



Electronic Signatures and Infrastructures (ESI); The framework for standardization of signatures: overview

Reference

DTR/ESI-0019000

Keywordse-commerce, electronic signature, security, 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 | 4 |
| Foreword..... | 4 |
| Modal verbs terminology..... | 4 |
| Introduction | 4 |
| 1 Scope | 6 |
| 2 References | 6 |
| 2.1 Normative references | 6 |
| 2.2 Informative references..... | 6 |
| 3 Definitions and abbreviations..... | 8 |
| 3.1 Definitions..... | 8 |
| 3.2 Abbreviations | 8 |
| 4 General framework for standardization related to digital signatures | 8 |
| 4.1 Introduction | 8 |
| 4.1.1 Objectives | 8 |
| 4.1.2 Approach | 8 |
| 4.2 Classification scheme for digital signature standards..... | 9 |
| 4.2.1 Functional areas | 9 |
| 4.2.2 Document types | 10 |
| 4.2.3 Structure with sub-areas..... | 11 |
| 4.2.4 Numbering scheme | 11 |
| 4.2.5 Possible extension of classification scheme to incorporate identification and authentication related standards | 12 |
| 4.2.6 Guidance documents addressing the framework functional areas | 12 |
| 4.3 The framework by area..... | 14 |
| 4.3.0 Foreword..... | 14 |
| 4.3.1 Introductory documents | 15 |
| 4.3.2 Signature creation & validation | 16 |
| 4.3.3 Signature creation and other related devices..... | 23 |
| 4.3.4 Cryptographic suites | 26 |
| 4.3.5 TSPs supporting digital signatures and related services | 27 |
| 4.3.6 Trust application service providers..... | 30 |
| 4.3.7 Trust service status lists providers | 33 |
| Annex A: TSP and CSP Concept..... | 35 |
| Annex B: Bibliography | 36 |
| History | 37 |

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 Report (TR) has been produced by ETSI Technical Committee Electronic Signatures and Infrastructures (ESI).

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

As a response to the adoption of Directive 1999/93/EC [i.1] on a Community framework for electronic signatures (eSignature Directive) in 1999, and in order to facilitate the use and the interoperability of eSignature based solution, the European Electronic Signature Standardization Initiative (EESSI) was set up to coordinate the European standardization organizations CEN and ETSI in developing a number of standards for eSignature products and services.

Commission Decision 2003/511/EC [i.2], on generally recognized standards for electronic signature products, was adopted by the Commission following the results of the EESSI. This decision was aimed to foster the use of electronic signature by publishing "generally recognized standards" for electronic signature products in compliance with article 3(5) of the Directive. However, by referencing only two standards (respectively on security requirements for trustworthy systems managing certificates for electronic signatures and secure signature creation devices), it had a limited impact on the mapping of the European standardization on eSignatures (which covers many more documents and topics, including ancillary services to eSignature) and the legal provisions and requirements laid down in Directive 1999/93/EC [i.1].

Emerging cross-border use of eSignatures and the increasing use of several market instruments (e.g. Services Directive [i.3], Public Procurement [i.4] and [i.5], eInvoicing [i.6]) that rely in their functioning on eSignatures and the framework set by the eSignature Directive emphasized problems with the mutual recognition and cross-border interoperability of eSignature.

Intending to address the legal, technical and standardization related causes of these problems, the Commission launched a study on the standardization aspects of eSignature [i.7] which concluded that the multiplicity of standardization deliverables together with the lack of usage guidelines, the difficulty of access and lack of business orientation is detrimental to the interoperability of eSignatures, and formulated a number of recommendations to mitigate this. Also due to the fact that many of the documents have yet to be progressed to full European Standards (ENs), their status may be considered to be uncertain. The Commission also launched the CROBIES study [i.8] to investigate solutions addressing some specific issues regarding profiles of secure signature creation devices, supervision practices as well as common formats for trusted lists, qualified certificates and eSignatures.

In line with Standardization Mandate 460 [i.9], consequently issued by the Commission to CEN, CENELEC and ETSI for updating the existing eSignature standardization deliverables, CEN and ETSI have set up the eSignature Coordination Group in order to coordinate the activities achieved for Mandate 460.