



**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

---

Keywordselectronic 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 notice***

The 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
<b>A.4</b>	<b>Requirements / statements on technical mechanisms and standards implementation.....</b>	<b>23</b>
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
<b>A.5</b>	<b>Other business and legal matters .....</b>	<b>38</b>
<b>A.6</b>	<b>Compliance audit and other assessments .....</b>	<b>39</b>
<b>Annex B (normative):</b>	<b>Commitment types.....</b>	<b>40</b>
<b>Annex C (normative):</b>	<b>Constraints in the context of EU legislation .....</b>	<b>41</b>
<b>Annex D (normative):</b>	<b>Signature application practices statements .....</b>	<b>42</b>
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	