Related Resources:

- Digital Signatures in PDF: *http://partners.adobe.com/public/developer/en/acrobat/DigitalSignaturesInPDF.pdf*
- How to Verify a Signed PDF (User Guide): *http://www.adobe.com/products/pdfs/AdobePDFSecurityGuide-c.pdf*

Adobe PDF Security & Authenticity

PDF for Electronic Records

Using digital signatures & PDF for definitive electronic records & transactions

Millions use 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 being used in an official capacity as a document of record. PDF can bridge paper and digital processes, and it is now being 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 in PDF to enhance its reliability and authenticity as an electronic record.

Part I - PDF and Electronic Records

Electronic records management involves consistently establishing the *authenticity* of electronic documents and content. The differences between what it takes to make an electronic document *authentic* as opposed to what makes it *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 are those that restrict who can view a document or what things they can do with it. An example would be requiring a password to open a document. Security features like these place restrictions on who can do what with a document, but they do little to actually 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.

Authenticity

Document Authenticity technologies are those that help to establish that a document has not been altered or tampered with (maliciously or otherwise). Authenticity technologies bring together two things:

1. **A way of showing that a document has not been altered**
2. **A means of establishing who the document came from**

Adobe

Both of these things are critical to document authenticity and to electronic records. It's difficult to have one without the other - if you can't firmly establish who or where a document came from, how can you trust that the contents have not been altered at some point? In the paper world, this *accountability* is established with things like 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 the document is actually from a trusted source? In the paper world, this *authenticity* is accomplished by well documented records 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.*

***Electronic* Signatures or *Digital* Signatures?**

There are many types of *Electronic* Signatures. An Electronic Signature can be anything from a record of a user clicking an "I Agree" button on a web page, to writing your name on an electronic signature pad. However, electronic signatures don't necessarily imply any built-in form of authentication. Often they are just the simple capture of an event or image. *Digital* Signatures are somewhat different - they may or may not include things like physical signature images, but they typically do include some form of technology to definitively establish authenticity of the signed content. Digital Signatures are used by Acrobat to establish authenticity in PDF and are based on Public Key Cryptography (commonly referred to as PKI, which is actually an acronym for Public Key Infrastructure). PKI systems use sets of "keys" to identify individuals (and organizations). These keys are used by the owner to "sign" documents, and by recipients to verify those signatures and the authenticity of signed documents. There are also a number of supporting technologies that help establish things like the time of signing and the current status of the signing keys. Digital signatures can be used in PDF to identify who a document came from, and can be used to show whether or not a signed document has been modified. For electronic records, digital signatures can be used to provide the same (or better) types of assurances that many paper based processes have in the past.

Other Electronic Signature Requirements - Legal & Regulatory

Electronic records and signatures require much more consideration than technology alone - for any electronic transaction or record to be valid, it still needs to be created and maintained in a way that complies with any relevant laws, regulatory mandates and/or corporate policies. Electronic records and signature laws vary widely by locale. When properly implemented, the combination of digital signature technology and PDF can go a long way to satisfy a variety of legal electronic record requirements. While individual legal and policy analysis is well outside the scope of this document, it's important to understand that technology alone is only half of any electronic records solution. Laws, regulations, and their levels of technical specificity vary by country, state or province, and industry. Any electronic records or signature implementation needs to consider not only the underlying technology issues, but also must address the legal and regulatory requirements of its particular focus or locale.

Part II - Technology Strategies for PDF Signatures

This section explores the various authenticity features of PDF and Adobe Acrobat. By bringing the elements here together, organizations can develop strategies that address the specific needs and goals of their electronic records requirements.

There are two basic types of signatures in PDF:

***Certification Signatures* -** Can be applied by the document's author. Adobe Reader or Acrobat automatically checks the authenticity of this signature when you open the document, and then displays a window that indicates whether the signature is valid (that is, authentic and current). Certification signatures are also referred to as the "Author Signa-

tures." Certification signatures are especially useful for documents that will be used outside of the control of the author. They are helpful for restricting and detecting changes that may occur to a document during or between subsequent signings. Look for the certification "Blue Ribbon" icon in the opening dialog box of certified documents, in the signature field or tab, and in the lower-left corner of a certified document.

Standard Signatures **-** Can be applied by anyone who has permission to digitally sign the document. Adobe Reader or Acrobat can automatically check the authenticity of standard signatures when you open the document, or you can check them manually from within the application. Look for the Signature status icon in the signature field or tab.

Digital Certificates

The keys used to create Digital Signatures are stored inside containers called Digital Certificates. When signing a PDF in Acrobat, users will be prompted to select a Certificate. Certificates can be stored on the computer (in Windows or Acrobat), or on a Smart Card or token. In many cases, Smart Card and token-based certificates are considered more qualified for higher authenticity signatures since they don't reside on any particular computer and are ideally found only in the possession of their owner. However, there are emerging software-based technologies (including Trusted Platform Modules & Roaming Credentials) that are closer in level of trust and security to Smart Card and token based certificates.

Certificates can be used 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 are things that might be signed or certified with an organizational certificate. Organizational certificates may also be employed by archiving systems that sign content as it enters the archive.

Signature Validity Status Icons *(from top)*: **Valid; Unknown; Invalid; Valid and Modified**

Certificates vary by their relative level of trust. The level of trust of a certificate is generally 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 generally considered those that are stored on a token or smart card, have a passphrase or biometric requirement to unlock the key, and were issued with strict controls regarding the establishment of the individual's identity.

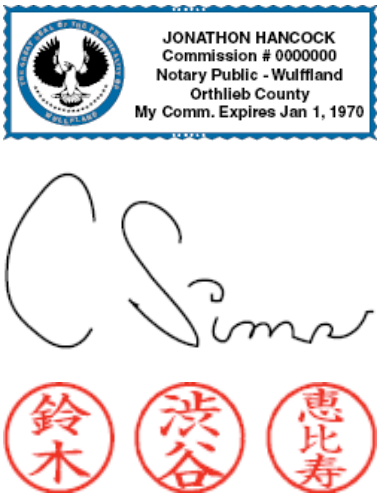
The prevalence and nature of certificate distribution varies worldwide by country & organization. Some countries and localities have issued certificates to citizens as part of smart card identity programs. Many companies and governments issue certificates as part of their citizen or employee identification 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 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, the notary will add her own digital signature to the notarized document.

Signature Validity

The validity of a PDF digital signature in Acrobat is indicated with an icon. More details can always be found by selecting a signature or viewing it in the Acrobat Signatures tab, but the signature icon presents an instant assessment of the validity and any potential trust concerns about a signature.

Signature Appearance
Signature appearances help human verifiers understand the nature of a signature. The appearance of a digital signature in a PDF is generally controlled by the signing party. The signature image can be a simple text box, a corporate or organizational logo, a photo, or even an image or capture of a hand-written signature. The type of appearance for a particular record depends on the nature of the transaction and the context of the signature. Users of personal certificates may choose to use a photo or a hand-written facsimile. Corporate or government sponsored credentials may use the seal or logo of the organization or department. Electronic notary signatures often include an image of a notary seal.

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



Example Signature Appearances

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
First, the certificate needs to be traceable back to a trusted source (often called a root or anchor). When organizations issue certificates, those certificates point back to the issuing organization. User certificates are usually signed with organizational certificates to prove their authenticity. This is important in that it establishes that a given certificate is part of a particular organization, so it is subject to whatever issuance or storage requirements established by that organization. Sometimes these paths may be very complex. For example, since notary signatures carry significant legal standing, there is a rigorous issuance process for electronic notarization credentials. When issued, those notary certificates can be traced back to the issuing association. That way, even if someone was 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 addition to Path Building and Validation, Acrobat can also be configured to perform certificate revocation checking. There are several specific methods used to perform revocation checking, but the principle is very simple. In revocation checking, the signing or verifying application contacts the issuer of a certificate and requests information about the current status of the certificate. The issuer generally sends a response indicating whether the certificate is valid or has been revoked. Certificates may be revoked for many reasons - they may just be re-issued prior to expiration, someone may loose their smart card, or there may even be fraudulent activity involved. Revocation checking lends more credibility to a digital signature because it can provide real-time status about a signing certificate.

Long Term Validation (LTV)
LTV is a special feature of Acrobat & PDF. It is a significant enhancement to traditional revocation checking, and can be especially valuable for maintaining the long-term validity of electronic records. When LTV is enabled, Acrobat captures the result of a revocation check and embeds it inside the PDF during signing. This means that the signed PDF contains a record of the verification of the certificate that was used to sign it. This allows for verification of the signing certificate at any point in the future - regardless of whether a certificate has expired or been revoked, or the issuing authority no longer exists. With traditional revocation checking, these events may result in inconclusive verification attempts at some point in the future after signing. LTV

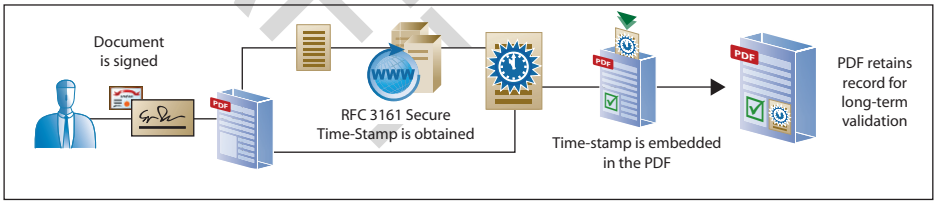
eliminates this by taking a "snapshot" of the certificate's sign-time status and storing it inside the document. Since the record is stored inside the signed document, it is also authenticated by the document's signature as well, further reducing the chances for errors or fraud.

Verifying Time

Some transactions and records are time-sensitive. Often the electronic records involved in those transactions need to record the time of signing in a secure manner. There are several potential sources of time in a PDF signature, each with a different level of trust. The most basic source for time is the system clock of the signing computer. This is where time is obtained for signatures by default. System time is generally accurate (especially in enterprise environments) but introduces the potential for inaccuracies or fraud. It is conceivable that a party could alter the date on their system in order to fraudulently pre-date a document signature. There are some simple ways to offset this though. In some cases, the signature time can be compared with other system logs to determine its accuracy. Also, if LTV is employed, the revocation response generally contains a time-stamp from the issuing system. Since the time on the revocation response is generally considered more secure than system time, this time can be cross-referenced with the signature time to compare. Acrobat does not perform these types of cross referencing natively, but the information may be obtained by other systems or viewed manually.

Secure Time Stamping

The most accurate way to establish the time of signing in Acrobat is with the addition of a *Secure Time Stamp* (RFC 3161) to a digital signature. When configured in conjunction with a secure time server, Acrobat can add a *time stamp* to a PDF at the time of signing. Secure time stamps are a standards-based method for recording the time of a transaction. In PDF, secure time stamps are added directly to a signature at the time of signing, and are visible directly in Acrobat when verifying signatures. They provide the strongest possible attestation of the date and time that a transaction occurred. While they may not be a requirement for all types of electronic records, their use is strongly encouraged for those records that are time-sensitive.



Secure Timestamping

PDF Formats

In addition to digital signatures, the actual content of a PDF can be critical to the veracity of a record. The PDF files of today can be very dynamic documents. They can contain multimedia, layers, dynamic forms, and other rich content. The use of this type of content needs to be very tightly controlled for some types of electronic records. That isn't to say that it absolutely may not be used - digital signatures on a PDF authenticate the entire document, including scripts, multimedia, and form data - the implications of dynamic content just need to be considered in the context of a particular transaction or record. For the sake of simplicity and transparency, legal and court documents should generally be limited with regard to dynamic content. The ISO standard **PDF/A** is an open standard developed for the long-term preservation of PDF. While PDF/A has somewhat limited support for digital signatures, it's 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*

Part III - Putting it All Together - Signed PDF eRecords

The definition of an ideal PDF eRecord varies widely among localities and business processes, but implementers building a robust PDF eRecord should consider:

1. **Use High-Assurance Certificates.** Certificates that are issued and maintained with a well documented and highly trustworthy process are beneficial to the creation of signed PDF eRecords because they add a great deal to verifying the identity of the signing party. Documents signed with certificates of lower assurance levels are not considered as trustworthy.

2. **Certify.** Documents that are being 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.

3. **Use Meaningful Appearances.** The use of meaningful signature appearances like images of hand-written signatures and official seals helps casual users better understand the meaning and nature of digital signatures.

4. **Revocation Checking.** Make sure that revocation checking is enabled in Acrobat (or server systems) for both signing and verification. This ensures that credentials are currently valid at signing, and that any available revocation information will be consulted in the verification process.

5. **Use LTV.** Long Term Validation promotes the long-term validity of a signed document. It helps reduce dependencies on external systems and reduces the potential for future ambiguity around expired or revoked certificates.

6. **Time Stamp (where appropriate).** Using Acrobat's built in support for standards-based secure time stamps with signatures is the most powerful way to establish the date and time that a signature was created.

7. **Control Dynamic Content.** Determine what requirements you eRecords have for dynamic content. Set clear guidelines on what dynamic content is allowed in a signed eRecord.

When implemented along with appropriate polices and procedures, these PDF authenticity features are the technology foundation for electronic documents that can meet many legal and regulatory requirements. While individual requirements vary by transaction type and location, some or all of these technology considerations can be combined to support the legal requirements for electronic records and transactions.

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

Adobe