ETSI SR 019 020 V1.1.2 (2016-08)

SPECIAL REPORT

The framework for standardization of signatures; Standards for AdES digital signatures in mobile and distributed environments

Reference

RSR/ESI-0019020v112

Keywords

e-commerce, electronic signature, mobile,
security

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

Contents

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

Modal verbs terminology

In the present document "**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

Electronic commerce has emerged as a common way of doing business. Trust in this way of doing business is essential for the success and continued development of electronic commerce. It is, therefore, important that companies using electronic means of doing business have suitable security controls and mechanisms in place to protect their transactions and to ensure trust and confidence with their business partners. In this respect the digital signature is an important security component that can be used to protect information and provide trust in electronic business.

ETSI EN 319 102-1 [i.19] defines processes for creation and validation of AdES digital signatures such as specified in ETSI EN 319 122 [i.2], ETSI EN 319 132 [i.3], ETSI EN 319 142 [i.4] or ETSI EN 319 162 [i.6]. Most standards for such digital signatures implicitly assume that all steps of these processes are carried out in one IT-system, e.g. by use of a signing device interfaced to a personal computer system local to the user. However, market solutions exist for digital signature creation and validation supported by remote systems accessed through a mobile or conventional network; the process steps devised by ETSI EN 319 102-1 [i.19] are partly carried out locally to the user and partly by these remote systems. In particular, such server-assisted signing/validation is used with mobile, and other personal devices that increasingly contribute to many aspects of the users' everyday life.

ETSI has previously published a set of standards for mobile commerce (M-COMM [i.9], [i.10], [i.11] and [i.12]) supporting digital signatures created on a personal device supported by remote networked services and communicating over mobile networks. Moreover, OASIS has developed the standard DSS (Digital Signature Standard [i.8], [i.30], [i.33] and [i.34]) for use of remote digital signature services, and this is applicable for use from mobile or other personal computing devices.

The present document considers scenarios for server-assisted signing/validation, in mobile and other distributed computing environments, based on a number of solutions available in the market. The report identifies requirements for further standardization, building on the existing M-COMM and OASIS DSS standards, considering both requirements for security assurance as well as interoperability. For security assurance, standards such as CEN TS 419 241 [i.15] is also considered.

The present document particularly considers standardization requirements for scenarios involving assistance of remote services supporting:

a) Local signing use cases where the signing key is held with the signer's personal device;

b) Server signing use cases where the signing key is held in a shared server;

c) Validation of signatures where the digital signature is verified supported by a remote server.

Where all the signing / signature functionality is carried out within a personal device and does not require any assistance of remote servers then existing standards for signing are considered appropriate and hence such cases are not considered in the present document. As it is considered that many of the cases described in the present document are similar to use of other personal devices such as laptop and personal computers the analysis takes into account the possibility of applying the same standard to any personal device not just mobile devices.

1 Scope

The present document provides a framework for further standardization for the creation and validation of AdES digital signatures, such as specified in ETSI EN 319 122 [i.2], ETSI EN 319 132 [i.3], ETSI EN 319 142 [i.4] or ETSI EN 319 162 [i.6], in mobile and distributed environments assisted by remote servers. The present document takes into account that the capabilities of personal devices will continue to evolve and is likely to increasingly overlap with the capabilities of other computing devices. The present document identifies the recommended scope of such standards and any suggested provision thought appropriate to these standards.

The standards framework in the present document is based on an analysis of scenarios commonly known to be in use or of potential interest. A classification scheme based on that used in ETSI TR 119 000 [i.1] is used to classify the standardization requirements based on the analysis of common scenarios.

The present document does not address standardization for mobile environments where the whole signature creation and/or validation process is carried out within the personal device. Whilst considered important to the market, this generally does not involve external interfaces which require further standardization beyond that already supported using existing standards within ETSI TR 119 000 [i.1].

The present document does not directly address specific requirements for mobile access to other supporting trust services such as time-stamping, revocation status or directory services as it is considered that these would either be addressed by signature creation or validation services, or that a personal device has the capabilities to address these services directly by use of existing standards within ETSI TR 119 000 [i.1].

The present document particularly considers standardization requirements for scenarios involving assistance of remote services supporting:

a) Local signing use cases where the signing key is held with the signer's personal device.

b) Server signing use cases where the signing key is held in a shared server.

c) Validation of signatures where the digital signature is verified supported by a remote server.

The present document does not include an analysis of the security risks nor identification of specific security requirements for AdES digital signatures in mobile and distributed environments; security requirements are addressed in CEN TS 419 241 [i.15]. It rather addresses the requirements for standards supporting the distribution of the functionality related to creation and validation of AdES digital signature between distributed system elements.

The present document is limited to AdES digital signatures supported by PKI and public key certificates, including use of secure signing devices such as qualified electronic signature (and seal) creation devices as defined in Regulation (EU) No 910/2014 [i.5], and aims to meet the general requirements of the international community to provide trust and confidence in electronic transactions, including, amongst other, applicable requirements from Regulation (EU) No 910/2014 [i.5].Whilst scenarios may be applicable to electronic seals, the present document concentrates on the use of services in support of digital signatures for natural persons or natural persons associated with legal persons.

The present document takes into account existing standards and publicly available specifications in the current framework for digital signature standardization ETSI TR 119 000 [i.1].

2 References

2.1 Normative references

Normative references are not applicable in the present document.

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.

Referenced documents which are not found to be publicly available in the expected location might be found at http://docbox.etsi.org/Reference.

NOTE 1: 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.

NOTE 2: ETSI and CEN documents referenced below may not be published at the time of publication of the present document.

[i.1] ETSI TR 119 000: "Electronic Signatures and Infrastructures (ESI); Rationalized structure for Electronic Signature Standardization".

[i.2] ETSI EN 319 122 (all parts): "Electronic Signatures and Infrastructures (ESI); CAdES digital signatures".

[i.3] ETSI EN 319 132 (all parts): "Electronic Signatures and Infrastructures (ESI); XAdES digital signatures".

[i.4] ETSI EN 319 142 (all parts): "Electronic Signatures and Infrastructures (ESI); PAdES digital signatures".

[i.5] Regulation (EU) No 910/2014 of the European Parliament and of the Council of 23 July 2014 on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC.

[i.6] ETSI EN 319 162: "Electronic Signatures and Infrastructures (ESI); Associated Signature Containers (ASiC)".

[i.7] Gene Itkis: "Forward Security; Adaptive Cryptography: Time Evolution" in Handbook of Information Security; Threats, Vulnerabilities, Prevention, Detection, and Management, Volume 3, John Wiley & Sons, 2006.

NOTE: Available at http://www.cs.bu.edu/~itkis/pap/forward-secure-survey.pdf.

[i.8] OASIS Digital Signature Service Core Protocols, Elements, and Bindings Version 1.0, 11th April 2007.

[i.9] ETSI TR 102 203: "Mobile Commerce (M-COMM); Mobile Signatures; Business and Functional Requirements".

[i.10] ETSI TS 102 204: "Mobile Commerce (M-COMM); Mobile Signature Service; Web Service Interface".

[i.11] ETSI TR 102 206: "Mobile Commerce (M-COMM); Mobile Signature Service; Security Framework".

[i.12] ETSI TS 102 207: "Mobile Commerce (M-COMM); Mobile Signature Service; Specifications for Roaming in Mobile Signature Services".

[i.13] CEN EN 419 211: "Protection Profiles for Secure Signature Creation Device".

[i.14] CEN EN 419 221: "Protection Profiles for TSP Cryptographic Modules".

[i.15] CEN TS 419 241: "Security Requirements for Trustworthy Systems supporting Server Signing".

[i.16] ETSI TS 119 312: "Electronic Signatures and Infrastructures (ESI); Cryptographic Suites".

[i.17] ETSI EN 319 401: "Electronic Signatures and Infrastructures (ESI); General Policy Requirements for Trust Service Providers".

[i.18] ETSI EN 319 403: "Electronic Signatures and Infrastructures (ESI); Trust Service Provider Conformity Assessment - Requirements for conformity assessment bodies assessing Trust Service Providers".

[i.19] ETSI EN 319 102-1: "Electronic Signatures and Infrastructures (ESI); Procedures for Creation and Validation of AdES Digital Signatures; Part 1: Creation and Validation".

[i.20] ETSI TS 133 221: "Digital cellular telecommunications system (Phase 2+); Universal Mobile Telecommunications System (UMTS); LTE; eneric Authentication Architecture (GAA); Support for subscriber certificates (3GPP TS 33.221 version 13.0.0 Release 13)".

[i.21] CEN TR 419 010: "The framework for standardization of signatures: Extended structure including electronic identification and authentication".

[i.22] GlobalPlatform Device Technology - TEE System Architecture, Version 1.0, December 2011.

[i.23] W3C XML Key Management Specification (XKMS 2.0).

[i.24] IETF RFC 3029: "Internet X.509 Public Key Infrastructure Data Validation and Certification Server Protocols".

[i.25] IETF RFC 5055: "Server-Based Certificate Validation Protocol".

[i.26] ISO/IEC 24760-1:2011: "Information Technology - Security Techniques - A framework for identity management - Part 1: Terminology and concepts".

[i.27] ETSI TR 119 001: "Electronic Signatures and Infrastructures (ESI); The framework for standardization of signatures; Definitions and abbreviations".

[i.28] ETSI TS 119 612: " Electronic Signatures and Infrastructures (ESI); Trusted Lists".

[i.29] ISO/IEC 15408 parts 1 to 3: "Information technology - Security techniques - Evaluation criteria for IT security".

[i.30] Advanced Electronic Signature Profiles of the OASIS Digital Signature Services Version 1.0, 11th April 2007.

[i.31] Asynchronous Processing Abstract Profile of the OASIS Digital Signature Services Version 1.0, 11th April 2007.

[i.32] Visible Signature Profile of the OASIS Digital Signature Services Version 1.0, 8th May 2010.

[i.33] DSS Extension for Local Signature Computation Version 1.0, 27th July 2015.

[i.34] OASIS DSS v1.0 Profile for Comprehensive Multi-Signature Verification Reports Version 1.0, 12th November 2010.

[i.35] ETSI EN 319 102-2: "Elecrtonic Signatures and Infrastructures (ESI); Procedures for creation and validation of AdES digital signatures; Part 2: signature validation report".

[i.36] ETSI TS 119 152: "Electronic Signatures and Infrastructures (ESI); Architecture for AdES digital signatures in distributed environments".

[i.37] ETSI TS 119 432 (all parts): "Electronic Signatures and Infrastructures (ESI); Protocol profiles for trust service providers providing AdES digital signature generation services".

[i.38] ETSI TS 119 431: "Electronic Signatures and Infrastructures (ESI); Policy and security requirements for trust service providers providing AdES digital signature generation services".

[i.39] ETSI TS 119 441: "Electronic Signatures and Infrastructures (ESI); Policy and security requirements for trust service providers providing AdES digital signature validation services".

[i.40] ETSI TS 119 442: "Electronic Signatures and Infrastructures (ESI); Protocol profiles for trust service providers providing AdES digital signature validation services".

[i.41] ETSI TS 119 101: "Electronic Signatures and Infrastructures (ESI); Policy and Security Requirements for Electronic Signature Creation and Validation".

[i.42] CEN EN 419 212 (all parts): "Application Interface for smart cards used as Secure Signature Creation Devices".

3 Definitions and abbreviations

3.1 Definitions

For the purposes of the present document, the terms and definitions given in ETSI TR 119 001 [i.27] and the following apply:

AdES digital signature: digital signature format compliant with one of the CAdES [i.2], XAdES [i.3], PAdES [i.4] format specifications

application provider: provider of a system, other than the personal device, which prepares document or other information which is required to be signed, for example as part of a work flow

NOTE: This can include a personal computer, a networked application service or service provided by a mobile operator. The application provider can prepare the request for a signature on behalf of a personal device.

communications network: mobile network or a fixed network which supports communications from personal devices to networked services

Identity Provider (IdP): entity that makes available identity information

NOTE: See ISO/IEC 24760-1 [i.26].

mobile device: personal device which can communicate over a mobile network, usually a device suitable for carrying in hand, purse or pocket such as a mobile or smart phone

mobile network: communications network operated specifically for mobile devices, usually requiring the mobile devices to incorporate a UICC in order to communicate

Mobile Network Operator (MNO): entity which offers mobile network services

mobile signature service: facility that coordinates and manages the process by which an end user can sign a document, or other information, using a signing key on or connected to a personal device

NOTE: This service supports local signing only.

Mobile Signature Service Provider (MSSP): provider of a mobile signature service

personal device: a networked device that is assumed to be under the sole control of a natural person at the time of signing/validation

NOTE: The term personal device includes mobile devices as well as other general computing devices such as personal computers, tablets and laptops.

Secure Element (SE): tamper resistant component used in a personal device to provide security, confidentiality, and multiple application environments required to support various business models

NOTE 1: Examples of SE technologies currently used for mobile devices are UICC (also known as SIM card), embedded SE, smartSD, smart microSD. An external, secure device, such as a smart card, can also be used with a personal device to support local signing.

NOTE 2: An SE can be a qualified electronic signature or seal creation device as specified in Regulation (EU) No 910/2014 [i.5] if meets the requirements of this regulation.

signer: entity identified as the creator of a signature

signing service: facility that coordinates and manages the process by which an end user, by use of a personal device, can remotely sign a document, or other information, using a signing key stored in the signing service remote from the user

Signing Service Provider (SSP): provider of a signing service

Trusted Execution Environment (TEE): specific execution environment on the mobile or personal device that consists of software and possibly hardware to define a boundary between an internal secure and an external unsecure (operating system) execution environment

NOTE: See GlobalPlatform Device Technology - TEE System Architecture [i.22].

Trusted Service Manager (TSM): trusted logical component that implements one or more service management roles related to the provisioning, the life cycle management and the deletion of a mobile service

NOTE: The TSM can be integrated with a mobile signature service or a signing service or can be provided by an independent party.

validation service: system accessible via a communication network, which validates a digital signature

3.2 Abbreviations

For the purposes of the present document, the following abbreviations apply:

AE	Acquiring Entity
ASiC	Associated Signature Container
CMS	Cryptographic Message Syntax
DSS	Digital Signature Service
DSS-X	OASIS Digital Signature Services-eXtended
GAA	3GPP Generic Authentication Architecture
GSM	Global System for Mobile communications
HMSSP	Home MSSP
IdP	Identity Provider
M-COMM	Set of ETSI specifications for mobile commerce

NOTE: ETSI TR 102 203 [i.9], ETSI TS 102 204 [i.10], ETSI TR 102 206 [i.11] and ETSI TS 102 207 [i.12].

MNO	Mobile Network Operator
MSSP	Mobile Signature Service Provider
MSSP	Mobile Signature Service Provider
NA	Not Applicable
NFC	Near Field Communications
OASIS	Organization for the Advancement of Structured Information Standards
PC	Personal Computer
PIN	Personal Identification Number
PKI	Public Key Infrastructure
RE	Routing Entity
SCVP	Server-Based Certificate Validation Protocol
SE	Secure Element
SIM	Subscriber Identity Module for a mobile phone
SMS	Short Message Service
SSP	Signing Service Provider

TEE	Trusted Execution Environment
TSM	Trusted Service Manager
TSP	Trust Service Provider
UICC	Universal Integrated Circuit Card (also known as a SIM card)
URI	Uniform Resource Identifier
VE	Verifying Entity
VS	Validation Service scenaio
XKISS	XML Key Information Service Specification
XKMS	W3C XML Key Management Specification
XML	eXtensible Markup Language

4 Usage scenarios for signing

4.1 Introduction

This clause identifies the features that are used to classify different usage scenarios and then models the most practical and commonly implemented scenarios for digital signature creation in distributed environments, including mobile environments. This set of scenarios is based on, and has been verified against, a survey of solutions in the market; however this does not intend to be exhaustive and to cover any possible scenario where a personal device may play a relevant role. The aim is to identify the main styles of operation with some of the variations primarily to identify requirements which impact on interoperability between the parties involved in signature creation.

Throughout this clause the term "digital signature value" is used to differentiate the cryptographical object from the encompassing AdES digital signatures. The term AdES refers to the result of serializing structures compliant with CAdES [i.2], XAdES [i.3] or PAdES [i.4].

The set of scenarios differentiates between local signing where the digital signature value is generated in the personal device upon request of a remote service connected to an application provider (local signing scenarios, see clause 4.4), and remote signing service where the digital signature value is generated in a remote server upon request from the personal device (server signing scenarios, see clause 4.5). The set of scenarios also includes a split-key alternative where the digital signature value is computed partly on the personal device and partly in a remote server (clause 4.6).

All the scenarios show synchronous interactions where a request waits for the production of the corresponding response, which is generated in due time. Asynchronous scenarios can also be derived with the inclusion of typical mechanisms for asynchronous interactions such as sending a request for a pending operation with enough information to allow the responder to correlate any response with the corresponding request, or providing the responder with an address to call when the response is ready.

Figures 1 to 7 provide a high level overview of the scenarios, showing the actors and the relevant exchanges of protocol messages, without further details about the contents of the exchanged protocol messages.

Figures 1 to 7 show messages coming from one actor to the other that include the generated digital signature. For each scenario, the message can instead contain only a reference to the digital signature. Correspondingly, a reference to a document to sign can be transferred instead of the entire document.

All the following scenarios may involve a Trusted Service Manager (TSM). Any interactions with a TSM are not covered in this clause. Use cases relating to service life cycle management including a Trusted Service Manager are considered in clause 6.

Following each scenario is an outline of the features for the scenario as described in clause 4.3 below.

4.2 Actors

These scenarios are modelled around the following actors which may be actively involved in the signing operation (see definitions in clause 3.1).

a) User (i.e. the signer).

b) Personal device.