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

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

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].