ETSI TS 102 778-6 V1.1.1 (2010-07)

Technical Specification

Electronic Signatures and Infrastructures (ESI); PDF Advanced Electronic Signature Profiles; Part 6: Visual Representations of Electronic Signatures

Reference

DTS/ESI-000085-6

Keywords

e-commerce, electronic signature, security, PAdES

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

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://webapp.etsi.org/IPR/home.asp).

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

Foreword

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

The present document is part 6 of a multi-part deliverable. Full details of the entire series can be found in part 1 [2].

Introduction

Electronic documents are a major part of a modern companies business. Trust in this way of doing business is essential for the success and continued development of electronic business. It is, therefore, important that companies using electronic documents have suitable security controls and mechanisms in place to protect their documents and to ensure trust and confidence with their business practices. In this respect the electronic signature is an important security component that can be used to protect information and provide trust in electronic business.

The present document covers visual aspects of electronic signatures for electronic documents. This includes the appearance of signatures within the document and evidence as to its validity even if the signer or verifying party later attempts to deny (i.e. repudiates; see ISO/IEC 10181-4 [i.1]) the validity of the signature.

Thus, the present document can be used for any document encoded in a Portable Document Format (PDF) produced by an individual and a company, and exchanged between companies, between an individual and a governmental body, etc. The present document is independent of any environment; it can be applied to any environment, e.g. smart cards, GSM SIM cards, special programs for electronic signatures, etc.

The European Directive on a community framework for Electronic Signatures defines an electronic signature as: "Data in electronic form which is attached to or logically associated with other electronic data and which serves as a method of authentication".

The present document applies to visual representations of advanced electronic signatures as defined in the Directive [8].

ISO 32000-1 [1] specifies a digital form for representing documents called the Portable Document Format (PDF) that enables users to exchange and view electronic documents easily and reliably, independent of the environment in which they were created or the environment in which they are viewed or printed.

ISO 32000-1 [1] identifies the ways in which an electronic signature, in the form of a digital signature, may be incorporated into a PDF document to authenticate the identity of the user and validate integrity of the document's content. This includes a means for visually representing the signature within the document. This "signature appearance" by convention often includes information identifying the signatory, but as it is not currently verified by the AdES signature does not in itself authenticate this identity.

1 Scope

The present document specifies requirements and recommendations for the visual representations of advanced electronic signatures (AdES) in PDFs. This covers:

a) Signature appearance: The visual representation of the human act of signing placed within a PDF document at signing time and linked to an advanced electronic signature; and

b) Signature verification representation: The visual representation of the verification of an advanced electronic signature.

The aim of the present document is to provide requirements and recommendations for signature appearances and the visual representation of advanced electronic signatures. This is particularly aimed to help the untrained human understanding of the signature and to further consistency between the signature appearance and the visual representations of the AdES verification in order to help human comparison.

The present document includes further explanation of the two different visual representations of electronic signatures related to PDF.

The present document does not cover printable forms of signature values (e.g. using barcodes) which may be verifiable from the printed document.

NOTE: This use of printable forms of signature value is to be covered in a separate report.

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.

[1] ISO 32000-1: "Document management - Portable document format - Part 1: PDF 1.7".

[2] ETSI TS 102 778-1: "Electronic Signatures and Infrastructures (ESI); PDF Advanced Electronic Signature Profiles; Part 1: PAdES Overview - a framework document for PAdES".

[3] OASIS: "Profile for Comprehensive Multi-signature Verification Reports for OASIS Digital Signature Services Version 1.0".

[4] IETF RFC 3709: "Internet X.509 Public Key Infrastructure: Logotypes in X.509 Certificates".

[5] IETF draft-ietf-pkix-certimage-04: "Internet X.509 Public Key Infrastructure - Certificate Image".

NOTE: Available at http://tools.ietf.org/html/draft-ietf-pkix-certimage-04.

[6] IETF RFC 3739: "Internet X.509 Public Key Infrastructure: Qualified Certificates Profile".

[7] ISO 19005-1 (2005): "Document management - Electronic document file format for long-term preservation - Part 1: Use of PDF 1.4 (PDF/A-1)".

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

[9] IETF RFC 3852: "Cryptographic Message Syntax (CMS)".

[10] ETSI TS 102 778-3: "Electronic Signatures and Infrastructures (ESI); PDF Advanced Electronic Signature Profiles; Part 3: PAdES Enhanced - PAdES-BES and PAdES-EPES Profiles".

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] ISO/IEC 10181-4 (1997): "Information technology - Open Systems Interconnection - Security frameworks for open systems: Non-repudiation framework".

3 Definitions and abbreviations

3.1 Definitions

For the purposes of the present document, the terms and definitions given in [1] and the following apply:

certificate image: image that is part of a X509 certificate as specified in draft-ietf-pkix-certimage-04 [5]

certified identity: information about the signer certified by a trusted source

claimed signing time: time of signing claimed by the signer which on its own does not provide independent evidence of the signing time

conforming signature handler: software application, or part of a software application, that knows how to perform digital signature operations (e.g. signing and/or verifying) in conformance with ISO 32000-1 [1] and the requirements of the appropriate profile

off page display: information displayed by a conforming signature handler that is unmistakable separated from the page content of a PDF document

PDF Signature: binary data object based on the CMS (RFC 3852 [9]) or related syntax containing a digital signature placed within a PDF document structure as specified in ISO 32000-1 [1] clause 12.8 with other information about the signature applied when it was first created

signature dictionary: PDF data structure, of type dictionary, as described in ISO 32000-1 [1], clause 12.8.1, Table 252 that contains all the information about the Digital Signature

signer: entity that creates an electronic signature

validation data: data that may be used by a verifier of electronic signatures to determine that the signature is valid (e.g. certificates, CRLs, OCSP responses)

verifier: entity that validates an electronic signature

signature appearance: visual representation of the human act of signing placed within a PDF document at signing time and linked to an advanced electronic signature

signature verification representation: visual representation of the verification of an advanced electronic signature

The present document makes use of certain keywords to signify requirements. Below follows their definitions:

may: means that a course of action is permissible within a profile

shall: means that the definition is an absolute requirement of a profile

NOTE: It has to strictly be followed in order to conform to the present document.

should: means that among several possibilities one is recommended, in a profile, as particularly suitable, without mentioning or excluding others, or that a certain course of action is preferred but not necessarily required

NOTE: Implementers may know valid reasons in particular circumstances to ignore this recommendation, but the full implications must be understood and carefully weighed before choosing a different course.

3.2 Abbreviations

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

AdES	Advanced Electronic Signature (as specified in Directive 1999/93/EC [8])
AP	Appearance Dictionary
CMS	Cryptographic Message Syntax (as specified in RFC 3852 [9])
CN	Common Name
CRL	Certificate Revocation List
FT	Field Type
OCSP	Online Certificate Status Protocol
PAdES	PDF Advanced Electronic Signature
PDF	Portable Document Format

4 General concepts

An advanced electronic signature (AdES) included within an electronic document is based on a sequence of bytes obtained by applying a cryptographic algorithm, and serving to protect the integrity of the electronic document as well as the identity of the signatory. Signatures that can be applied to a PDF document, as described in ISO 32000-1 [1] and other parts of this multi-part document, are referenced to as a PDF Signature.

PDF (ISO 32000-1 [1]) also includes features to represent electronic signatures in a human understandable way as part of the human readable and printable content. This is referred to in the present document as the signature appearance (as implemented by the value of the AP key in a widget annotation dictionary of a signature field in ISO 32000-1, section 12.7.5.4 [1])

A signature appearance is linked to an AdES which it represents. It can include information identifying the signer (e.g. textual name and/or graphical image of a signature or logo) as separately authenticated by the advanced electronic signature, as well as other information about the signature such as time, reason and location. Some of this information may be extracted by the conforming signature handler from the X509 certificate. The time will be a claimed signing time which may differ from the signature time-stamp which is applied subsequently. The content and appearance of the signature appearance is under the control of the signer and is "sealed" by the advanced electronic signature (digital signature).

The signature appearance is created by the signer and any identification included in the signature appearance is not directly verifiable by the AdES signature. However, this information may be visually checked against the visual representation of the electronic signature (AdES) verification.

A conforming reader may also show a signature verification representation which includes authenticated information derived from the AdES (e.g. identity within the certificate and time-stamp) and the results of its validation. This information is shown as a report off-page from the document being viewed. Such a report will have a hierarchical nature, such that information important for the untrained human like the overall verification result and the signers common name are displayed at top level, while results of the evaluation of long term validation data included in the document are displayed on demand to the user in a lower level of the report. Such a report could be organized in a way similar to DSS-X verification reports [3].

The signature appearance is created at signing time, the signature verification representation is created at validation time; both are visible with a conforming signature handler one on the document page the other off-page.

Unlike signature appearances the visual representation of the signature verification is not placed within the document, but is recreated from the AdES every time the document has been verified by a conforming signature hander.

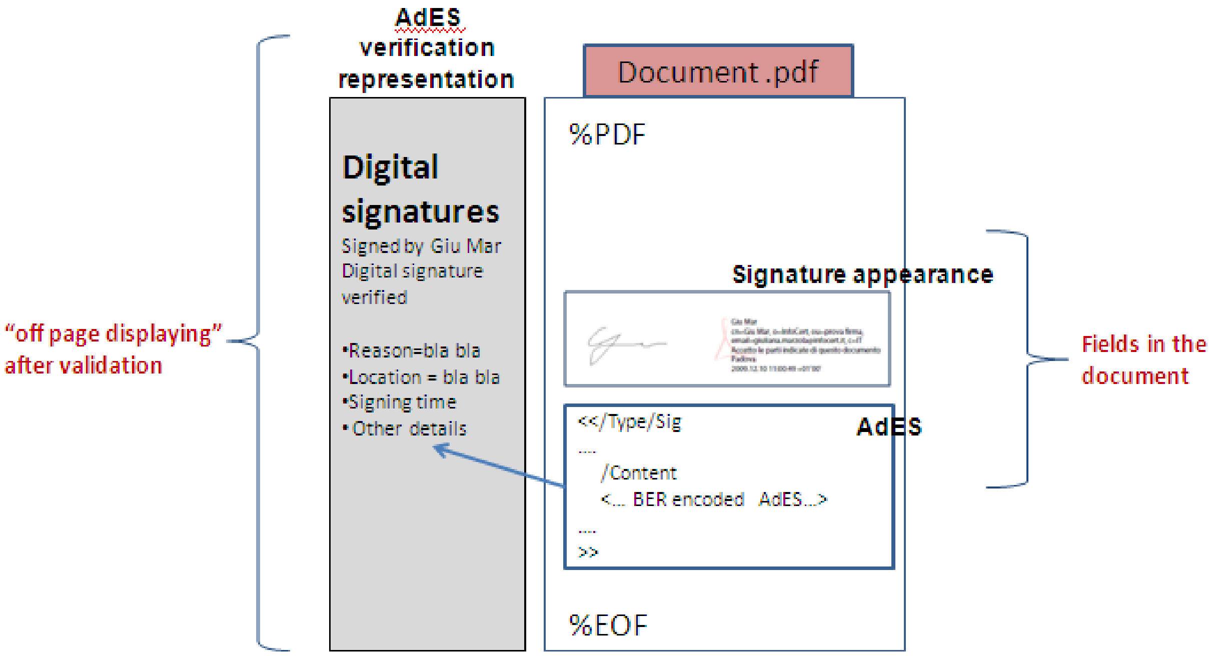

Figure 1: Signature appearance and signature verification representation

The present document provides requirements for the signature appearance, the signature verification representation signature and their relationship to the AdES itself.

The signature appearance is to convey information to the reader about the signature and by being placed within a given context within the document provides meaning to the reader (e.g. authorisation). This information is created by the signer and, while it may include identification and other information also include in the AdES, it is not directly verifiable by the AdES. It could contain some information different from what is present in the visual representation of AdES verification. The present document provides guidance for ensuring consistency between signature appearance and visual representation of AdES verification to aid human comparison so that the signature appearance can be checked against the signature verification representation. This is done by recommending a signature appearances with information about the signatories certified identity in a layout similar to the required visual representation of the AdES signature verification.

5 The signature appearance

5.1 Recommended information in signature appearances

The following requirements are applicable to a conforming signature handler when creating a visual representation of the signature inserted in document at the signing time. A signature appearance represents elements of the AdES signature and other attributes of the signature such as signing time and location.

A conforming signature handler should not use information identifying the signer (e.g. name, graphics) that is not derived from certificate, when creating the signature appearance. The signature appearance may include additional contextual information not included in the certificate (e.g. signing time, location).

The conforming signature handler should include the certified identity of the signatory and the claimed signing time into the signature appearance. The certified identity can be included in two alternative ways:

If the signatories certificate contains a certificate image then the certificate image (draft-ietf-pkix-certimage-04 [5]) should be included in the signature appearance.

NOTE: The certificate image contains information about the signatories identity.

If the signatories certificate contains no certificate image the following information should be included in the signature appearance, in the given order:

a) Name of signatory (as in CN).

b) Affiliation of signatory, if relevant (as in O).

c) Any logo image in the signatories certificate (as defined in RFC 3709 [4]).

d) Any image of a handwritten signature in certificate (as defined in RFC 3739 [6], section 3.2.5).

A signature appearance conformant to this profile may contain the following information that aids the untrained user to validate the signature:

- That the signature appearance is not a source of trust.

5.2 Encoding of signature appearances in PDF

Signatures are stored inside a PDF document using a Signature Field (ISO 32000-1 [1], section 12.7.4.5). A signature field is the type of form field that contains the signature and its field type (**FT**) shall be Sig, and the field value (**V**), which is added at the time of signing, shall be a signature dictionary containing the signature and specifying various attributes of the signature field as defined in TS 102 778 (PAdES) [2].

Like any other field, a signature field may be described by a widget annotation dictionary containing entries pertaining to an annotation as well as a field (ISO 32000-1 [1], section 12.5.6.19). The annotation rectangle (**Rect**) in such a dictionary shall give the position of the field on its page. Although it is possible to have a Signature fields that is not visible, signatures that comply with the present document shall specifying a rectangle whose height and width are greater than zero. In addition, in order to ensure visibility of the signature field, shall not have the **Hidden** bit and not the **NoView** bit of the **F** entry set to true.

NOTE 1: The **F** entry is described in ISO 32000-1 [1], Table 164, and annotation flags are described in ISO 32000-1 [1], Table 165.

The conforming signature handler shall ensure that all text fits into the annotation rectangle.

NOTE 2: Information to be included in the signature appearance is of potential variable length. The above requirement can either achieved by scaling the text at signing time or by denying signature creation where accessibility is an issue.

The actual visual appearance of the signature field on the page is defined by the appearance dictionary (**AP**) of the signature field's widget annotation (ISO 32000-1, section 12.5.5 [1]). In order to ensure compliance with PDF/A (ISO 19005 [7]) all signature fields shall have an appearance dictionary.

When constructing the appearance, a single content stream shall be used, though it may refer to external objects such as Images and Form XObjects as necessary.

NOTE 3: Use of multiple content streams in order to visualize different verification results in the page content as present in some legacy implementations are explicitly deprecated in this profile by above requirement.

It is strongly recommend that the fonts used for any text in the content stream should be embedded. This ensures not only compliance with PDF/A but also guarantees that the recipient will see exactly what the author saw as part of the signing process.

6 The visual representation of AdES signature verification

When verifying a signature a conforming signature handler is often required to display the information of the validity, identity and other information derived from the AdES not only in a precise way that can be used to provide detailed evidence relating to validity of an AdES, but also in a way that is understandable for the untrained human. In order to meet these potentially conflicting needs it is recommended that the verification results are organised in a hierarchical way firstly displaying basic information in way that is easily understood by the untrained human then providing more detailed and specific information as may be needed for evidence when investigating the validity of a signature.

It is recommended that images are included in the certificates as described in RFC 3709 [4] and draft-ietf-pkix-certimage-04 [5] to help the user to reliably match the visual representation of the electronic signature verification to a signature appearance that might be included in the document.

This clause gives requirements and recommendation on how a conforming signature handler should display the results of AdES verification to the human user to maximize the security and the trust of the user towards the AdES signature. Since the page content of a PDF document is outside the control of the conforming signature handler and could present information aimed at misleading the user (e.g. masquerading as verification results providing misleading information) a conforming signature handler is to display the result of the AdES signature verification and the content of signed attributes in a context clearly separated from the page display, called off-page display. For example in a graphical user interface the visual representation of a signature verification is to be displayed in a frame or window different from the display of the page content.

The conforming signature handler shall ensure that such a separated display cannot be faked by use of active document content.

A conforming signature handler **shall not** display the result of the signature validation inside the page content.

NOTE: The conforming signature handler will use off-page display to present the verification result.

The visual representation of the AdES signature verification should be displayed in hierarchical manner showing levels of detail and complexity, initially display basic information in a simple form but enabling the user to obtain further details from an outline where these are required and can be understood by the user.

The outline should contain a visual representation of the verification result of all AdES signatures and document timestamps that conform to PAdES [2] in the present document.

A conforming signature handler shall enable the user to display the visual representations of each and every individual AdES signature and document timestamps in a document, for example in a list. This shall be displayed such that can be easily related to the signature appearances appear to the document.

6.1 The visual representation of individual AdES signature verification

For any AdES signature in a PDF document a conforming signature handler shall at least enable for the user display the following information on the top level of the visual representation of the individual signature.

a) Status of the signature: valid, invalid or indeterminate.

b) The reasons of an invalid or indeterminate result.

NOTE: This may include the document integrity and the certificate validity. A trusted viewer may display these detail results even if they are valid.

c) The document revision that the signature applies to and give the user the opportunity to display PDF revision as applicable at the time of signing.

d) The signing time and an indication of the potential trustworthiness of that time (e.g. claimed by signer or from trusted signature time-stamp).

e) Summary information of certified identity (see clause 6.2) that can be expanded in the next level (see clause 6.3).

A conforming signature handler may display further information at the top level. Redundancy should be avoided with information required in further clauses of this profile.

6.2 Summary representation of certified identity verification

If the certified identity has been successfully validated the following information shall also be displayed at top level:

- If the signatories certificate contains a certificate image then the certificate image as defined in draft-ietf-pkix-certimage-04 [5].
- If the signatories certificate contains no certificate image the following information should be included in that order:

  a) Name of signatory (as in CN)

  b) Affiliation of signatory (as in O).

  c) Any logo image in the signatories certificate (as defined in RFC 3709 [4]).

  d) Any image of a handwritten signature in certificate (as defined in RFC 3739 [6], section 3.2.5).

  e) The identity of the trusted CA which is used as the basis for certificate path validation. This may be in the form of a "friendly name" by which is configured for the conformant reader or information derived from the issuer name (e.g. using the O field).

The visual representation of certified identity validation should be such that it can be easily related to the signature appearance layout recommended in clause 5.1.

Apart from above information the following shall also be displayed:

a) Whether the certificate is valid at the time of signing (see clause 6.1 item d)).

6.3 Detailed representation of AdES signature verification

The user should be able to display all the elements of the signer and all CA Certificates used in the validation path if required.

The signature details shall contain the following information if available in the verification result:

a) The algorithm validity as in section 3.5.2 of [3].

b) The certificate path validity as in section 3.5.3 of [3]. The certificate path validity shall contain further levels of detail with information about all data used to determine the certificate path validity like the validation data. For any element in the validation data the details of their validation shall be displayed in another level of detail. The structure of this visual representation shall follow the same rules as for the visual representation of the AdES signature verification.

c) Any signed properties included from the AdES-signature. This includes all attributes defined in clauses 4.4 and 4.5 of TS 102 778-3 (V1.1.1) [10] and information included by the keys M, Location, Reason, ContactInfo in the signature dictionary defined in clause 12.8.1 of ISO 32000-1 [1].

d) The signature value.

e) If the AdES is a PAdES-EPES as defined in PAdES Part 3 [10], the value of the `signature-policy-identifier` attribute and the value of the `commitment-type` attribute if present.

A conforming signature handler may allow the creation and print of a separate document containing the visual representation of the AdES signatures described above as verification protocol. Verification results shall not print with the verified document.

6.4 The visual representation of the document timestamp verification

A document timestamp is typically not signed by a person but by an organisation providing trusted timestamp. Visual representation of document time-stamp verification should be similar to individual AdES signature verification where applicable. It should contain at least the following information at top level:

a) The result of the verification of the timestamp.

b) The time included in the timestamp.

c) At least the common name and organisation of the server providing the timestamp.

History

Document history		
V1.1.1	July 2010	Publication