Adobe® PDF for electronic records

Digital signatures and PDF combine for definitive electronic records and transactions

Contents

Millions of people use Adobe PDF every day to communicate, making it the de facto standard for electronic documents. Individuals, governments, and corporations use PDF for the reliable exchange and storage of many types of documents and other content. PDF is increasingly used in an official capacity as a document of record. PDF can bridge paper and digital processes, and it is currently used as the electronic format of choice for contracts, legal and court documents, negotiable instruments, and formal and/or regulated electronic records. There are many methods of reliably authenticating and controlling PDF files in these situations. This document is an overview of some of the technologies that can be employed to enhance the reliability and authenticity of PDF as an electronic record.

PDF and electronic records

Electronic records (or eRecords) management involves consistently establishing the authenticity of electronic documents and content. The difference between what it takes to make an electronic document *authentic* as opposed to what makes it more *secure* can be confusing. While some of the underlying technologies that make each of these possible are similar, the business drivers for each are entirely different. Document security technologies restrict who can view a document or what things users can do with it. An example is requiring a password to open a document. These security features place restrictions on who can do what with a document, but they do little to establish the origin or authenticity of an electronic document. Where document security is like a lock on a door, authenticity is more like an electronic alarm system—it might not do anything to keep an intruder out, but it lets you know when an intrusion has occurred.

Document authenticity

Document authenticity technologies help establish that a document has not been altered or tampered with, maliciously or otherwise. Authenticity technologies also provide a means of establishing who created or signed a document.

Both of these requirements are critical to document authenticity and to electronic records, and it's difficult to have one without the other—if you can't firmly establish who created or signed a document, how can you trust that the contents have not been altered at some point? In the paper world, this accountability is established with physical signatures and notary seals. The reverse is also true: if you can't show definitively that a document has not been altered, how do you know that it's from a trusted source? In the paper world, this authenticity is accomplished by well-documented record-keeping practices and the formal recording and retention of original documents. When it comes to electronic documents, accountability and authenticity can be achieved through the use of digital signatures.

Digital signatures

There are many types of electronic signatures. You can write your name on an electronic signature pad, or it can simply be a record of a user clicking an I Agree button on a web page. However, electronic signatures don't necessarily provide integrity or authentication. Often they are just the capturing of an event or image.

A digital signature is a specific type of electronic signature that includes technology to establish the authenticity of the signed content. Adobe Acrobat® software uses digital signatures that are based on public key infrastructure (PKI) technologies to establish authenticity in PDF documents. PKI systems use certificates and keys to identify individuals or organizations. The owner uses a key to "sign" the document, and the recipient uses a key to verify the signature and the authenticity of the signed document. Supporting technologies help establish other non repudiation features like the time of signing and the status of the signing keys. You can use digital signatures to identify whom a PDF document came from and how a signed document has been modified. Digital signatures can provide electronic records the same, or better, assurances that many paper-based processes have in the past.

Legal and regulatory considerations

Technology is only part of any electronic records solution. In addition to the technological considerations, an electronic solution must take legal and regulatory requirements into account. For any electronic transaction or record to be valid, it must be created and maintained in a way that complies with relevant laws, regulatory mandates, or corporate policies. Electronic records and signature laws vary widely by locale and industry. When properly implemented, the combination of digital signature technology and Adobe PDF can satisfy a variety of legal electronic record requirements.

Digital certification

Adobe PDF provides two types of digital signatures: standard and certification. By combining standard and certification signatures, organizations can develop strategies that address the specific needs and goals of their electronic records requirements.

Certification signatures, also called author signatures, are applied by the document author. Adobe Reader® or Acrobat automatically checks the authenticity of this signature when the document is opened, and then displays a window indicating whether the signature is valid. Certification signatures are especially useful for documents that are used outside the authors control. They are helpful for restricting and detecting changes that may occur to a document during or between subsequent signings. Certified documents contain a Blue Ribbon icon in the opening dialog box, in the signature field or tab, or in the lower left or upper right corner of the document.

Ordinary document signatures, also known as approval signatures, can be applied by anyone who has permission to digitally sign the document. Adobe Reader or Acrobat can automatically check the authenticity of document signatures when a document is opened, or you can check them manually from within the application. A signature status icon appears in the signature field or tab.

Digital certificates

The keys used to create digital signatures are represented by digital certificates. When signing a PDF document in Acrobat, users are prompted to select a certificate to sign with. Certificates can be stored locally, or on an external smart card or token. In many cases, smart card and token-based certificates provide higher assurance signatures because they more effectively limit unauthorized use. However, there are emerging technologies (including Trusted Platform Modules and Roaming Credentials) that offer a similar level of trust and security as smart card and token-based certificates.

You can use certificates to represent the identity of an individual or an entire organization. Organizational certificates are often used in automated document generation and certification. A college transcript, a mortgage loan document package, or a company's financial statements may be signed or certified with an organizational certificate. Archiving systems may also use organizational certificates to sign content as it is archived.

Certificates vary by their level of trust, which is determined by the nature of its storage (software or token), the requirements for access (none, passphrase, biometric), and the manner in which it is issued (in-person identity verification). The most trustworthy certificates are considered those that are stored on a token or smart card, have a passphrase or biometric requirement to unlock the key, and are issued with strict controls regarding the establishment of the individual's identity.

The prevalence and nature of certificate distribution to individuals varies worldwide by country and organization. Many companies and governments issue certificates as part of their citizen or employee identification process. In countries like the United States, where few individuals are in possession of their own certificate, there are a number of methods for attaching someone's identity to a digital signature in a PDF. These solutions typically use other forms of identity authentication or a trusted individual with a certificate to vouch for the identity and intent of a signing party. An example of this is electronic notarization. After viewing the appropriate identity documents, and possibly capturing an electronic hand-written signature, notaries add their own digital signature to the notarized document.

Signature appearance

Signature appearances help human verifiers understand the nature of a signature. The signing party usually determines the appearance of a digital signature in a PDF document. The signature image can be a simple text box, a corporate or organizational logo, a photo, or even an image or capture of a handwritten signature, depending on the nature of the transaction and the context of the signature.

In Acrobat, signature appearances are set in user preferences and then accessed at the time of signing. A user can have multiple appearances; for example, one for a corporate certificate and another for a personal certificate. A user can even have multiple appearances for the same corporate certificate depending on whether it's used internally or externally.

Validating signing credentials

When using PDF signatures for electronic records, it's crucial that the signing certificate be properly verified. Acrobat can perform the following types of verification.

Path building and validation

A certificate needs to be traceable back to a trusted source, often called a root or anchor. When organizations issue certificates, those certificates contain references that point back to the issuing organization. Individual user certificates are usually signed with organizational certificates to provide proof of their source and authenticity and that it is subject to the rules or requirements established by that organization.

For example, notary signatures carry significant legal standing, so there is a rigorous issuance process for electronic notarization credentials, to be sure they can be traced back to the issuing association. So if someone were to create a fraudulent notary certificate, it could be easily detected because it would not be traceable back to the correct issuing authority. Acrobat performs this path building and validation as part of the signing and verification process.

Revocation checking

In revocation checking, the signing or verifying application may contact the issuer of a certificate and requests information about the current status of the signing certificate. The issuer sends a response indicating whether the certificate is valid or has been revoked. Certificates may be revoked for many reasons, such as a lost smart card, or fraudulent activity. Revocation checking lends more credibility to a digital signature because it can provide real-time status of a certificate at the time of signing.

Long-term validation

Long-term validation (LTV) is a special feature of Adobe Acrobat and PDF. LTV is a significant enhancement to traditional revocation checking in that it allows for validity checking years after the certificate was created. When LTV is enabled, Acrobat captures the certificate's sign-time status and stores it inside the PDF document. This verification certificate remains in the file so that its validity can be determined even at some later date, regardless of whether the certificate has expired or been revoked, or the issuing authority no longer exists. Because the record is stored inside the signed document, it is also authenticated by the document's signature, further reducing the chances for error or fraud.

Time verification

Some transactions and records are time-sensitive, and often electronic records need to record the time of signing in a verifiable manner. PDF signature features can increase the accuracy and trust of the signature time. The most basic source for time is the system clock of the signing computer. System time is usually accurate, especially in enterprise environments, but there is the possibility that the system date could be altered to fraudulently predate a document. In some cases, the signature time can be compared with other system logs to determine its accuracy. For example, if LTV is employed, the revocation response contains a time stamp from the issuing system. Because the time on the revocation response is usually more secure than system time, this time can be cross-referenced and compared with the signature time.

The most accurate way to establish the time of signing is to add a secure time stamp to a digital signature. A secure time stamp is a standards-based method (based on RFC 3161) for recording the time of a transaction. In Adobe PDF documents, secure time stamps are added directly to a signature at the time of signing and are visible in Acrobat and Reader when verifying signatures. Although secure time stamps may not be a requirement for all types of electronic records, their use is strongly encouraged for time-sensitive or high-value records.

PDF formats

In addition to digital signatures, the actual content of a PDF file can be critical to the veracity of a record. PDF files can be very dynamic documents, containing multimedia, layers, dynamic forms, and other rich content. For some types of electronic records, this type of content needs to be very tightly controlled. PDF digital signatures can authenticate the entire document, including scripts, multimedia, and form data. The ISO standard PDF/A is an open standard developed for the long-term preservation of PDF documents. While PDF/A has somewhat limited support for digital signatures, its guidance can serve as an excellent baseline for the development of PDF requirements for electronic records. For more information on PDF/A, visit *http://www.aiim.org/pdf_a*.

Signed PDF eRecords

The requirements for a PDF eRecord vary widely among localities and business processes, but implementers building a robust PDF eRecord strategy should consider the following features.

High-assurance certificates—Certificates that are issued and maintained with a well-documented and highly trustworthy process increase certainty of verifying the identity of the signing party. Documents signed with certificates of lower assurance levels are not considered as trustworthy.

Certification—Documents distributed outside the author's control should be certified. Certification protects a document, especially those that are being signed by multiple parties. It also provides those parties with a higher level of trust in the documents they are signing.

Meaningful appearances—Using meaningful signature appearances like images of handwritten signatures and official seals helps casual users better understand the nature of digital signatures.

Revocation checking—Make sure that revocation checking is enabled in Adobe Acrobat (or server systems) for both signing and verification to ensure that credentials are currently valid at signing and that available revocation information is consulted in the verification process.

Certified Document Services

For documents requiring an added level of assurance, Adobe also offers Certified Document Services (CDS). CDS allows authors to create PDF files that automatically certify to the recipient that the author's identity has been verified by a trusted organization, and that the document has not been altered in any way. Unlike other PKI solutions, CDS signatures are automatically trusted by the free and ubiquitous Adobe Reader and do not require the recipient of a certified document to configure any settings.

LTV—LTV helps reduce dependencies on external systems and reduces the potential for future ambiguity around expired or revoked certificates.

Time stamps—Using Acrobat's built-in support for secure, standards-based time stamps with signatures is the most powerful way to establish the date and time that a signature was created.

Dynamic content—Set clear guidelines on what type of dynamic content is allowed in each signed eRecord.

When implemented along with appropriate polices and procedures, these PDF authenticity features are the technological foundation that can meet many legal and regulatory requirements for electronic records and transactions, regardless of location or type of industry.

Adobe

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

Adobe, the Adobe logo, Acrobat, and Reader are either registered trademarks or trademarks of Adobe Systems Incorporated in the United States and/or other countries. All other trademarks are the property of their respective owners.

© 2007 Adobe Systems Incorporated. All rights reserved. Printed in the USA.

95009267 6/07