A primer on electronic document security

How document control and digital signatures protect electronic documents

Table of contents

Purpose

This white paper is intended to provide the reader with a brief overview of relevant document security issues and technologies, as well as to introduce the Adobe suite of document security solutions. The white paper also summarizes Adobe implementations for document control and digital signatures.

Executive summary

As organizations move more business processes online, protecting the confidentiality and privacy of information used during these processes, as well as providing authenticity and integrity, are essential. Because many automated processes rely on electronic documents that contain sensitive information, organizations must properly protect these documents. Many information security solutions attempt to protect electronic documents only at their storage location or during transmission. However, these solutions do not provide protection for the entire lifecycle of an electronic document. When the document reaches the recipient, the protection is lost, and the document can be intentionally or unintentionally forwarded to and viewed by unauthorized recipients.

A significantly more effective solution is to protect a document by assigning security parameters that travel with it. Six criteria must be met in order to provide more effective protection for an electronic document throughout its lifecycle:

1 Confidentiality

2 Authorization

3 Accountability

4 Integrity

5 Authenticity

6 Non-repudiation

The two major security techniques used to establish these six document security criteria are document control and digital signatures.

The Adobe suite of security solutions delivers document control and digital signature services that simplify the process of protecting sensitive electronic documents and forms. Organizations can easily integrate Adobe document security solutions into current business processes and enterprise infrastructure to support a wide range of simple and complex processes. Adobe solutions dynamically protect electronic documents inside and outside the network, online and offline to provide persistent, end-to-end protection throughout an electronic document's lifecycle.

Adobe

Introduction

As organizations move more business processes online, protecting the confidentiality and privacy of the information used during these processes is essential. Because many automated processes rely on electronic documents that contain mission-critical, personal, and sensitive information, organizations must make significant investments to properly protect these documents.

There are three main reasons that organizations need to address the security of electronically shared documents:

Regulatory requirements—Many companies are directly or indirectly affected by government mandates and regulations for providing consumer privacy. These include:

- Health Insurance Portability and Accountability Act (HIPAA)—Protection for health-related data
- Gramm-Leach-Bliley Act—Financial privacy
- European Union Directive on Privacy and Electronic Communications
- Privacy Acts of Japan and Australia
- California SB 1368—Privacy notification
- California AB 1950—Protection of customer data

Return on investment (ROI)—Organizations can achieve significant ROI by migrating to electronic business processes. Automated workflows allow prospects, customers, partners, and suppliers to participate, enabling organizations to reap significant cost savings while improving customer satisfaction and loyalty. However, many workflows cannot be automated until adequate protections are put in place on the electronically shared information. For instance, how can you be sure that the bank statement you received is truly from your bank (authenticity), that it has not been altered in transit (integrity), and that it has not been viewed by someone other than the intended recipient (confidentiality)?

Information security—Thefts of proprietary information are increasing, which can jeopardize revenue, competitive advantage, and customer relationships; generate negative publicity; and result in significant penalties and fines for failure to comply with privacy laws.

Many information security solutions attempt to protect electronic documents only at their storage location or during transmission. For example, organizations rely on document management systems and virtual private networks (VPNs) to protect documents. With this approach document security remains a problem because these solutions secure only the communication line or storage site; they do not provide protection for the actual content of an electronic document throughout its lifecycle. When the document reaches the recipient, the protection is lost, and the document can be intentionally or unintentionally forwarded to and viewed by unauthorized recipients. Consequently, many organizations are forced to engage in an inconsistent combination of online and paper processes in which sensitive documents must still be printed and physically delivered to achieve adequate security. As a result, the potential benefits of online processing cannot be fully realized.

How to provide persistent document security

Document control plus digital signatures means persistent document security

A significantly more effective solution for protecting an electronic document is to assign security parameters that are an integral part of the document itself. The following criteria define persistent document security:

Confidentiality—Who should have access to the document?

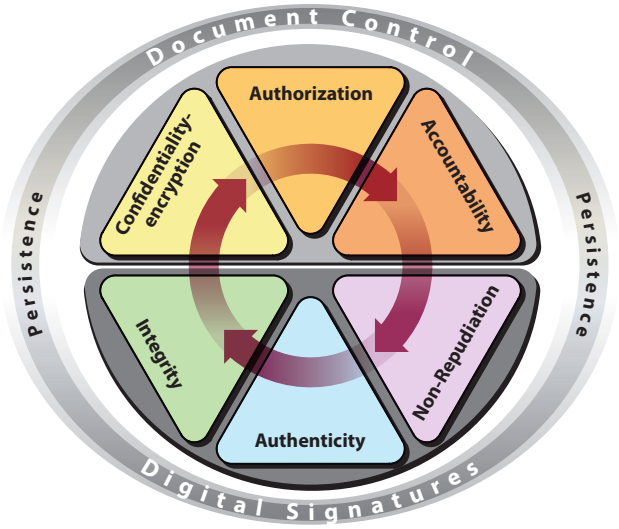
Authorization—What permissions does the user have for working with the document?

Accountability—What has the recipient done with the document?

Integrity—How do you know if the document has been altered?

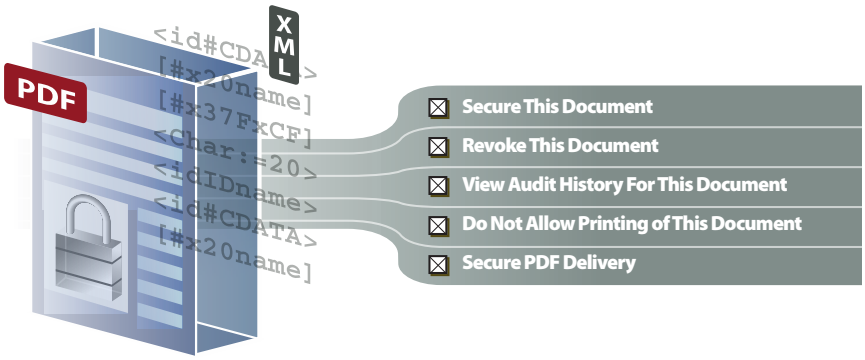
Authenticity—How do you know where the document came from?

Non-repudiation—Can the signatory deny signing the document?



Six key criteria for providing persistent document security

The following sections survey the major technologies used to provide document control and digital signatures and identify the technologies Adobe has implemented for its document security solutions.



Document control provides confidentiality, authorization, and accountability. The illustration above shows some of the document control options available with Adobe LiveCycle™ Policy Server and Adobe® Acrobat® software.

Document control

Confidentiality—encryption

Encryption is the process of transforming information *(plaintext)* into an incomprehensible form *(ciphertext)*. Encryption is an effective technique for managing document access.

Decryption is the reverse process that transforms ciphertext back to the original plaintext.

Cryptography refers to the two processes of encryption and decryption and its implementation is referred to as a *cryptosystem*.

Popular encryption systems use the concept of keys. An encryption key is data that combines with an encryption algorithm to create ciphertext from plaintext and recover plaintext from ciphertext. Today, security experts widely agree on "Kerckhoff's" principle as the basis of an effective cryptosystem. Kerckhoff's principle states that the key is the only portion of a cryptosystem that must remain secret for the entire system to be secure. If the strength of the cryptosystem relies on the fact that an attacker does not know how the algorithm works, then it is just a matter of time before it can be reverse-engineered and broken.

Two main types of encryption keys include symmetric and asymmetric.

Symmetric keys

Symmetric key cryptography uses the same key for both encryption and decryption and is very fast and diffcult to break with large keys. However, because both parties need the same key for effective communication to occur, key distribution becomes an issue. Today, common symmetric key encryption algorithms are AES, DES, 3DES, and RC4. Adobe products leverage AES (128- and 256-bit) and RC4 (128-bit), as they have evolved into very strong standards.

Asymmetric keys

Asymmetric key cryptography, also called *public key cryptography,* uses key pairs for encryption and decryption. For instance, if the first key encrypts the content, then the second key of the pair decrypts the content. Similarly, if the second key is used to encrypt the information, then the first key must be used to decrypt the content.

Typically, one key in the pair is labeled as the public key and the other as the private key. An individual keeps the private key secret, while the public key is freely distributed to others who wish to communicate with the individual. When someone wishes to send the individual a confidential message, he or she can encrypt it with the freely available public key and send the ciphertext to the individual. Because the individual is the only one who has the private key, he or she is the only one who can decrypt the content.

Asymmetric keys help solve the key distribution problem, but the algorithms tend to be slower for equivalent strengths. Some common asymmetric algorithms are RSA, DSA, and El Gamal. Adobe leverages RSA (512-, 1024-, and 2048-bit) as it has evolved into a global standard.

Hybrid Encryption

Security systems tend to use a hybrid solution to increase the security and speed of encrypting documents. One approach is to use asymmetric keys to protect the symmetric keys, and then use the symmetric keys for encrypting the information. This technique helps to solve both the key distribution challenge of symmetric key cryptography while solving the performance problem of asymmetric key cryptography. Adobe Acrobat software leverages hybrid approaches so single documents can be protected for multiple recipients, each possessing unique key pairs. The file size is not significantly increased during this method because the entire document does not need to be encrypted for each person. Instead, the document is encrypted with a single symmetric key and that symmetric key is encrypted for each recipient with their respective public key.

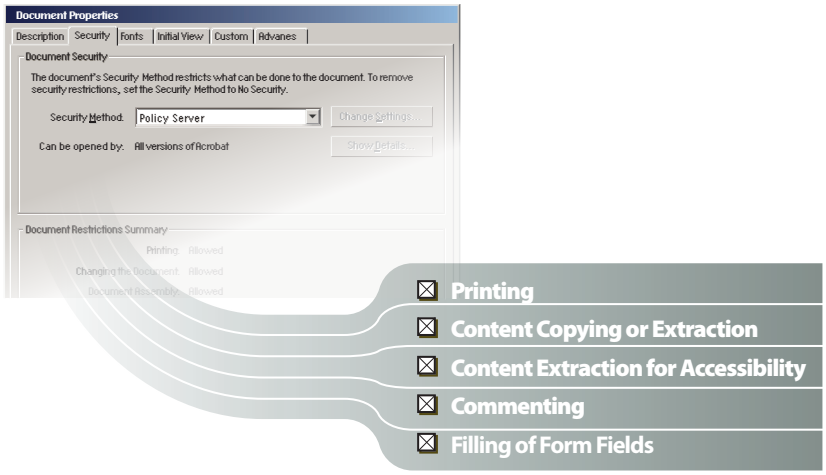
Authorization

In addition to managing who can open a document, organizations gain additional protection through authorization. Authorization specifies what a user can do with a document and is achieved via permissions and dynamic document control.

- **Permissions** govern a user's actions while working with a protected document. Permissions can specify whether or not a recipient who has access to the document is allowed to print or copy content, fill in fields, add comments or annotate the document, insert or remove pages, forward the document, access the document offline, digitally sign the document, and so forth.
- **Dynamic document control** maintains access rights and permissions assigned to an electronic document once it has been published and distributed. A document's author can make changes to a released document without having to manually redistribute it since the changes are automatically pushed to all existing versions of the document no matter where they reside. Using dynamic document control, organizations can manage and monitor electronic document use inside and outside the firewall, online and offline, and across multiple documents.

Dynamic document control includes the following capabilities:

- **Document expiration and revocation**—Post-publication document control can be maintained through the application of expiration dates and the ability to revoke access to a document. For example, an author can send a document that will expire in two weeks so that recipients will not be able to access it once the expiration date has passed. Or, access to a document can be automatically revoked if an authorized recipient leaves the project or changes departments.
- **Offline access management**—Organizations can manage how long an authorized recipient can access a document offline. Once the specified length of time has passed, the recipient can no longer view the document and must go back online to gain further access. Any access or permission changes that the author has made to the distributed document will be applied when the recipient goes back online.
- **Persistent version control**—Content and document management systems provide an effective mechanism for version control as long as a document stays within the confines of the system. Persistent version control expands on these capabilities by maintaining version control outside the system and offline. It allows document authors to make changes to a document's usage policies and prevent the obsolete version from being accessed while providing end users with the location of the updated version, no matter where the document resides.



Authorization is achieved via permissions and dynamic document control. These are some of the authorization options and levels of dynamic document control available with Adobe Acrobat and Adobe LiveCycle™ Policy Server.

Accountability

Document auditing allows organizations to maintain accountability with regard to the use of protected documents, because they can know precisely:

- How a recipient has used a document
- How often each type of usage occurred
- When that usage occurred

Accountability is achieved when an author can track each recipient's use of a document for each permission assigned (such as allowing a user to fill in fields on a form, print, forward, save a copy, and so forth.) Auditing should include automatic notifications about the use of protected documents. For example, a customer service representative sends a customer a time-critical electronic statement that requires an action on the customer's part, such as a reply or digital signature. Once the customer receives the electronic document, the representative is automatically notified when the customer opens it. If the customer fails to open the document, the representative is notified after 24 hours. Alternatively, a customer relationship management (CRM) system can leverage failure notification to initiate an escalation or specific follow-up task by the customer service representative.

Digital signatures

When enterprises distribute documents electronically, it is often important that recipients can verify:

- That the content has not been altered *(integrity)*
- That the document is coming from the actual person who sent it *(authenticity)*
- That an individual who has signed the document cannot deny the signature *(non-repudiation)*

Digital signatures address these security requirements by providing greater assurances of document integrity, authenticity, and non-repudiation.

Integrity

Digital signatures enable recipients to verify the integrity of an electronic document that is used in one-way or round-trip workflows. For example, when a digital signature is applied to a quarterly financial statement, recipients have more assurance that the financial information has not been altered since it was sent. Methods for maintaining integrity include:

- **Parity bits or cyclical redundancy checking (CRC) functions**—CRC functions work well for unintentional modifications, such as wire interference, but they can be circumvented by a clever attacker.
- **One-way hash**—A one-way hash creates a fixed-length value, called the hash value or message digest for a message of any length. A hash is like a unique fingerprint. With a hash attached to the original message, a recipient can determine if the message was altered by recomputing the hash and comparing his or her answer to the attached hash. Common hashing algorithms are MD5, SHA-1, and SHA-256. Adobe has adopted the SHA-1 and SHA-256 algorithms because of their wide acceptance as a security standard.
- **Message Authentication Codes (MAC)**—A MAC prevents an attacker from obtaining the original message, modifying it, and attaching a new hash. In this case, a symmetric key is connected to the MAC and then hashed (HMAC). Without the key, an attacker cannot forge a new message. Adobe uses HMACs where appropriate.

Digital signatures verify the integrity of an electronic document

Adobe Acrobat tracks all previously signed versions within the document for easy verification of changes made during the document's lifecycle

Authenticity

Digital signatures provide document authenticity by verifying a signer's digital identity. For example, a digitally signed quarterly financial statement allows recipients to verify the identity of the sender and assures them that the financial information has not been altered since it was sent.

Digital signatures are created using asymmetric key cryptography. For document encryption, a document's author encrypts a document using a public key. Because the recipient is the only person with the private key, he or she is the only one who can decrypt the message. Digital signatures reverse the use of public and private keys for document authenticity. The author encrypts the hash of the message with a private key. Only the public key can correctly decrypt the hash and use it to see if it matches a new hash of the document. Because recipients of the document have the author's public key, they gain greater assurances that the individual who signed the document was the person who encrypted the original hash.

The process that constitutes a digital signature is as follows:

- A hash is created of the original document.
- The digital signature is created, which encrypts the hash with a private key.
- The signature is included with the document.

Adobe Acrobat supports multiple digital signatures placed anywhere in the document for proper presentation. In fact, Adobe Acrobat tracks all previously "signed" versions within the document for easy verification of changes made during the document's lifecycle. Furthermore, Adobe offers a certified signature, which is the first signature on the document. With a certified signature, the author can specify what changes are allowed for integrity purposes. Adobe Acrobat will then detect and prevent those modifications.

Digital signatures verifying a signer's digital identity

Non-repudiation

Non-repudiation is a document security service that prevents the signor of the document from denying that they signed the document. Support for this service is often driven by authentication and time-stamping capabilities.

Public key infrastructure (PKI)

Public key infrastructure (PKI) mainly provides a digital certificate that enables a document's recipient to know whether or not a specific public key really belongs to a specific individual. Digital certificates bind a person (or entity) to a public key. Certificate authorities (CA) issue these certificates and recipients must trust the CA who issued the certificate. X.509 is the widely accepted certificate standard that Adobe uses.

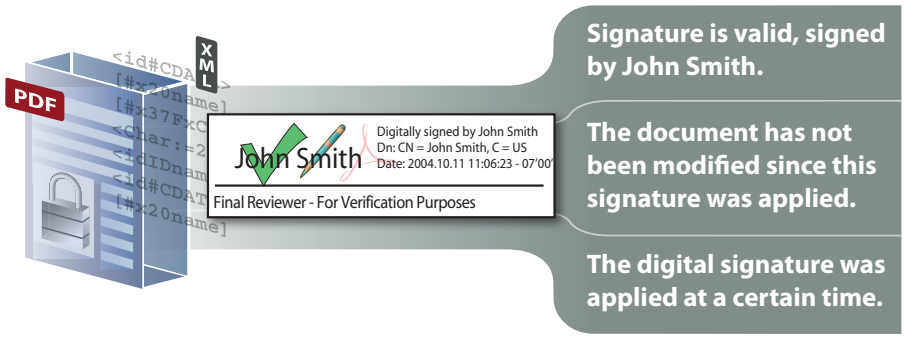
If a certificate expires or a private key is compromised, the CA will revoke the certificate and record the revocation. As part of the process of authenticating a digital certificate, recipients can check the certificate's status. Certificate validity can be checked using the following standard methods:

- Certificate revocation list (CRL)
- Online Certificate Status Protocol (OCSP)

Adobe uses both CRL and OCSP.

The following additional mechanisms can make up a PKI:

- **Public-Key Cryptography Standards (PKCS)**—A set of standard protocols for PKI used by multiple vendors. The standards include RSA encryption, password-based encryption, extended certificate syntax, and cryptographic message syntax for secure multipurpose Internet mail extensions (S/MIME).
- **Registration authority**—Used to run background checks on individuals who wish to obtain a certificate.
- **Certificate repository**—Repositories that house digital certificates.
- **Key update, backup, recovery, and history**—Mechanisms for key maintenance and archiving.
- **Cross-certification**—In the absence of a single global PKI, which is highly unlikely, this mechanism allows users from one PKI to validate certificates from users in another trusted PKI.
- **Time stamping**—A critical component of non-repudiation that offers a time stamp from a trusted third party.



Digital signatures address security requirements by providing greater assurances of document integrity, authenticity, and non-repudiation.

Adobe security solutions for end-to-end document protection

Adobe has been delivering persistent document security solutions for more than ten years

In partnership with leading security vendors, Adobe has been delivering persistent document security solutions for more than ten years. Since Adobe Acrobat was introduced in 1994, Adobe has enabled organizations to more successfully manage electronic document use by encrypting Adobe PDF files and assigning user access permissions. Beginning in 1999, Adobe Acrobat 4.0 offered organizations the ability to apply digital signatures to Adobe PDF files for greater assurance of document authenticity, integrity, and non-repudiation.

A significantly more effective solution for protecting an electronic document is to assign security parameters that are an integral part of the document itself. This approach differentiates the Adobe document security solutions, which enable organizations to more effectively manage the use of electronic documents with persistent protection. By applying security parameters to the individual document, organizations gain greater assurance in the confidentiality, authenticity, and integrity of electronically shared documents in addition to securing the communication line or storage location.

As organizations accelerate online processing, Adobe security solutions deliver document control and digital signature services that simplify the process of protecting sensitive electronic documents and forms. Because Adobe solutions are designed to protect electronic documents inside and outside the network, online and offline, organizations can more easily extend the use of electronic processes to reduce costs for sharing information and increase customer satisfaction and loyalty. It is important to note that security is not an all or nothing proposal. Security professionals must practice proper risk mitigation when evaluating solutions for their organizations. Adobe helps with this endeavor by offering a wide range of support from solutions for simple assurance levels, such as click-wrap agreements, personal identification numbers (PINs), and passwords to those requiring stronger assurance levels, such as software PKI, two-factor authentication with tokens, or three-factor authentication with biometrics.

Adobe document security provides persistent, end-to-end protection throughout an electronic document's lifecycle, including desktop solutions that make it easy for every user in an organization to protect documents and server-based solutions that automate the application and monitoring of document protection on an enterprise-wide basis. Whether e-mailing monthly

statements, making tax forms available on citizen portals, sending design documents to partners for review, approving loan applications, or preparing financial reports, Adobe helps organizations conduct these processes with greater assurance of document confidentiality, integrity, authenticity, non-repudiation, and accountability.

Summary of Adobe security capabilities

Adobe Acrobat Family*	Adobe Reader®	Adobe LiveCycle Reader Extensions ES	Adobe LiveCycle Digital Signatures ES	Adobe LiveCycle Rights Management ES
Quickly create secure documentsfrom native applications	Use the free, cross-platform solution to view and interact with protected documents	Easily share protected interactive Adobe PDF documents with external parties	Automate the process of encrypting and digitally signing thousands of electronic documents	Dynamically apply document usage rights to manage use online, offline, inside the network, and outside the network
Encrypt/decrypt documents using shared passwords, PKI, and Adobe LiveCycle Policy Server software	Validate recipient's digital signatures	Activate additional functionality in the free Adobe Reader to enable offine form filling and digital signatures	Encrypt/decrypt documents using shared passwords and PKI	Manage printing, content copying, form filling, digital signature use, screen reader access, review and comment use, page insertion, deletion, and rotation
Apply and validate recipient's digital signatures	Verify author-certified documents		Automatically apply digital signatures	Manage online and offine access
Create and verify author-certified documents	Apply recipient digital signatures†		Automatically verify digital signatures	Includes server and client extensions for PDF, Word, and Excel
Manage printing, content copying, form filling, digital signature use, screen reader access, review and comment use, page insertion, deletion, and rotation	Support for Microsoft CryptoAPI on Windows		Create and verify author-certified documents	Revoke access after distribution
Support for Microsoft CryptoAPI (MSCAPI) on the Microsoft® Windows® operating system	Decrypt documents using shared passwords, PKI, and Adobe LiveCycle Rights Management ES software		Support for Hardware Security Modules (HSMs) using PKCS#11	Establish time controls for access
			Pre-built support for VeriSign credentials in Adobe Reader	Audit user actions
			Support for FIPS mode	Leverage existing authentication infrastructure (Lightweight Directory Access Protocol [LDAP]/ Active Directory) for document control

* Includes Adobe Acrobat Professional, Adobe Acrobat Standard, and Adobe Acrobat Elements. Not all security features are available in all products.

† Requires documents to be rights-enabled with Adobe LiveCycle Reader Extensions ES.

Adobe Acrobat and Adobe Reader

Document control and digital signature capabilities are built into the Adobe Acrobat interface, making it easy for users to add security parameters to documents

Document authors can use Adobe Acrobat software to create Adobe PDF documents, and apply encryption, permissions, and digital signatures to Adobe PDF files. The ease and convenience of assigning security parameters to electronic documents via Adobe Acrobat encourages users to keep information private and confidential.

Protected Adobe PDF documents can be viewed using free Adobe Reader software. With more than 700 million copies distributed worldwide, Adobe Reader provides multi-platform access to Adobe PDF files, enabling organizations to share secured documents with users outside the firewall and on a wide variety of client computers. Adobe Reader users can view protected documents, validate digital signatures, and verify document certification. In addition, when documents are rights-enabled via Adobe LiveCycle Reader Extensions ES, Adobe Reader users can digitally sign Adobe PDF files.

With more than 700 million copies distributed worldwide, Adobe Reader software provides cross-platform access to Adobe PDF files, enabling organizations to share protected documents with users outside the firewall and on a wide variety of client computers

Adobe PDF, the Portable Document Format, is a general document representation language that has been in use for document exchange on the Internet since 1993. RFC 3778 provides updated information on the registration of the MIME Media Type "application/pdf," with particular focus on the features that help to mitigate security concerns.

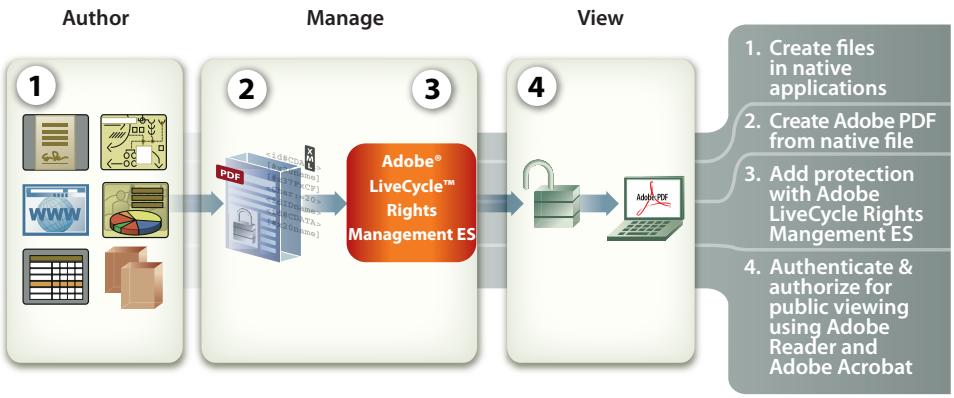
Adobe LiveCycle Reader Extensions ES

Adobe LiveCycle Reader Extensions ES enables organizations to extend the use of automated business processes to participants who are outside the network and using disparate client technologies. Using Adobe LiveCycle Reader Extensions ES, organizations embed usage rights in Adobe PDF files that will activate functionality within Adobe Reader software. This hidden functionality is automatically activated when the Adobe Reader user launches a rights-enabled Adobe PDF document. When the user is finished working with the document, those functions are once again disabled until the user receives another rights-enabled PDF file.

Rights-enabled Adobe PDF files allow users of Adobe Reader to save the file to a local hard drive, fill it out, add comments and mark up content, share it with others, and submit a completed document electronically. In addition, Adobe PDF files can be rights enabled to allow users to digitally sign, certify, and authenticate a document. As a result, organizations can easily include Adobe Reader users in simple and complex business processes that provide greater assurance of document authenticity and confidentiality for users outside the network.

Adobe LiveCycle Rights Management ES

Adobe LiveCycle Rights Management software is a document control solution that addresses the challenges of managing access to and use of electronic documents on an enterprise-wide basis. Adobe LiveCycle Rights Management software offers a platform-independent solution for dynamic, persistent, and robust document policy management. Adobe LiveCycle Rights Management software manages three aspects of document security—confidentiality, authorization, and accountability.



Adobe LiveCycle Rights Management ES provides a solution for assigning and managing access rights and user permissions

Adobe LiveCycle Rights Mangement ES capabilities include the following:

Adobe LiveCycle Rights Management ES offers a multi-platform solution for dynamic, persistent, and robust document policy management

- **Persistent access management**—Adobe LiveCycle Rights Management ES provides all of the persistent document control features available with Adobe Acrobat. Security policies established on the server can include access rights and user permissions. Document authors simply select the appropriate policy stored on the server to be applied to an Adobe PDF document.
- **Dynamic security policy management**—Adobe LiveCycle Rights Management ES provides dynamic policy management so that organizations can manage document access and use after an Adobe PDF file has been published and distributed. Authors can update a security policy stored on the server to change any of the user permissions, add recipients, expire documents,

revoke previous recipients' access rights, and so forth. When a document recipient is offline, any changes are automatically applied to the document when the recipient contacts Adobe LiveCycle Rights Mangement ES again.

- **Network independence**—Whether used online or offline, inside or outside the network, the security policy applied to an Adobe PDF file remains.
- **Document auditing**—Authors can easily monitor use of protected Adobe PDF documents with Adobe LiveCycle Rights Management ES auditing capabilities. For each user permission assigned to a document, Adobe LiveCycle Rights Management ES software provides a detailed audit trail that keeps track of what each recipient did with the document, when, and how often.
- **Enterprise integration**—Adobe LiveCycle Rights Management ES software can be integrated with current user administration and content management technologies for cost-efficient, centralized document control administration. It can access existing LDAP and Active Directory implementations to check recipients' credentials, and it can maintain a security policy assigned to a document in a content management system and wherever the document travels.
- **Integration with Adobe LiveCycle products**—Adobe LiveCycle Rights Management ES software provides an Adobe Document Service that can be used by other Adobe LiveCycle ES server products to facilitate automated workflows. Organizations can expand use of cost-effective automated business processes with greater assurances that documents are more effectively protected and regulatory requirements for maintaining information privacy can be met.
- **Integration with Adobe Acrobat and Adobe Reader**—Authoring and viewing protected documents is simple and convenient. Authors can assign document control policies to documents with the same controls they use to create Adobe PDF files from popular applications such as Microsoft Word. Recipients can access Adobe LiveCycle Rights Management ES–controlled PDF files with the Adobe Reader Mac OS, Microsoft Windows, or Linux® client platforms.

Adobe LiveCycle Digital Signatures ES

Adobe LiveCycle Digital Signatures ES software enables organizations to bring more paper-based processes online by providing digital signature and encryption capabilities in a server environment, thus eliminating the need to manually open each file and add or verify digital signatures. With Adobe LiveCycle Digital Signatures ES, organizations can effciently integrate protected electronic documents with core systems and existing workflows. Adobe LiveCycle Digital Signatures ES software automates the processes of:

- Digitally signing and certifying Adobe PDF files
- Validating digital signatures applied to Adobe PDF files
- Encrypting and decrypting Adobe PDF files
- Integrating with a Hardware Security Module for added security capabilities and performance

Enterprises can process Adobe PDF documents with digital signatures from third-party vendors to enable large volumes of certified documents in batch (or bulk) on the server. Before a transaction is processed, Adobe LiveCycle Digital Signatures ES software opens the document and validates it based on signature status. This validation includes determining whether or not a document has been altered and whether or not it was really approved by the person who signed it. Since Adobe LiveCycle Digital Signatures ES software can validate any Adobe PDF file regardless of its use inside or outside the network, it enables organizations to extend automated processes beyond the firewall to include customers, partners, and constituents while meeting corporate and government regulations for protecting the privacy of electronic information.

For organizations that have deployed a PKI, Adobe LiveCycle Digital Signatures ES software provides encryption and decryption capabilities. Documents that are automatically generated can be automatically encrypted for distribution and encrypted documents that are submitted to

Adobe LiveCycle Digital Signatures ES can be automatically decrypted. These capabilities allow enterprises to leverage existing technology investments in PKI and smart card solutions to provide enhanced document protection. In addition, Adobe LiveCycle Digital Signatures ES software is the only solution that provides bulk digital signature capabilities for Adobe PDF files using HSMs.

Summary of Adobe document control implementation

The following table summarizes the Adobe document control capabilities and the technologies used:

Control Type	Control Mechanism	Technologies
Encryption	Symmetric algorithm	AES (128- and 256-bit) RC4 (128-bit) 3DES
	Asymmetric algorithm	RSA (up to 2048-bit)
Authorization	Document permissions (modifications and use)	No changes allowed Any changes except extracting pages Fill in form fields Comment and annotate Digitally sign Insert, delete, and rotate pages Copy text, images, and other content Enable text access for screen reader devices for the visually impaired No printing allowed Low-resolution printing only (150 dpi) High-resolution printing
	Dynamic document control	Modify permissions after publication and distribution Expire and revoke distributed documents Manage offline access Enforce content management system security policies outside system
Accountability	Auditing	Know how recipient has used document Know when usage occurred Know how often usage occurred

Summary of Adobe digital signature implemention

The following table summarizes the Adobe digital signature capabilities and the technologies used in their implementation:

Control Type	Control Mechanism	Technologies
Integrity	One-way hash	SHA-1 and SHA-256 algorithms MD5
	MAC/HMAC	HMAC support with symmetric keys and SHA-1
Authenticity	Digital signatures	May be applied to any Adobe PDF document Partnerships with leading digital signature vendors PKCS #1, #7, #11, and #12 RSA (512-, 1024-, and 2048-bit) DSA Long-term signature validation support Seed values (enforcement of certificate usage criteria) eXtensible Markup Language (XML) signatures MSCAPI support
	Certificate validity check	Certificate revocation list Online Certificate Status Protocol (future) Nation Institute of Standards and Technology (NIST) Public Key Interoperability Test Suite (PKITS) MSCAPI support
Non-repudiation	Supported with authentication and time-stamping	Adobe follows RFC 3161

Partner integrations

Adobe has partnered with leading global organizations to help provide an effective document security environment. Whether digital signatures requiring certificates, certificate authorities, smart cards, HSMs, or dynamic document control requiring authentication via LDAP providers, databases, or integration services, Adobe and its partners can solve specific business needs that require secure solutions. For more information about Adobe security partners, please visit: *http://partners.adobe.com/security.*

Conclusion

The use of sensitive and mission-critical information in electronic processes is essential for thousands of businesses and government agencies. Adobe security solutions leverage standards-based techniques for document control and digital signatures to provide effective solutions that enhance the privacy and confidentiality of electronic documents and forms.

With a comprehensive set of desktop- and server-based solutions, Adobe offers convenient, easy-to-use document security capabilities that encourage users to keep information private and help organizations meet the strictest regulations for sharing information electronically. Adobe security solutions enable organizations to replace paper-based business processes with electronic processes to reap the benefits of improved operational effciency, reduced costs, and increased customer and constituent satisfaction.

Appendix: Adobe standards and technology

AES—Advanced Encryption Standard is an encryption algorithm used by U.S. government agencies for securing sensitive but unclassified material.

Authentication Token—A small hardware device that the owner carries to authorize access to a network service. The device may be in the form of a smart card or may be embedded in a commonly used object such as a key fob. Security tokens provide an extra level of assurance through a method known as two-factor authentication. The user has a personal identification number that authorizes him or her as the owner of that particular device; the device then displays a number which uniquely identifies the user to the service, allowing the user to log in. The identification number for each user is changed frequently, usually every five minutes or so.

CA—A certificate authority is an authority in a network that issues and manages security credentials and PKI for message encryption and digital signatures. As part of a PKI, a CA checks with a registration authority (RA) to verify information provided by the requestor of a digital certificate. If the RA verifies the requestor's information, the CA can then issue a certificate.

CAPI/MSCAPI—Common Application Programming Interface is an international standard interface that applications can use to communicate directly with ISDN equipment. Using CAPI, an application program can be written to initiate and terminate phone calls in computers equipped for ISDN. MSCAPI is the Microsoft implementation.

Certificate (X.509)—A common certificate format used in PKI systems.

CP/CPS—A certificate policy and certification practice statement explain the practices employed by a CA to provide certification services including issuing, managing, revoking, and renewing certificates.

CRL (RFC 3280)—Certificate revocation list is one of two common methods (OCSP is the other) when using a PKI for maintaining access to servers in a network.

CSP—Cryptographic Service Provider

FIPS—Federal Information Processing Standards are a set of standards that describe document processing, provide standard algorithms for searching, and provide other information processing standards for use within government agencies.

Kerberos—Kerberos is a secure method for authenticating a request for a service in a computer network. Kerberos lets a user request an encrypted "ticket" from an authentication process that can then be used to request a particular service from a server. The user's password does not have to pass through the network.

LDAP—Lightweight Directory Access Protocol is a software protocol for enabling anyone to locate organizations, individuals, and other resources, such as files and devices, in a public or corporate network.

MAC/HMAC—A MAC provides a digital fingerprint of a file by means of a hash. In this case, a symmetric key is concatenated to the message and then hashed (HMAC). Without the key, an attacker cannot forge a new message.

MD5—An algorithm used to verify data integrity through the creation of a 128-bit message digest from data input (which may be a message of any length) that is claimed to be as unique to that specific data as a fingerprint is to a specific individual.

OCSP (RFC 2560)—Online Certificate Status Protocol is one of two common schemes (CRL is the other) for maintaining the security of a server and other network resources.

PKCS—Public-Key Cryptography Standards are a set of inter-vendor standard protocols for making secure information exchange on the Internet using a public key infrastructure. Adobe supports the following standards:

PKCS 1—RSA Cryptography standard

PKCS 7— Cryptographic message syntax standard

PKCS 11—Cryptographic token interface standard

PKCS 12—Personal information exchange syntax standard

RA—A registration authority is an authority that verifies user requests for a digital certificate and tells the CA to issue it. RAs are part of a PKI, a networked system that enables companies and users to exchange information and money safely and securely.

RC4—A shared key stream cipher algorithm that requires a secure exchange of a shared key outside the specification.

RSA—An asymmetric encryption and authentication system that uses an algorithm developed in 1977 by Ron Rivest, Adi Shamir, and Leonard Adleman. The RSA algorithm is a commonly used encryption and authentication algorithm and is included as part of the Web browsers from Microsoft and Netscape.

SAML—Security Assertion Markup Language is an XML standard that allows a user to log in once for affliated but separate Web sites. SAML is designed for business-to-business and business-to-consumer transactions.

SHA-1, SHA-256—Secure Hash Algorithm used to generate a condensed representation of a message called a message digest. The SHA-1 algorithm is required for use with the Digital Signature Algorithm (DSA) as specified in the Digital Signature Standard (DSS) and whenever a secure hash algorithm is required. Both the transmitter and intended receiver of a message in computing and verifying a digital signature use the SHA-1.

Smart Card—A plastic card about the size of a credit card with an embedded microchip that can be loaded with data and used for telephone calling, electronic cash payments, and other applications, and then periodically refreshed for additional use.

SSL/TLS—Secure Socket Layer/ Transport Layer Security. Internet protocols that ensure privacy between communicating applications and their users. When a server and client communicate, TLS ensures that no third party may eavesdrop or tamper with any message. TLS is the successor to the SSL.

Time-stamp Protocol (RFC 3161)—A time-stamping service supports assertions of proof that a datum existed before a particular time. RFC 3161 describes the format of a request sent to a time-stamping authority (TSA) and of the response that is returned. It also establishes several security-relevant requirements for TSA operation, with regards to processing requests to generate responses.

For more information

For more information about Adobe security solutions, please visit *www.adobe.com/security*

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

95009146 5/07