ETSI TS 119 101 V1.1.1 (2016-03)

TECHNICAL SPECIFICATION

Electronic Signatures and Infrastructures (ESI); Policy and security requirements for applications for signature creation and signature validation

Reference

DTS/ESI-0019101

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

Copyright Notification

Contents

Intellectual Property Rights 5
Foreword 5
Modal verbs terminology 5
Introduction 5
1 Scope 6
2 References 6
2.1 Normative references 6
2.2 Informative references 7
3 Definitions and abbreviations 8
3.1 Definitions 8
3.2 Abbreviations 10
4 Signature creation/validation/augmentation model 10
5 General requirements 13
5.1 User interface 13
5.2 General security measures 14
5.3 System completeness requirements 15
6 Legal driven policy requirements 15
6.1 Introduction 15
6.2 Processing of personal data 15
6.3 Accessibility for persons with disabilities 16
7 Information security (management system) requirements 16
7.1 Introduction 16
7.2 Network protection 16
7.3 Information systems protection 16
7.4 Software integrity of the application 17
7.5 Data storage security 17
7.6 Event logs 18
8 Signature creation, validation and augmentation processing requirements 18
8.1 Signature creation process and systems 18
8.1.1 General 18
8.1.2 Main functionalities requirements 18
8.1.3 Data content type requirements 19
8.1.4 Signature attribute requirements 21
8.1.5 Time and sequence 23
8.1.6 Signature invocation requirements 23
8.1.7 Cryptographic algorithm choice 24
8.1.8 Signer's authentication requirements 25
8.1.8.1 General requirements 25
8.1.8.2 Requirements for biometric authentication methods 26
8.1.9 DTBS preparation requirements 27
8.1.10 DTBSR preparation 27
8.1.11 Signature creation device 27
8.1.12 SCDev/SCA interface (SSI) requirements 28
8.1.13 Bulk signing requirements 28
8.2 Signature validation process 28
8.2.1 Introduction 28
8.2.2 Main functionalities requirements 29
8.2.3 Validation process rules 29
8.2.4 Validation policy 30
8.2.5 Validation user interface 30
8.2.6 Validation inputs and outputs 31
8.3 Signature augmentation process 32

8.3.1 Introduction....32
8.3.2 The three use cases....32
8.3.2.1 Signature augmentation process used by a SCA....32
8.3.2.2 Signature augmentation process used by a SVA....32
8.3.2.3 Independent signature augmentation process....32
8.3.3 Main functionalities requirements....33
8.3.4 Augmentation procedures....33
8.3.5 Data inclusion....33
8.3.6 Validation of the input signature to the augmentation process....33

9 Development and coding policy requirements....34
9.1 Secure development methods and application security....34
9.2 Testing conformance requirements....34

10 Signature application practice statement....35

Annex A (normative): Table of content for signature application practice statement....37

A.0 The right to copy....37

A.1 Introduction....37
A.1.1 Overview....37
A.1.2 Business or application domain....37
A.1.2.1 Scope and boundaries of SAPS....37
A.1.2.2 Domain of applications....37
A.1.2.3 Transactional context....37
A.1.3 SAPS distribution points....37
A.1.4 SAPS issuer....38
A.1.5 SAPS administration....38
A.1.5.1 Organization administering the document....38
A.1.5.2 Contact person....38
A.1.6 Definitions and acronyms....38

A.2 Signature creation/augmentation/validation application practice statements....38
A.2.1 General requirements....38
A.2.2 Legal driven policy requirements....39
A.2.3 Information security (management system) requirements....39
A.2.4 Signature creation, signature validation and signature augmentation processes requirements....39
A.2.5 Development and coding policy requirements....40

Annex B (informative): Bibliography....41

History....42

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 Specification (TS) 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

Several aspects are important to ensure trust in digital signatures. Their successful implementation in electronic processes requires standards for related services, processes, systems and products as well as guidance for conformity assessment of such services, processes, systems and products.

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".

The different players and the environment of the signature creation, validation and augmentation follow rules to allow them to be trusted. The present document concentrates on policy and security requirements to consider when creating, validating and augmenting signature in a trustworthy manner, in particular within the context of applications for signature creation, signature validation and signature augmentation.

1 Scope

The present document provides general security and policy requirements for applications for signature creation, validation and augmentation.

The present document is primarily relevant to the following actors:

- Implementers and providers of applications for signature creation, signature validation and/or signature augmentation, who need to ensure that relevant requirements are covered.
- Actors that integrate applications for signature creation, signature validation and/or signature augmentation components with business process software (or use standalone software), who want to ensure proper functioning of the overall signature creation/validation/augmentation process and that the signature creation/validation is done in a sufficiently secure environment.

The present document is applicable to these actors, and their evaluators (for a self-evaluation or an evaluation by a third party) to have a list of criteria against which to check the implementation.

The requirements cover applications for signature creation, signature validation and/or signature augmentation, i.e. the implementation and provision of the Signature Creation/Validation/Augmentation Application modules (SCA/SVA/SAA), the driving application (DA), the communication between the SCA and the signature creation device (SCDev) and the environment in which the SCA/SVA/SAA is used. It also specifies user interface requirements, while the user interface can be part of the SCA/SVA/SAA or of the DA which calls the SCA/SVA/SAA. Any entity using SCA/SVA/SAA components in its business process acts as driving application.

The document covers:

- Legal driven policy requirements.
- Information security (management system) requirements.
- Signature creation, signature validation and signature augmentation processes requirements.
- Development and coding policy requirements.
- General requirements.

Protection Profiles (PP) for signature creation applications and signature validation applications are out of scope and are defined in the CEN standard "Protection Profiles for Signature Creation & Validation Applications" [i.9].

General requirements for trust service providers are provided in ETSI EN 319 401 [i.24]. Requirements for trust service providers providing signature creation or validation services are out of scope. Requirements on trust service providers providing signature creation services are to be defined in ETSI TS 119 431 [i.22], with CEN EN 419 241 [i.21] defining requirements for a remote signature creation device. Requirements on trust service providers providing signature validation services are to be defined in ETSI TS 119 441 [i.23].

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.