandatedUnsignedQProperties-signature-policy-inclusion-in-archival-form: This constraint indicates the requirement to include the signature policy document as part of the corresponding unsigned qualifying property.			
(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 augmenting process (e.g. signature, certificates, CRLs, OCSP responses, time-stamps). They will be typically be represented by a list of entries as in table A.3.			
(q)	Technological environment			**(q)1. TechnologicalEnvironmentConstraints:** This constraint indicates the requirements on the technological environment in which signatures are processed.			
Summary of the selected signature format(s) (e.g. [3], [i.8], [i.9], [i.20] to [i.23], [i.25] to [i.28], [i.33] to [i.35]) including details on the format of the signed data, the relative placement of the signature and the signed data (e.g. enveloped, enveloping, detached), the relevance of use of a container to package the signature(s) together with signed data, the specific attributes (signed or unsigned) of the signature, and the expected level of selected signature format.							

Table A.3

(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				

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

This clause shall specify the requirements, derived from the BSPs applicable to each signature covered in the policy, on the output of the signature validation procedure. To this respect, this clause should use the table A.4 per concerned signature.

Table A.4

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

A.4.2.3 Output constraints to be used for generating/augmenting signatures in the context of the identified signature policy

This clause shall specify the requirements, derived from the BSPs applicable to each signature covered in the policy, on the output of the signature creation/augmentation procedure. To this respect, this clause should use table A.5 per concerned signature.

Table A.5

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

A.5 Other business and legal matters

This clause shall describe and specify general business and legal matters that would not fit in the previous clauses while being of importance for the specifications and policy description of signature use in the considered business process scenario, such as:

1) Consent to accept signatures: Indication whether the parties' consent to accept signature is actual or deemed. E.g. consent can be required by the laws of some jurisdictions, and can be revoked on notice to the other party.

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

3) Applicable fees.

4) Financial responsibility.

5) Confidentiality of business information.

6) Privacy of personal information.

7) Intellectual property rights.

8) Representations and warranties.

9) Disclaimers of warranties.

10) Limitations of liability.

11) Indemnities.

12) Term and termination.

13) Individual notices and communications with participants.

14) Amendments.

15) Dispute resolution procedures.

16) Governing law.

17) Compliance with applicable law.

18) Miscellaneous provisions (e.g. entire agreement, assignment, severability, enforcement, force majeure).

19) Other provisions.

NOTE: The scope and description of the above listed matters is similar to the ones described in clause 4.9 of IETF RFC 3647 [i.24] transposed to the context of signature policies and signature policy documents.

A.6 Compliance audit and other assessments

This clause shall indicate:

a) whether signature creation/validation applications claiming compliance with the signature policy document and all or some of the signature policies it covers are required to pass a compliance audit and/or other types of assessments to confirm claimed compliance; and

b) whether determining if one or more separate signature policies are allowed to be subordinated, included in or include a signature policy defined in the signature policy document, requires a compliance audit and/or other types of assessments.

It shall describe and specify accordingly the following:

1) The list of topics covered by the audit/assessment and/or the audit/assessment methodology used to perform the assessment.

2) Frequency of compliance audit or other assessments:

   i) for each subordinate signature policy to be assessed pursuant to a signature policy, or the circumstances that will trigger such an assessment;

   ii) for each application to be assessed pursuant to the signature policy or a compliant (subordinate) signature policy, or the circumstances that will trigger such an assessment.

EXAMPLE 1: 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.

3) The identity and/or qualifications of the personnel performing the audit or other assessment.

4) The relationship between the assessor and the entity being assessed, including the degree of independence of the assessor.

5) Actions taken as a result of deficiencies found during the assessment.

EXAMPLE 2: A temporary suspension of operations until deficiencies are corrected, triggering special investigations or more frequent subsequent compliance assessments, and claims for damages against the assessed entity.

6) 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.

Annex B (normative): Commitment types

The following generic commitment types are defined in the present document:

1) Proof of origin

- Description: It indicates that the signer recognizes to have created, approved and sent the signed data.
- Object identifier: id-cti-ets-proofOfOrigin OBJECT IDENTIFIER ::= { iso(1) member-body(2)us(840) rsadsi(113549) pkcs(1) pkcs-9(9) smime(16) cti(6) 1}
- URI: The URI for this commitment is http://uri.etsi.org/01903/v1.2.2#ProofOfOrigin.

2) Proof of receipt

- Description: It indicates that signer recognizes to have received the content of the signed data.
- Object identifier: id-cti-ets-proofOfReceipt OBJECT IDENTIFIER ::= { iso(1) member-body(2) us(840) rsadsi(113549) pkcs(1) pkcs-9(9) smime(16) cti(6) 2}
- URI: The URI for this commitment is http://uri.etsi.org/01903/v1.2.2#ProofOfReceipt.

3) Proof of delivery

- Description: It indicates that the TSP providing that indication has delivered a signed data in a local store accessible to the recipient of the signed data.
- Object identifier: id-cti-ets-proofOfDelivery OBJECT IDENTIFIER ::= { iso(1) member-body(2) us(840) rsadsi(113549) pkcs(1) pkcs-9(9) smime(16) cti(6) 3}
- URI: The URI for this commitment is http://uri.etsi.org/01903/v1.2.2#ProofOfDelivery.

4) Proof of sender

- Description: It indicates that the entity providing that indication has sent the signed data (but not necessarily created it).
- Object identifier: id-cti-ets-proofOfDelivery OBJECT IDENTIFIER ::= { iso(1) member-body(2) us(840) rsadsi(113549) pkcs(1) pkcs-9(9) smime(16) cti(6) 3}
- URI: The URI for this commitment is http://uri.etsi.org/01903/v1.2.2#ProofOfSender.

5) Proof of approval

- Description: It indicates that the signer has approved the content of the signed data.
- Object identifier: id-cti-ets-proofOfApproval OBJECT IDENTIFIER ::= { iso(1) member-body(2) us(840) rsadsi(113549) pkcs(1) pkcs-9(9) smime(16) cti(6) 5}
- URI: The URI for this commitment is http://uri.etsi.org/01903/v1.2.2#ProofOfApproval.

6) Proof of creation

- Description: It indicates that the signer has created the signed data (but not necessarily approved, nor sent it).
- Object identifier: id-cti-ets-proofOfCreation OBJECT IDENTIFIER ::= { iso(1) member-body(2) us(840) rsadsi(113549) pkcs(1) pkcs-9(9) smime(16) cti(6) 6}
- URI: The URI for this commitment is http://uri.etsi.org/01903/v1.2.2#ProofOfCreation.

Any organization may choose to create its own URIs and OIDs for its own specific purposes commitment types. Any organization may request an object identifier under the etsi-identified organization node or a URI root as detailed on https://portal.etsi.org/PNNS.aspx.

Annex C (normative): Constraints in the context of EU legislation

The following constraints indicates requirements on specific certificate metadata whose semantic applies in the context of the EU legislation:

a) **EUQualifiedCertificateRequired:** 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; expressed as a boolean.

b) **EUQualifiedCertificateSigRequired:** This constraint indicates that the signer's certificate used in validating the signature is required to be a qualified certificate for electronic signature as defined in [i.1]; expressed as a boolean.

c) **EUQualifiedCertificateSealRequired:** This constraint indicates that the signer's certificate used in validating the signature is required to be a qualified certificate for electronic seal as defined in [i.1]; expressed as a boolean.

d) **EUSSCDRequired:** 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 secure signature creation device as defined in [i.1]; expressed as a boolean.

e) **EUAdESigRequired:** This constraint indicates that the signature is required to be an advanced electronic signature as defined in the applicable EU legislation; expressed as a boolean.

f) **EUAdESealRequired:** This constraint indicates that the signature is required to be an advanced electronic seal as defined in [i.1]; expressed as a boolean.

g) **EUQSigCDRequired:** 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 a qualified signature creation device as defined in [i.1]; expressed as a boolean.

h) **EUQSealCDRequired:** 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 a qualified seal creation device as defined in [i.1]; expressed as a boolean.

Annex D (normative): Signature application practices statements

D.1 General requirements

When the policy and security practices requirements applicable to SCA and/or SVA are included explicitly in the signature policy document (see clause A.2), the table of content of this clause shall be as specified in clause D.2 with the numbering of the clauses of the table of content appearing in the signature policy document is obtained by removing the starting "D.".

This clause shall describe a set of rules applicable to the application and/or its environment implementing the creation, the augmentation and/or the validation of signatures.

It shall cover rules with regards to the practices used by the application and its environment to properly implement the generation, augmentation and/or validation of signatures.

EXAMPLE 1: A community of users can 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.

EXAMPLE 2: A signature policy can also refer to an external set of practices statements that describes the practices used by an application or an application provider that generate/validate signatures according to several signature policies defined by several communities of users.

EXAMPLE 3: A signature policy can 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.

This clause shall include, either by reference or explicitly, the set of policy and security practices requirements that the SCA and/or the SVA will have to meet when generating, augmenting and/or validating signatures in compliance with the signature policy document.

D.2 Signature application practices statements

D.2.1 Legal driven policy requirements

This clause 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.

D.2.2 Information security (management system) requirements

This clause 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; and

6) audit trail security.

NOTE: The above controls are mainly addressing service providers integrating SCA/SVA components. These latter can implement information security based on ISO/IEC 27001 [i.6] and ISO/IEC /27002 [i.7].

D.2.3 Signature Creation and Signature Validation processes requirements

This clause 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 and access control management;
   g) DTBS preparation;
   h) DTBS representation;
   i) signature creation device management;
   j) protection of the communication between signature creation device and SCA;
   k) robustness of signature cryptographic suites;
   l) community adaptability; and
   m) bulk signing operation.
2) signature validation process and systems; and in particular:
   a) validation process rules enforcement;
   b) validation user interface;
   c) appropriate format of the signature;
   d) lifetime of the signature; and
   e) validation input/output relative conformance (i.e. correctness of the implemented validation procedure).

D.2.4 Development & coding policy requirements

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

1) the secure development methods; and
2) testing compliance and interoperability.

D.2.5 General requirements

This clause 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.

History

Document history		
V1.1.1	July 2015	Publication