Draft SR 019 020 v0.0.4 (2013-11)

Rationalised Framework of Standards for Advanced Electronic Signatures in Mobile Environment

STABLE DRAFT FOR PUBLIC REVIEW UNTIL 15 JANUARY 2014

Download the template for comments:

http://docbox.etsi.org/ESI/Open/Latest_Drafts/Template-for-comments.doc

Send comments to E-SIGNATURES_COMMENTS@LIST.ETSI.ORG

CAUTION: This DRAFT document is provided for information and is for future development work within the ETSI Technical Committee ESI only. ETSI and its Members accept no liability for any further use/implementation of this Specification.

Approved and published specifications and reports shall be obtained exclusively via the ETSI Documentation Service at

http://pda.etsi.org/pda/queryform.asp

Attention is draw to the inventory file accompanying this document and input is requested from reviewers for additional information on systems, whose design is publicly available, which could be added to this inventory. It is requested that this input be related to the scenarios and features described in this document in the form similar to other entries to this inventory.

Reference
DSR/ESI-0019020

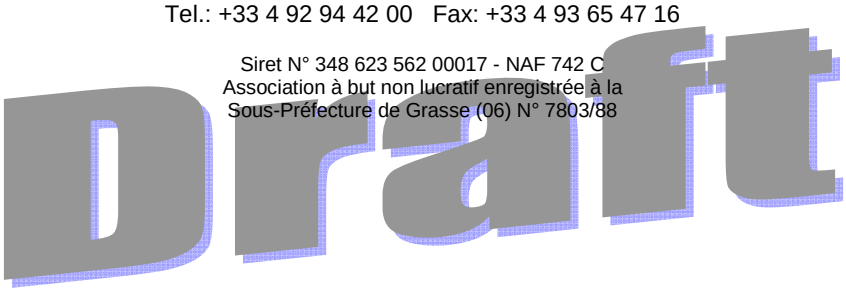
Keywords
e-commerce, electronic signature, security, mobile

ETSI

650 Route des Lucioles
F-06921 Sophia Antipolis Cedex - FRANCE

Tel.: +33 4 92 94 42 00 Fax: +33 4 93 65 47 16

Siret N° 348 623 562 00017 - NAF 742 C
Association à but non lucratif enregistrée à la
Sous-Préfecture de Grasse (06) N° 7803/88



Important notice

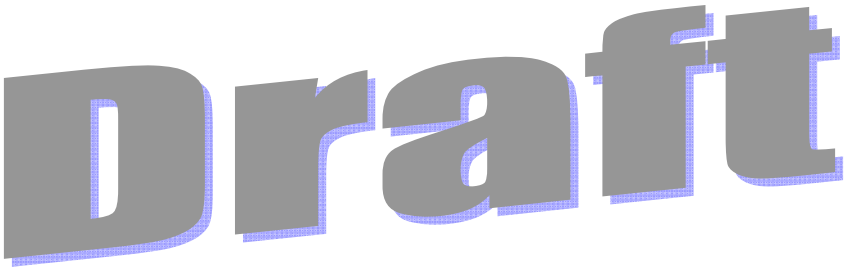
Individual copies of the present document can be downloaded from:
http://www.etsi.org

The present document may be made available in more than one electronic version or in print. In any case of existing or perceived difference in contents between such versions, the reference version is the Portable Document Format (PDF). In case of dispute, the reference shall be the printing on ETSI printers of the PDF version kept on a specific network drive within ETSI Secretariat.

Users of the present document should be aware that the document may be subject to revision or change of status. Information on the current status of this and other ETSI documents is available at
http://portal.etsi.org/tb/status/status.asp

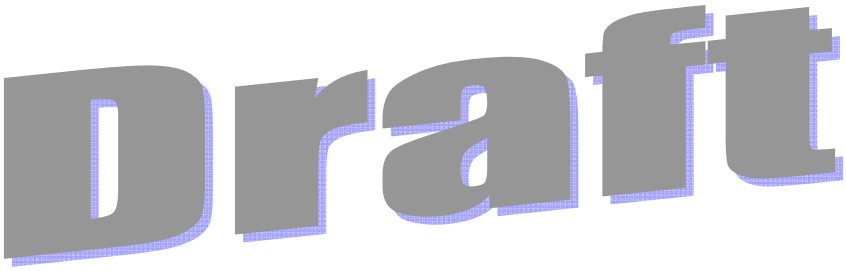
If you find errors in the present document, please send your comment to one of the following services:
http://portal.etsi.org/chaircor/ETSI_support.asp

Copyright Notification



Contents

If you need to update the table of content you would need to first unlock it.
To unlock the Table of Contents: select the Table of Contents, click simultaneously: Ctrl + Shift + F11.
Then lock it: reselect the Table of Contents and then click simultaneously: Ctrl + F11.



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 (http://ipr.etsi.org).

Pursuant to the ETSI IPR Policy, no investigation, including IPR searches, has been carried out by ETSI. No guarantee can be given as to the existence of other IPRs not referenced in ETSI SR 000 314 (or the updates on the ETSI Web server) which are, or may be, or may become, essential to the present document.

Foreword

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

Introduction

This clause is to be completed.

Text to be provided describing server signing, OASIS DSS, MCOMM and AdES for the directive 1999/93.

1 Scope

The present document provides the framework for further standardisation for the creation and validation of advanced electronic signatures (AdES) in mobile environments (i.e. in environments where mobile devices are supported by networked services for signature creation and/or validation) taking into account recent improvements in the capabilities of mobile devices and their overlap with the capabilities other computing devices. It identifies the recommended scope of such standards and any suggested provision thought appropriate to these standards.

Editor's note: Comments are invited as to whether the title properly reflect the scope and suggestions for alternative titles invited.

This standards framework 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 TR 119 000 [i.1] is used to classify the standardisation requirements based on the analysis common scenarios.

The report does not address standardisation for mobile environments where the whole signature creation and / or validation process is carried out within the mobile device. Whilst it is considered important to the market this generally does not involve external interfaces which require further standardisation beyond that already supported using existing standards within TR 119 000..

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

As described in clause 4, this document particularly considers standardisation requirements for scenarios involving:

a) *Local signing* where the AdES is created using a signing key held on the user's mobile device .

b) *Remote signing* where the AdES is created using a signing key held on a remote server.

c) *Remote signature validation* where the AdES is verified supported by a remote server.

Whilst variations of solutions being standardised may be applicable to electronic seals, this report concentrates on the use of services in support of AdES for natural persons or natural persons associated with legal persons.

This document takes into account existing standards and publicly available specifications for AdES in the current framework for electronic signature standardisation TR 119 000 [i.1].

2 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.

2.1 Normative references

The following referenced documents are necessary for the application of the present document.

Not applicable.

2.2 Informative references

The following referenced documents are not necessary for the application of the present document but they assist the user with regard to a particular subject area.

[i.1] ETSI TR 119 000 Rationalised Framework for Electronic Signature Standardisation

[i.2] EN 319 422 CAdES - CMS Advanced Electronic Signatures

[i.3] EN 319 432 XAdES - XML Advanced Electronic Signatures

[i.4] EN 319 442 PAdES - PDF Advanced Electronic Signatures

[i.5] Directive 1999/93/EC of the European Parliament and of the Council of 13 December 1999 on a Community framework for electronic signatures

[i.6] EN 319 142 Associated Signature Containers (ASiC)

[i.7] Internet draft Mediated RSA cryptography specification for additive private key splitting (mRSAA)
http://tools.ietf.org/html/draft-kutylowski-mrsa-algorithm-03

[i.8] IT Security for Citizens http://itsci.borgernesitsikkerhed.dk/

[i.9] OASIS Digital Signature Service Core Protocols, Elements, and Bindings Version 1.0, 11 April 2007

[i.10] ETSI TR 102 203 Mobile Commerce (M-COMM); Mobile Signatures; Business and Functional Requirements

[i.11] ETSI TS 102 204 Mobile Commerce (M-COMM); Mobile Signature Service; Web Service Interface

[i.12] ETSI TR 102 206 Mobile Commerce (M-COMM); Mobile Signature Service; Security Framework

[i.13] ETSI TS 102 207 Mobile Commerce (M-COMM); Mobile Signature Service; Specifications for Roaming in Mobile Signature Services

[i.14] EN 419 211 Protection Profiles for Secure Signature Creation Device (SSCD)

[i.15] EN 419 221 Protection Profiles for TSP Cryptographic Modules

Note: Under development

[i.16] TS 419 241 Trustworthy Systems supporting Server Signing

[i.17] TS 119 312 Cryptographic Suites for Secure Electronic Signatures

[i.18] EN 319 401 General Policy Requirements for TSPs Supporting Electronic Signatures

[i.19] EN 319 403 Trust Service Provider Conformity Assessment - Requirements for conformity assessment bodies assessing Trust Service Providers

[i.20] EN 319 102 Procedures for Signature Creation and Validation

[i.21] 3GPP TS 33.221 Generic Authentication Architecture (GAA); Support for subscriber certificates

[i.22] TR 419 010 Extended rationalized structure for electronic signature standardisation to include electronic identification and authentication

[i.23] The Trusted Execution Environment: Delivering Enhanced Security at a Lower Cost to the Mobile Market

[i.24] W3C XML Key Management Specification (XKMS 2.0)

[i.25] IETF • RFC 3029 Internet X.509 Public Key Infrastructure Data Validation and Certification Server Protocols

[i.26] IETF RFC 5055 Server-Based Certificate Validation Protocol

3 Definitions, symbols and abbreviations

3.1 Definitions

For the purposes of the present document, the [following] terms and definitions [given in ... and the following] apply:

Digital signature value: data appended to, or a cryptographic transformation of, a data unit that allows a recipient of the data unit to prove the source and integrity of the data unit and protect against forgery, e.g. by the recipient.

Note: This excludes any public key certificate or other information required to conform to advanced electronic signature standards such as EN 319 122 [i.2], EN 319 132[i.3], EN 319 142 [i.4]

Advanced Electronic signature: electronic signature which meets the following requirements:
a) it is uniquely linked to the signatory;
b) it is capable of identifying the signatory;
c) it is created using means that the signatory can maintain under his sole control; and
d) it is linked to the data to which it relates in such a manner that any subsequent change of the data is detectable.

Note 1: See Directive 1999/93 [i.5].

Mobile device: A handheld device: (i.e. a small form factor receiving device suitable for carrying in hand, purse or pocket. The antenna is built-in, either internal or deployable. Normal operation is either at pedestrian speeds walking or at vehicular speeds in a moving vehicle. This is typically the mobile phone or smart phone) or portable device (i.e. A receiving device that uses a built-in or set-top antenna, transportable to different locations but stationary during use. This is typically the tablet.*)*

Note: It is assumed that this device is under sole control of the signatory at time of signing.

Editor's Note: The term and its definition may be subject to further consideration

Mobile network: Network operated specifically for mobile devices (e.g. 3G network).

Mobile signature service: Facility that coordinates and manages the mobile signing process.

Note: This service supports local signing only.

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

Signing service: A shared service accessible via a network, or a service provided by a network operator, which signs data on behalf of a remote signatory using a mobile device.

Note: This service supports remote signing only.

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

Validating server: A shared system accessible via a network, or a service provided by a mobile operator, which validates an advanced electronic signature

Application provider:: A system, other than the mobile 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 may prepare the request for a signature on behalf of a mobile device.

Mobile network operator (MNO): The entity which offers telecommunications services over an air interface.

Identity Provider (IdP) (editor's note to be defined based on TR 419 010).

Secure Element (SE): a tamper resistant component which is used in a device to provide the security, confidentiality, and multiple application environments required to support various business models. Such a Secure Element may exist in any form factor such as UICC, embedded SE, smartSD, smart microSD, etc.

Trusted Service Manager (TSM): 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 Mobile service.

Note: The TSM may be integrated with the mobile signature services or signing service or may be provided by an independent party.

Trusted Execution Environment (TEE) An execution environment that runs alongside but isolated from a rich execution environment (i.e. environment governed by a rich operating systems). A TEE has security capabilities and meets certain security-related requirements: It protects TEE assets from general software attacks, defines rigid safeguards as to data and functions that a program can access, and resists a set of defined threats. There are multiple technologies that can be used to implement a TEE, and the level of security achieved varies accordingly.

3.2 Abbreviations

For the purposes of the present document, the [following] abbreviations [given in ... and the following] apply:

3G	3rd Generation mobile network
AdES	Advanced Electronic Signature
IdP	Identity Provider
MNO	Mobile Network Operator
GSM	Global System for Mobile Communications
SE	Secure element (e.g. Universal Integrated Circuit Card commonly called “SIM”)
TEE	Trusted Execution Environment (see [i.23])
MCOMM	Mobile commerce as specified in TR 102 203 [i.10], TS 102 204 [i.11], TS 102 206 [i.12] and TS 102 207 [i.13]
MSSP	Mobile Signature Service Provider
SSP	Signature Service Provider
DSS	Digital Signature Service [i.9]
TSM	Trusted Service Manager

4 Usage Scenarios for Signing

This clause identifies the features that are used to classify different usage scenarios and then models some the most common scenarios and their features. An analysis of existing systems for AdES mobile environment against the features and common scenarios is given in Annex A.

4.1 Parties

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

a) mobile device

b) Mobile Signature Service Provider (MSSP)

c) Signing service provider (SSP)

d) Validating server

e) Application provider

f) Identity provider

g) Trusted Service Manager

Note: 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 AdES they are not directly considered in this document.

4.2 Features

The following describes the features of mobile advanced electronic signature scenarios which are used to distinguish between the different scenarios:

a) Whether document created on to the mobile device or provided by an external application;

b) where is document, plus any signed attributes, hashed ;

c) what is displayed to user when signing (document hash, whole document, summary of essential elements e.g. value); note that some of the information may be displayed on another device (e.g. PC) rather than on the mobile device itself.

d) Where user sole control over the signature creation is initiated;
Note: This is generally expected to be on the mobile device.

e) Where is the private key held & digital signature computed; In case the private key is held on server, does the solution provide level 1 or level 2 sole control as specified in CEN TS 419 241;

f) In case digital signature is created on mobile device is this done within
   i. SE
   ii. TEE
   iii. An external signature creation device interfaced to the mobile device, e.g. NFC Contactless Smart card using NFC (near field communication) with the mobile device.
   iv. Other form of trusted environment

Note: Use of software for secure signing is not necessarily supported by the resulting standardisation.

g) Where are steps relating to the completion of the AdES signature structure carried out. This can include:

   i. creation of a AdES structure,
   ii. creating the AdES within a document,
   iii. extending the AdES structure with AdES structure with time-stamps and / or validation data;

Note: Further work in this area should take into account procedures for signature creation specified in EN 319 102 [i.20].

h) how is signatory authenticated ;

i) Whether mobile specific networking (e.g. small message service - SMS) is employed;

j) When the scenario is applicable to general computing devices as well as mobile devices or just mobile devices.

Note: It is to be assumed that such general computing devices are under sole control of signatory at the time of signing.

4.3 Common Scenarios

4.3.1 General Introduction to Scenarios

This clause identifies the most practical and commonly implemented scenarios where Advanced Electronic Signatures are generated and/or validated in mobile environments. This set of scenarios, however, does not intend to be exhaustive and cover any possible scenario where a mobile device may play a relevant role in the generation of an electronic signature.

Throughout this clause the term “digital signature value” refers to the result of applying an encryption algorithm with an asymmetric private key to the digest value of the document and other elements to be included in the data-to-be-signed. The term AdES refers to the result of serializing structures compliant with ASN.1 CMS or XML Signature.

For generation the set of scenarios range from those where the electronic signature is generated in the mobile device upon request of a remote service connected to an application provider (local signing scenarios), up to those where the electronic signature is generated in a remote server upon request from the mobile device (remote signing scenarios) and

also including a sort of mid-way scenario where mobile device computes the digital signature value and the remote server builds up the actual electronic signature.

All the scenarios show synchronous interactions where a request waits for the production of the corresponding response, which is actually generated in due time. Asynchronous scenarios could also be derived from these ones with the corresponding inclusion of typical asynchronous interactions between the different entities (like sending requests for pending operations with enough information as to allow the responders to correlate any response with its corresponding request).

The figures 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.

The figures below show messages coming from one actor to the other that include the generated electronic signature. Readers should take into account that for each scenario, there could be another where the message contains a reference to the electronic signature instead of the actual generated electronic signature. Correspondingly, reference to a document to sign may 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 sub clause. Use cases relating to service life cycle management including a Trust Service Manager is considered in section 4.4.

Following each scenario there is an outline of the features for each scenario as described in clause 4.2 above.

4.3.2 Local Signing Scenarios

4.3.2.1 Local Signing Scenarios – General Introduction

The following scenarios apply where the AdES is created using a signing key held on the user's mobile device (e.g. within a security element) supported by a remote server.

Currently existing mobile devices incorporate cryptographic capabilities that range from ability to compute the digital signature value but not to build up the whole AdES structure (the corresponding CMS or XML Signature), to those ones that are actually able to completely build up the whole AdES. These different capabilities are shown in the following scenarios.

4.3.2.2 Partial generation of AdES in mobile devices

In this scenarioL1 the document is generated by the mobile device, the digest is computed by the MSSP, the digital signature is computed by the mobile device and the AdES structure is built by the MSSP.

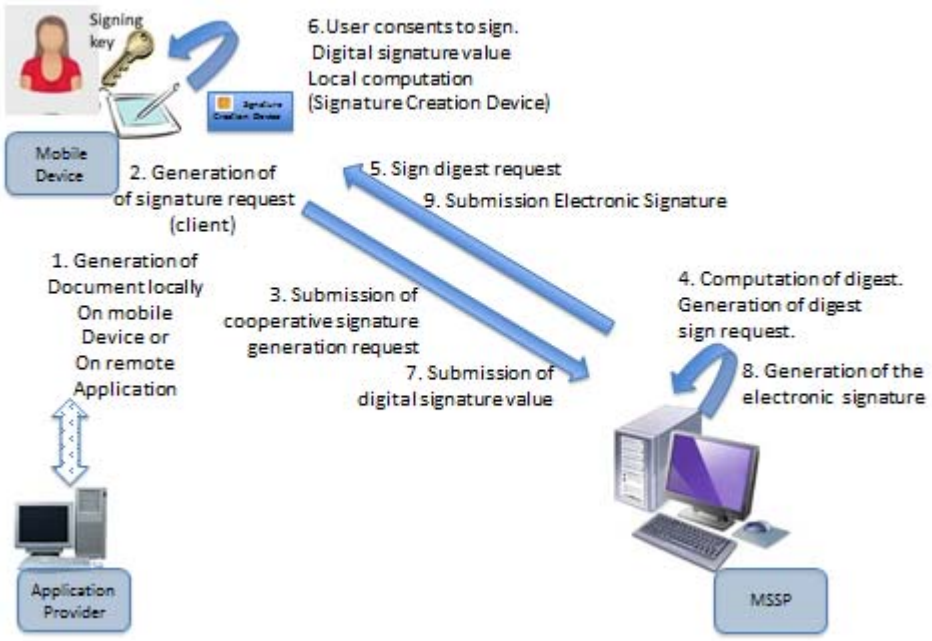


Figure 1: Scenario L1 Document generated by mobile device. Digest computed by MSSP. Digital Signature computed by mobile device. AdES built by the MSSP.

In this scenario the document to be signed is created either within the mobile device or by a remote application that is accessed by the user (step 1). The MSSP protocol client then builds up (step 2) a request for generating an AdES in a cooperative mode (i.e. a mode where the mobile device computes the digital signature value and the MSSP builds up the AdES). The client then submits this request to the MSSP (step 3), which computes the digest (step 4) that has to be signed. If necessary, the MSSP must fetch 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 it to the mobile 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) to the mobile device. The mobile device then passes the digest to the signature creation device (which in the case of use of the mobile network usually will be the SIM), which, after the authorisation 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 is capable to build up (step 8) the whole AdES and to submit it (step 9) to the client, finalizing the AdES creation process. The client may pass the signed document on to the application provider (not shown in the figure, may be added as an optional step 9).

Editor's note: There may be a WYSIWYS problem in scenarios shown in this scenario. One relies on the MSSP returning the hash of the actual document but the mobile/user has no way to tell whether the hash belongs to another document. May be OK but the trust in the MSSP (which perhaps is not adequately secured since it does not hold private keys) should be pinpointed.

Editor's Note: This scenario is aimed primarily at supporting existing basic mobile devices. The requirement for further standardisation relating to this scenario requires further consideration.

The following table describes of the features of this scenario:

Feature	Description of approach in this scenario
a) Whether document created on to the mobile device or provided by an external application;	On mobile device or remote application provider.
b) where is document hashed	On MSSP
c) what is displayed to user when signing	Full document or hash of the document and optionally help text

d) Where user sole control over the signature creation is initiated	On mobile device
e) Where is the private key held & digital signature created	In mobile device
f) In case digital signature is created on mobile device is this done within SE, TEE, external device, other trusted environment	SE, TEE ,-external device or other trusted environment
g) Where are steps relating to the completion of the AdES signature structure carried out	MSSP
h) How is signatory authenticated	By showing her ability to use secure signing device e.g. by using signing PIN
i) Mobile network specific	Steps 5 & 7 above may be sent over a mobile specific network
j) Applicable to general computing devices as well as mobile devices or just mobile devices	Just mobile device

4.2.2.3 Partial or complete generation of AdES in mobile devices with Application Provider / MSSP Interaction

In this scenarioL2 the document is generated by the mobile device, the digest is computed by the MSSP, the digital signature is computed by the mobile device and the AdES structure is built by the MSSP. But a variant of the former scenario appears when the user uses her mobile device for accessing an Application Provider that implements a MSSP Protocol Client capable of interacting with the MSSP.

In this scenario the application provider triggers the activity of the MSSP, as shown in the figure below:

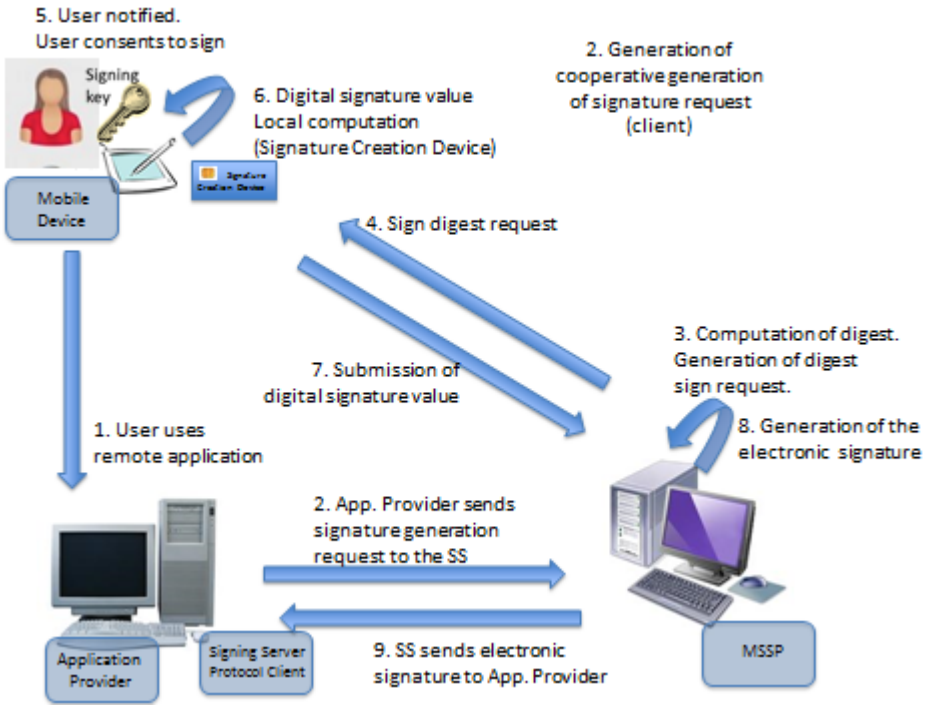


Figure 2: Scenario L2. Document generated by application provider. MSSP activity triggered by application provider. Digest computed by MSSP. Digital Signature computed by mobile device. AdES built by the MSSP.

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. It 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 mobile device (step 4). Once the user is notified and authorises the computation of the digital signature (step 5), the SCD performs the computation (step 6) and the mobile 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 & 6.). For example the application access may be from a PC, while the signature is computed on a mobile phone.

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

The following table describes of the features of this scenario:

Feature	Description of approach in this scenario
a) Whether document created on to the mobile device or provided by an external application;	On remote application provider
b) where is document hashed	On remote application provider or MSSP
c) what is displayed to user when signing	Full document or hash of the document and optionally help text
d) Where user sole control over the signature creation is initiated	On mobile device
e) Where is the private key held & digital signature created	In mobile device
f) In case digital signature is created on mobile device is this done within SE, TEE, external device, other trusted environment	SE, TEE ,-external device or other trusted environment
g) Where are steps relating to the completion of the AdES signature structure carried out	On remote application provider or MSSP
h) How is signatory authenticated	By showing her ability to use the private key held in the mobile device, e.g. by using signing PIN towards a hardware signature creation device.
i) Mobile network specific	Steps 4 & 7 above are sent over a mobile specific network
j) Applicable to general computing devices as well as mobile devices or just mobile devices	Just mobile device

4.3.2.4 AdES completely generated in a mobile device.

This clause shows a high level approach to scenarios where the mobile device is able, not only to compute the digital signature value, but to generate the whole AdES. Below follows the scenario L3 where the mobile device is a handheld device equipped with a secure element (e.g. SIM) that has capability for generating the whole AdES structure.

In this scenario the signing key is held at the mobile device (e.g. within a SIM).

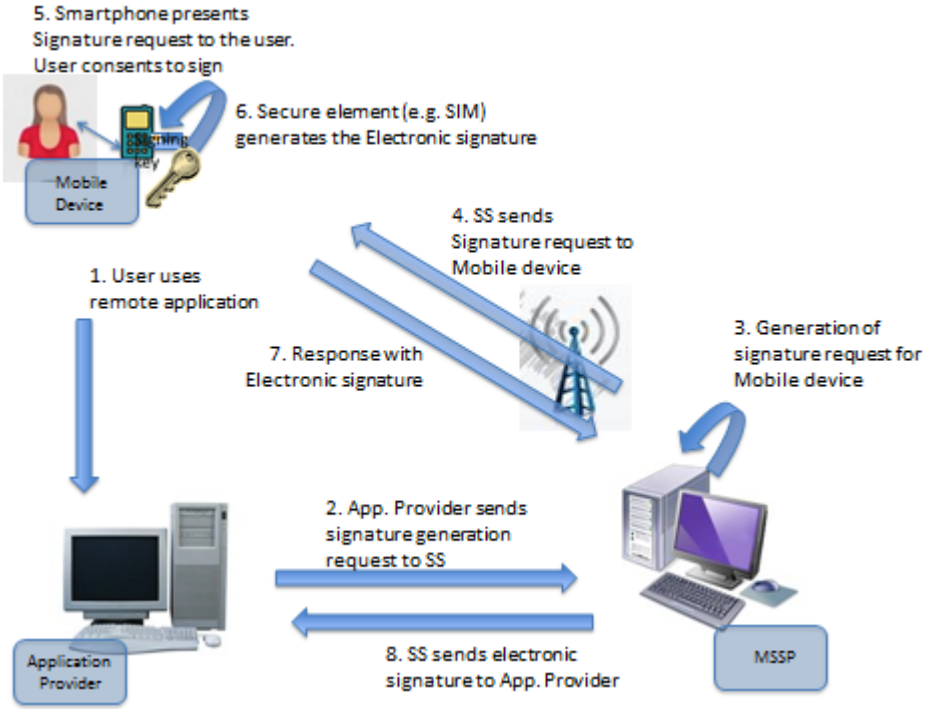


Figure 3: Scenario L3. Document generated by application provider. MSSP activity triggered by application provider. AdES generated by mobile device. AdES passed to the application provider by the MSSP.

In this scenario the user makes use of an application provider. This use may be from the mobile device or from another device, e.g. a PC.As a result of certain operation performed by the user (step 1), the AP concludes that it needs an AdES to be generated by the user. It then builds up and sends (step 2) a signature generation request to the MSSP. 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 mobile device (step 4). Once the mobile device receives this request, the user is presented some text notifying the request (could be the entire document), as well as other data clearly indicating the consequences of satisfying that request. The user then consents to signing e.g. by entering the signing PIN for the SIM card (step 5). The SIM then proceeds to generate the AdES (step 6), possibly adding elements such as certificates and signing time if not done by the signing server. The mobile device then sends the response including the signature (step 7) to the signing server, which in turn, sends to the application provider the AdES obtained from the user's mobile device (step 8).

Variants of the scenario are possible. For example, the mobile device may generate only a digital signature, leaving extension to an AdES to the signing server. In another variant, the signing server (or the application provider) generates the hash to be signed and only the hash value is sent to the mobile device. The same hash value should be displayed in a user interface either by the signing server or the application provider for comparison. The user only sees the hash value on the mobile device signs this value and returns the digital signature. The signing server (or the application provider) extends this to an AdES signature.

ETSI TS 102 204 specifications cover a variant of the former scenario: that document does not specify a protocol covering the exchanges between the SS and the mobile device.

A variant of this scenario is also possible, where communication between the signing server and the mobile device is not over the mobile network. Signing will be carried out as described above but access to the SIM from the signing software on the mobile device may in this case be restricted, meaning that the signing key may have to be stored in another (secure) environment.

The following table describes of the features of this scenario:

Feature	Description of approach in this scenario
a) Whether document created on to the mobile device or provided by an external application;	On remote application provider
b) where is document hashed	On mobile device
c) what is displayed to user when signing	Full document displayed on mobile, alternatively full document displayed from application provider or signing server and hash or other identification of document displayed on mobile
d) Where user sole control over the signature creation is initiated	On mobile device
e) Where is the private key held & digital signature created	In mobile device
f) In case digital signature is created on mobile device is this done within SE, TEE, external device, other trusted environment	SE, TEE or secure external device
g) Where are steps relating to the completion of the AdES signature structure carried out	On mobile device
h) How is signatory authenticated	By showing her ability to use secure signing device
i) Mobile network specific	Steps 4 & 7 are sent over a mobile specific network
j) Applicable to general computing devices as well as mobile devices or just mobile devices	Just mobile device

4.3.3 Remote Signing Scenarios

4.3.3.1 Remote Signing Scenarios – General Introduction

The following scenarios are where the AdES is created using a using a signing key held by a signing service provider within a cryptographic security module.

Note: For such scenarios, it is considered that solutions are available which are equally applicable mobile devices and other computing devices which at the time of signing are be under the sole control of the signatory (e.g. personal computers).

4.3.3.2 Generation of AdES in a server

In this common scenario, a mobile device is able to generate a document or to receive a document generated elsewhere. The mobile device (or other computing device) is powerful enough as to run client software of a protocol that requests the generation of an AdES to a remote signing service provider. The complexity of the requests (that could range from

only one type, always requesting the generation of an AdES of the same type, to a more elaborated set of requests allowing to generate different types of AdESs) will directly depend on the mobile device power and the specific protocol/profile actually implemented by the client software. The signing service provider takes care of the whole process of generating the AdES. After its generation the server returns the AdES to the mobile device, which may process it accordingly. This service "type 1" sole control as specified in CEN TS 419 241

In this scenario the signing key is held by the signing service provider within a cryptographic security module.

The diagram below shows the relevant participating entities and information flows for a scenario where the document is generated either within the mobile device or by an external application provider.

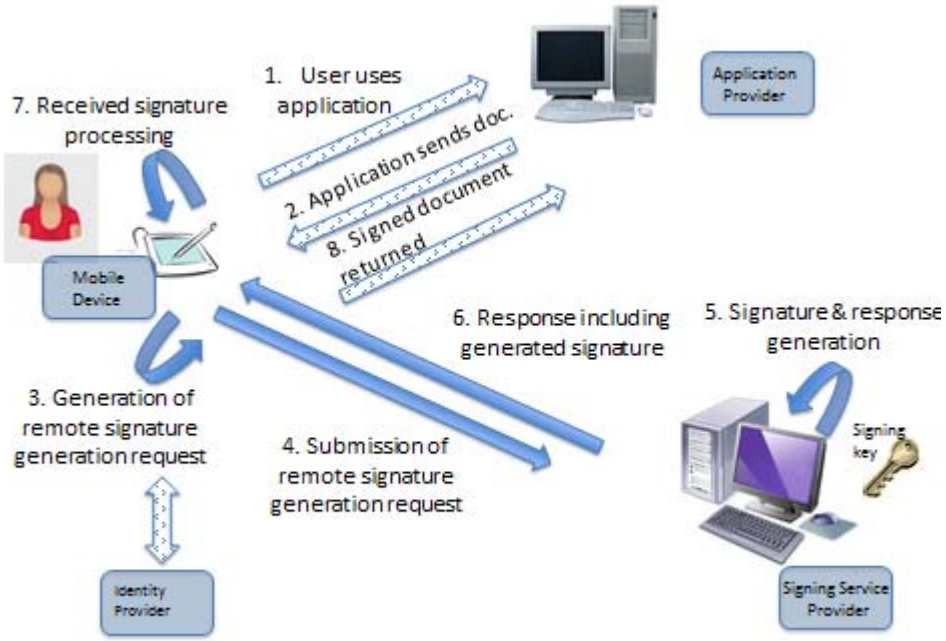


Figure 4: Scenario R1: Document generated by an application provider. Signature requested by Mobile Device. AdES generated by the Signing Service Provider.

In this scenario, a user may be using an application provided by an application provider as a result of which that application generates (step 1) and submits a document to be signed (step 2). If the document is created locally these steps are skipped.

The signing service provider protocol client running in the mobile device generates (step 3) and sends (step 4) a request for generating an AdES to the signing service provider. The signing service provider generates the AdES and the response to the request (step 5) and sends it back to the client (step 6). The user may then process the received AdES (step 7) as allowed by the application running on the mobile device. In many cases, the signed document will be sent to the application provider.

In step 3, either the hash of the data to be signed will be computed on the mobile device, or the document and possibly signature attributes to be signed, for example signing certificate and signing time, will be gathered into the request. In step 5, the signing service provider may gather further signature attributes to be included with the data to be signed, if not provided by the mobile device, unless this is supplied by the mobile device. Generation of an SDO format according to AdES standard can be done on the mobile device (step 7). In the signing service provider (step 5) or in some cases even in the application provider.

Following these exchanges the document may be passed back to the application (step 8).

The authentication of the user to the signing service provider may involve an external identity provider.

The following table describes of the features of this scenario:

Feature	Description of approach in this scenario
a) Whether document created on to the mobile device or provided by an external application;	On mobile device or remote application provider. The server signer function and the application provider may be supported by the same service provider.
b) where is document hashed	Mobile device or signing service provider
c) what is displayed to user when signing	Whole document displayed on mobile device
d) Where user sole control over the signature creation is initiated	Mobile device
e) Where is the private key held & digital signature created	Signing service provider
f) In case digital signature is created on mobile 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	Mobile device or signing service provider, possibly also the application provider.
h) How is signatory authenticated	The signatory authenticates him/herself to the signing service provider. This may include support of remote identity provider.
i) Mobile network specific	This scenario is not expected to be specific to mobile networks
j) Applicable to general computing devices as well as mobile devices or just mobile devices	A general computing device may be used instead of the mobile device.

4.3.3.3 Generation of AdES in a server with direct control over signing

This clause shows a scenario where the AdES is created on a server with the user of the mobile device (or other intelligent device under the sole control of the signatory at time of signing) having direct control over the use of the use of its private key for signing, providing “type 2” sole control as specified in CEN TS 419 241. This direct control provides equivalent to use of a secure signature creation device (as defined in Directive 1999/93 **Error! Reference source not found.**). This may be used, for example, to provide strong evidence of the consent to the content of a document. The figure below shows a high level approach of the relevant actors and exchanges in this scenario.

Note: The specific requirements of the user device is under consideration within CEN TC 224 WG17.

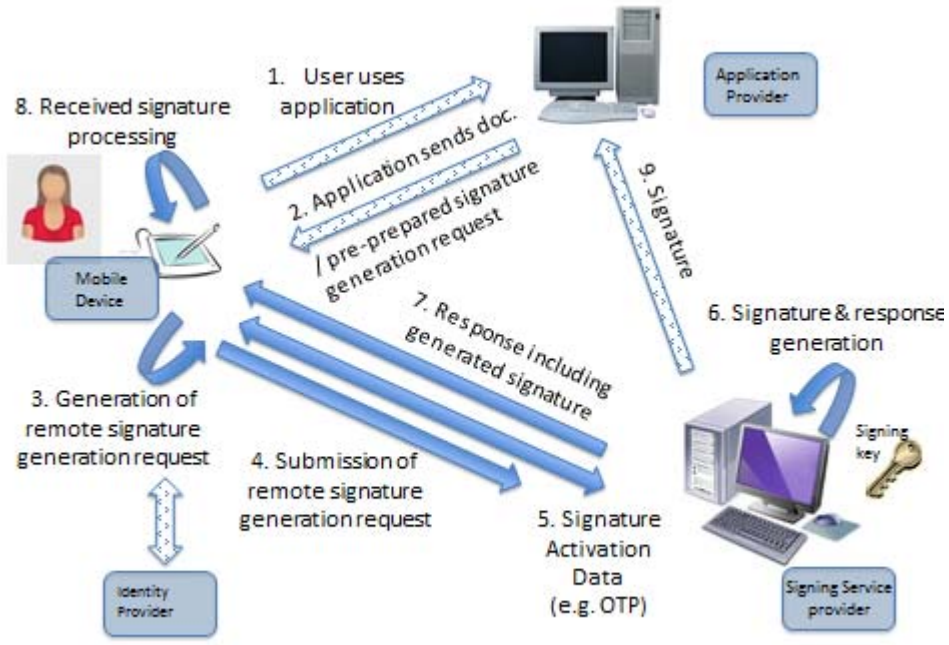


Figure 5: Scenario R2. AdES generated by signing service provider with Direct Control over signing.

The exchange is similar to the server signing scenario above with the extra step 5 where "signature activation data" is provided from the mobile device which activates use of the signing key for a specific document (e.g. using a one-time password).

This scenario may begin with the document created on the mobile device or in connection with a remote application provider (steps 1 &2). The mobile device (or an application provider on behalf of the mobile device) then prepares a signature request including the document to be signed along with any signature attributes, and may compute the hash of all the data to be signed (step 3). The signature request, including the document and any signature attributes, or a hash value of all the data to be signed, or some other form of data to be signed representation, is sent to the signing service provider (step 4). Further signature activation data exchanges will occur as required to enable use of the user's signing key (step 5). The signature server may just create the digital signature value, or create the AdES value containing the digital signature value if necessary collecting any additional signature attributes (step 6). The resulting signature (digital signature value or AdES or AdES within a document) is returned to the mobile device (step 7). If just the digital signature value is returned to the mobile device then this may complete the creation of the AdES structure (step 8). The signed document may be sent back to the application by the mobile device for further processing or storage.

As an alternative to including the signature in step 7 the generated signature may be returned directly to the application provider to integrate the signature with the document.

There are several variants of step 5 this scenario depending on the means of authentication of the user from the mobile device to the server.

Editor's note: Further work may be required on the variations possible. This document does not currently consider in details the requirements and options for authentication that meet the requirements of TS 419 241

Feature	Description of approach in this scenario
a) Whether document created on to the mobile device or provided by an external application;	On mobile device or remote application provider. The server signer function and the application provider may supported by the same service provider.
b) where is document hashed	Mobile device or signing service provider

c) what is displayed to user when signing	Whole document displayed on mobile. There are several scenarios, which may be combined: Application server displays document (e.g. web interface), document stored locally on mobile device for display, signing server displays document as part of a signing dialogue with the user.
d) Where user sole control over the signature creation is initiated	Mobile device using activation data (e.g. one time password).
e) Where is the private key held & digital signature created	Signing service provider
f) In case digital signature is created on mobile 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	Mobile device or signing service provider or application provider.
h) How is signatory authenticated	The signatory authenticates him/her self to the signing service provider. This may include support of remote identity provider. Additional data is provided to activate the user's signing key (step 5).
i) Mobile network specific	For some variations of this scenario part of the exchange may be via a mobile specific network.
j) Applicable to general computing devices as well as mobile devices or just mobile devices	A general computing device may be used instead of the mobile device except for certain options which may involve mobile network communication in part of the exchange.

4.3.4 Split Local and Remote Signing Scenario

This clause shows a scenario where the signing function split between the mobile device and the signing service provider, each with part of the signing key. Thus the digital signature creation function is split between the mobile device and the signing service provider. Examples of such a scheme are given in [i.7] and [i.8]. The figure below shows a high level approach of the relevant actors and exchanges in this scenario.

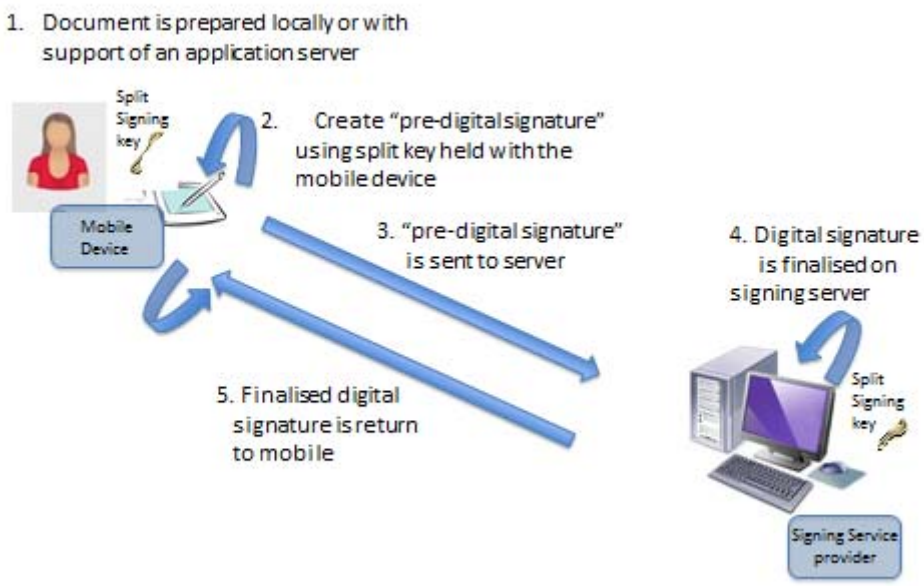


Figure 6: Scenario LR Signatures created Using a Split Key

In this scenario the Document is prepared locally or by a remote application provider (step 1). A "pre-digital signature" is created on the mobile device using the part of the split key held locally (step 2). The pre-signature is sent to the signing service provider (step 3), the digital signature creation is completed using the split key held on the signing service provider for the identified signatory (step 4). The finalised digital signature is then returned to the mobile device.

Feature	Description of approach in this scenario
a) Whether document created on to the mobile device or provided by an external application;	On mobile device or remote application provider. The server signer function and the application provider may supported by the same service provider.
b) where is document hashed	Mobile device
c) what is displayed to user when signing	Whole document displayed on the mobile device
d) Where user sole control over the signature creation is initiated	Mobile device
e) Where is the private key held & digital signature created	Split between mobile device and signing service provider
f) In case digital signature is created on mobile device is this done within SE, TEE, external device, other trusted environment	The mobile half of the split key may be held in SE, TEE or other trusted environment.
g) Where are steps relating to the completion of the AdES signature structure carried out	Mobile device (or signing service provider)
h) How is signatory authenticated	To be defined. May include support of remote

	identity provider.
i) Mobile network specific	Currently, known implementations are not mobile specific.
j) Applicable to general computing devices as well as mobile devices or just mobile devices	A general computing device may be used instead of the mobile device.

4.3.5 Remote Validation scenario

Managing validation of AdESs in the mobile environment may also become a frequent scenario given the increasing mobility in business. The figure below provides a high level view of such a scenario:

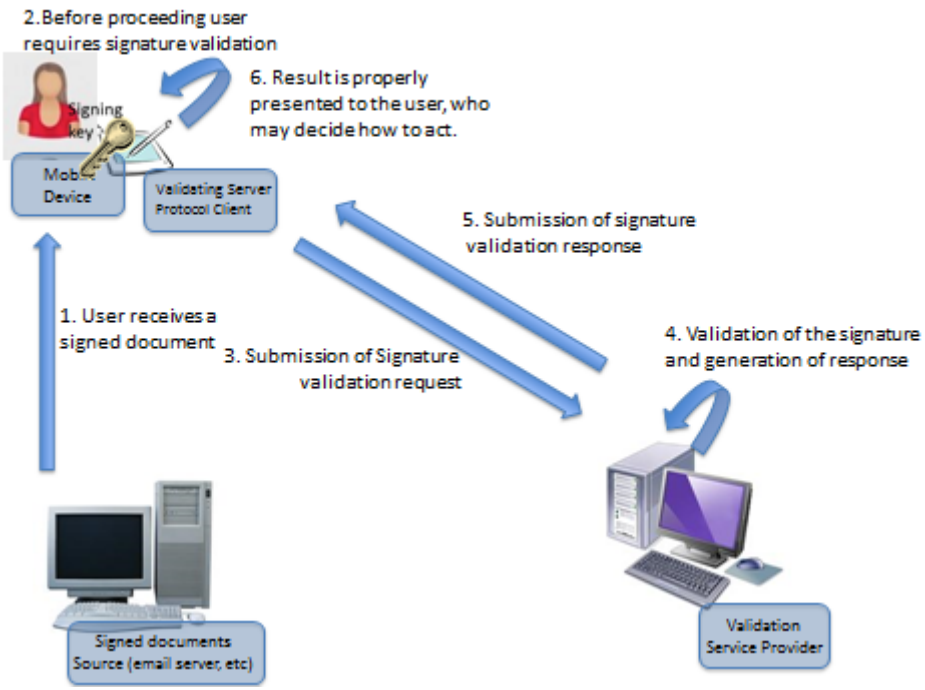


Figure 7: Scenario RV. Using mobile device in an AdES validation scenario.

In this scenario a user equipped with a mobile device receives a signed document (step 1). The user requires signature validation (step 2) to the validating server protocol client that is running in her mobile device. The client generates and submits a signature validation request (step 3) to the remote Validation Server (RVS henceforth). The RVS will proceed to validate the AdES(s) in the document (step 4) and to build and submit the validation response (step 5) to the client. The result of the validation is then properly presented to the user (step 6) in her mobile device.

In a variant of this scenario, only certificate validation is performed by the RVS, while other signature processing is done on the user's mobile device. The signature validation request will then include the certificate or certificate chain to validate, and the response will include information on validity, including revocation status, and possibly auxiliary information such as quality parameters (e.g. whether the certificate is qualified or not).

4.4 Use cases for service life cycle management

The following use cases related to the life cycle management of the service are analysed in order to understand whether they put requirements on the standardization activities.

4.4.1 Use Cases Related to Mobile Signature Service Life Cycle Management

Editor's note: Introductory paragraph required explaining the following.

The following scenarios are aimed primarily at local signing scenarios.

USE CASE	ACTORS INVOLVED
Use Case #1: Mobile Signature Service Deployment: The end-user subscribes to a mobile signature service provided by a Mobile Signature Service Provider.	Registration authority, a Certification authority and the MSSP (see TR 102 203, clause 13.2.1).
Use Case #2: Mobile Signature Service Activation: Following its deployment, the service may require an explicit activation operation	user and MSSP
Use Case #3: Mobile Signature Service Suspension: the Mobile Signature Service Provider may require to the signature service to be temporarily un-usable by the end-user.	user, MSSP, Registration authority, Certification authority
Use Case #4: Mobile Signature Service Resumption: the Mobile Signature Service Provider may require the service to be made usable again	user, MSSP, Registration authority, Certification authority
Use Case #5: Mobile Signature Service Upgrade:	user, MSSP
Use Case #6: Mobile Signature Service Data Exchange/Update	user, MSSP
Use Case #7: Mobile Signature Service Un-Deployment.	user, MSSP

4.4.2 Use Cases Related to End-User Life Cycle Management

Editor's note: Introductory paragraph required explaining the following.

USE CASE	ACTORS INVOLVED
Use Case #8: Secure Element Change.	user, MSSP, Registration authority, Certification authority
Use Case #9: Mobile Phone Number Change.	user, MSSP, Registration authority, Certification authority
Use Case #10: Mobile Device Change.	user, MSSP
Use Case #11: Lost or Stolen Mobile Device	user, MSSP
Use Case #12: Recover Mobile Device After a Loss.	user, MSSP
Use Case #13: Get a New Mobile Device After a Loss,	user, MSSP
Use Case #14: Mobile Subscription Termination.	user, MSSP, Registration authority, Certification authority
Use Case #15: MNO Swap	user, MSSP, Registration authority, Certification authority

5. Analysis of Standardisation Requirements

5.1 Requirements on protocols for requesting signatures creation and validation

This clause summarizes a list of potential requirements that the protocols used by entities within the scenarios described in clause 4 should fulfil in order to properly manage the generation and validation of the Advanced Electronic Signatures and ASiC containers specified within the rationalized framework. The following requirements are identified for technical specifications to be developed for AdES in mobile environments:

Below follows the list of requirements that the (set of) technical specifications included within the rationalized framework should include fulfil:

1) This set of technical specifications should work properly with any identification/authentication scheme provided that the level of assurance of the authentication meets the identified authentication requirements.

2) This set of technical specifications should allow clients to request to remote servers the generation / validation of AdES according to the constraints specified within a certain signature policy.

3) This set of technical specifications should allow clients to request to a remote server the generation of a CAdES, XAdES, PAdES signature or an ASiC container fully compliant with the corresponding Baseline Profile.

   Editor's note references to be added.

4) This set of technical specifications should allow clients to request to a remote server the generation of an AdES signature/ASiC container as specified in (reference).

   Editor's note references to be added.

5) This set of technical specifications should allow clients to request both the generation of an AdES signature and the incorporation of a signature time-stamp.

6) This set of technical specifications should allow clients to request to a remote server the computation of a digest value to be signed by a (secure) signature creation device owned by the client's user. They should also allow, when necessary, to request to a remote server, the building up of the complete AdES signature / ASiC package once the client passes the signature value computed in the client's (secure) signature creation device to the remote server.

7) This set of technical specifications should allow clients to send to a remote server a pre-generated (with a part of the private key stored within the (secure) signature creation device) AdES and request the server to complete the generation of the AdES with the other part of the private key stored at the server's premises.

8) This set of technical specifications should allow clients to request, for certain types of documents, both the generation of AdES(s) and the inclusion of its(their) visual representation(s) in selected places of the signed document. They should also allow to provide details on the components of the visual representation(s) of the AdES(s) to be incorporated.

9) This set of technical specifications should allow to work with two modes of operation, namely: synchronous and asynchronous where this possible with the available protocols.

10) This set of technical specifications should allow clients to request the validation of AdES(s) to a remote server.

11) When requesting the validation of AdES(s), this set of technical specifications should allow to also request a detailed validation report for each validated AdES, fully aligned in its contents with the validation results specified within EN 319 102.

12) When requesting the validation of AdES(s), this set of technical specifications should allow to also request that the remote server signs the validation report.

13) This set of technical specifications should allow support the AdES signatures and ASiC containers lifecycle. This means that clients should be able to submit a certain signature/container to a remote server and request its validation and subsequent upgrade to a more evolved form.

Specific instantiations of the scenarios described in clause 4 of the present document, could impose any subset of the set of requirements listed above, with the following exceptions:

- Requirement 6) is applicable only in the scenarios described in scenarios R1 and R2. In these scenarios, requirements 1 to 5, 8, and 9 still apply if one takes into account that "request to a remote server the generation of an AdES" should be understood as a "request to a remote server the building up of an AdES with the digital signature value passed from the client".

- Requirement 7) is applicable only in the scenario described in scenario LR. In this scenario, requirements 1 to 5, 8, and 9 still apply if one takes into account that "request to a remote server the generation of an AdES" should be understood as a "request to a remote server the completion of an AdES from the pre-generated signature passed from the client".

- Scenario L3, where the generation of the AdES is allocated to a mobile device, will very likely to consist in generating exactly the same type of AdES, not needing in consequence most of the requirements listed above. Scenario 6, however, may impose requirements within 1 to 5, 8 and 9, because the actual generation of the signature is done within the remote server, and because the protocol supports the interaction between the Application Provider and the Signing Server.

Editor's note: The applicability of the requirements to the specific scenarios above requires further consideration.

5.2 Requirements related to service life cycle management

The following standardization requirements are dictated by the service life cycle management for local signing use cases analysed in clause 4.5.2

5.2.1 Use Cases Related to Mobile Signature Service Life Cycle Management

USE CASE	IMPACT ON STANDARDIZATION
Use Case #1: Mobile Signature Service Deployment: The end-user subscribes to a mobile signature service provided by a Mobile Signature Service Provider.	The set of technical specifications should allow a Registration Authority to ask for a Proof of Possession from a MSSP with respect to a specific user; it should also allow for pushing a certificate or a certificate identifier to the MSSP.
Use Case #2: Mobile Signature Service Activation: Following its deployment, the service may require an explicit activation operation	--
Use Case #3: Mobile Signature Service Suspension: the Mobile Signature Service Provider may require to the signature service to be temporarily un-usable by the end-user.	The set of technical specifications may allow a MSSP to request the certification authority to suspend a certificate.
Use Case #4: Mobile Signature Service Resumption: the Mobile Signature Service Provider may require the service to be made usable again	The set of technical specifications may allow a MSSP to send a reactivation request to the Certification Authority
Use Case #5: Mobile Signature Service Upgrade:	--
Use Case #6: Mobile Signature Service Data Exchange/Update	--
Use Case #7: Mobile Signature Service Un-Deployment.	The set of technical specifications should allow a MSSP to send a suspension/reactivation/revocation request to the Certification Authority

5.2.2 Use Cases Related to End-User Life Cycle Management

USE CASE	IMPACT ON STANDARDIZATION
Use Case #8: Secure Element Change.	The set of technical specifications should allow a MSSP to send a revocation request to the Certification Authority
Use Case #9: Mobile Phone Number Change.	??
Use Case #10: Mobile Device Change.	??
Use Case #11: Lost or Stolen Mobile Device	The set of technical specifications should allow a MSSP to send a suspension/ /revocation request to the certification authority
Use Case #12: Recover Mobile Device After a Loss.	The set of technical specifications should allow a MSSP to send a reactivation request to the Certification Authority
Use Case #13: Get a New Mobile Device After a Loss,	??
Use Case #14: Mobile Subscription Termination.	The set of technical specifications should allow a MSSP to send a revocation request to the Certification Authority

Use Case #15: MNO Swap	The set of technical specifications should allow a MSSP to send a revocation request to the Certification Authority

5.3 Standardisation Requirements summary

See following table analysis the standardisation requirements for the above scenarios against the rationalised framework for electronic signature standardisation (TR 119 000).

Requirements address by existing standardisation or standardisation already in the ETSI work plan is highlighted in green.

Requirements requiring further standardisation are highlighted in red.

See Annex B for a detailed analysis of requirements against the two most relevant standards for AdES in mobile environments: OASIS DSS [i.9] and other associated specifications and MCOMM [i.10], [i.11], [i.12], [i.12], [i.13].

Table 1 – Analysis of standardisation requirements for mobiles in AdES environments

	Scenario L1	Scenario L2	Scenario L3	Scenario R1	Scenario R2	Scenario LR	Scenario RV
Area 1 Sig. create / val'n	All existing standards TS 119 152 Note 5	All existing standards TS 119 152 Note 5	All existing standards TS 119 152 Note 5	All existing standards TS 119 152 Note 5	All existing standards TS 119 152 Note 5	All existing standards TS 119 152 Note 5	All existing standards
Area 2 Sig devices	EN 419 211	EN 419 211	EN 419 211	EN 419 221 &	EN 419 221 & EN 419 241	EN 419 221	EN 419 221
Area 3 Algo	TS 119 312	TS 119 312	TS 119 312	TS 119 312 Note 1	TS 119 312 Note 1	To be determined	TS 119 312
Area 4 TSP	No Policy requ. see note 2. EN 319 432 Note 3 Note 6	No Policy requ. see note 2. EN 319 432 Note 3 Note 6	No Policy requ. see note 2. EN 319 432 Note 3 Note 6	EN 319 431 EN 319 432 EN 319 403 Note 3	EN 319 431 EN 319 432 EN 319 403 Note 3	Note 4 EN 319 432 Note 3 Note 6	EN 319 441 EN 319 442 EN 319 403
Area 5 TASP	Not applicable	Not applicable	Not applicable	Not applicable	Not applicable	Not applicable	Not applicable
Area 6 TSSLP	See note 2	See note 2	See note 2	Extension may be required to EN 612 for new TSP type	Extension may be required to EN 612 for new TSP type	Note 4	Extension may be required to EN 612 for new TSP type
Area xx eID (see note 1)				TR 419 010	TR 419 010		

Note 1: Area XX eID standards may include standards in other areas relating to eID as described in TR 419 010.

Note 2: Assuming signature is validated after creation the MSSP does not need to be trusted.

Note 3: Requirements for Testing conformance and interoperability to be determined later.

Note 4: Analysis of the risks of a server holding a split key is required to determine whether this requires an audited "trust service"

Note 5: An architecture document is considered necessary to describe the interaction between the TSP related elements and other elements of the mobile solution (document preparation, AdES format creation etc.). This is not necessary for the validation service.

Note 6: Further consideration required of analysis of certificate & private key lifecycle specific to mobiles. This should take account of 3GPP TS 33.221 "3GPP GAA (Generic Authentication Architecture) support for subscriber certificates [i.21]

The main new areas of standardisation required (as indicated in red) are:

As indicated above it is considered that a framework is required:

TS 119 152: a document is required which takes the work of this document forward providing a framework for all the interactions between the TSP related elements and other elements of the mobile solution (document preparation, AdES format creation etc.).

EN 319 431 For remote signing scenarios the operation of the TSP providing the signing services needs to be trusted to ensure that the keys held on the server are not subject to the open to hostile attack .

EN 319 432 This needs to address protocol requirements for use of TSPs (MSSP and signing service providers) to support both local and remote signing. For local signing both MCOMM and DSS are applicable. MCOMM already has a significant installed base and can take advantage of particular features of mobile environment. DSS has the advantage of being generally applicable to both mobile and of computing environments. For remote signing DSS is directly applicable.

EN 319 441 For remote validation scenarios the operation of the TSP providing the validation services needs to be trusted to ensure the service is not subject to the open to hostile attack .

EN 319 442 This needs to address protocol requirements for use of TSPs (validation service providers) to signature validation. DSS is directly applicable although other services may be used to support signature validation:

- W3C XML Key Management Specification [i.24] XML Key Information Service Specification. This allows only certificate validation – the signatures themselves are processed on the "device". In many cases this may be sufficient.
- IETF RFC 3029 Data Validation and Certification Server protocols [i.25].
- RFC 5055 Server-Based Certificate Validation Protocol) [i.26]. This only certificate validation.

5.4 Applicability to General Computing Devices

Whilst the scenarios identified in clause 4 derived from consideration of the mobile environment much of the required standardisation could be equally applicable to any environment employing general computing devices provided they are under sole control of the signatory at the time of signing. Only scenario L3 is specific to mobile devices, although variations of all the local scenarios (L1, L2, and L3) and potential options within the remote signing scenario R2 can require mobile devices connected to a mobile network. Moreover the existing and planned standards highlighted in green are already aimed at the general computing environments.

6. Further standardisation requirements

Based upon the analysis for the standardisation given in clause 5, the following further standardisation is required.

Editor's note: Input is requirested from reviewers on specifications that may be relevant to the following standardisation activities.

6.1 TS 119 152 –Architecture for Advanced AdES in Distributed environments

Scope

The goal of this specification is to provide details on the framework for standards (including potential architectures and relevant scenarios) required for the creation of advanced AdES in the mobile environment (Advanced Electronic Signatures in Mobile Environments).

Starting Points

This framework is to be based upon:

- OASIS DSS [i.9] and other associated specifications and MCOMM [i.10],
- MCOMM [i.10], [i.11], [i.12], [i.12], [i.13]

6.2 EN 319 431 –Policy Requirements for TSPs providing Signature Generation Services

Scope

This document specifies policy requirements for TSPs providing signature generation services. This document will reference EN 319 401 for general requirements.

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

Note 2: This activity may identify requirements for changes to TS 319 612 to identify further trust services.

Starting Points

This framework is to be based upon:

- EN 319 401 [i.18]
- TS 419 241 [i.16]

6.3 EN 319 441 –Policy Requirements for TSPs providing Signature Validation Services

Scope

This document specifies policy requirements for TSPs providing signature validation services. This document will reference EN 319 401 for general requirements.

Note 1: This activity may identify requirements for changes to TS 319 612 to identify further trust services.

Starting Points

This framework is to be based upon:

- EN 319 401 [i.18]

6.4 EN 319 432 –Profiles for TSPs providing Signature Generation Services

Scope

This multi-part document profiles the MCOMM and DSS protocols to support local and remote signature validation.

Note: The titles below are provisional and subject to revision.

Part 1: Trusted Service manager

The document 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 Mobile service. This is based on TS 102 204 [i.11] and potentially other specifications in the MCOMM series.

Part2: Local signing on mobile device

This document specifies the use of mobile devices for local signing supported by Mobile Signing Service Providers based on TS 102 203 [i.10], TS 102 204 [i.11] , TS102 206 [i.12] and TS 102 207 [i.13]. It will take into account requirements identified in 5.1, 5.2.

Part 3: Local signing on general computing device

This document specifies the use of mobile or other computing devices for local signing supported by services based OASIS DSS [i.9]. It will take into account requirements identified in 5.1, and the use of DSS as in 5.3.1.

Part 4: Remote signing

This document specifies the use of mobile or other computing devices for remote signing supported by services based OASIS DSS [i.9]. It will support both the level 1 and level 2 sole control as specified in TS 419 241 [i.16]. It will take into account requirements identified in 5.1, and the use of DSS as in 5.3.1.

Note: Additional parts may be added for Split Key Local & Remote Signing as described in clause 4.3.4 Split Key Local and Remote Signing Scenario

Starting Points

- OASIS DSS [i.9]
- MCOMM [i.10], [i.11], [i.12], [i.12], [i.13]
- TS 419 241 [i.16]

6.6 EN 319 442 –Profiles for TSPs providing Signature Validation Services

Scope

This document specifies a profile for the format and procedures for TSPs providing Signature Validation Services.

This service is equally applicable to mobile devices and other computing devices.

Starting Points

- OASIS DSS [i.9] – This expected to be the primary source.

The following may provide additional features that should be considered.

- W3C XML Key Management Specification [i.24] XML Key Information Service Specification. This allows only certificate validation – the signatures themselves are processed on the "device". In many cases this may be sufficient.
- IETF RFC 3029 Data Validation and Certification Server protocols [i.25].
- RFC 5055 Server-Based Certificate Validation Protocol) [i.26].

Annex A Inventory of Existing Systems

An inventory of know specifications relating to advanced electronic signatures is given in spread-sheet file (AdESMobileInventory.xls) which accompanies the present document.

Editor's note input is requested from reviewers of the present document on information relating to systems for AdES in mobile environment if with the details as included in the accompanying spread-sheet file.

Annex B: Most Relevant Standards

B.1 Introduction

Nowadays there are a number of technical 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 clause first reviews two of the most relevant sets of specifications that are widely used worldwide: OASIS DSS [i.9] and other associated specifications and MCOMM [i.10], [i.11], [i.12], [i.12], [i.13].

B.2 OASIS DSS and DSS-X Specifications

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

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

2) A VerifyRequest / VerifyResponse protocol. This protocol specified the semantics and the syntax of a XML message (VerifyRequest) that a client may use to request to a remote server the validation of one (or more if there are more than one AdES within a certain document) electronic. It also specified the semantics and the syntax of a XML message (VerifyResponse) that the aforementioned remote server may use to return to the client the result of the requested validation process on the AdES(s) passed in the request.

The basic features of both protocols were defined within the so-called OASIS DSS Core Protocol/Specification. A number of Profiles were also defined that sometimes constrained the degree of optionality and sometimes incorporated features to the protocol that had not been specified within the core document.

The approach taken by DSS and DSS-X when conceiving such profiles was to build coherent profiles, i.e., to devote one profile to solve one specific problem roughly speaking. As a result of that approach, it is not unusual that certain scenarios may require the combination of a certain subset of the features of the DSS Core plus a number of profiles, each one providing one feature required by such scenario.

In order to propose a rationalized framework of standards for requesting the generation/validation of AdES to a remote server, which fulfils the listed in clause 5.1, it is unavoidable to review the features provided by the core protocol and a subset of relevant profiles.

B.2.1 OASIS DSS Core Specification

B.2.1.1 SignRequest / SignResponse protocol

This protocol allows to request generation of both XML Signatures and CMS Signatures. The SignRequest protocol allows to request the generation of one and only one AdES of one specific format.

When requesting XML Signatures the protocol provides the following features:

3) 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 the document(s) itself (themselves), or even the result of applying to the document(s) a set of transformations.

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

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

6) In the case of requesting an enveloped signature, 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:

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

8) It allows to request a detached or an attached CMS signature.

When requesting a XML or a CMS signature the protocol:

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

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

11) Allows to simultaneously request a signature time-stamp, be it an RFC 3161 time-stamp token or a DSS XML time-stamp token.

When returning the generated signature, the protocol:

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

B.2.1.2 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:

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

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

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

B.2.2 AdES Profile

This profile was conceived for supporting the remote generation, validation and upgrade of the existing AdES signatures at the time it was produced, namely CAdES and XAdES signatures.

In consequence, it does not provides these features for requesting generation/validation of PAdES signatures and ASiC packages.

B.2.2.1 SignRequest / SignResponse protocol

The SignRequest operation supports the following features:

16) It allows to request the generation of predefined advanced signature forms defined in XAdES/CAdES.

17) 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:

18) It allows to return predefined advanced signature forms defined in XAdES/CAdES.

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

B.2.2.2 VerifyRequest/VerifyResponse protocol

The VerifyRequest operation supports the following features:

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

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

22) 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:

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

24) It allows to return the result of validating the XAdES/CAdES passed in the request, PLUS the upgraded signatures as requested.

However, there are a number of XAdES/CAdES properties, not existing at the time of producing such profile, which are not properly managed.

Also, at the time this profile was created, PAdES signatures, ASiC containers, and the Baseline Profiles for all the AdES signature formats and ASiC containers, did not exist.

B.2.3 Asynchronous Profile

OASIS DSS Core Protocols were designed as synchronous protocols. The Asynchronous Profile specifies a mechanism for asynchronously manage the generation and validation requests submitted to a remote server.

Under this mode of operation a server may return an empty result to any request submitted by the client, with an indication of 'Pending' result. The client may, at any time, pull the result by submitting a PendingRequest with an identifier of the result requested. The server may, 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 it may be combined with them for obtaining the suitable behaviour of both client and server whenever asynchronous interchanges between them are needed.

B.2.4 Visible Signature Profile

This profile is at present in a Committee Specification status.

The SignRequest / SignResponse protocol of this profile allows a client to request the generation of an AdES and, within the same request, the incorporation of its visual representation within certain part of the signed document. The request may 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 it may be combined with them for obtaining the suitable behaviour of both client and server whenever incorporation of visual information within the signed document is needed.

B.2.5 Local Signature Computation Profile

This profile is in a working draft status.

This profile extends the SignRequest/SignResponse DSS Core protocol for allowing that the actual computation of the signature value is performed within a (secure) signature creation device under the direct control of the user of the client, instead of performing it within the (secure) signature creation device at the server side. The remote server then computes the hash to be signed with the private key by the user's (secure) signature creation device, and builds up the final AdES to be passed to the client.

The features provided by this profile are orthogonal to the features provided by the DSS Core and AdES Profile, which means that it may be combined with them for obtaining the suitable behaviour of both client and server whenever the requirement exist that the computation of the signature value is performed by the user's (secure) signature creation device and the actual building of the resulting AdES is performed at the server side.

B.2.6 Profile for Comprehensive Multi-Signature Verification Reports

This profile is at present in a Committee Specification status.

This profile extends the VerifyRequest/VerifyResponse DSS Core protocol for allowing the server (in reaction to the corresponding request from the client) to include within the response a complete validation report for each AdES 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 document was produced before the publication of ETSI TS 102 853, which identified a number of potential validation output codes, and in consequence, there is a mismatch between both documents.

B.2.7 Other profiles under construction that could have some interest

Apart from the core and the aforementioned profiles, the DSS-X is also working in other profiles that could be of interest for the framework of standards, namely:

25) Signature policy profile: this profile would allow to request the generation/verification of AdES according to a certain signature policy.

26) Signed validation report profile: this profile would allow the server to issue a signed VerifyResponse. This type of feature would allow the establishment of communities where AdES generated inside and even outside are validated by a central server, and the members of such community do not need to worry about the validation of AdES supported by complex and external PKIs. Instead, they only would need to worry about the validation of the signatures generated by this central server.

B.2.8 Usability of DSS protocols within the analysed scenarios

The table below provides details of which of the different DSS protocols could be used in the scenarios described in clause 4, and under which conditions such a use would make sense.

The first column “Features” list the potential features that a certain scenario may require, as this set 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, in consequence, what DSS protocol could be used within 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 does not make sense in the corresponding scenario. A value “Needed New” indicates that there is no protocol within the DSS set of protocols covering that particular feature.

Features	Scenario L1	Scenario L2	Scenario L3	Scenario R1	Scenario R2	Scenario LR
Default Configuration	DSS Core	NA	DSS Core	DSS Core	DSS Core	DSS Core
Request XAdES/ CAdES	AdES Profile	NA	AdES Profile	AdES Profile	AdES Profile	NA
SignatureValue computation in mobile device	Local Signature Computation Profile	NA	NA	NA	NA	NA
Private Key Split	NA	NA	Needed New	NA	NA	NA
Request PAdES / ASiC	Needed new	NA	Needed new	Needed new	Needed new	NA
Request insert visible information	Visible Signature	NA	Visible Signature	Visible Signature	Visible Signature	NA

on signature	Profile		Profile	Profile	Profile	
Select signature policy	Signature Policy Profile	NA	Signature Policy Profile	Signature Policy Profile	Signature Policy Profile	Signature Policy Profile
Request detailed validation report	Validation Report Profile	NA	Validation Report Profile	Validation Report Profile	Validation Report Profile	Validation Report Profile
Request signed validation report	Signed Response Profile	NA	Signed Response Profile	Signed Response Profile	Signed Response Profile	Signed Response Profile
Asynchronous Operation	Asynchron ous Profile	NA	Asynchron ous Profile	Asynchron ous Profile	Asynchron ous Profile	Asynchrono us Profile

B.3 ETSI M-COMM Specifications

ETSI Project (M-COMM) produced mobile commerce and mobile signature service standards that define registration, signature and other important functions required for mobile commerce. Mobile Signature Service offers operations that give control for flexible deployment of Mobile Signature Service platform.

The protocols defined by this specification are generic and gives flexibility to define an implementation based on the implementer needs. The review of important features of these protocols is presented here.

B.3.1 MSS_Signature

This protocol defines mechanism for receiving signature from end user through syntax of an xml message. An Application Provider can request a remote server to generate AdES on a data to be signed.

Mobile Signature profile: The Mobile Signature profile is a way to assure certain signature quality by end user as specification allows different level of capabilities for end users. An Application Provider who wants a specific level of signature quality may request it by using Mobile Signature profile. Mobile Signature profile may also define or link to desired user experience during signing as well. It includes some signature policy enforcement and using specific signature device for signing etc.

Mobile Signature messaging modes: Mobile Signature requests communicated to end user for signing may take variable time due to different reasons e.g. bad network or user is not ready. In such cases, calling party may want to perform this operation asynchronously. M-COMM specification describes three different messaging modes which can be used for Mobile Signature requests depending on the situation and implementation.

- Synchronous mode that binds a caller to wait for signature response.
- Asynchronous ClientServer mode is one way messaging system. Client request status of signature readiness after delivering it continuously until it gets the signature response. The status request call is additionally defined for this purpose.
- Asynchronous ServerServer mode is a two way messaging system. MSS platform responds to client at its specified URL proactively once the signature response is ready. The definition of call-back notification is also provided by specification.

Signature format: The type of signature is not restricted to be any specific by the protocol and instead Application Provider can request signature based on its need if that format is being offered by the platform. A Mobile Signature Service platform may offer XML DSig, CMS, PKCS#7, CAdES, XAdES or even an implementation specific signature format. Application Provider in such case may request specific format in response or just use the default signature format returned by the platform. This gives an opportunity to make use of Mobile Signature Service platform by many different kind of applications including those who already use a specific signature format. Signature can be generated by sending the document to the platform or otherwise its hash may be sent.

Additional Services: An Application Provider may ask standard services offered by platform which are specified by M-COMM or platform specific additional services. The standard additional services include signature validation, time stamping and archiving etc.

B.3.2 MSS_ Status

This protocol defines syntax for an AP in order to get information on a mobile signature transaction whether it has been completed or still outstanding.

B.3.3 MSS_Receipt

This protocol defines a way to issue a receipt of the transaction proceedings. An Application Provider may use this to send a formal receipt to end user specifying the proceedings that has happened.

Signed receipt: Optionally, an Application Provider may send a digitally signed receipt to end user.

B.3.4 MSS_Registration

This protocol specifies mechanism to enrol an end user to Mobile Signature Server platform so that it can later use the service. The registration of an end user to the platform may require initializing user's signing PIN, downloading user's certificate to the SIM and activating the client application.

B.3.5 MSS_Handshake

This protocol defines handshake method that can be used if the Application Provider and Mobile Signature Service platform do not know each other. In such a case they can inquire each other's capabilities by using it. This can happen for example when an Application is not in contract with the platform but coming from a roaming partner.

This protocol may also be used in a situation when both Application Provider and Mobile Signature Service platform know each other and their capabilities but current transaction may require a bit different security level.

History

Document history		
V0.0.2	September 2013	Early draft for review by ESI
V0.0.3	November 2013	Stable draft proposed for public review
V0.0.4	November 2013	Draft for public review