The AdES family of standards: CAdES, XAdES, and PAdES

Implementation guidance for using electronic signatures in the European Union

Table of contents

Acknowledgments

Special thanks to Olivier Delos and Sylvie Lacroix from SEALED, www.sealed.be, and Nick Pope, co-chair ETSI Special Task Force 364 on PAdES, and principal consultant, Thales e-Security Limited for their contributions to this paper.

This white paper is a guide for choosing and deploying electronic signature technology in the European Union (EU). It will help business managers, system integrators, and partners understand the choices available for implementing electronic signature applications that can be readily deployed and are assured to meet the requirements of the European Commission (EC) Electronic Signature Directive 1999/93/EC[1] (hereafter referred to simply as “the Directive”). Additionally, government policy makers and practitioners will also find this paper useful.

This paper briefly describes the regulatory environment in Europe related to electronic signatures and discusses how open signature standards are critical to adoption across Member States. This is followed by an explanation of the sequence of European Telecommunications Standards Institute (ETSI)[2] electronic signature standards. ETSI is recognized as an official European Standards Organization by the EC and produces globally applicable standards for information and communications technologies including fixed, mobile, radio, broadcast, Internet, aeronautical, and other areas. The ETSI digital signature standards include Cryptographic Message Syntax Advanced Electronic Signature (CAdES), XML Advanced Electronic Signature (XAdES), and most recently PDF Advanced Electronic Signature (PAdES). PAdES describes how to use the digital signature features of the Portable Document Format (PDF)[3] to meet EU requirements. The primary utility of each of the standards is also described and distinguished by their unique properties.

Electronic signatures and efficiencies

Over the last decade, business processes have moved to the web at an astounding rate. Today, millions of people in the EU and around the world engage in business-to-consumer (B2C), government-to-consumer (G2C), and business-to-business (B2B) processes over the Internet. When moving from a paper world to the promising electronic society, electronic signatures serve as a catalyst to support electronic communications, transactions, and commerce. The availability of electronic signatures has driven an increase in eBusiness and eGovernment applications as demonstrated by numerous implementations over the past few years.

[1] Directive 1999/93/EC of the European Parliament and of the Council of 13 December 1999 on a Community framework for electronic signatures: http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX%3A31999L0093%3AEN%3ANOT.

[2] For more details about the European Telecommunications Standards Institute, visit www.etsi.org.

[3] PDF is now accessible as an ISO International Standard, ISO 32000-1. For more details about the ISO 32000-1 standard, visit www.iso.org/iso/pressrelease.htm?refid=Ref1141.

An electronic signature[4] is a paperless way to sign a document using a unique credential associated with a given person that is logically attached to or associated with the document. Electronic signatures can be used to authenticate the signer as well as detect any changes made to the document after it was signed.

Electronic signatures provide real benefits. For example, they promote the emergence of fully automated purchasing processes by enabling buyers and sellers to sign and approve transactions without the need for traditional "wet" (paper-based) signatures. In Europe, electronic signatures enable non-repudiation from a legal perspective and under some strict circumstances can be legally equivalent to handwritten signatures. For transactions, electronic signatures can provide greater efficiency and faster turnaround times by eliminating costly paper printing and mailing delays, making it possible to reduce errors associated with rekeying of information, and improving convenience for end users. They also complement regulatory compliance and long-term document retention.

> *"With the addition of PAdES to the set of solutions for advanced electronic signatures, we now have a way of providing both live and long-term signatures for PDF in line with EU legal requirements."*
>
> –Nick Pope

Today, electronic signatures make organizations more agile in the face of a continuously changing business landscape. As eGovernment and eBusiness programs reap savings by moving from paper to electronic processing, investing in electronic signature technologies becomes a very attractive proposition. Efficiency and financial benefits are accelerated when widely available tools, such as European citizen cards, can be used by large numbers of people (yielding high return on investment or ROI).

Europe has a decade of experience in setting up legal, technical, trustworthy, and standardized frameworks to facilitate the interoperable and cross-border use of electronic signatures. Leveraging the lessons learned from this experience and seeking to resolve the issues that were exposed as a result, the EC enacted an ambitious but pragmatic Action Plan[5] at the end of 2008 to further improve the efficiency of cross-border use of electronic signatures throughout the EU and beyond.

European electronic signatures: Legal overview[6]

In the Directive, which is currently in force in every EU Member State, the term "electronic signature" is defined in Article 2.1 as follows: "data in electronic form which are attached to or logically associated with other electronic data and which serve as a method of authentication."

Being deliberately neutral regarding technology and security requirements, this definition confers to all kinds of electronic signatures a potential legal validity, provided their authenticity is not contested. Additionally, two upper levels are defined in addition to the previously mentioned electronic signatures—namely the advanced electronic signature (AdES)[7] and the qualified electronic signature (QES).[8]

An AdES is an electronic signature that meets the following requirements:

1. It is uniquely linked to the signatory.
2. It is capable of identifying the signatory.
3. It is created in a way that the signatory can maintain sole control.
4. It is linked to the data to which it relates in such a manner that any subsequent change of the data is detectable.

[4] The term *electronic signature* is usually defined in very general terms to include nearly any and all technology for signing electronic documents. The term *digital signature* usually refers to electronic signatures that make use of public key infrastructure (PKI) technology and digital certificates.

[5] Communication from the Commission to the Council, the European Parliament, the European Economic and Social Committee and the Committee of the Regions on an Action Plan on e-signatures and e-identification to facilitate the provision of cross-border public services in the Single Market, COM(2008)798 of 28.11.08: http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2008:0798:FIN:EN:PDF.

[6] For a more comprehensive picture, visit www.law.kuleuven.ac.be/icri/publications/954eIDPDFSignatures.pdf.pdf? This article was used as a reference for some parts of this section.

[7] Defined in reference 2, the Directive, in article 2.2.

[8] Advanced electronic signatures using qualified certificates and protected signing devices as defined in the Directive, article 5.1. These have come to be referred to as QES.

While this definition is also formulated in a general and technologically neutral way, security experts generally agree that the only electronic signatures that currently meet all of the four requirements are those that use standardized public key cryptography and infrastructures.[9] Electronic signatures that use cryptographic technology are often referred to as "digital signatures." The binding between a signatory's identity and their signature cryptographic material is provided in the form of an X.509 open standard digital certificate.[10] The Directive legally defines a certificate as "an electronic attestation that links signature-verification[11] data to a person and confirms the identity of that person."[12] Certificates are issued by Certification Service Providers (CSP) who must be trustworthy and impartial, and be accepted as such by all.

When created by means of state-of-the-art standardized technology and based on trustworthy certificates, the electronic signature will fulfill the four conditions of an AdES, provided it is linked to the data to which it relates in such a manner that any subsequent change of the data is detectable.[13] As a consequence, such electronic signatures are considered legally valid in all cases where the law accepts or requires the use of an AdES.

QESs are AdESs based on a qualified certificate and created by means of a secure signature-creation device (SSCD). An SSCD is defined in the Directive as "configured software or hardware used to implement the signature-creation data[14] which meets the requirements laid down in Annex III." An appropriate smart card can be one example of an SSD.

The notion of a qualified certificate has been defined in Annex I of the Directive with stringent requirements on CSPs, as listed in Annex II of the Directive, to further enhance the trustworthiness of digital certificates.

The adoption of qualified electronic signatures does not require their use in every situation in which, up to now, the use of handwritten signatures was obligatory. Either the law explicitly defines the type of electronic signature required in a particular context or the law merely requires a document to be "signed." In this latter case, a qualified electronic signature must be considered to have the same value as a handwritten signature. This principle is valid in every Member State of the European Union—meaning that a qualified electronic signature created in any Member State will have authority equivalent to a handwritten signature in every other one.

Open standards support electronic signature workflows

A document created and signed in one Member State must be able to be checked for validity in another Member State, without the parties involved being required to have advanced degrees in computer science or be experts in international law. The proper level of interoperability can be established by publishing and adopting open standards that define the technical steps that must be taken by the software and the agencies involved (for example, CSPs). It is also necessary, in those cases not clearly covered in the Directive, to map the signature technology to existing laws.

The previous section described the high-level framework established by the Directive. However, that framework is purposely vague with regards to details recommending any particular technology to be used for electronic signatures. Efforts have been made to more clearly define activities, services, and items that are direct consequences of the Directive's adoption, including:

- The definition of qualified cryptographic certificates
- What it takes for a smart card or token to become an SSCD
- The requirements that CSPs must meet

[9] For a good general introduction to PKI, visit the Wikipedia website: http://en.wikipedia.org/wiki/Public_key_infrastructure.

[10] See RFC 5280: www.ietf.org/rfc/rfc5280.txt.

[11] Legal term for public key; for example, the cryptographic material used by a verifier to validate a certain person's signature.

[12] "Person" is interpreted according to national laws. This may cover not only natural persons but also legal persons. Technically, digital certificates can also be issued to subjects such as machines, applications, and so on.

[13] As basic PKI technology may not be inherently sufficient to help ensure such compliance in mid or long term, this can be achieved, for example, by use of trusted time-stamping facilities.

[14] Legal term for private key; for example, the cryptographic material used by a signatory to accompany a signature on data.

- How certificates are revoked
- How lists of CSPs and their qualified certificates that have been officially supervised/accredited by a government authority (Trust Status Lists) can be communicated across borders
- How to represent a digital signature as a data structure tied to the data or document being signed

Much of these technical details have been spelled out or described in open standards such as those produced by the Internet Engineering Task Force (IETF), International Standards Organization (ISO), ETSI, the European Committee for Standardization (ECS), and other recognized standards organizations. For example, see Public-Key Infrastructure (X.509) (pkix)[15] for a summary of many of these standards. By approving the use of these standards, synchronization among Member States can be established.

In order to promote cross-border interoperability, it's important that signers and recipients of signed documents know ahead of time that others will be able to understand and "consume" those signed documents. The next section goes into more detail on the open standards governing the structure and representation of digital signatures. It also addresses which of these standards is most appropriate for use in different workflows.

Technical standards for digital signatures

As a result of the Directive, ETSI formed an Electronic Signatures and Infrastructures (ESI) technical committee to construct standards for digital signature data structures that meet European requirements for AdES and QES. This has resulted in the development of CAdES[16] and XAdES,[17] both of which are widely recognized within the EU. For the last year these experts have turned their attention to PAdES[18] as explained in more detail in the following sections.

Long-term validity

A major concern while developing all three standards (CAdES, XAdES, and PAdES) has been the ability to validate signatures many years after the signing took place—a concept known as long-term validation (LTV).

Assuming a document has been or can be validated just after it has been signed, we can then gather all the information that was needed to do that validation and archive it together with the document or signature. Then, 50 or 100 years later, the same validation process can be repeated on the same data confirming that the signature was valid at the time it was signed.

Consideration for the weakening of cryptographic methods over time is also taken into account provided that, from time to time, additional timestamps using the most modern cryptography are applied to the archived documents/signatures. These LTV technologies resolve the two major obstacles to archiving signed material: loss of the key information to do the validation and weakening of the encryption methods due to advances in hardware and mathematical techniques.

CAdES

CAdES is built around the Cryptographic Message Syntax (CMS),[19] a basic building block for digital signatures based on standard public key infrastructure (PKI) principles. CAdES adds to CMS an infrastructure for a set of increasingly ambitious standards for digital signatures that can be applied to any kind of digital data. Basic signing capabilities are defined by CAdES-BES

[15] For more details about Public-Key Infrastructure (X.509) (pkix), visit www.ietf.org/dyn/wg/charter/pkix-charter.html.

[16] To obtain the standard from ETSI, visit http://webapp.etsi.org/workprogram/Report_WorkItem.asp?WKI_ID=28069.

[17] To obtain the standard from ETSI, visit http://webapp.etsi.org/workprogram/Report_WorkItem.asp?WKI_ID=28064.

[18] PAdES is a five-part standard; each of these standards may be obtained from ETSI:
Part 1 : http://webapp.etsi.org/workprogram/Report_WorkItem.asp?WKI_ID=31003
Part 2 : http://webapp.etsi.org/workprogram/Report_WorkItem.asp?WKI_ID=31004
Part 3 : http://webapp.etsi.org/workprogram/Report_WorkItem.asp?WKI_ID=31005
Part 4 : http://webapp.etsi.org/workprogram/Report_WorkItem.asp?WKI_ID=31007
Part 5 : http://webapp.etsi.org/workprogram/Report_WorkItem.asp?WKI_ID=31008

[19] CMS is defined in RFC 2630: www.ietf.org/rfc/rfc2630.txt.

(Basic Electronic Signatures) and CAdES-EPES (Explicit Policy Electronic Signatures). The most advanced forms of CAdES support LTV of signatures.

CAdES as a technology has been incorporated into many products and is in use within the EU. No ubiquitous software employs CAdES yet, but it has been instrumental in many special applications. For those developing applications involving electronic signatures, CAdES defines how their signature-processing component, which will use the established signature infrastructure, should work, but does not define a standardized way in which the signature information should be carried inside, around, or alongside the document itself.

XAdES

XAdES is built around the XML Digital Signatures (XML-DSIG)[20] standard for digital signatures represented in XML. (Note that these signatures can be applied to any kind of data, not just XML data.) Like CAdES, XAdES-BES defines Basic Electronic Signatures and XAdES-EPES defines Explicit Policy Electronic Signatures. XAdES also adds the same LTVchecking to XML-DSIG as CAdES does to CMS.

XAdES as a technology has been incorporated into many products and is in use within the EU. Similarly to CAdES, no ubiquitous software employs XAdES yet, but it has been instrumental in many special applications. For those developing applications involving electronic signatures that require XML, XAdES defines how their signature-processing component, which will use the established signature infrastructure, should work.

PAdES

PAdES articulates the same capabilities featured in CAdES and XAdES for PDF. PDF has supported digital signatures based upon PKCS#7,[21] a precursor to CMS, for more than 10 years and this support is defined in ISO 32000-1 (PDF 1.7). PAdES differs from CAdES and XAdES in that it applies only to PDF documents and defines requirements that PDF viewing and editing software must follow when using digital signatures in PDF documents. As the standard for viewable documents, PDF also defines how a signature can be displayed as it might with an ink-on-paper signature at a particular position on a particular page, and how digital signatures can be integrated with the form-filling features of PDF. This is a key factor that distinguishes it from CAdES and XAdES, which are more suited for applications that may not involve human-readable documents.

PAdES should be of interest to those establishing document workflows. Using PAdES may not involve the detailed development or customization of application software because it can be deployed by making use of widely available PDF software—for example, the free Adobe® Reader.®

Recently, ETSI/ESI, the same group that developed CAdES and XAdES, has teamed up with PDF experts to review where ISO 32000-1 stands with respect to the Directive and the signature technologies of CAdES and XAdES. The result is a new five-part ETSI standard, PDF Advanced Electronic Signature Profiles—TS 102 778, approved in June 2009 and broken down as follows:

- Part 1: PAdES Overview—a framework document for PAdES
- Part 2: PAdES Basic—Profile based on ISO 32000-1
- Part 3: PAdES Enhanced—PAdES-BES and PAdES-EPES Profiles
- Part 4: PAdES Long Term—PAdES-LTV Profile
- Part 5: PAdES for XML Content—Profiles for XAdES signatures of XML content in PDF files

Part 2 describes how to use ISO 32000-1 (the current PDF) for AdES and QES today. ISO 32000-1 offers many choices for digital signatures. This section weaves a path through those choices in a manner that satisfies basic AdES requirements. It should also be noted that it is possible to use the current version of Adobe Reader, or any other software that fully supports ISO 32000-1, to

[20] For more details about XML Digital Signatures, visit www.w3.org/TR/2009/WD-xmldsig-core1-20090730.

[21] For more details about PKS#7, visit www.rsa.com/rsalabs/node.asp?id=2129.

validate signatures created with these choices. PDF signing software also exists that can be configured to produce PAdES Part 2 signatures for existing PDF files.

Part 3 brings PDF to the level of CAdES-BES and CAdES-EPES. This version can be thought of as using basic CAdES within PDF files.

Part 4 provides the same LTV features defined for CAdES and XAdES in PDF.

Part 5 describes how to update the existing usage of XML-DSIG that is already supported within ISO 32000-1 for fillable forms data (and in some cases the form descriptions as well) to use XAdES to obtain the additional LTV features. This enables existing XML workflows using PDF to gather and display XML data, to use XAdES.

The new PDF features defined for Parts 3 through 5 call for extensions to the existing PDF standard, and will be submitted to the ISO 32000 committee to consider including in the next release of PDF, ISO 32000-2, expected to be published in late 2011 or early 2012. As such, updates to existing PDF software will be needed to support the new profiles spelled out in Parts 3 through 5. The profile information needed to make the proper choice among the many available capabilities in PDF will remain defined by the TS 102 778 ETSI standard.

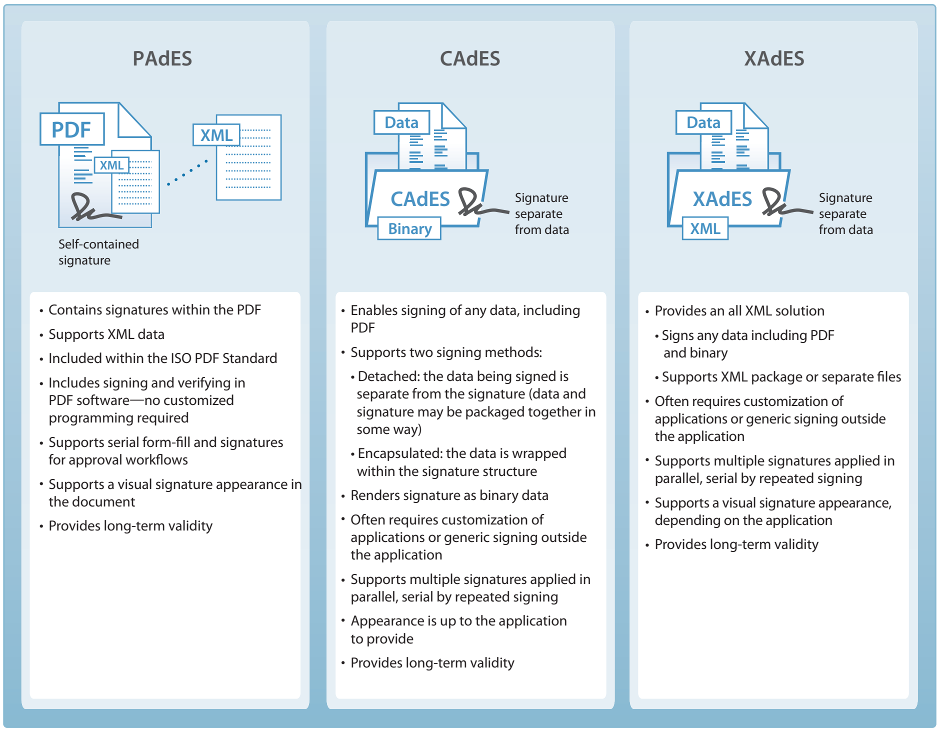
CAdES, XAdES, and PAdES in use

The biggest difference between PAdES, CAdES, and XAdES is that PAdES defines how software that processes digital signatures in PDF documents should operate—whereas both CAdES and XAdES define technology to be used in developing any kind of application that needs to process electronic signatures in a standard manner. Various document workflows employing digital signatures are supported by standard off-the-shelf PDF software. The following sections discuss CAdES and XAdES signed data and PAdES support for PDF.

CAdES and XAdES signed data

There are two typical methods for keeping the digital signature together with the original data that is being signed. One is to define a place within the digital signature data format to hold the original data. The other is to make use of some "packaging" format into which both the electronic signature and the original data are placed, side by side. Both of these methods are possible with CAdES and XAdES, and both present a mixed blessing. When using CAdES or XAdES, the original data can be of any kind, including a PDF document, and the signature creation and checking can be done independently from the software that processes the original data. However, it does mean that the original data needs to be "unpackaged," either from the signature format or from the package format, in order to make it available to normal processing. It also means that two applications have to be dealt with, the software that processes the original data and the signing software that understands the signature and/or packaging format. If any visible representation of the signature is to be presented to users, it will be done by the signing software and generally out of the context of the original data/processing software. (If a PDF document is signed in this way, no visible signature presentation will be shown as part of displaying the PDF contents. Any signature presentation will be displayed by the CAdES or XAdES software outside the context of the PDF document.)

It is also possible to extend the software that processes the original data to also process the digital signature and packaging. This is a specialization that the authors of the original software have to decide to support for their data format. Figure 1 shows a comparison of PAdES, CAdES, and XAdES.



PAdES

- Contains signatures within the PDF
- Supports XML data
- Included within the ISO PDF Standard
- Includes signing and verifying in PDF software—no customized programming required
- Supports serial form-fill and signatures for approval workflows
- Supports a visual signature appearance in the document
- Provides long-term validity

CAdES

- Enables signing of any data, including PDF
- Supports two signing methods:
  - Detached: the data being signed is separate from the signature (data and signature may be packaged together in some way)
  - Encapsulated: the data is wrapped within the signature structure
- Renders signature as binary data
- Often requires customization of applications or generic signing outside the application
- Supports multiple signatures applied in parallel, serial by repeated signing
- Appearance is up to the application to provide
- Provides long-term validity

XAdES

- Provides an all XML solution
  - Signs any data including PDF and binary
  - Supports XML package or separate files
- Often requires customization of applications or generic signing outside the application
- Supports multiple signatures applied in parallel, serial by repeated signing
- Supports a visual signature appearance, depending on the application
- Provides long-term validity

Figure 1. Comparison of PAdES, CAdES, and XAdES

PDF and PAdES

PDF provides an electronic analogue to paper as well as allowing for richer digital content to be stored and presented to the user. This accounts for the popularity of PDF and its widespread use as organizations move to electronic forms of information distribution and commerce. For centuries, commerce has recorded its transactions as paper documents. Wax seals and various forms of signatures have been applied to those paper documents as evidence of agreement by individuals or organizations represented by those individuals or as evidence that the document actually originated with the designated author. The transition from paper to PDF is eased by PDF's ability to electronically represent nearly any form of paper document and by its support for PKI-based digital signatures (PAdES) that provide the same function, or more, as ink signatures and wax seals.

With PDF, the signature data is incorporated directly within the signed document, much as an ink signature becomes an integral part of a paper document. This allows the complete self-contained PDF file to be copied, stored, and distributed as a simple electronic file.

Signing PDF documents has broad application for the following reasons:

- PDF is used in much the same way as paper documents, to record many different types of transactions, enabling it to support a comprehensive range of signing needs.
- PDF provides a visual representation of multipage documents. Signatures in PDF support both pre-allotting locations within the document where the particular signing is to take place and providing a visual appearance of the signature at that location. Multiple signatures within documents are also supported, complete with visual appearances.
- Transactions that involve adding information to a document, such as a date, a printed version of the signature or making checkbox choices, are possible using signatures with the PDF fillable form features.
- A signatory needs assurance that the blank form to be filled-in and signed is authentic. With PDF, the creator of the document can protect against damage or tampering by applying a special kind of signature, a "certifying signature." Subsequent form filling and signing can be

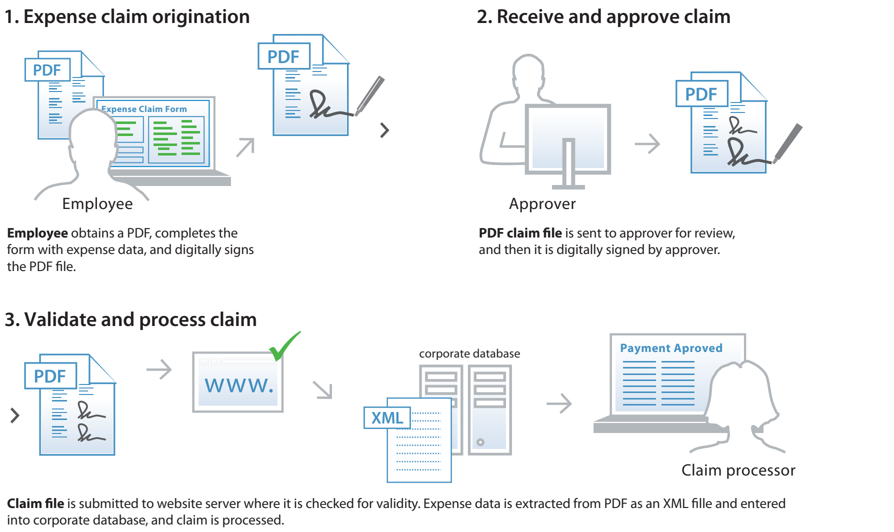
completed, without impacting the ability to check that the original document has not been tampered with.

- PDF can be used as the packaging mechanism for holding other documents by making them attachments to a parent PDF document, similar to attaching files to e-mail messages. A signature on the parent PDF file will make it possible to detect changes to any attachments contained within the PDF file. And the parent document can provide metadata about the document or data being signed.
- Software from many different vendors, as well as from numerous open source organizations, is available for creating, signing, and validating PDF digital signatures. Free Adobe Reader is ubiquitously available.

Today, end-to-end electronic workflows involving signed documents are implemented worldwide based on PDF and PDF digital signatures. PDF is an international standard (ISO 32000-1) and is supported by thousands of applications provided by hundreds of suppliers.

Figure 2 shows how PAdES can be deployed in a typical workflow: completing, submitting, and processing an expense form. A PDF form is completed by the employee and requires the digital signatures of both the employee and supervisor. It is then submitted to the corporation via its website where the form data can be extracted into an XML file and/or submitted to the proper database for normal processing and reimbursement. Using LTV, an additional document archiving step may also be added.

Digital signatures workflow for expense approval



Employee obtains a PDF, completes the form with expense data, and digitally signs the PDF file.

PDF claim file is sent to approver for review, and then it is digitally signed by approver.

Claim file is submitted to website server where it is checked for validity. Expense data is extracted from PDF as an XML fille and entered into corporate database, and claim is processed.

Figure 2. Sample signature workflow using PAdES digital signatures

Digital signature technical standards and trust

The digital signatures produced by CAdES, XAdES, and PAdES rely on PKI, as does any AdES today. The established PKI standards support two basic requirements: establishing the identity of the signer while binding it with the signer's cryptographic material and helping to ensure that the object signed cannot be changed without detection.

However, there is a third aspect of digital signatures that is only now being addressed by standards—establishing trust in the credential, and in turn the signature itself. How you go about establishing that the owner of a digital certificate and the creator of a signature is who he or she says they are is not an easy task. Much like the paper world, a structure needs to be set up to define how to establish that trust and at what level, for various workflows and relationships.

Organizations can, and have, created bilateral and multilateral trust relationships wherein each other's digital signatures and certificates will be trusted. Yet this does not provide a framework for broader, general use of digital signatures by disparate populations of users. Industry has reacted to this lack of trust and created infrastructures through which trust can be leveraged. Operating systems and browsers have answered the need for protected websites, software, and electronic commerce with trusted certificate stores: lists of trusted "root" certificates that meet particular requirements set by the vendor (for example, the Windows® Certificate Store[22]) or by industry (for example, Secure Socket Layer (SSL) or Extended Validation (EV) SSL[23]). Any certificate that is related (chained) to one of these root certificates will be trusted, provided that the security level of the certificate is deemed sufficient to be accepted by the particular application.

There are now a large number of CSPs issuing certificates and some have become well established as trusted anchors (also called "trusted roots") in hierarchical PKIs—in other words, a CSP commonly recognized by both parties in the mutual trust relationship between a signer and a validator. One technical point that is important to understand is that the trusted anchors cannot be part of the signatures or the object being signed. They are the trust link between signer and validator and are certifying the signer's identity in digital certificates linked to the signer's signatures. Hence, the person validating a signature must establish to their own satisfaction which CSPs they trust. Provided the signer and the validator have at least one trust anchor in common, their mutual trust relationship is established.

When it comes to digital signatures on documents, the question of trust is paramount. The certificates issued by CSPs are only as trustworthy as the procedures used by the CSP to thoroughly check the identity of those applying for certificates and the care with which they protect the private keys being issued. There is little utility in saving costs by moving to electronically signed documents if you cannot trust those signatures. While existing certificate stores can be used to provide some kind of trust to these signatures, to date, only Adobe has created mechanisms built into its software that provide a consistent level of assurance and broader scope of impact. Starting with technical requirements that are more comprehensive and stringent than most alternate certificate store systems, Adobe's Certified Document Services (CDS)[24] and recently launched (July 2009) Adobe Approved Trust List (AATL)[25] programs extend trust to PDF-based digital signatures across operating systems, regions, and software.

The CDS program provides trust to signatures created by certificates provided by commercial CSPs that chain to the Adobe Root certificate embedded in Adobe products, and also enables automatic embedding of LTV information into the document being signed. The AATL program downloads a list of trusted certificates to every copy of Adobe Acrobat® and Reader version 9 and above software, and can include government root certificates, eID certificates, CSPs issuing qualified certificates, and other high-assurance credentials.

Trust anchors should be trusted for exactly what they were intended and not more. Commercial lists of trust anchors found in widespread browsers and applications usually only imply that the issuing legal "person" is well known to and/or trusted by these large vendors—but this is irrespective of the type of certificate which is issued or used by a signer. Blind trust in such a trust anchor will make a validator accept whatever type of certificate such a trust anchor issues, from the weakest to the most secure certificate. Additionally, it is not sufficient to trust a trust anchor by itself; the type of the certificate must be assessed for compliance with the level of security that is required by an application when validating an electronic signature.

Recently, the EC has also been taking a closer look at trust interoperability and cross-border use of signatures. Qualified certificates, required to support qualified electronic signatures equivalent to handwritten signatures, have been defined in the Directive to maximize

[22] For more about the Windows Certificate Store, visit http://technet.microsoft.com/en-us/library/cc757138%28WS.10%29.aspx.

[23] For example, see the offering from GlobalSign: http://www.globalsign.com/ssl/ssl-certificates/ev-ssl/index.htm.

[24] For more details about the Adobe CDS program, visit www.adobe.com/security/partners_cds.html.

[25] For more details about the AATL program, visit www.adobe.com/security/approved-trust-list.html.

trustworthiness. They must meet certain formal requirements as listed by Annex I of the Directive and must be issued by a CSP that meets a series of security requirements in Annex II of the Directive. These latter requirements relate to the financial stability, the quality of the personnel, the security measures taken, and other quality controls used by the CSP in question.

CSPs issuing qualified certificates to the public must be supervised by the Member State in which they are established (if they are established in a Member State) and may be voluntarily accredited in any Member State for compliance with the provisions laid down in the Directive, including requirements from Annex I and II. Until now, the Member States' lists of these CSPs were maintained in different ways and not harmonized with regards to the information provided. In the context of the Electronic Signature Action Plan[26] and the implementation of the 2006 Services Directive,[27] Member States of the EU are expected to agree on a common template for their national "Trusted List of supervised/accredited Certification Service Providers," by which information will be provided by each Member State regarding the supervision or accreditation status of these CSPs, Trust Services[28] and their compliance with the relevant provisions of the 1999 Directive.

This common template is compliant with an implementation based on the Trust-service Status List (TSL) specifications from ETSI TS 102 231 v3.[29] As announced in its Action Plan and in order to facilitate the practical usability of the national Trusted Lists, the EC plans to create, publish and maintain, on a protected website, a Compiled List of pointers towards Member States' Trusted Lists. Any application that wishes to verify the supervision/accreditation status of those CSPs when validating electronic signatures (for example, a QES or an AdES based upon qualified certificates), can consult the Commission website and Compiled List.

Standardized Member States' Trusted Lists will most likely be integrated in widespread applications because it is the only way to fully validate via trustworthy references, qualified electronic signatures and advanced electronic signatures supported by qualified certificates. This is the only method to legally validate protected electronic communications, transactions, and commerce within the EU.

[26] See earlier reference to this Action Plan.

[27] Full text of this directive 2006/123/EC can be found at: http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2006:376:0036:0068:EN:PDF.

[28] Listed Trust Services can be provisioning of qualified certificates, provisioning of nonqualified certificates, provisioning of time-stamps, or any other trust service token resulting from the provision of certification services ancillary to electronic signatures.

[29] Version 3 has not been published as of this writing. For the latest information, visit http://webapp.etsi.org/workprogram/SimpleSearch/QueryForm.asp (enter 102 231 in search window).

Summary

The rush to go paperless has often fallen short of its true potential because manually signing a document often brings business critical processes to a halt. Electronic signatures provide organizations with the ability to close the loop and create real efficiencies and cost savings. Moreover, improved legal, standardization, and trust frameworks are converging to facilitate cross border use of electronic signatures. Combined with standards like PAdES and others that can provide long-term authenticity and properly managed trust across national boundaries, electronic signatures become not only feasible, but a requirement to remain competitive.

Organizations doing business in the EU that may have hesitated to switch to PDF as a replacement for their paper processes must now consider reevaluating these solutions as viable and credible alternatives. Not only is PDF a ubiquitous and open document format, PDF signatures are nonproprietary, standardized, and now, when used properly, are recognized as an AdES format, just like XAdES and CAdES. Today, PDF signatures are available to help make organizations more agile and flexible in the face of constantly changing business requirements.

Adobe Systems Incorporated
345 Park Avenue
San Jose, CA 95110-2704
USA
www.adobe.com

91014620 9/09