



**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

Important noticeThe present document can be downloaded from:
<http://www.etsi.org/standards-search>

The present document may be made available in electronic versions and/or in print. The content of any electronic and/or print versions of the present document shall not be modified without the prior written authorization of ETSI. In case of any existing or perceived difference in contents between such versions and/or in print, the only prevailing document is the print of the Portable Document Format (PDF) version kept on a specific network drive within ETSI Secretariat.

Users of the present document should be aware that the document may be subject to revision or change of status. Information on the current status of this and other ETSI documents is available at
<http://portal.etsi.org/tb/status/status.asp>

If you find errors in the present document, please send your comment to one of the following services:
<https://portal.etsi.org/People/CommitteeSupportStaff.aspx>

Copyright Notification

No part may be reproduced or utilized in any form or by any means, electronic or mechanical, including photocopying and microfilm except as authorized by written permission of ETSI.

The content of the PDF version shall not be modified without the written authorization of ETSI.
The copyright and the foregoing restriction extend to reproduction in all media.

© European Telecommunications Standards Institute 2015.
All rights reserved.

DECT™, **PLUGTESTS™**, **UMTS™** and the ETSI logo are Trade Marks of ETSI registered for the benefit of its Members.
3GPP™ and **LTE™** are Trade Marks of ETSI registered for the benefit of its Members and of the 3GPP Organizational Partners.
GSM® and the GSM logo are Trade Marks registered and owned by the GSM Association.

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".