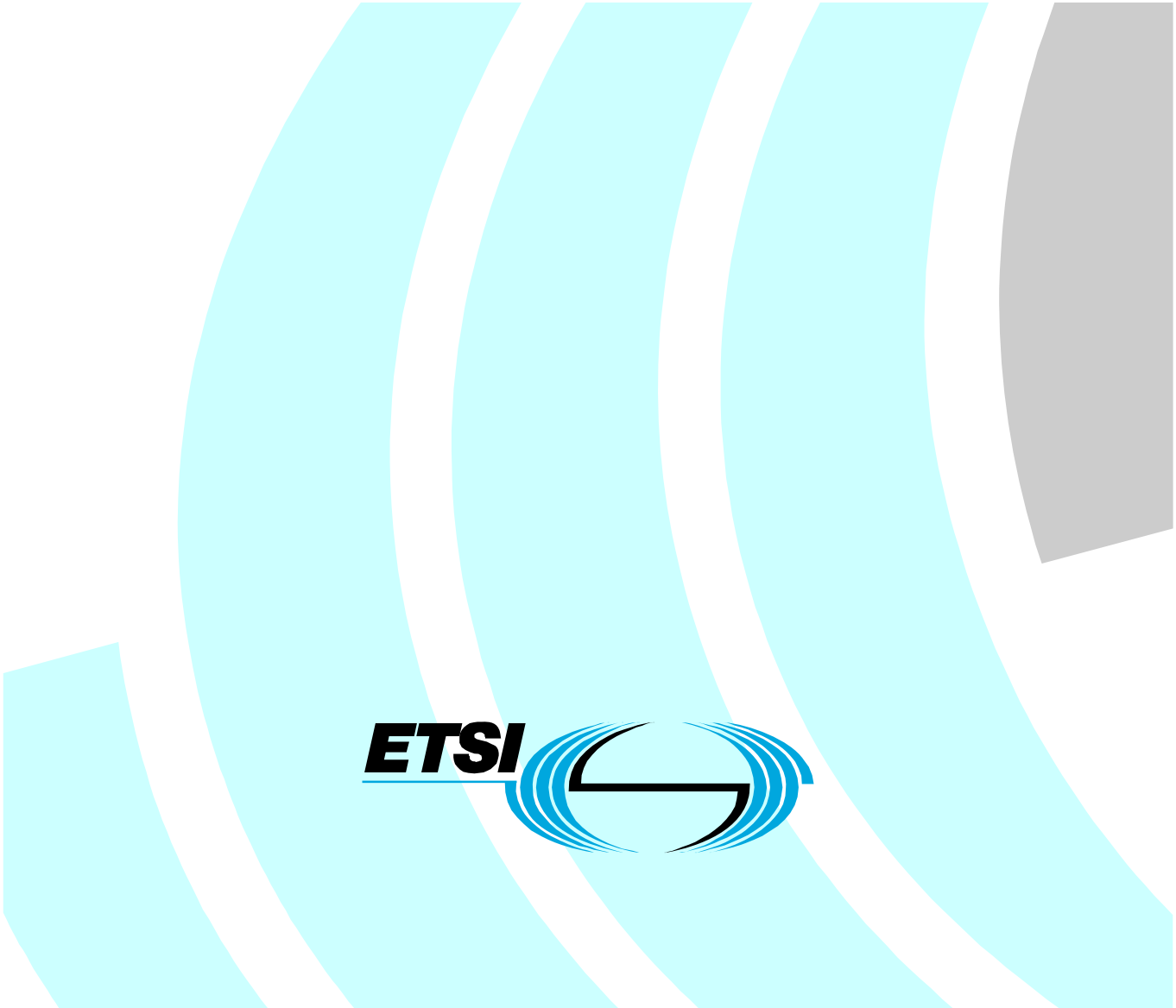
ETSI SR 003 232 V1.1.1 (2011-02)

Special Report

Electronic Signatures and Infrastructures (ESI); PDF Advanced Electronic Signature Profiles (PAdES); Printable Representations of Electronic Signatures



Reference
DSR/ESI-000113

Keywords
electronic signatures, 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

No part may be reproduced except as authorized by written permission.
The copyright and the foregoing restriction extend to reproduction in all media.

© European Telecommunications Standards Institute 2011.
All rights reserved.

DECT™, **PLUGTESTS**™, **UMTS**™, **TIPHON**™, the TIPHON logo and the ETSI logo are Trade Marks of ETSI registered for the benefit of its Members.
3GPP™ is a Trade Mark of ETSI registered for the benefit of its Members and of the 3GPP Organizational Partners.
LTE™ is a Trade Mark of ETSI currently being registered
for the benefit of its Members and of the 3GPP Organizational Partners.
GSM® and the GSM logo are Trade Marks registered and owned by the GSM Association.

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

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 European Directive 1999/93/EC [i.5] 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".

TS 102 778 [i.8] specifies the use of the advanced electronic signature, as defined in this Directive for documents represented in an electronic format called Portable Document Format (PDF). This includes Part 6 which covers visual representation of electronic signatures. In producing TS 102 778-6 [i.4] a number of points were identified relating to the representation of electronics signatures applied when the signed PDF document has been converted to printed form (termed printable signatures). It was not possible to fully address these points in TS 102 778-6 [i.4].

The present document looks more specifically at these points, discussing the issues and identifying some potential solutions for the handling of printable signatures.

1 Scope

The present document discusses the techniques that may be used for printable representations of advanced electronic signatures (AdES) in PDFs. Specifically, focusing on the printable representation of the AdES signature value, for example as a alphanumeric string or bar code. A separate document (TS 102 778-6 [i.4]) covers the issues of visually displaying other information contained in the signature.

The printable representation of the advanced electronic signature value is aimed at electronic signatures created on electronic documents which are then printed. It can be used to verify that a printed signature value stored on an authoritative printed document equals to that one derived from the electronic version of the document. It does not necessarily enable the authenticity of the printed document to be verified using electronic techniques without reference back to the electronic document from which the printed document was derived. As such, electronic/digital documents need to be validated using the included electronic signature and the standard methods for verification & validation of that signature. The printed representation should mainly be used to provide a way to match the printed version to the electronic version from which it originates - a form of "secured fingerprint".

The present document discusses the techniques that may be used in applying printable signatures to PDF documents. It is not aimed at providing a normative set of requirement but rather collects together information that may at a later date by used to form the basis of a formal ETSI specification.

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

[i.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".

[i.3] ETSI TS 102 778-4: "Electronic Signatures and Infrastructures (ESI); PDF Advanced Electronic Signature Profiles; Part 4: PAdES Long Term - PAdES LTV Profile".

[i.4] ETSI TS 102 778-6 "Electronic Signatures and Infrastructures (ESI); PDF Advanced Electronic Signature Profiles; Part 6: Visual Representations of 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] IETF RFC 3852 (2004): "Cryptographic Message Syntax (CMS)".

[i.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)".

[i.8] ETSI TS 102 778 (all parts): "Electronic Signatures and Infrastructures (ESI); PDF Advanced Electronic Signature Profiles".

3 Definitions and abbreviations

3.1 Definitions

For the purposes of the present document, the terms and definitions given in [i.1], [i.2] and [i.4] and the following apply:

PDF Signature: binary data object based on the CMS (RFC 3852 [i.6]) or related syntax containing a digital signature placed within a PDF document structure as specified in ISO 32000-1 [i.1] clause 12.8 with other information about the signature applied when it was first created

printable signature value: printable representation of, or derived from, the AdES signature value, for example as a alphanumeric string or bar code

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

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

signer: entity that creates an electronic signature

verifier: entity that validates an electronic signature

3.2 Abbreviations

For the purposes of the present document, the abbreviations given below apply:

AdES Advanced Electronic Signature

NOTE: As specified in Directive 1999/93 [i.5].

CMS Cryptographic Message Syntax

NOTE: As specified in RFC 3852 [i.6].

PAdES PDF Advanced Electronic Signature
PDF Portable Document Format

4 The printable representation of an AdES signature value

The AdES signature value is sequence of bytes that is a result of cryptographic algorithms and can be used to mathematically prove the integrity of some data and authenticate the signer who applied the AdES. In the case of a PDF signature, the AdES signature value applies to the complete document at the time of signing. This proof is done with the aid of computers and therefore is best kept in electronic form as part as the PDF signature. Nevertheless there are use-cases where the inclusion of the signature value in a printable form may be required to provide a reliable proof of equivalence between an electronic document and the document in printed form. In addition to the signature value, further information could be printed along with the printable signature value. Such information could point to guidelines describing the verification of documents or give further details about the signer.

For example, the printable signature value may serve the purpose of demonstrating that an electronic document version is equivalent to a trusted printed document by comparing a AdES signature value of the electronic document to the printed signature value from a printed document. Alternatively, a printed document (such as an e-ticket) which includes the printable signature value can be presented as proof that the document held is equivalent to an electronic original.

The common practice is to include the AdES signature value or a digest of the signature value somewhere in the printable content of the document, usually in an area explicitly designated for such a value. This information could be displayed as alphanumeric encoded text or a 2D barcode in order to make a machine-aided reconstruction of the signature value from the printed document possible. By using a digest, the amount of numeric data that needs to be printed in the document is reduced which is also a benefit.

How the signing applications adds the printable signature value to the document's content bears some challenges since the AdES signature value, by definition, is created as the last step of creating a signed document. Since the signature covers all visible content ("what you see is what you sign"), any change to the document content would invalidate the signature. To address this cyclic dependency between the printable signature value and visible content, a variety of methodologies exist, each with their pros & cons. In the following clauses, we will present some of these and discuss their usability in various workflows.

The most important thing when choosing which method to use is that there be a common understanding between creator and processor of the printable signature value on how these values are created and processed to ensure interoperability. This understanding includes:

- Whether a digest is applied to the signature value and, if one is applied what digest algorithm is used.
- The mechanism used to encode the signature value (e.g. Alphanumeric text, barcode). If a barcode is used, the identity of the standard barcode "symbology" which was used.
- Where the actual certificate used to sign, and any associated revocation information, is to be stored.

4.1 Methods of Display

4.1.1 Alphanumeric Strings

The most common visible representation is to convert the digest/hash of the document (or the signature) into a alphanumeric string using an algorithm such as Base64 or ASCII85 and then add it to the displayed page content. Usually this string is part of a larger block of explanatory or information text that incorporates useful metadata for a human to identify the present document and where it may have come from and how to validate it.

An alphanumeric string is simple to compute and does not take up a large amount of space on the page, mostly determined by the length of the hash and the font and font size chosen for display. It can be read, and if required for verification purposes, typed in by humans and (with some aid to knowing where on the page to look) by machine.

4.1.2 Barcodes

A barcode is an optical machine-readable representation of data where the details of the representation are described through the specification of a symbology. The specification of a symbology includes the encoding of the single digits/characters of the message as well as the start and stop markers into bars and space, the size of the quiet zone required to be before and after the barcode as well as the computation of a checksum. There are numerous symbologies available, both in 1D (linear) or 2D. The choice should be based on what data is chosen to be encoded.

A single implementation may choose to, as in the case of alphanumeric strings, encode the digest/hash of the document (or the signature) into a simple 1D barcode.

Figure 1

Another option would be to take some (or all) of the page's content, perhaps only the textual data, or a set of variable field values, and encode those into a 2D barcode. One of the problems with such barcodes is that the larger the data being encoded, the larger the barcode - so that it would be possible to have a barcode that takes up more physical space on the page than the actual content being encoded!

Figure 2

One advantage of PDF when working with barcodes is that it is possible to have them computed dynamically at the time of display by a conforming reader, rather than at signing time, through the use of a barcode field. These are a standard type of form field available in both the XFA and AcroForm form technologies of PDF.

NOTE: Since they were introduced in PDF 1.5, they are not compatible with PDF/A-1 (ISO 19005-1 [i.7]) but would be with PDF/A-2.

4.2 Scope of Printable Signature

Currently, standard advanced electronic signatures for PDF, such as specified in ISO 32000-1 [i.1] and profiled in TS 102 778 [i.8] (PadES), apply to the whole PDF document as its stands when the signature is created. This includes any graphics and layout in the signature. PDF does not specify any means of selecting parts of a PDF document to be included in the signature, or restricting signatures to specific aspects such as only the textual content.

These same technical restrictions currently apply to printable signatures. The entire PDF document, including any graphics and layout are used to derive the printable signature. The encoding of graphics and text formatting cannot be precisely created from a printed document. It is only possible to verify a printable signature reference with the original digitally encoded document.

4.3 Where does the actual certificate live?

A reason that the application of a printable signature value on the page content is quite problematic with PDF is that the process of signing actually modifies the document by embedding the certificate and the signature value (and possibly associated revocation information) inside of the document. Thus the hash generated prior to signing is not the same as it is after signing.

One way in which to avoid this problem is to not embed the certificate inside the PDF as a standard PDF signature but instead of do a traditional detached signature, storing the detached information on a server or other data storage system and usually also including a reference to it in the visual representation of the signature.

While this avoids the problem described above, it now means that the PDF is no longer self-contained and the signature can be verified without a connection to that same system in which the data is stored and a knowledge of how to use the referencing information. This makes is problematic for workflows that may take place disconnected from a network or system as well as for long term archiving and storage.

4.4 Use of incremental updates

PDF supports the ability to add incremental updates (ISO 32000-1 [i.1], clause 7.5.6) to the end of the document representing new or changed objects. If the printable representation is placed in an incremental update section, it will not invalidate the hash of the document's signature. However, the way in which the printable representation is added to the visible page content will impact the validation status displayed by a conforming ISO 32000-1 [i.1] reader.

When adding the representation as standard page content, a conforming reader will identify the document as changed as the actual page content has been modified and so it is no longer what was actually signed. However, the use of annotations (ISO 32000-1 [i.1], clause 12.5) to add additional information on a top layer of information does not invalidate the signature. Therefore the use of annotations is strongly recommend in a workflow involved embedded signatures.

4.5 Use of Document Timestamps

TS 102 778-4 [i.3] describes a special type of signature that can be applied to a PDF that uses only a secure timestamp to sign the document rather than a full certificate. This type of signature is useful to apply a secure "wrapper" around the original document, its signature and the newly added incremental update containing the printable representation. It is therefore recommended to use this in a workflow involved embedded signatures.

NOTE: The document timestamp signature would not have any legal meaning, but would simply prove that the document was signed at a specific time and has not been modified since then. Thus it provides the validation features of signatures but without the need for a certificate.

Some uses for Document timestamps involve the need to incorporate a visual appearance and the specification fully supports this requirement. However, at least one known use for this also includes the time from the timestamp in the appearance - similar to the earlier requirements to display the signature value in the appearance. Just as that requirement cannot be met, this too is problematic for the same reason. The same techniques described above could also be used to accomplish something similar though not exactly what is desired.

History

Document history		
V1.1.1	February 2011	Publication