ETSI SR 019 020 V1.1.1 (2016-02)

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

Reference
DSR/ESI-0019020

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 "**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

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

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: 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.

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.

NOTE 1: Whilst a cellular phone is used in the figures 1 to 7 illustrating the scenarios this is used to denote any form of personal device as defined in clause 3.1.

c) Mobile Signature Service Provider (MSSP).

d) Signing service provider (SSP).

e) Validation service.

f) Application provider.

g) Identity provider (IdP).

h) Trusted Service Manager (TSM).

NOTE 2: Additional parties are likely to exist (e.g. Certification Authority, Registration Authority) but as these do not have any specific implications on the scenarios for mobile and other forms of distributed signatures they are not directly considered in the present document.

4.3 Features

The following describes the features for mobile and other forms of distributed digital signature scenarios which are used to distinguish between the different scenarios.

a) Whether the document is created on the personal device or provided by an external application.

b) Where the document, plus any signed attributes, are hashed.

c) What is displayed to the user when signing (document hash, whole document, summary of essential elements); some of the information may be displayed on another device rather than on the personal device itself.

NOTE 1: When the document is displayed on a device separate from the device used to control signing then there will be some link between the act of signing and the document displayed.

d) Where the user's sole control over the signature creation is initiated.

NOTE 2: For the scenarios considered in this clause this is expected to be on the personal device.

e) Where the private key is held and the digital signature value computed

f) In the case that the digital signature value is created on the personal device, is this done within:

   i) SE (Secure Element);

   ii) TEE (Trusted Execution Environment);

   iii) An external signature creation device interfaced to the personal device, e.g. a smart card using an NFC (near field communication) interface from the personal device; or

   iv) Other form of trusted environment.

NOTE 3: Use of software for secure signing is not necessarily considered capable of meeting the requirements for sole control needed for advanced forms of electronic signature such as identified in Regulation (EU) No 910/2014 [i.5].

NOTE: 4: When the signature is created in remote service it is always assumed that the key will be held in a cryptographic device such as a hardware security module.

g) Where the steps related to the completion of the AdES signature format (e.g. CAdES, XAdES, PAdES) are carried out. This can include:

   i) Creation of an AdES signature format;

   ii) Creation of an AdES within a document;

   iii) Upgrading the AdES signature format, e.g. to include time-stamps and/or validation data.

h) How the signer is authenticated.

i) Whether mobile specific networking (e.g. Short Message Service - SMS) is employed.

j) Whether the scenario is applicable to any personal devices or just mobile devices.

k) Whether multiple communication channels are involved in the scenario.

4.4 Local signing scenarios

4.4.1 Local signing scenarios - general introduction

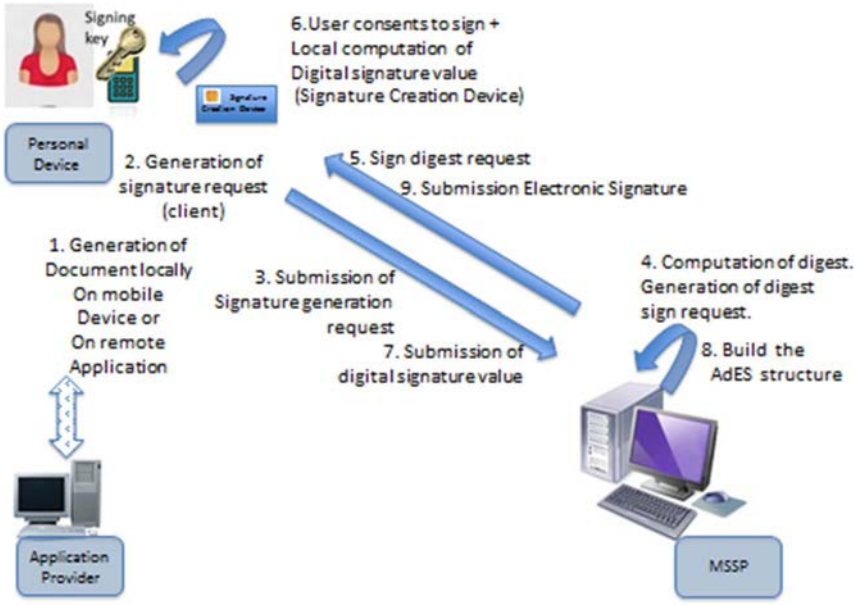
The following scenarios apply where the AdES is created using a signing key held on the personal device (e.g. within a Secure Element (SE)).

Personal devices can incorporate cryptographic capabilities suitable for computing only the digital signature value but the personal device can also build the entire AdES structure. These different capabilities are shown in the following scenarios.

NOTE: In all scenarios, authentication of the MSSP towards the personal device is assumed. Various authentication mechanisms are possible depending on the communication protocols and networks used. Authentication or any security requirement is out of scope of the present document.

4.4.2 L1: Digital signature value generation in personal device

In this scenario (identified as scenario L1) the personal device produces the digital signature value only. The document exists on the personal device, the digest is computed by the MSSP, the digital signature value is computed by the personal device and the AdES structure is built by the MSSP.



NOTE: Document exists on personal device.
Digest computed by MSSP.
Digital signature value computed by personal device. AdES built by the MSSP.

Figure 1: Scenario L1

In this scenario the document to be signed is created either within the personal device or by a remote application that is accessed by the user (step 1); in both cases the document is assumed to exist on the personal device.

The MSSP protocol client on the personal device builds up (step 2) a request for generating an AdES. The client then submits this request, including the document to be signed, to the MSSP (step 3), which computes the hash digest of the document (step 4). If necessary, the MSSP fetches additional elements to include in the digest, such as certificates, signing time and content type. The MSSP then sends (step 5) a request for signing to the personal device. This request may be sent to the service protocol client, or it may be sent over a separate channel (e.g. a mobile network). The personal device then passes the digest to the signature creation device (which in the case of use of the mobile network usually will be the UICC), which, after the authorization of the user, computes (step 6) the digital signature value, which is then submitted (step 7) as a response to the MSSP.

Once the MSSP has this digital signature value it builds up (step 8) the whole AdES and submits it (step 9) to the MSSP protocol client, finalizing the AdES creation process. The client can pass the signed document on to the application provider (not shown in figure 1, may be added as an optional step 10).

In this scenario the device used to interface to the remote application (step 1) can be different from that used to apply the signature. For example the application access can be from a PC, while the signature is requested (step 1) from a mobile phone. Figure 1 shows the situation where the user's personal device is used also for remote application access.

This scenario as described above is aimed primarily at supporting personal devices with minimal computational capabilities. If functions such as digest computation can be carried out on the personal device, then step 3 can contain the hash digest instead of the entire document and step 4 can be avoided.

Table 1 describes the features of this scenario.

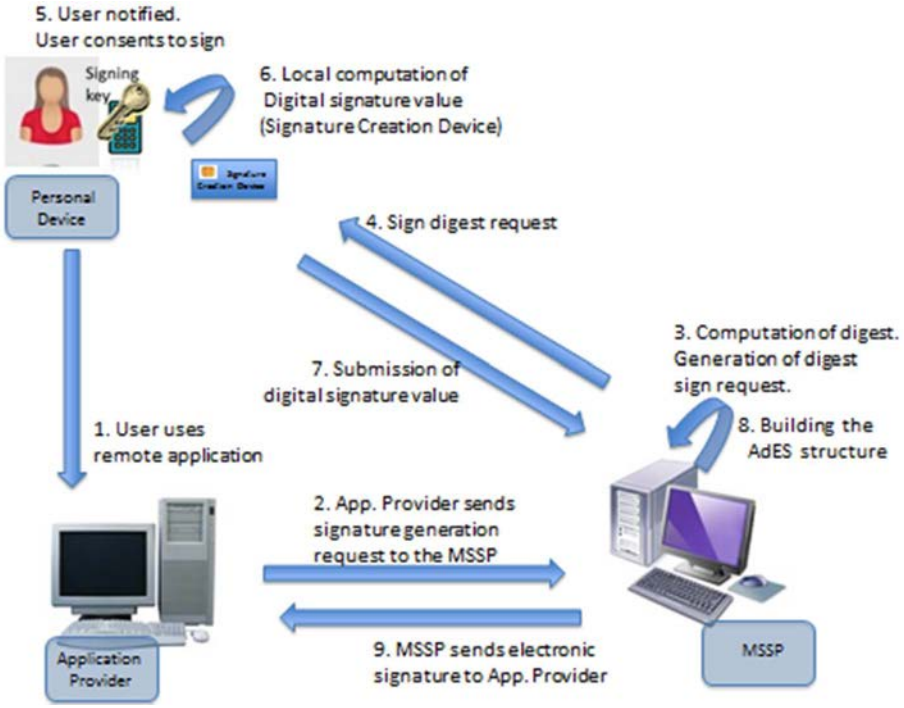
Table 1: Features for scenario L1

Feature	Description of approach in this scenario
a) Whether the document exists on the personal device or is provided by an external application.	Document exists on the personal device (mobile or other).
b) Where the document is hashed.	By MSSP.
c) What is displayed to user when signing.	The full document is presented to the user in step 1. In the signing step (step 6), usually only a unique representation of the document (e.g. hash) is displayed. See note 1.
d) Where is user sole control over the signature creation initiated.	On personal device.
e) Where is the private key held and the digital signature value created.	In personal device.
f) In case the digital signature value is created on personal device, is this done within SE, TEE, external device, or other trusted environment.	All variants can be used: SE, TEE, external device or other trusted environment. See note 2.
g) Where are steps relating to the completion of the AdES signature structure carried out.	By MSSP.
h) How is signer authenticated.	By showing his/her ability to use the private key held in the personal device, e.g. by using signing PIN towards a hardware signature creation device which authenticates the user before signing the data.
i) Mobile network specific or not.	As described the scenario is not mobile network specific, however steps 5 and 7 can be performed over a mobile network. See note 3.
j) Applicable to any personal device or just mobile devices.	As above, the scenario is in principle not limited to mobile devices, however if steps 5-7 are performed by use of a mobile network, then use of a mobile device can be assumed.
k) Whether multiple channels are involved.	Multiple channels can be involved.
NOTE 1: It is not considered necessary that the full document is presented provided that there is a secure link between the act of signing and the document to be signed. NOTE 2: A frequent scenario today is use of UICC card as SE with steps 5 and 7 carried out by an SMS-type protocol over a mobile network. NOTE 3: If a UICC card is used as SE, then use of a mobile network can be assumed.	

4.4.3 L2: Digital signature value generation in personal device with application provider / MSSP Interaction

In this scenario (identified as scenario L2) the document exists at an application provider (e.g. generated in a dialogue with the user) capable of interacting with the MSSP. The digest is computed by the MSSP, the digital signature value is computed by the personal device and the AdES structure is built by the MSSP.

In this scenario the application provider triggers the activity of the MSSP, as shown in figure 2.



NOTE: Document generated by application provider.
MSSP activity triggered by application provider. Digest computed by MSSP.
Digital signature value computed by personal device. AdES built by the MSSP.

Figure 2: Scenario L2

In this scenario the user makes use of a remote application (step 1), as a result of which the application provider concludes that it needs an AdES of that user. In figure 2 the user uses the personal device for the interaction but the interaction may also use another device. The application provider then builds and submits (step 2) a request for generating the AdES to the MSSP, which in turn computes the digest over the document and other attributes to sign (step 3). Then a request for signing the digest is sent to the personal device (step 4). The user is notified and authorizes the computation of the digital signature value (step 5), the user's signature creation device performs the computation (step 6) and the personal device submits the response including the digital signature value (step 7) to the MSSP. The MSSP finally generates the whole AdES (step 8), incorporates it in its response to the application provider, and submits the response (step 9).

In this scenario the device used to interface to the remote application (step 1) may be different from that used to apply the signature (steps 5 and 6). For example the application access can be from a PC, while the signature is computed on a mobile phone.

The scenario as described above is aimed primarily at supporting personal devices with minimal computational capabilities. A variation of this scenario is possible where the personal device carries out the digest computation. Alternatively, the digest computation can be carried out by the application provider. As a further variant, the application provider can itself generate the AdES, receiving only the digital signature value from the MSSP.

This scenario describes the usual application of the M-COMM specifications [i.9], [i.12], [i.11] and [i.10]. The M-COMM specification ETSI TS 102 204 [i.10] specifies an interface between the application provider and the MSSP but M-COMM does not cover the interface between the MSSP and the personal device.

NOTE: This scenario requires some mechanism to ensure that what is shown by the application is the same document as being signed on the personal device.

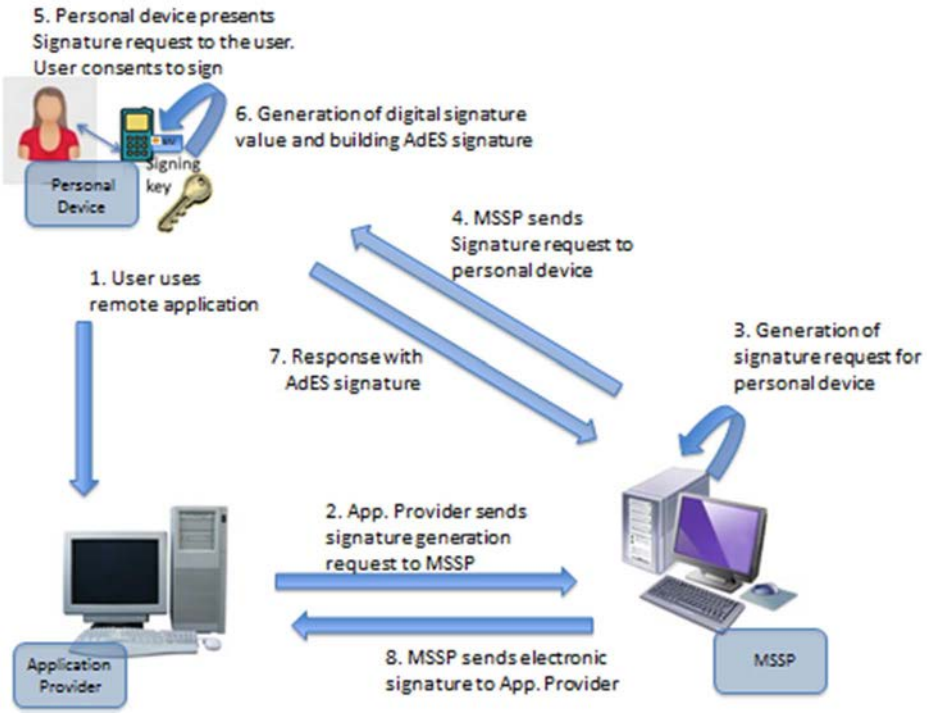
Table 2 describes the features of this scenario.

Table 2: Features for scenario L2

Feature	Description of approach in this scenario
a) Whether the document exists on the personal device or is provided by an external application.	Document exists at remote application provider.
b) Where the document is hashed.	At MSSP or alternatively at remote application provider.
c) What is displayed to user when signing.	Full document is displayed to user by the application provider (step 1). For the digital signature value computation (step 6), usually only some unique representation of the document (e.g. hash) is displayed. See note 1
d) Where is user sole control over the signature creation initiated.	On personal device.
e) Where is the private key held and the digital signature value created.	In personal device.
f) In case the digital signature value is created on personal device, is this done within SE, TEE, external device, other trusted environment.	All variants can be used: SE, TEE, external device or other trusted environment. See note 2.
g) Where are steps relating to the completion of the AdES signature structure carried out.	At MSSP or alternatively at remote application provider.
h) How is signer authenticated.	By showing his/her ability to use the private key held in the personal device, e.g. by using signing PIN towards a hardware signature creation device which authenticates the user before signing the data.
i) Mobile network specific or not.	As described the scenario is not mobile network specific, however steps 4 and 7 can be performed over a mobile network. See note 3.
j) Applicable to any personal device or just mobile devices.	As above, the scenario is in principle not limited to mobile devices, however if steps 4-7 are performed using a mobile network, then use of a mobile device can be assumed.
k) Whether multiple channels are involved.	Multiple channels can be involved.
NOTE 1: If the document is displayed separately from step 6, then it is considered necessary to have some link between the act of signing and the document displayed. NOTE 2: A frequent scenario is use of UICC as SE with steps 4 and 7 carried out by an SMS-type protocol over a mobile network. NOTE 3: If a UICC card is used as SE, then use of a mobile network can be assumed.	

4.4.4 L3: AdES completely generated in a personal device.

This scenario (identified as scenario L3) is an extension of scenario L2 showing a high level approach to the case where the personal device is able not only to compute the digital signature value, but to generate the whole AdES.



NOTE: Document generated by application provider. MSSP activity triggered by application provider. AdES generated by personal device. AdES passed to the application provider by the MSSP.

Figure 3: Scenario L3

In this scenario the user makes use of an application provider. This use may be from the personal device or from another device, e.g. a personal computer. As a result of the user dialogue (step 1), the application provider concludes that it needs an AdES to be generated by the user. The document to sign exists at the application provider. The application provider then builds up and sends (step 2) a signature generation request to the MSSP, including the document to sign. The MSSP then builds up a signature request (step 3) for the user, possibly adding elements such as certificates and signing time, and submits that request to the personal device (step 4) usually including the entire document to sign; alternatively the MSSP can compute the hash. Once the personal device receives this request, the user is presented with some text notifying the request (can be the entire document). The user then consents to signing e.g. by entering the signing PIN to enable the secure element (step 5). Then, the personal device computes the hash digest (unless already done by the MSSP), possibly adding elements such as certificates, signing time and document type if not done by the MSSP. The secure element then creates the digital signature value and the personal device proceeds to generating the AdES (step 6). The personal device then sends the response including the AdES (step 7) to the MSSP, which in turn, sends to the application provider the AdES obtained from the user's personal device (step 8).

Communication between the MSSP and the personal device can be over a mobile network or any other network. If a UICC card on the personal device is used as signature creation device, communication can be restricted to use of a mobile network.

Table 3 describes the features of this scenario.

Table 3: Features for scenario L3

Feature	Description of approach in this scenario
a) Whether the document exists on the personal device or is provided by an external application.	Document exists at remote application provider.
b) Where the document is hashed.	Usually at personal device, alternatively at MSSP (or application provider).
c) What is displayed to user when signing.	Usually full document (step 5) but can also be some unique representation of the document (e.g. hash). The document is usually also displayed to the user by the application provider as part of step 1. See note.
d) Where is user sole control over the signature creation initiated.	On personal device.
e) Where is the private key held and the digital signature value created.	In personal device.
f) In case the digital signature value is created on personal device, is this done within SE, TEE, external device, other trusted environment.	All variants can be used: SE, TEE, external device or other trusted environment.
g) Where are steps relating to the completion of the AdES signature structure carried out.	On personal device.
h) How is signer authenticated.	By showing his/her ability to use the private key held in the personal device, e.g. by using signing PIN towards a hardware signature creation device.
i) Mobile network specific or not.	In general not mobile network specific but if a UICC card on the personal device is used as signature creation device, communication can be restricted to use of a mobile network.
j) Applicable to any personal device or just mobile devices.	As above, the scenario is in principle not limited to mobile devices, however if steps 4-7 are performed using a mobile network, then use of a mobile device can be assumed.
k) Whether multiple channels are involved.	Multiple channels can be involved.
NOTE: If the document is displayed separately from step 5, then it is considered necessary to have some link between the act of signing and the document displayed.	

4.5 Server signing scenarios

4.5.1 Server signing scenarios - general introduction

Clause 4.5 describes scenarios where the AdES is created using a signing key held within a cryptographic security module operated by a signing service provider. Security requirements for such scenarios are described in CEN TS 419 241 [i.15], which is being further refined in "protection profiles" being defined in accordance with the "common criteria" [i.29]. This clause considers primarily the requirements for the business exchange.

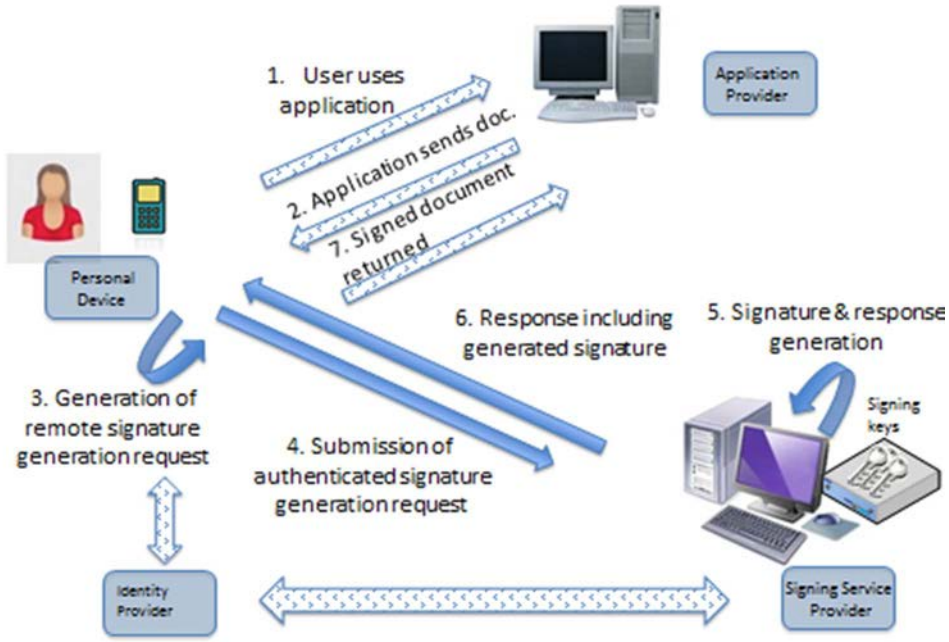
ETSI TS 419 241 [i.15] identifies two levels of sole control. The first level provides a general level of control that can be achieved using existing authentication mechanisms. The second level is aimed at meeting the sole control requirements for remote creation of qualified electronic signatures as defined in Regulation (EU) No 910/2014 [i.5]. The second level will need to take into account the specific requirements of CEN TS 419 241 [i.15] and further related standardization for support of signature activation data exchanged via a signature activation protocol. The present document does not analyse the implications of ETSI TS 419 241 [i.15], and the specific requirements for level 2 sole control, as this is subject to ongoing standardization in CEN. However, protocols to support this scenario will need to take this into account.

NOTE: In all scenarios, authentication of the signing service towards the personal device is assumed. Various authentication mechanisms are possible depending on the communication protocols and networks used. Authentication or any security requirement is out of scope of the present document.

4.5.2 S1: Generation of AdES in a server

In this common scenario (identified as scenario S1), a personal device is able to run client software of a protocol that requests the generation of an AdES from a signing service that holds the user's signing key within a cryptographic security module. This involves passing a hash or the entire document to be signed to the signing service. The signing service generates the digital signature value and may take care of the whole process of generating the AdES.

Figure 4 shows the relevant participating entities and information flows for a scenario where the document is generated either within the personal device or by an external application provider and transferred to the personal device.



NOTE: Document generated by an application provider. Signature requested by personal device. AdES generated by the signing service.

Figure 4: Scenario S1

In this scenario, the user accesses a service provided by an application provider, and as a result the application provider generates (step 1) and submits a document to be signed (step 2) to the personal device. If the document is created locally steps 1 and 2 are skipped. The signing service protocol client running in the personal device generates (step 3; note that the application provider can optionally contribute to generation) and sends (step 4) an authenticated (see below) request to the signing service. The protocol used between the client software on the personal device and the signing service can be more or less complex, ranging from always requesting the same type of AdES to a more elaborated set of options allowing to supply more parameters (see below) to generate different types of AdESs. The signing service generates the digital signature value and possibly the AdES to form the response to the request (step 5) and sends this response back to the client (step 6). In many cases, the signed document is sent to the application provider (step 7).

The alternative where the entire document is sent to the signing service in the request (steps 3 and 4) requires least processing on the personal device but exposes document content to the signing service. In this case, the signing service gathers (part of step 5) signature attributes to be signed, for example signing certificate and signing time, unless these are provided in the request from the personal device. The signing service computes the hash value before generating the digital signature value and in this case usually also the AdES (step 5).

Alternatively, hashing, including collection of attributes to be signed, can be done by the personal device, or even by the application provider. In this case, only the hash value is transferred to the signing service (steps 3 and 4). The AdES can be generated by either the signing service, the personal device, or even by the application provider.

An alternative scenario can also be described where the application provider initiates the signing process by sending a request to the signing service, cf. scenarios L2 and L3 above.

In order for the signing service to select the correct private key for signing, the request (step 4) is authenticated. The authentication can involve an external identity provider. Several alternative authentication exchanges (before, during or immediately after the signature generation request) can be envisaged. For authentication, the personal device can optionally be supported by another external device such as a one-time password generator.

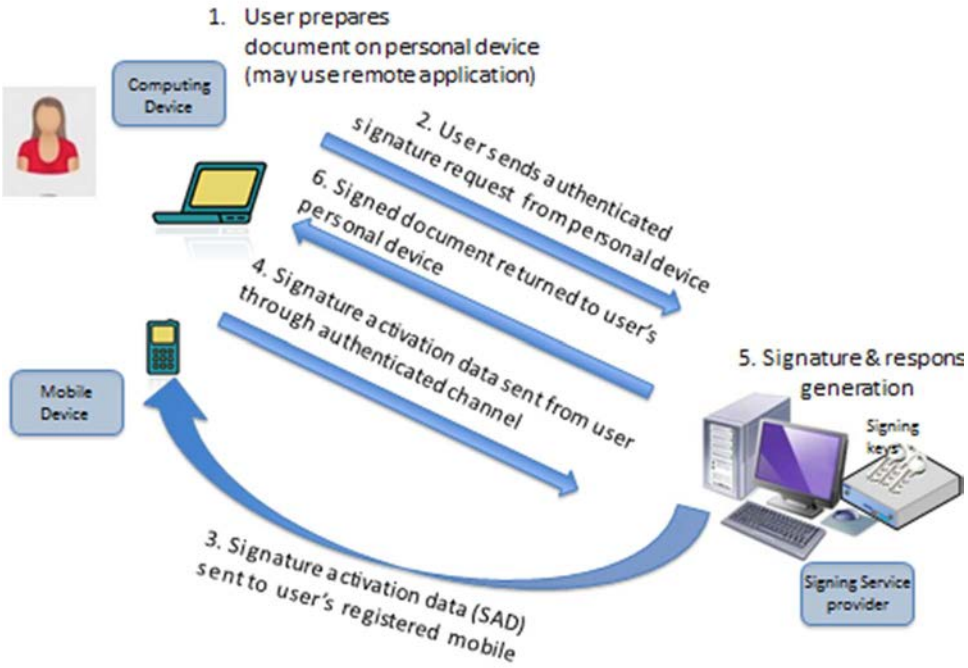
Table 4 describes the features of this scenario.

Table 4: Features for scenario S1

Feature	Description of approach in this scenario
a) Whether the document exists on the personal device or is provided by an external application.	Normally on the personal device, unless hashing is done by the application provider.
b) Where the document is hashed.	Personal device or signing service, may also be the application provider.
c) What is displayed to user when signing.	Full document is normally displayed on the personal device before signing. Alternatively the document is displayed by the application provider; in this case a mechanism is in place to ensure that what is sent to the signing service is the same.
d) Where is user sole control over the signature creation initiated.	On personal device.
e) Where is the private key held and the digital signature value created.	In a cryptographic security module at the signing service.
f) In case the digital signature value is created on personal device, is this done within SE, TEE, external device, other trusted environment.	Not applicable.
g) Where are steps relating to the completion of the AdES signature structure carried out.	Personal device or signing service, possibly also the application provider.
h) How is signer authenticated.	The signer authenticates him/herself to the signing service. This can include support from a remote identity provider.
i) Mobile network specific or not.	No.
j) Applicable to any personal device or just mobile devices.	In general applicable to any personal device.
k) Whether multiple channels are involved.	Usually a single channel but multiple channels can be involved, e.g. separate channel for authentication.

4.5.3 S2: Generation of AdES in a server with multi-channel

This scenario (identified as scenario S2) extends scenario S1 by using different channels for authentication and activation of the signature creation process. This increases security by requiring attackers to compromise both channels to gain full control over the signature creation process. In this scenario, the user's personal device is used only for activating the transaction. Figure 5 shows a high level approach of the relevant actors and exchanges in this scenario.



NOTE: AdES generated by signing service with multi-channel control over signing.

Figure 5: Scenario S2

The scenario is similar to scenario S1. The main difference is that one communication channel, typically over the Internet, is used for document preparation and sending of an authenticated signature request to the signing service, and another communication channel, typically using a mobile network, is used to confirm this transaction by use of the personal device. To prepare the document and the signature request, any kind of device can be used; however if this device is the same personal device used to confirm the signature, extra security measures can apply as this means that both channels are to the same personal device.

This scenario begins with the document being created on the computing device (step 1). The document can also be provided by an application provider. The signing service client on the computing device generates and sends (step 2; note that an application provider can optionally contribute to the generation) an authenticated (possibly involving an identity provider, not shown in figure 5) signature request. In order to confirm the transaction, signature activation data (e.g. a one-time password) is sent from the signing service to the user's personal device over a separate communication channel (step 3). The address of the user's personal device is usually registered in advance with the signing service; at a minimum the signing service checks that the address provided is linked to a device that belongs to the user. The user then confirms the transaction through one of the communication channels in use, either from the personal device or from the computing device (step 4). The signing service generates the digital signature value and possibly the AdES to form the response to the request (step 5) and sends this response back to the computing device (step 6). If an application provider is involved, the signed document is usually sent from the computing device to the application provider (not shown in figure 5).

The variants to this scenario are the same as those described for scenario S1 in clause 4.5.2, including the possibility of sending the signature request directly from an application provider to the signing service.

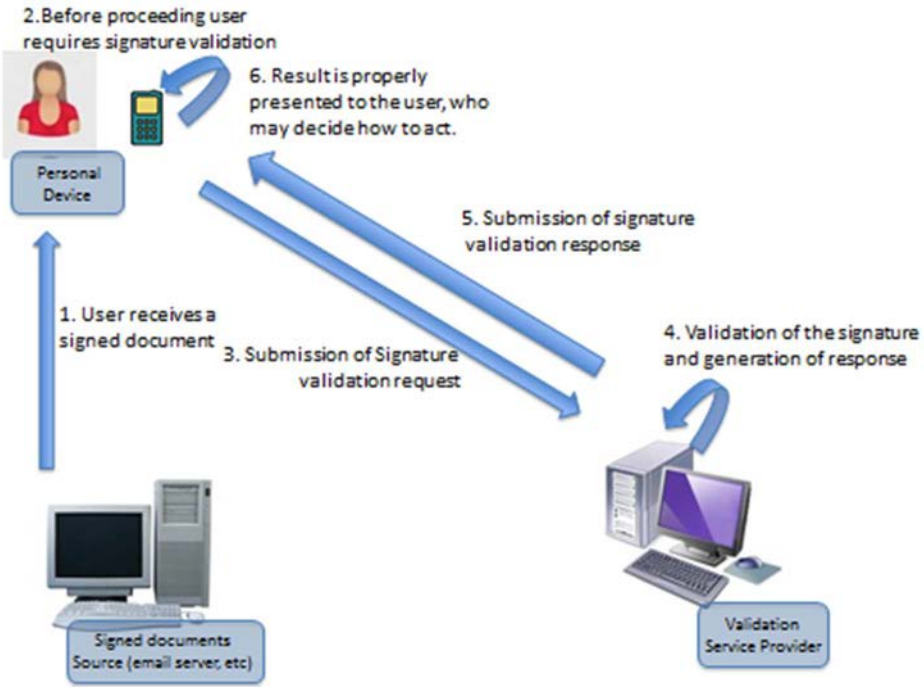
For the extra communication channel used in step 3, several mechanisms are conceivable, e.g. SMS or use of client software like a smartphone app on the personal device. The concrete scenarios of steps 3 and 4 are out of scope of the present document; they can provide either level 1 or level 2 sole control as required by CEN TS 419 241 [i.15].

Table 5: : Features for scenario S2

Feature	Description of approach in this scenario
a) Whether the document exists on the personal device or is provided by an external application.	Normally on the computing device, which can be the same as the personal device, unless hashing is done by the application provider.
b) Where the document is hashed.	Computing device or signing service, can also be the application provider.
c) What is displayed to user when signing.	Full document is displayed on the computing device before signing. Alternatively the document is displayed by the application provider; in this case mechanisms are in place to ensure that what is sent to the signing service is the same.
d) Where is user sole control over the signature creation initiated.	On computing device or personal device depending on the solution used for step 4 in the description above.
e) Where is the private key held and the digital signature value created.	In a cryptographic security module at the signing service.
f) In case the digital signature value is created on personal device, is this done within SE, TEE, external device, other trusted environment.	Not applicable.
g) Where are steps relating to the completion of the AdES signature structure carried out.	Computing device or signing service, possibly also the application provider.
h) How is signer authenticated.	The signer authenticates him/herself to the signing service. This can include support from a remote identity provider. Additional data is provided to activate the user's signing key (steps 3 and 4).
i) Mobile network specific or not.	The additional channel used for step 3 can be over a mobile network or other network.
j) Applicable to any personal device or just mobile devices.	Unless a mobile network is used for the additional channel, a personal device can be used instead of the mobile device.
k) Whether multiple channels are involved.	Multiple channels are used.

5 VS: validation service scenario

Managing validation of AdESs in mobile environments may become a frequent scenario given the increasing mobility in business. Figure 7 provides a high level view of such a scenario.



NOTE: Using personal device in an AdES validation scenario.

Figure 7: Scenario VS

In this scenario a user equipped with a personal device receives a signed document (step 1). The user requires signature validation (step 2) to the validation service protocol client that is running in the personal device. The client generates and submits a signature validation request (step 3) to the remote validation service. The request can include the document with full AdES signature(s). The validation service proceeds to validate the AdES(s) of the document (step 4) and to build and submit the validation response (step 5) to the client. The result of the validation is then presented to the user (step 6) on the personal device.

In a variant, to avoid exposing document content to the validation service, the validation service protocol client processes the AdES format locally to extract pairs of document digests (hash values) and digital signature values that are submitted to the validation service. In this case each document digest is checked against the value obtained from decryption of the corresponding digital signature value.

In yet another variant, only certificate validation is performed by the validation service, while other signature processing is done on the personal device. The signature validation request then includes the certificate or certificate chain to validate, and the response includes information on validity, including revocation status, and possibly auxiliary information such as quality parameters (e.g. whether the certificate is qualified or not).

Variations of this scenario exist where validation is requested directly from the application provider.

6 Further standardization requirements

6.1 Requirements on protocols for signing and validation

This clause summarizes a list of potential requirements that the protocols used for the scenarios described in clauses 4 and 5 should fulfil in order to manage generation and validation of the AdES signatures and ASiC containers in distributed environments:

1) The protocols should work with any identification/authentication scheme for user authentication provided that the level of assurance of the identity proofing (registration) and authentication meets authentication requirements as identified in ETSI TS 419 241 [i.15] or equivalent European Norm currently under development.

2) The protocol for signature generation should support the signature activation protocol requirements as identified in ETSI TS 419 241 [i.15] or equivalent European Norm currently under development.

3) The protocols should allow requests to remote servers for all of signature generation, signature augmentation and signature validation.

4) The protocols should allow requests to remote servers to generate, validate and augment AdES signatures according to constraints specified in a signature policy.

5) The protocols should allow a request to a remote server for generation of a CAdES [i.2], XAdES [i.3] or PAdES [i.4] signature or an ASiC [i.6] container fully compliant with all of these standards.

6) The protocols should allow a request to a remote server for generation of an AdES signature with an incorporated time-stamp and incorporated certificate status information.

7) The protocols should allow a request to a remote server to compute a digest value to be signed by a (secure) signature creation device operated in or in conjunction with the personal device.

8) The protocols should allow a request to a remote server to build an AdES signature based on a digital signature value computed at the personal device.

9) The protocols should allow inclusion of a visual representation of an AdES at a specified place within the signed document according to specifications for visible signatures.

10) The protocols should permit both synchronous and asynchronous communication where this is possible given the communication protocols in use.

11) The communication channels and protocols used should prevent man-in-the-middle and other attacks that may result in fraudulent signatures, changes to documents before signing, erroneous status messages and reports and other security critical events.

12) The protocols should incorporate mechanisms that verify that the personal device is under control of the signer at the time of signing.

13) When the document is displayed on a device separate from the personal device, a link between the act of signing and the document displayed should be in place to ensure that the correct document is signed.

14) The protocols should allow multiple communication channels to be used in the signing process.

15) When multiple communication channels are used in the signing process, the security implications of attacks on one of the channels may need to be taken into account in the protocol.

16) Protocols should support split-key solutions where a pre-digital signature is generated on the personal device with the signature completed by a signing server.

17) When requesting validation of AdES(s), the protocols should allow to request a detailed validation report for each validated AdES, fully aligned in its contents with the validation results specified by ETSI EN 319 102-1 [i.19] and the validation report to be specified in ETSI EN 319 102-2 [i.35].

18) When requesting validation of AdES(s), the protocols should allow to request a signed validation report from the validation service.

19) The protocols should take into account the need to identify and authenticate any service involved in the signing or validation towards the user/personal device.

Specific instantiations of the scenarios described in clauses 4 and 5 of the present document can impose a subset of the requirements listed above as applicable to that scenario.

6.2 Requirements related to service life cycle management

6.2.1 Use cases for life cycle of user subscription to MSSP/SSP

The use cases in clauses 6.2.1 and 6.2.2 are specifically aimed at supporting mobile devices supported by a mobile network operator working with trust service provider. In the case of other personal devices it is expected that this will be directly supported by the TSP.

The following use cases identify typical life cycle activities from a user's subscription to un-subscription of a MSSP or SSP service. The use cases exclude usage, which is described in the scenarios in clauses 4 and 5. Table 7 identifies how events can influence the operation of a trust service provider.

Table 7: Use cases for life cycle of user subscription to MSSP/SSP

Use Case	Potential impact on standardization
Use Case #1: Mobile signature service subscription: The user subscribes to a mobile signature service provided by a MSSP or a SSP.	In addition to a normal registration procedure, identification of the mobile device (e.g. UICC number and mobile phone number) may need to be obtained and securely linked to the user, e.g. in certificate extensions.
Use Case #2: Mobile signature service activation: Following subscription, the service may require an explicit activation operation by the user.	For local signing, this may require a proof of possession to be submitted from the mobile device to the MSSP.
Use Case #3: Mobile signature service suspension: The MSSP/SSP may decide that the signature service is temporarily unusable by the user, e.g. if the user reports the mobile device as suspected lost.	If suspension is used, the MSSP/SSP, possibly also the MNO, is an additional actor that may request the certification authority to suspend a certificate.
Use Case #4: Mobile signature service resumption: The MSSP may require the service to be made usable again, e.g. if the mobile device is recovered.	If suspension is used, the MSSP/SSP, possibly also the MNO, is an additional actor that may send a reactivation request to the certification authority.
Use Case #5: Mobile signature service certificate revocation or renewal: Events related to the service provisioning or to the mobile user/device results in a need for revocation or renewal of a certificate. See below for some examples (in addition to the obvious loss of mobile device).	The MSSP/SSP, possibly also the MNO, is an additional actor that may request the certification authority to revoke or renew a certificate.
Use Case #6: Mobile signature service termination or unsubscription: The user decides to unsubscribe from the mobile signature service, or the MSSP/SSP terminates the subscription	The MSSP/SSP is an additional actor that may request revocation of certificates from the certification authority

4.6 LS: Split local and server signing scenario (threshold cryptography)

This clause shows a scenario (identified as scenario LS) where the signing function is split between the personal device and the signing service, each holding a part of the signing key. Thus the digital signature value creation function is split between the personal device and the signing service. Figure 6 shows a high level approach of the relevant actors and exchanges in this scenario.

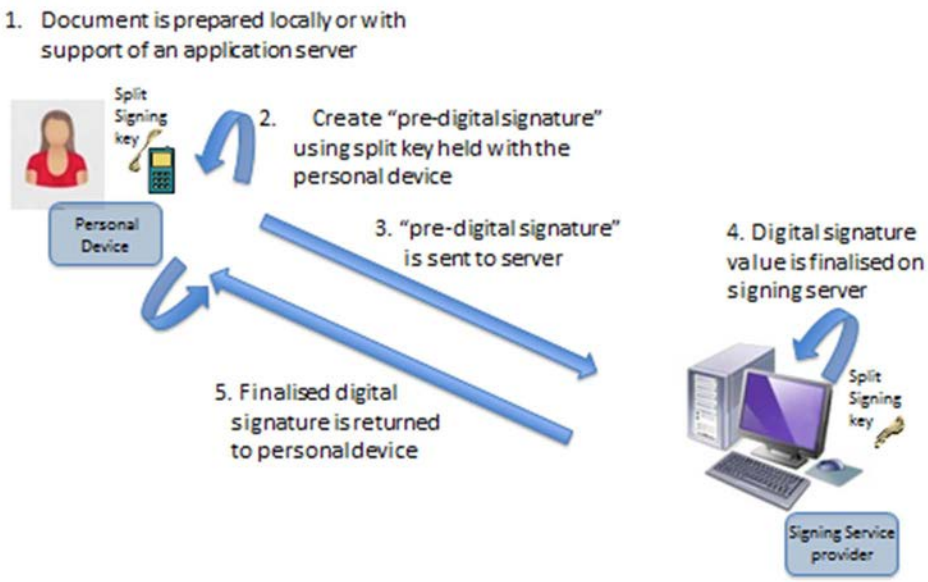


Figure 6: Scenario LS signatures created using a split key

The scenario is a specialization of threshold cryptography signing where the basic idea is that the private key is split between T actors, and at least N of these need to be involved to use the key. In the scenario both T and N are 2. A survey of threshold cryptography mechanisms is given in [i.7].

In this scenario the document is prepared locally or by a remote application provider (step 1). A "pre-digital signature value" is created on the personal device using the part of the split key held locally (step 2). The pre-signature is sent to the signing service (step 3), and the digital signature value creation is completed using the split key held on the signing service for the identified signatory (step 4). The finalized digital signature value is then returned to the personal device. The AdES can be generated either by the signing service or by the personal device.

Table 6: Features for scenario LS

Feature	Description of approach in this scenario
a) Whether the document exists on the personal device or is provided by an external application.	Document is presumed to exist on the personal device but can be obtained from an application provider. In a variant the application provider transfers only the hash value to the personal device.
b) Where the document is hashed.	Usually on personal device but can be at application provider or signing service (see previous row).
c) What is displayed to user when signing.	Usually whole document is displayed on the personal device. The document can also be displayed by an application provider with only the hash or some other unique data being displayed on the personal device.
d) Where is user sole control over the signature creation initiated.	On the personal device.
e) Where is the private key held and the digital signature value created.	Split between personal device and signing service.
f) In case the digital signature value is created on personal device, is this done within SE, TEE, external device, other trusted environment.	The personal device's part of the split key can be held in SE, TEE or other trusted environment.
g) Where are steps relating to the completion of the AdES signature structure carried out.	Personal device or signing service, potentially also application service if document is held there.

Feature	Description of approach in this scenario
h) How is signer authenticated.	For access to the part of the key held by the signing service: support of a remote identity provider can be required or local authentication mechanisms can be employed. For personal device part of the key: By showing the ability to use the private key held in the personal device, e.g. by using signing PIN towards a hardware signature creation device. Additionally, the signing service is authenticated towards the personal device.
i) Mobile network specific or not.	Currently known implementations are not mobile specific.
j) Applicable to any personal device or just mobile devices.	In general applicable to any personal device.
k) Whether multiple channels are involved.	Multiple channels can be involved.

6.2.2 Use cases for events related to mobile device and MNO

The following use cases describe events related to a mobile device and in particular devices that include a subscription for mobile network services from a MNO. When a mobile device is used for digital signatures, such events may affect the operation of a certification service provider as indicated in table 8.

Table 8: Use cases for events related to mobile device and MNO

Use Case	Potential impact on standardization
Use Case #7: Secure element change: The user's SE (e.g. UICC) is replaced by a new one.	For local signing, the user's key will change, necessitating renewal of the user's certificate.
Use Case #8: Mobile phone number change.	Depending on the implementation, certificate renewal may be necessary.
Use Case #9: Mobile device change: The user changes device but not SE.	Depending on the implementation, effects such as certificate renewal may result.
Use Case #10 Mobile subscription termination.	Effects depend on implementation, but normally this will mean mobile signature service termination or un-subscription with resulting revocation of certificate.
Use Case #11: MNO swap: The user changes subscription from one MNO to another.	Depending on the specific implementation and whether or not the MSSP/SSP is specific to a MNO, the event may cause mobile signature service termination or revocation/renewal of certificate.

6.3 Standardization requirements and rationalized framework

Table 9 provides an analysis of the standardization requirements for the scenarios in clauses 4 and 5 against the six areas of the rationalized framework for digital signature standardization (ETSI TR 119 000 [i.1]).

Standards that are already in place, under development or in the CEN and ETSI work plans are highlighted in bold.

Requirements for further standardization are marked by the word "new" and shown in italics. See clause 6.4 for a description of the scope of each of the new standards required.

Clause A.2.9 provides an analysis of requirements against the OASIS DSS [i.8] specifications.

Table 9: Analysis of standardization requirements for AdES digital signatures in distributed environments

Area	Local signing scenarios: L1, L2, L3	Signing service scenarios: S1, S2	Split-key signing scenario: LS	Validation service scenario: VS
Area 1 Signature creation and validation	All existing standards New: ETSI TS 119 152 [i.36] See note 4	All existing standards New: ETSI TS 119 152 [i.36] See note 4	All existing standards New: ETSI TS 119 152 [i.36] See note 4	All existing standards
Area 2 Signature creation and other related devices	CEN EN 419 211 [i.13] CEN EN 419 212 [i.42]	CEN EN 419 221 [i.14] CEN EN 419 241 [i.15] CEN EN 419 212 [i.42]	CEN EN 419 221 [i.14]	CEN EN 419 221 [i.14]
Area 3 Cryptographic suites	ETSI TS 119 312 [i.16]	ETSI TS 119 312 [i.16]	To be determined	ETSI TS 119 312 [i.16]
Area 4 Trust service providers supporting digital signatures	No policy requirements, see note 1. New: ETSI TS 119 432 [i.37] See note 2 See note 5	ETSI EN 319 401 [i.17] New: ETSI TS 119 431 [i.38] New: ETSI TS 119 432 [i.37] ETSI EN 319 403 [i.18] Note 2	See note 4 New: ETSI TS 119 432 [i.37] See note 2 See note 5	ETSI EN 319 401 [i.17] New: ETSI TS 119 441 [i.39] New: ETSI TS 119 442 [i.40] ETSI EN 319 403 [i.18]
Area 5 Trust application service providers	Not applicable	Not applicable	Not applicable	Not applicable
Area 6 Trust service status list providers	See note 1	Extension may be required to ETSI TS 119 612 [i.28] for new TSP type	Note 4	Extension may be required to ETSI TS 119 612 [i.28] for new TSP type

NOTE 1: Assuming signature is validated after creation the MSSP does not need to be trusted.
NOTE 2: Requirements for testing conformance and interoperability are for further study.
NOTE 3: Analysis of the risks of a server holding a split key is needed to determine whether this requires the signing server to be a trusted service.
NOTE 4: An architecture document is considered necessary to describe the interaction between the TSP related elements and other elements of the distributed solution (document preparation, AdES format creation, etc.). This is not necessary for the validation service.
NOTE 5: Further analysis is required for certificate and private key life cycle specific to personal devices. This will take account of ETSI TS 133 221 [i.20] 3GPP GAA (Generic Authentication Architecture) support for subscriber certificates.

6.4 Scope of new standards identified

6.4.1 Overview

Based upon the analysis for the standardization requirements given in clause 6.3, the following new standards are proposed. The scope of each of them is described in the subsequent clauses.

- ETSI TS 119 152 [i.36]: Architecture for digital signatures in distributed environments.
- CEN EN 419 241 [i.15]: Trustworthy Systems Supporting Server Signing.
- ETSI TS 119 431 [i.38]: Policy and security requirements for trust service providers providing AdES digital signature generation services.
- ETSI TS 119 432 [i.37]: Protocol profiles for TSPs providing AdES digital signature generation signing.
- ETSI TS 119 441 [i.39]: Policy and security requirements for trust service providers providing AdES digital signature validation services.
- ETSI TS 119 442 [i.40]: Protocol profiles for trust service providers providing AdES digital signature validation services.

6.4.2 ETSI TS 119 152: Architecture for digital signatures in distributed environments

Scope: ETSI TS 119 152 [i.36] will specify an architecture for the creation of AdES digital signatures in distributed environments, i.e. when parts of the functionality are requested from remote servers. It will use the protocols to be defined in ETSI TS 119 432 [i.37] and ETSI TS 119 442 [i.40], as well as protocols defined for mobile commerce (M-COMM 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]). It will identify the functional elements of the distributed support of users by third parties (TSP or otherwise) for AdES digital signatures and the interactions between them. This is to encompass signatures used for electronic signatures and seals as defined in the eIDAS Regulation. The architecture should support the exchanges necessary to meet the security requirements identified in CEN EN 419 241 [i.15] including requirements for authentication and signature activation.

Starting Points: This framework is to be based upon:

- OASIS DSS [i.8], [i.30], [i.33] and [i.34].
- M-COMM [i.9], [i.10], [i.11] and [i.12].
- CEN TS 419 241 [i.15].

6.4.3 CEN EN 419 241: Trustworthy Systems Supporting Server Signing

Scope: CEN EN 419 241 [i.15] identifies the security requirements for systems Trustworthy System Supporting Server Signing that generate advanced electronic signatures including one or more protection profiles which cover security requirements to reach compliance with Annex II of Regulation (EU) No 910/2014 [i.5] (Requirements for Qualified Electronic Signature Creation Devices) of the remote (qualified TSP operated) parts of the system.

Starting Points: CEN EN 419 241 [i.15] is to be based upon:

- CEN TS 419 241 [i.15].

6.4.4 ETSI TS 119 431: Policy and security requirements for trust service providers providing AdES digital signature generation services

Scope: ETSI TS 119 431 [i.38] will specify policy requirements building on the general policy requirements specified in ETSI EN 319 401 [i.17] for signature generation trust services where users' private keys are stored and accessed in trusted hardware modules in the TSP environment. This is to encompass signatures used for electronic signatures and seals as defined in the Regulation (EU) No 910/2014 [i.5]. This will take into account requirements specified in CEN TS/EN 419 241 [i.15], [i.15], and the present document.

NOTE 1: Support for split keys is for further study.

NOTE 2: This activity may identify requirements for changes to ETSI TS 119 612 [i.28] to identify further trust services.

Starting Points: ETSI TS 119 431 [i.38] is to be based upon:

- ETSI EN 319 401 [i.17].
- ETSI TS 119 101 [i.41].
- CEN TS 419 241 [i.15] and planned CEN EN 419 241 [i.15].

6.4.5 ETSI TS 119 441: Policy and security requirements for trust service providers providing AdES digital signature validation services

Scope: ETSI TS 119 441 [i.39] specifies policy requirements for TSPs providing validation services. ETSI TS 119 441 [i.39] will reference ETSI EN 319 401 [i.17] for general requirements.

Starting Points: ETSI TS 119 441 [i.39] is to be based upon:

- ETSI EN 319 401 [i.17].
- ETSI TS 119 101 [i.41].

6.4.6 ETSI TS 119 432: Protocol profiles for TSPs providing AdES digital signature generation services

Scope: This multi-part document profiles the M-COMM and DSS protocols to support local signing and server signing in distributed environments. Further base standards may be considered.

Part 1: Trusted Service manager

ETSI TS 119 432 [i.37] specifies protocols for a trusted logical component that implements one or more service management roles related to the provisioning, the life cycle management and the deletion of a distributed service. This is based on ETSI TS 102 204 [i.10] and potentially other specifications in the M-COMM series.

Part 2: Local signing on personal device

ETSI TS 119 432 [i.37] specifies the use of personal devices for local signing supported by MSSP services based on the M-COMM specifications 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].

Part 3: Local signing on general computing device

ETSI TS 119 432 specifies the use of mobile or other computing devices for local signing supported by services based on OASIS DSS [i.8]. It will take into account requirements identified in 6.1, and the use of DSS as in clause A.2.

Part 4: Remote signing

ETSI TS 119 432 [i.37] specifies the use of mobile or other computing devices for remote signing supported by services based on OASIS DSS [i.8]. It will support both level 1 and level 2 sole control as specified in CEN TS 419 241 [i.15] and its planned future equivalent. The protocol profile should support the exchanges necessary to meet the security requirements identified in CEN EN 419 241 [i.15] including requirements for authentication and signature activation.

NOTE: Additional parts may be added for split key signing.

Starting Points: ETSI TS 119 432 [i.37] will be based upon at least:

- OASIS DSS [i.8].
- M-COMM [i.9], [i.10], [i.11] and [i.12].
- CEN TS 419 241 [i.15].

6.4.7 ETSI TS 119 442: Protocol profiles for trust service providers providing AdES digital signature validation services

Scope: ETSI TS 119 442 [i.40] specifies a profile for formats and protocols to be used by TSPs providing validation services. A validation service is equally applicable to personal devices and other computing devices.

Starting Points: ETSI TS 119 442 [i.40] will be based upon at least:

- OASIS DSS [i.8] - This expected to be the primary source.

The following may provide additional features:

- The W3C XML Key Management Specification (XKMS) [i.23], the part titled XML Key Information Service Specification (XKISS) as a basis for a service interface for certificate validation; personal device.
- IETF RFC 3029 [i.24] Data Validation and Certification Server protocols.
- IETF RFC 5055 [i.25] Server-Based Certificate Validation Protocol (SCVP) for certificate validation.

Annex A:
Most relevant standards

A.1 Introduction

There are a number of specifications that define protocols that support remote use of SSP or MSSP in support of creation of AdES.

There also exist specifications defining protocols that allow to request the validation of AdES to a remote server.

This annex reviews two of the most relevant sets of specifications that are widely used worldwide: OASIS DSS [i.8], [i.30], [i.32], [i.33], [i.34], [i.35] and [i.36] and other associated specifications, and M-COMM [i.9], [i.10], [i.11] and [i.12].

A.2 OASIS DSS and DSS-X specifications

A.2.1 Introduction

OASIS Digital Signature Services Technical Committee (DSS henceforth) has produced a set of OASIS specifications that define two protocols, namely:

1) A SignRequest/SignResponse protocol. This protocol specifies the semantics and the syntax of an XML message (SignRequest) that a client can use to request to a remote server the generation of one digital signature on one or more data objects. It also specifies the semantics and the syntax of an XML message (SignResponse) that the aforementioned remote server can use to return to the client the digital signature created following the SignRequest.

2) A VerifyRequest/VerifyResponse protocol. This protocol specifies the semantics and the syntax of an XML message (VerifyRequest) that a client can use to request to a remote server the validation of all the digital signatures of one document. It also specifies the semantics and the syntax of a XML message (VerifyResponse) that the aforementioned remote server can use to return to the client the result of the requested validation process on the digital signatures passed in the request.

The basic features of both protocols are defined within the OASIS DSS Core Protocol/Specification [i.8]. A number of profiles are also defined that sometimes constrain the degree of optionality and sometimes incorporate features to the protocol that are not specified within the core document. The original DSS specifications have since been augmented by further work done by the OASIS Digital Signature Services eXtended (DSS-X) Technical Committee.

The approach taken by DSS and DSS-X is to build coherent profiles, i.e. to devote one profile to solve one specific problem. As a result of that approach, certain scenarios can require a combination of a subset of the features of the DSS Core plus a number of profiles, each providing one feature required by the scenario.

In order to propose a framework of standards for requesting the generation/validation of AdES to a remote server, which fulfils the list in clause 7, the features provided by the core protocol as well as relevant profiles are considered. Some relevant profiles are described below in clauses A.2.3 to A.2.7. This is not a complete list, and other existing profiles may need to be taken into account. Ongoing work in OASIS DSS-X will result in new profiles that can be relevant.

A.2.2 OASIS DSS Core specification

A.2.2.1 SignRequest/SignResponse protocol

The OASIS DSS protocol [i.8] allows to request generation of both XML Signatures and CMS Signatures. The SignRequest protocol allows to request the generation of one and only one digital signature of one specific format.

When requesting XML signatures the protocol provides the following features:

1) It allows to pass to the server one or more documents to be collectively signed by the XML signature. It also allows to pass the hash of the document(s) instead of the entire document(s), or even the result of applying to the document(s) a set of transformations.

2) It allows to request the three types of XML signatures: detached, enveloped or enveloping.

3) It allows to pass the critical details of the `ds:Reference` elements to be generated.

4) In the case of requesting an enveloped signature, it also allows to specify where exactly in the document the signature has to be placed.

When requesting CMS signatures, the protocol provides the following features:

1) It allows to pass to the server one document or its hash, for it to be signed.

2) It allows to request a detached or an enveloping CMS signature.

When requesting an XML or a CMS signature the protocol:

1) Provides an element for passing the claimed identity of the requesting entity, including optional supporting information (for instance for conveying authentication information).

2) Provides a placeholder for including a selector of the private key to be used during the signature generation.

3) Allows to simultaneously request a signature time-stamp.

When returning the generated signature, the protocol:

1) Allows for returning a detached, enveloping or enveloped signature (the last one only if the requested signature is an XML signature and if the enveloping document is also an XML document).

A.2.2.2 VerifyRequest/VerifyResponse protocol

The protocol allows requesting the validation of one XML signature or all the XML signatures embedded within a XML document. The protocol allows requesting the validation of exactly one CMS signature.

Independently of the format of the signature(s) to be validated the protocol includes the following features:

1) Allows the client to instruct the server to perform the validation at a certain date and time.

2) Allows the client to instruct the server to return an indication of the signing time.

3) Allows the client to instruct the server to return an indication of the signer's identity.

A.2.3 AdES profile

A.2.3.1 Introduction

This profile [i.30], was conceived for supporting remote generation, validation and upgrade of CAdES and XAdES signatures. The profile may need changes to accommodate that latest versions of CAdES [i.2] and XAdES [i.3].

The profile does not currently provide features for requesting generation/validation of PAdES signatures and ASiC containers.

A.2.3.2 SignRequest/SignResponse protocol

The SignRequest operation supports the following features:

1) It allows to request the generation of predefined formats defined in XAdES/CAdES.

2) It allows to request the generation of XML/CMS signatures incorporating specific signed/unsigned properties whose combination does not fit any predefined XAdES/CAdES signature form.

The SignResponse operation supports the following features:

1) It allows to return predefined formats defined in XAdES/CAdES.

2) It allows to return XML/CMS signatures with specific properties whose combination does not fit any predefined XAdES/CAdES signature form.

A.2.3.3 VerifyRequest/VerifyResponse protocol

The VerifyRequest operation supports the following features:

1) It allows to request the validation of a predefined form defined in XAdES/CAdES.

2) It allows to request the validation of a XAdES/CAdES signature and its augmentation to a certain form predefined in XAdES/CAdES by incorporation of the required properties (time-stamp tokens, certificates, certificate revocation information, etc.).

3) It allows to request the validation of a XAdES/CAdES signature and the incorporation of certain properties for obtaining a certain combination that does not fit any predefined XAdES/CAdES signature form.

The VerifyResponse operation supports the following features:

1) It allows to return the result of validating the XAdES/CAdES passed in the request.

2) It allows to return the result of validating the XAdES/CAdES passed in the request plus the augmented AdES format as requested.

Since the profile predates the latest versions of CAdES and XAdES, a number of XAdES/CAdES properties are not currently properly managed. For the same reason, PAdES and ASiC formats are currently not supported.

A.2.4 Asynchronous profile

OASIS DSS Core Protocols are designed as synchronous protocols. The asynchronous profile [i.31] specifies a mechanism for asynchronous generation and validation requests submitted to a remote server.

Under this mode of operation a server can return an empty result to any request submitted by the client, with an indication of "Pending" result. The client can, at any time, pull the result by submitting a PendingRequest with an identifier of the result requested. The server can, when it is able to return the result, generate the corresponding response to the PendingRequest (a SignResponse or a VerifyResponse).

The features provided by this profile are orthogonal to the features provided by the DSS Core and AdES profile, which means that these can be combined.

A.2.5 Visible signature profile

This profile [i.32] is at present in a Committee Specification status.

The SignRequest/SignResponse protocol of this profile allows a client to request generation of a digital signature and, within the same request, request the incorporation of a visual representation of the digital signature. The request can include details on the precise position of the visual representation and also the details to be represented (its generation time, its reason, information of the signer, etc.).

The VerifyRequest/VerifyResponse protocol of this profile allows a client to request the incorporation within the document of a visual notification of the signature validation result, including a visual mark representing such a result, an indication of the verification time, etc.

The features provided by this profile are orthogonal to the features provided by the DSS Core and AdES profile, which means that these can be combined.

A.2.6 Local signature computation profile

This profile [i.33] is at present in a Committee Specification status.

This profile extends the SignRequest/SignResponse DSS Core protocol to allow the actual computation of the digital signature value to be performed within a (secure) signature creation device under the direct control of the user, instead of within the (secure) signature creation device at the server side. The remote server computes the hash to be signed and returns this to the user device, which computes the digital signature value and sends this back to the remote server. The remote server builds up the final AdES to be passed to the user device.

The features provided by this profile are orthogonal to the features provided by the DSS Core and AdES Profile, which means that these can be combined.

A.2.7 Profile for comprehensive multi-signature verification reports

This profile [i.34] is at present in a Committee Specification status.

This profile extends the VerifyRequest/VerifyResponse DSS Core protocol to allow the server (in reaction to the corresponding request from the client) to include within the response a complete validation report for each digital signature validated. This report includes detailed information of all the material used during the validation process, including keys, certificates, certificate status data, time-stamp tokens, etc.

This profile [i.34] was produced before ETSI EN 319 102-1 [i.19] and in consequence these documents are not aligned.

A.2.8 Usability of DSS profiles within the analysed scenarios

Table A.1 provides details of possible use of the different DSS protocols in the signing scenarios described in clause 4, and under which conditions (features desired) such a use would apply.

The first column "Features" lists the potential features that a certain scenario may require, as this sets the conditions for the applicable DSS protocols.

The rest of the columns contain the information specific to one of the scenarios identified and described in clause 4.

A certain cell in the table identifies the DSS profile that could be used for the scenario identified in the first cell of the column if the feature identified in the first cell of the row is required.

NA values indicate that a certain feature is not applicable in the corresponding scenario. A value "Needed New" indicates that there is no protocol within the DSS set of protocols covering that particular feature.

For remote validation (see clause 5), the DSS Core validation profile may be used, if desired augmented with the profiles described in clauses A.2.7 and A.2.8 above and possibly also with the Visible Signature Profile (clause A.2.5).

Table A.1: Usability of DSS profiles within the analysed scenarios

Features	Scenario L1	Scenario L2	Scenario L3	Scenarios S1, S2	Scenario LS
Default Configuration	DSS Core	NA	DSS Core	DSS Core	DSS Core
Request XAdES/ CAdES	AdES Profile	NA	AdES Profile	AdES Profile	AdES Profile
SignatureValue computation in personal device	Local Signature Computation Profile	NA	NA	NA	NA
Private Key Split	NA	NA	NA	NA	Needed new
Request PAdES / ASiC	Needed new	NA	Needed new	Needed new	Needed new
Request visible information on signature	Visible Signature Profile	NA	Visible Signature Profile	Visible Signature Profile	Visible Signature Profile
Asynchronous Operation	Asynch. Profile	NA	Asynch. Profile	Asynch. Profile	Asynch. Profile

A.3 ETSI M-COMM specifications

A.3.1 Introduction

In 2003, ETSI published a set of specifications for mobile signatures for mobile commerce (M-COMM) [i.9], [i.10], [i.11] and [i.12]. These specifications are in use in several deployed systems and are relevant as a basis for future work on signatures in mobile environments.

Most of the deployed M-COMM systems use the control channel from the MNO to the UICC card to communicate with the user's personal device, using a signing key securely stored in the UICC. The communication from the MSSP to the personal device is however out of scope of the M-COMM specifications and left to the individual MSSP.

When the MSSP uses the control channel to UICC mode of communication, the data to be signed is sent directly to the UICC. The UICC usually embeds a minimum solution to display the data on the personal device and ask for input of signing PIN. Usually the UICC needs direct access to display and keyboard on the device to avoid use of the operating system on the personal device. Since the communication channel has limited capacity, data to be signed is limited in size, either only very short documents can be used or the hashing is done by the MSSP (displaying only hash or other reference data on the personal device).

The digital signature value is computed in the UICC. The UICC can also build the AdES format, or this can be done by other actors involved such as the MSSP.

In this mode of operation, M-COMM signing is used as a second communication channel, different from the communication channel used to access the application provider. Use of a second communication channel can support not only Internet-based application providers but also transactions that are initiated by a voice-call, via interactive voice response systems, and other electronic communications channels. The signing operation carried out on the personal device can be used to authenticate the user or to produce a digital signature on a document.

A.3.2 Mobile signature service

A mobile signature service is usually provided under the terms of a commercial agreement between a Mobile Signature Service Provider (MSSP) and those parties who choose to rely on mobile signatures. The features of the MSSP role and responsibilities are described in clause 13 of ETSI TR 102 203 [i.9].

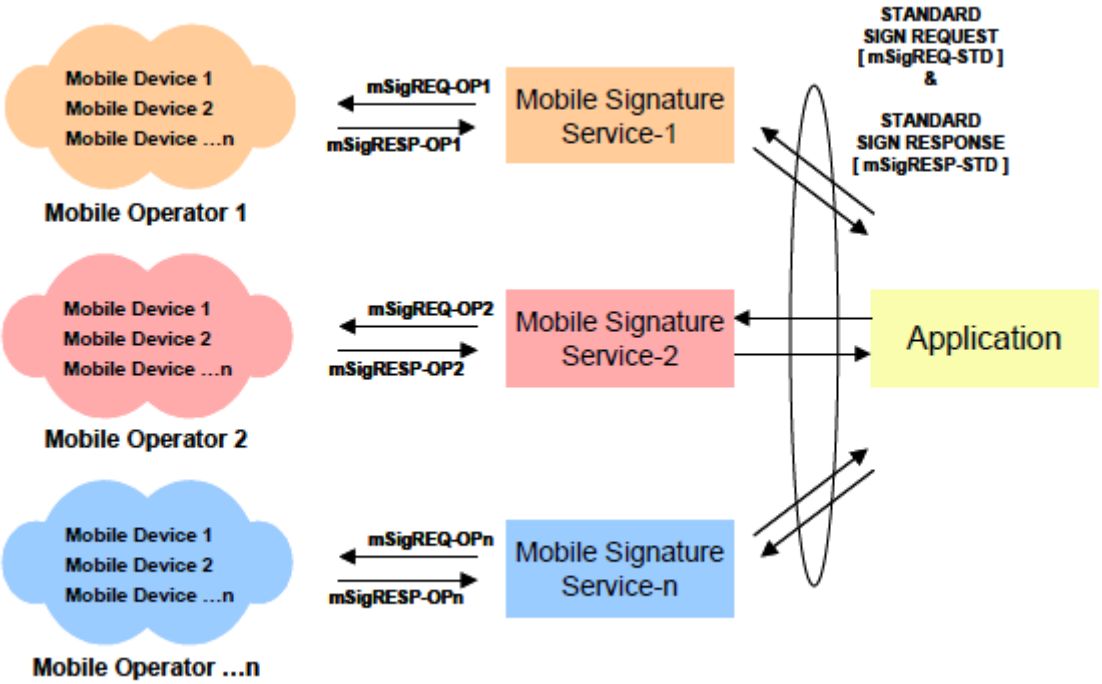


Figure A.1: Mobile signature service (extracted from ETSI TR 102 203 [i.9])

ETSI TS 102 204 [i.10] defines the web service interface offered by an MSSP to application providers using the mobile signature service. As shown in figure A.1, an application provider can interact individually with several MSSPs, e.g. representing different MNOs. The M-COMM roaming specification, ETSI TS 102 207 [i.12], see clause A.3.4, aims at reducing this complexity for the application provider.

Over the interface, the application provider submits the document or other data to be signed (e.g. an authentication challenge) together with other parameters like the phone number and/or other identification of the user. The response includes the signed data together with a status indication and other parameters.

The interface/protocol supports both synchronous and asynchronous operation.

The communication between the MSSP and the personal device is out of scope of M-COMM standardization.

A.3.3 Mobile signature service - web service

A.3.3.1 Introduction

The mobile signature service is specified as a web service. All MSSP functions are implemented over a simple request - response message exchange pattern.

The protocols defined in the specification are generic and give flexibility to define an implementation based on the needs of the MSSP and the application providers. In the following some important features of these protocols are presented.

A.3.3.2 MSS_Signature

This core of M-COMM is the basic sign request and response web service interface. The interface, defined in ETSI TS 102 204 [i.10], allows substantial flexibility for the requests and responses; details are not described here.

M-COMM describes three different messaging modes which can be used for mobile signature requests:

- Synchronous mode that binds an application provider to wait for signature response.
- Asynchronous ClientServer mode uses one way messaging. After submitting the MSS_Signature request, the application provider repeatedly uses the MSS_Status call (see below) to query the MSSP for status until the signature response is ready.
- Asynchronous ServerServer mode uses a two way messaging system. The application provider provides a URI that the MSSP can use to call back when the signature response is ready.

The MSSP can return in principle any digital signature format, such as an AdES format, as long as the personal device returns a result (e.g. a digital signature value) that can be used for the specific format. A specific format can be agreed as default between the application provider and the MSSP, or the application provider can specify a specific format in the request.

An application provider can also request platform specific additional services from the MSSP, such as signature validation, time stamping, archiving, etc.

A request can use the "mobile signature profile" element of a request to specify that a specific level of signature quality is required, e.g. that a software only signing application on the personal device is not acceptable. The mobile signature profile can also be used to specify other signature policy elements.

A.3.3.3 MSS_Status

This protocol defines the message format used to request information on status of an asynchronous request. The response indicates whether the request has been completed or is still outstanding.

A.3.3.4 MSS_Receipt

This protocol defines a way to issue a receipt of the transaction proceedings. An application provider can use this to send a formal receipt to the user specifying the proceedings that has happened. The receipt can be signed by the MSSP or by the application provider.

A.3.3.5 MSS_Registration

This protocol specifies mechanism to enrol a user to the MSSP in order to enable later use of the mobile signature service by the user. This may require initialization of the user's signing PIN, download of the user's certificate or certificate URI to the personal device and activation of the client application on the personal device (may be within the UICC).

A.3.3.6 MSS_Handshake

This protocol defines a handshake method that can be used by the application provider and the MSSP to discover the capabilities of the other party. This is particularly relevant for roaming (see below) but can also be used in other cases.

A.3.4 Mobile signature roaming service

The scenario shown in figure 5 does not scale as it requires the application provider to enter commercial relationships with a potentially large number of MSSPs and to know which MSSP to use for each specific user. ETSI TS 102 207 [i.12] specifies a roaming arrangement to cope with this problem.

With roaming, an application provider can obtain a signature from any user covered by any of the MSSPs that take part in the roaming system, and the situation is transparent to the application provider.

Mobile signature roaming requires commercial agreements between the entities that facilitate it. The roaming system represents as a mesh of members undertaking one or several of the following roles (This list is not necessarily exhaustive):

- Acquiring entity (AE): an entity serving as an entry point to the mesh, and handling commercial agreements with application providers. The entry point in the mesh can be for instance a MSSP, or an aggregator of application providers in the context of particular communities of interests (e.g. payment associations, banks, MNOs, etc.), which is why this is described as a separate role. An acquiring entity implements the web service interface specified in ETSI TS 102 204 [i.10].
- Home MSSP (HMMSP): this is the MSSP that is able to deal with the current user and the current transaction.
- Routing entity (RE): any entity that facilitates communication between the AE and the HMSSP.
- Attribute provider: one or several mesh members can undertake this role to provide relevant attributes in order to facilitate discovery of the HMSSP by other mesh members.
- Identity issuer: an entity that is able to make a link between a Mobile Signature and a user identity, such as a certification authority for a PKI system.
- Verifying entity (VE): an entity that can verify a mobile signature; the role can be taken by a MSSP or by some other actor.
- Acquiring MSSP (AMSSP): this is a MSSP acting as an AE or serving the AE and that acquires MSSP services from other MSSPs (and other actors) in the mesh, usually according to commercial agreements.

Figure A.2 shows the path taken by a mobile signature transaction through the mesh of a roaming system.

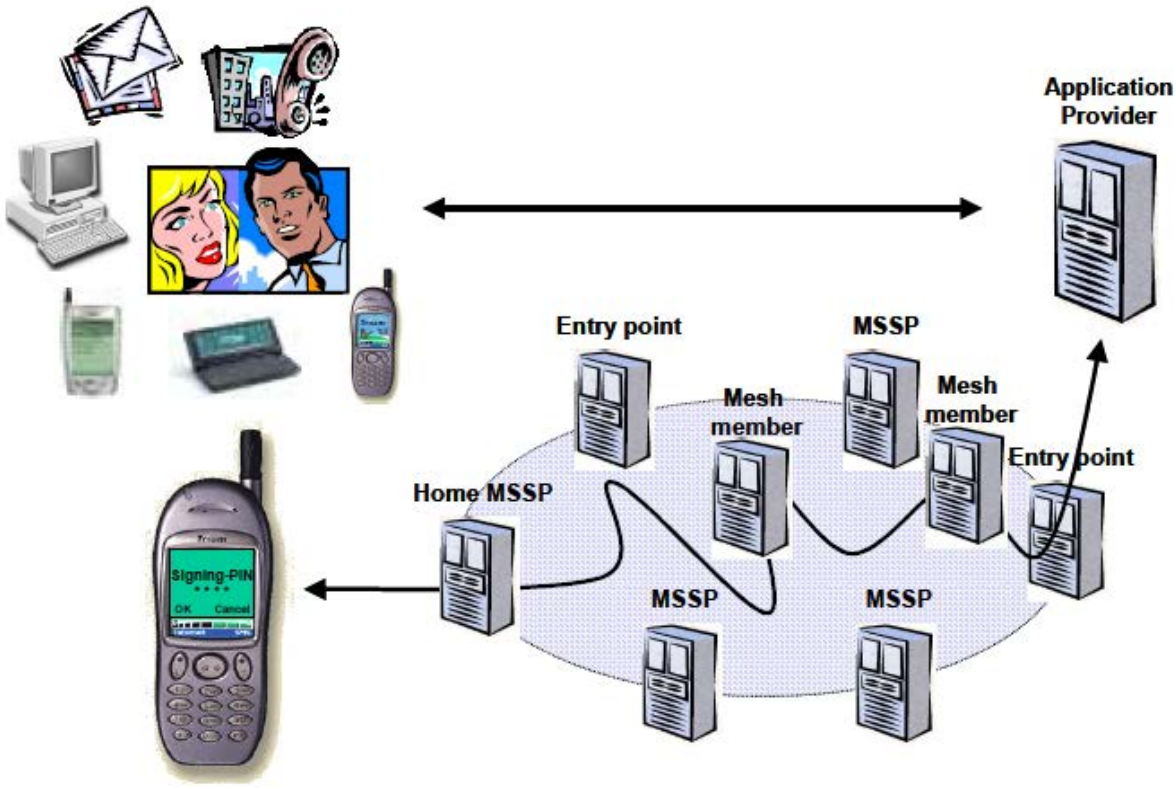


Figure A.2: Mobile signature mesh (extracted from ETSI TS 102 207 [i.12])

Within the mesh, different commercial ecosystems are possible. ETSI TS 102 207 [i.12] does not mandate any commercial ecosystem but states that each ecosystem model has a technical implementation, with its own transaction flows.

History

Document history		
V1.1.1	February 2016	Publication