ETSI TR 119 100 V1.1.1 (2016-03)

TECHNICAL REPORT

Electronic Signatures and Infrastructures (ESI); Guidance on the use of standards for signature creation and validation

Reference

DTR/ESI-0019100

Keywords

e-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
https://portal.etsi.org/TB/ETSIDeliverableStatus.aspx

If you find errors in the present document, please send your comment to one of the following services:
https://portal.etsi.org/People/CommiteeSupportStaff.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 2016.
All rights reserved.

DECTTM, **PLUGTESTS**TM, **UMTS**TM and the ETSI logo are Trade Marks of ETSI registered for the benefit of its Members.
3GPPTM 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 6

Foreword 6

Modal verbs terminology 6

Introduction 6

1 Scope 7

2 References 7
2.1 Normative references 7
2.2 Informative references 7

3 Definitions and abbreviations 10
3.1 Definitions 10
3.2 Abbreviations 12

4 Introduction to the guided implementation process 13
4.1 How to use the present document 13
4.2 An overview of the guided implementation process 13

5 Analysing the Business Requirements 16

6 Managing the policy and security requirements 17

7 Business scoping parameters 17
7.1 Introduction 17
7.2 Business scoping parameters mainly related with the business process 18
7.2.1 Introduction 18
7.2.2 BSP (a): Workflow (sequencing and timing) of digital signatures 18
7.2.2.1 Introduction 18
7.2.2.2 Multiple signatures 18
7.2.2.3 Timing and sequencing 19
7.2.3 BSP (b): Data Object(s) to be signed 20
7.2.4 BSP (c): Relationships of signatures with signed data object(s) and signature(s) 20
7.2.5 BSP (d): Targeted community 21
7.2.6 BSP (e): Allocation of responsibility of signatures validation and augmentation 21
7.3 Business scoping parameters mainly influenced by legal/regulatory framework where the business process is conducted 21
7.3.1 Introduction 21
7.3.2 BSP (f): Legal Effect of the signatures 21
7.3.3 BSP (g): Commitment assumed by signer 22
7.3.4 BSP (h): Level of assurance of timing evidences 23
7.3.5 BSP (i): Formalities of signing 23
7.3.6 BSP (j): Longevity and resilience to change 24
7.3.7 BSP (k): Archival 24
7.4 Business scoping parameters mainly related to the actors involved in generating the signature 24
7.4.1 BSP (l): Identity (and roles/attributes) of the signer 24
7.4.2 BSP (m): Level of assurance required for the authentication of the signer 25
7.4.3 BSP (n): Signature creation devices 25
7.5 Other Business scoping parameters 25
7.5.1 Introduction 25
7.5.2 BSP (o): Other information to be included within the signatures 25
7.5.3 BSP (p): Cryptographic suites 26
7.5.4 BSP (q): Technological environment 26

8 Selecting the most appropriate standards, options, and technical mechanisms 26
8.1 Introduction 26
8.2 Format of signatures: CAdES, XAdES or PAdES 27
8.2.1 Introduction 27
8.2.2 Format of the document 27
8.2.3 Relative placement of signatures and signed data objects 28

8.2.3.1 Introduction 28
8.2.3.2 Enveloped signatures 28
8.2.3.3 Enveloping signatures 28
8.2.3.4 Detached signatures 29
8.2.3.5 Simultaneous multiple relative positions 29
8.2.4 Number of signatures and signed data objects 29
8.2.4.1 Introduction 29
8.2.4.2 One document is signed by only one signature 29
8.2.4.3 One document is signed by more than one signature 29
8.2.4.4 One signature is required to sign more than one data object 30
8.3 A container for packaging together signatures and detached signed data objects 30
8.4 Baseline or extended/additional? 31
8.5 Selecting the proper quality of the signature 31
8.6 Mapping formalities of signing to the electronic domain 32
8.7 Satisfying timing and sequencing requirements 32
8.7.1 Satisfying sequencing requirements 32
8.7.1.1 Introduction 32
8.7.1.2 Including counter-signatures 32
8.7.2 Satisfying timing requirements 33
8.7.2.1 Introduction 33
8.7.2.2 Time-stamping the data objects to be signed before signature generation 33
8.7.2.3 Including claimed signing time 33
8.7.2.4 Including time-stamp token on the digital signature value 34
8.8 Including indication of commitments assumed by the signer 35
8.9 Including and protecting indication of signer's identity, signer's roles and/or attributes 36
8.9.1 Including and protecting indication of signer's identity 36
8.9.2 Including signer's roles and/or attributes 37
8.10 Including additional signed information 38
8.10.1 Introduction 38
8.10.2 Including explicit indication of the signature policy 38
8.10.3 Including indication of the signed data object format 39
8.10.4 Including indication of the signature production place 40
8.11 Supporting signatures lifecycle 40
8.11.1 Introduction 40
8.11.2 Including time-stamp tokens on the digital signature value 40
8.11.3 Including references to validation data 41
8.11.3.1 Rationale 41
8.11.3.2 Including references to certificates 42
8.11.3.3 Including references to certificate status data 42
8.11.4 Time-stamping references to validation data 43
8.11.5 Enlarging longevity and resilience to change 44
8.11.5.1 Introduction 44
8.11.5.2 Incorporating containers for validation material 46
8.11.5.3 Incorporating time-stamp tokens for long term availability and integrity of the validation material 47
8.11.6 Digital signatures lifecycle 49
8.11.6.1 Generation, validation and augmentation of digital signatures. 49
8.11.6.2 Lifecycle and levels of digital signatures 55
8.11.6.3 Transitions between levels of baseline signatures and containers 60
8.11.6.4 Transitions between levels of extended signatures 61
8.11.7 ASiC containers lifecycle 65
8.12 Selecting proper Signature Creation Devices 73
8.13 Selecting proper cryptographic suites 74
8.14 Signature generation, augmentation and validation applications 74
8.14.1 Introduction 74
8.14.2 Selecting the suitable Protection Profile 74
8.14.3 Implementing the signature generation and augmentation processes 74
8.14.4 Implementing the signature validation process 75

9 Signature creation and validation catalysing toolkit 77
9.1 Introduction 77
9.2 Technical Specifications 77

9.3 Conformance testing software tools 78
9.4 Interoperability test events 78

10 Evaluation processes 79

11 Corollary: the process within the context of the Standardization Framework 80

Annex A: Securing signed detached objects in XAdES signatures in the long term 81

A.1 Introduction 81

A.2 Securing detached objects signed with `ds:SignedInfo` 81

A.3 Detached objects signed with signed `ds:Manifest` 81
A.3.1 The initial situation 81
A.3.2 The problem: detached data objects signed through ds:Manifest and their resilience to digest algorithm break 83
A.3.3 The solution: `xadesv141:RenewedDigests` element 85

Annex B: Bibliography 88

History 89

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 (https://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

ETSI TR 119 000 [i.1]: "The framework for standardization of signatures: overview", describes the structure of a general framework for digital signatures standardization (hereinafter denoted as Rationalized Framework or Framework) outlining existing and potential standards related to the implementation of digital signatures and the provision of related trust services by trust service providers. This framework identifies six areas of standardization with a list of existing and potential future standards in each area.

ETSI TR 119 000 [i.1] includes a set of guidance documents to assist business stakeholders, users and their suppliers in mapping or deriving from their business driven requirements the appropriate selection of digital signature standards and their options. Each guide addresses a particular area as identified in the aforementioned Rationalized Framework. A complete solution will need to address requirements in most of these areas.

This series is based on the selection of the business scoping parameters for each area of standardization. The selection of these scoping parameters is based on a process involving an analysis of the business requirements and associated risks leading to an identification of the policy and security requirements and to an analysis of the resulting business scoping parameters from which the appropriate standards and options can be selected. From the requirements expressed in terms of business scoping parameters for an area, each guidance document provides assistance in selecting the appropriate standards and their options for that area. Where standards and their options within one area make use of another area this is stated in terms of scoping parameters of that other area.

This general process of the selection of standards and options is described further in ETSI TR 119 000 [i.1], clause 4.2.6.

1 Scope

The present document, which addresses area 1 of the Framework [i.1], provides a **business driven guided process for implementing generation and validation of digital signatures in business' electronic processes**. Starting from a business analysis and risk analysis of the business' electronic processes, stakeholders are guided for making the best choice among the wide offer of standards in order to ensure the best implementation of digital signatures within the addressed application/business electronic processes.

The target audience includes enterprise/business process architects, application architects, application developers, and signature policy issuers.

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 referenced document (including any amendments) applies.

Referenced documents which are not found to be publicly available in the expected location might be found at https://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.

Not applicable.

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 referenced 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] ETSI TR 119 000: "Electronic Signatures and Infrastructures (ESI); The framework for standardization of signatures: overview".

[i.2] ETSI EN 319 122-1: "Electronic Signatures and Infrastructures (ESI); CAdES digital signatures; Part 1: Building blocks and CAdES baseline signatures".

[i.3] ETSI EN 319 122-2: "Electronic Signatures and Infrastructures (ESI); CAdES digital signatures; Part 2: Extended CAdES signatures".

[i.4] ETSI EN 319 132-1: "Electronic Signatures and Infrastructures (ESI); XAdES digital signatures; Part 1: Building blocks and XAdES baseline signatures".

[i.5] ETSI EN 319 132-2: "Electronic Signatures and Infrastructures (ESI); XAdES digital signatures; Part 2: Extended XAdES signatures".

[i.6] ETSI EN 319 142-1: "Electronic Signatures and Infrastructures (ESI); PAdES digital signatures; Part 1: Building blocks and PAdES baseline signatures".

[i.7] ETSI EN 319 142-2: "Electronic Signatures and Infrastructures (ESI); PAdES digital signatures; Part 2: Additional PAdES signatures profiles".