Electronic signatures: Solution scenarios for your IT environment

Table of contents

Introduction

Over the last decade, business processes have moved to the web at an astounding rate. Today, millions of people around the world are engaging in business-to-consumer (B2C), government-to-consumer (G2C), and business-to-business (B2B) processes over the Internet. Until recently, there was a lag in this trend due to the slow emergence of fully automated processes that enable electronic transactions to be signed or approved without traditional "wet" paper-based signatures. That obstacle has been removed with the electronic signature—a paperless way to sign a document using an electronic symbol or process that is attached or associated with a document. This automation of the "last mile" using electronic signatures is driving real business efficiencies, reducing the time it takes businesses, governments, and citizens to close sales orders, execute purchase orders, gain management approval, and apply for government programs.

The technology that enables electronic signatures provides a variety of benefits. It can validate the identity of a signer, verify the authenticity of a document, and enable nonrepudiation from a legal perspective. For transactions, electronic signatures can provide greater efficiency and speed turnaround times, eliminating costly printing requirements, reducing errors, and improving convenience for end users. Electronic signatures may also help support regulatory compliance and long-term document retention strategies. Many laws and regulations that attempt to address the efficacy of electronic signatures have been carefully worded to accommodate technology changes over time and offer flexibility based on the assurance-level requirements for a particular deployment.

This paper is primarily intended for a technical audience. However, line of business managers may find it useful to learn how electronic signatures can help improve business processes and expand engagement with key stakeholders. It outlines and prescribes a number of different scenarios based on the particular signing workflow, as well as the underlying technology and application. It also discusses Adobe's best-of-breed solutions for electronic signatures and how they map to each scenario. As a comprehensive guide for customers interested in choosing and deploying electronic signature technology, this white paper outlines a variety of deployment options and examines tradeoffs to assist in decision-making.

Adobe

Basic signature flow

Two primary requirements drive the deployment of electronic signatures:

- Assure all parties that documents are authentic and data has not been altered.
- Verify receipt and acceptance.

The first requirement is for institutions, governments, or enterprises that need to assure their constituents that forms or documents are authentic and have maintained their integrity. In this scenario, author signatures assure the recipient that the document is actually from the attributed signer (authentic) and that the contents have not been changed since the attributed signer executed the signature (document integrity).

The second requirement is for employees, customers, or citizens that need to provide approval or acknowledgement that a document or form has been read and approved or agreed to in principal. In this scenario, approval signatures assure the issuing organization that the recipient (the signee) has consumed the intended document with its intended format/contents and has approved or acknowledged its contents.

Electronic signature legality

"Assurance level," in the context of electronic signatures, is a term that helps answer the question, "How secure is this particular signature process?" The establishment of an assurance level for a particular signature type is helpful in determining whether or not a signature is likely to be considered legally admissible in court. To be entered into evidence in a trial, a signature needs to be assessed for admissibility, regardless of whether it's signed in ink or electronically. The following questions typically determine admissibility:

- Does the signature represent the intent of the signatory?
- Could the document have been altered?
- How certain is the identity of the signer?

In general, a higher assurance level signature offers stronger authentication, identity management, and integrity.

Authentication

Authentication provides information on how users verify themselves to a signing system. Do they simply click a button, or do they first have to enter a username and password? Authentication to a system is stronger if two factors are required—for instance, the user must present a physical device such as a token or smart card and enter a PIN or password into the system. Biometric data such as a fingerprint or iris scan can also be used as an authentication factor, as can LDAP data that defines user permissions and access controls at the server level.

Identity management

Identity management answers the question, "Why did the system trust this signer?" In other words, how did an organization or system grant signers their signing credentials or access to the signing system? Are signers asked to appear in person and present multiple forms of government ID, or are they simply required to enter their name and click OK? Another aspect of identity management is to consider the legitimacy of the user's signing credential or access to it at the time of signature. Even though a user may have used the proper methods for authentication, the signing credential could have been revoked before the time of signing due to user termination by an organization.

Integrity

An electronic signature often includes the capability to "fingerprint" or generate a hash value of a document so that a recipient can verify that a signed document was not changed post-signature. Integrity can be achieved in a number of ways, including use of a signed hash value or secure archival of original electronic documents combined with a strong audit trail of events that lead to the signature event itself.

Digital vs. e-signature technology

The term "electronic signature" encompasses all signature methods that include electronic components. Two main categories of electronic signatures have evolved based on the underlying technology: digital signatures and e-signatures.

Digital signatures require the use of public/private key cryptography as well as cryptographic keys to provide authenticity and integrity. The private key is retained securely by the user, while the public key is signed by a certificate authority and given an expiration date. This latter combination is known as a digital certificate or digital ID. A digitally signed record binds signers' identities to the documents they sign, and any change to the data can be detected. When a document is digitally signed, the user's private key encrypts the "fingerprint" or hash of the document, and the result is then attached to the document. The recipient validates the signature by decrypting the signature on the document using the signer's public key assuring only the private key of the signer was used to generate the signature and that the document hasn't been changed.

Keys and certificates for digital signatures are usually managed by a central certificate authority, which is responsible for issuing and verifying certificates and providing the certificate management system, including revocation as needed. A public key infrastructure (PKI) system also provides the directories that publish the certificates and their associated public keys. All of these elements need to be tied to corporate policies that drive the business requirements and standards around this process. The combination of policy and technology allows digital certificates to be used for authentication, signatures, approvals, and confidentiality in both open and closed systems.

E-signatures, on the other hand, do not usually require a PKI. The binding of a signer's identity to the data is accomplished in a different fashion, often with identity management and audit logs. The assurance level of e-signatures is typically less than a corresponding digital signature. Therefore, e-signatures should be used for lower-value signatures and approvals in closed systems, where records won't be leaving the system or be required to interoperate with other vendors' solutions.

This paper addresses solutions and use cases from Adobe in detail. However, it is important to distinguish the use of electronic signatures in Adobe® Acrobat® and Adobe Reader® software from that in Adobe LiveCycle® ES (Enterprise Suite) software. Customers typically deploy Adobe LiveCycle Digital Signatures ES software on the server for certifying outbound documents or validating inbound documents. Or, they may deploy Adobe LiveCycle Forms ES or LiveCycle Barcoded Forms ES software and rely on Acrobat and Reader on the desktop to collect and show signatures in a work flow.

Finding the right solution

An organization's business drivers and security requirements help determine the choice of an appropriate electronic signature method and technology. The following are some common questions to keep in mind when reviewing the scenarios described in the following section.

- Is there a need for author signing, reviewer signing, or both? For approval signatures, are you required to provide visual confirmation of "what you see is what you signed"? Or do you only need to capture the intent and forgo benefit of a document with a visually apparent signature?
- What is the value and/or sensitivity level of the documents to be signed? What level of assurance is required to prove the signature and/or signer are authentic?
- What levels and strength of identity management are needed? What type of user will need to interact with the identity management system—internal, external, general public?
- Are there particular industry standards, regulations, or legal/contractual constraints that need to be followed in your environment, such as SAFE-BioPharma for life sciences organizations?
- Is long-term retention and archiving a requirement?
- What is the budget for this implementation? Can you trade off assurance levels for lower cost?
- What services will the organization require to successfully deploy and use electronic signature processes and technology?

Use case scenarios

Use case scenario 1: Document publishing

Institutions and governments often must provide a digital version of their official documents to their customers or stakeholders. These documents include a certifying signature that assures recipients that a document or group of documents is authentic and unmodified. The certifying signature allows a publisher to control changes that are permitted to the document to enable form fill-in and review-and-approval workflows.

Customer use case: Government Printing Office

The Government Printing Office (GPO) supports crucial U.S. Federal Government operations, producing documents for legislative bodies such as the U.S. Congress and security agencies such as the U.S. Department of State. In its service to 130 federal departments and agencies, the GPO must assure that its documents are secure, allowing users to verify authenticity and notifying them if any changes have occurred to alter the state of a document. When readers are notified of potential tampering, the GPO can more easily take proactive steps to deter or prevent illegitimate or unauthorized use of the documents going forward.

After evaluating several options, the GPO implemented a solution based on Adobe LiveCycle Digital Signatures ES, LiveCycle Reader Extensions ES, and Acrobat Pro software to generate, authenticate, and disseminate documents electronically. Digital signatures on GPO documents are automatically validated with Acrobat and Reader version 7 and later on Mac OS and Windows® via the Certified Document Service (CDS) program. Find more information about CDS online at *http://www.adobe.com/security/partners_cds.html*.

The GPO's initiative to publish the Federal Budget electronically is estimated to save the government 20 tons of paper and save as much as US $1 million over five years. The Office of Management and Budget (OMB), emphasized the value of the E-Budget initiative in the following statement:

> *The visible digital signatures on online PDF documents serve the same purpose as handwritten signatures or traditional wax seals on printed documents. A digital signature, viewed through the GPO Seal of Authenticity, verifies document integrity and authenticity on GPO online Federal documents, at no cost to the customer.*

Use case scenario 2: Single and multiple approval processes

In this scenario, forms are typically routed to a participant for approval or for authorization of payments. Finally, the form is sent to the appropriate department for processing. Certifying the form before distributing for approval or data collection assures recipients that the form is authentic and was sent from the issuing organization. It also assures the issuing organization that they are receiving the same form that was originally sent.

This use case may also be used for digitally signed forms or documents that are typically routed through a multiperson approval process, such as a clinical trial or financial statement workflow in which constituents in a value chain sign off at each stage of a particular process.

Customer use case: Multinational bank

A large multinational bank was building a secure payment authorization application for digital cash management. Specifically, they needed a way for multiple bankers to apply approval signatures to a form that was customized to show a certain batch of transactions.

Secure payments authorization was a new product for the bank that was intended to drive top-line revenue and further its brand as a trusted provider of business services. The bank wanted to give customers the ability to electronically authorize payments rather than using a manual process, with a goal to enable greater B2C collaboration for bank customers.

The solution was ultimately developed and deployed by Adobe Consulting. It presents the client with electronic forms that initiate different bank transactions and allows the client to authorize those transactions with digital signatures. Once signed, the document is returned to the bank and stored in an electronic vault, where it may be used in the future as a nonrepudiable authorization of the payments captured therein. Adobe LiveCycle ES is used to provide a forms mechanism, digital signatures, and intelligent processing—all key capabilities in a comprehensive solution.

Implementation and technology scenarios

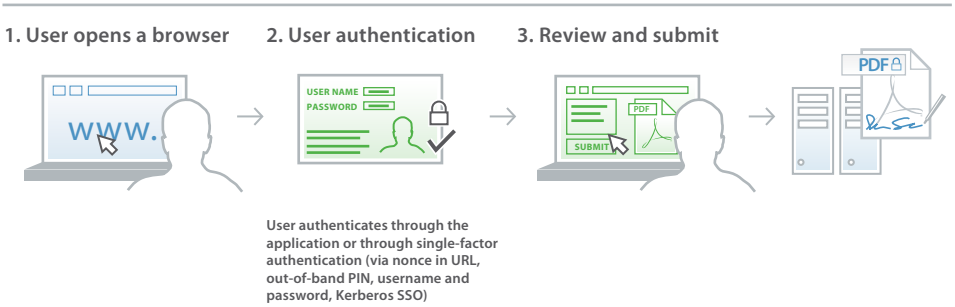
Scenario 1: Authenticate user and click to sign

Click-through electronic signatures are typically used as part of an internal workflow or with lower risk, external-facing transactions. This scenario may be attractive in situations where issuing individual digital identities to signers is not feasible. Even though nonrepudiation may still be an important requirement, usability concerns and low risk levels may drive a solution toward a reliance on authentication mechanisms or audit records rather than higher assurance user signature credentials.

A typical use case might involve deploying an employee timecard sign-off for Human Resources where the signature capture is embedded in a web application. In this scenario, the server simply applies a stamp acknowledging that the user has previously approved the document, before adding it to an audit log or moving it through a workflow.

Alternatively, click-through electronic signatures may be used in conjunction with simple authentication to sign off on documents in an environment with an existing identity management infrastructure. A typical use case might involve signing a PDF document during a new hire orientation process for an internal code of conduct training. Another example would be a signature process that applies a stamp to the document acknowledging that the user has approved and authenticated it using a simple LDAP username and password to seal the integrity of the document. This could be displayed as a visible field in which the stamp is the signature appearance or even an invisible signature on the document.

Scenario 1: Authenticate user and click to sign



Advantages—These signature solutions are easy to deploy and use, and they can cost less than alternatives, since no client PKI or significant client software is required. Authentication is typically intrinsic through the application. However, alternative authentication mechanisms may be supported. For users accessing portals with directory services, a username/password is often sufficient. For internal deployments, single sign-on (SSO) with Kerberos may be the preferred method.

Disadvantages—These solutions may be less secure because of lower assurance authentication mechanisms. They are heavily reliant on audit records, so may produce signatures with a relatively low level of portability. These systems often do not include built-in tamper-evidence mechanisms.

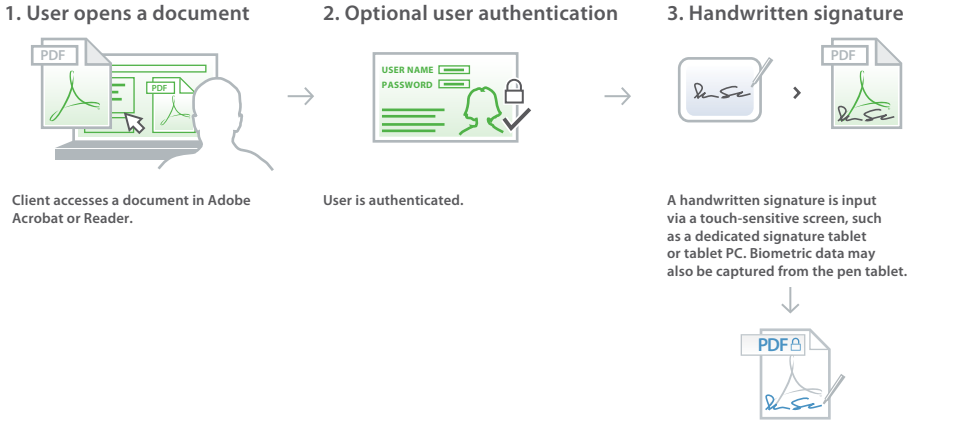
"Signed by Adobe" solution components—The forms to be filled out and signed come from LiveCycle Forms ES, and they are submitted back to LiveCycle ES for storage or further processing. Adobe LiveCycle Workflow and LiveCycle Workspace ES may also be used in these scenarios to create defined signature process workflows.

Scenario 2: Using a signature image or biometrics

These types of electronic signatures allow the signer to use an electronic stylus on a signing pad, add-on peripheral, or a tablet PC, so the written signature is transposed to the document. For additional security, a hybrid PKI deployment may be warranted.

Depending on security requirements, the solution can be extended by capturing the image as well as signature biometrics, such as the pressure and speed of the pen that may be used to later identify the signer. This solution requires a device-specific software plug-in, which inserts this metadata into the document at the time of signature.

Scenario 2: Using a signature image



Advantages—The solution may be used for both internal and external applications and may have stronger nonrepudiation elements when used with PKI and biometric options. This system is very easy for signers to use since the process is identical to that of the traditional "wet" signature.

Disadvantages—This solution requires a plug-in for Acrobat and Reader to enable tablet signatures, and the signing tablet itself must be purchased and maintained. The biometrics option requires an Acrobat or Reader plug-in for every signing participant.

"Signed by Adobe" solution components—A full solution from Adobe typically includes Acrobat or Reader and LiveCycle Reader Extensions ES. To enable signing in Reader, you must first generate a signature-enabled document using either Acrobat 8 Professional and later or LiveCycle Reader Extensions ES software. These components are typically deployed in conjunction with Adobe partners, who offer the signature pad, the signing plug-in, and optional PKI certificates for hybrid deployments. For a current list of Adobe security partners, visit the Adobe Security Partner Community online at *http://partners.adobe.com/security*.

Customer use case: Snap-on Credit

As a provider of financial services to Snap-on Incorporated, a leading global manufacturer and distributor of professional tools and equipment, Snap-on Credit, works with the company's national network of 3,500 franchisees to provide customers with financing for product purchases.

Traditionally, franchisees input data into a standalone system in their vans and print and sign the resulting forms by hand. The retail installment contract forms are then submitted to a franchisee's regional office. The regional office forwards—often at the expense of next-day delivery services—the contracts to Snap-on Credit's main office for processing.

Recognizing the power of digital technologies to automate application and contract processing, Snap-on Credit deployed a solution tightly integrated with the franchisee's point-of-sale system from Hatala Systems Group. The company decided to extend the capabilities of the point-of-sale system by adding an electronic signature component built around CIC's patented Sign-it technology and a Topaz Systems Inc. electronic signature pad. "Adobe PDF forms support for

electronic signatures and the ability to complete forms using free Reader software were integral to our decision to use Adobe solutions," explains Thomas Niman, director of business operations and systems integration at Snap-on Credit.

In less than six months, Snap-on Credit developed and introduced dynamic PDF contracts to franchisees. Franchisees simply enter information into a software application on their computers. Electronic signatures are applied to designated form fields using the Topaz electronic signature pad and CIC's Sign-it software. The process conducts a series of edit checks to help ensure the accuracy of the contract and compliance with any promotional financing terms offered.

Scenario 3: Desktop signing for digital signatures

This type of signature allows the signer to use PKI-based credentials, available either on external hardware tokens or as software installed directly on a client computer, to digitally sign an electronic document. When a user accesses a document in Acrobat or Reader, opening it and clicking the signature field, the solution presents the available credentials for signing.

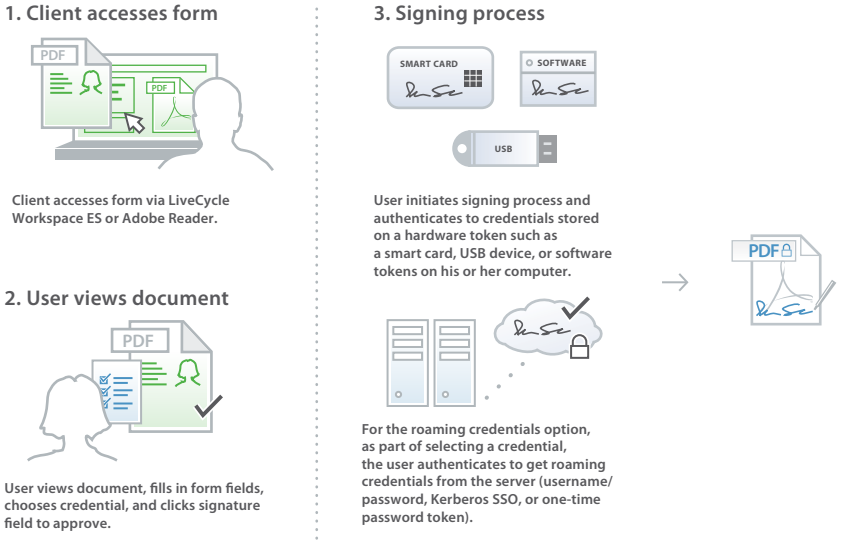
Alternatively, roaming credentials can be used to provide additional flexibility to sign without a hardware-based certificate such as a smart card or token. The signing keys are stored on a centralized, hardened server.

Hardware tokens are physical devices that authorized users possess to store cryptographic keys and to aid in authentication. They come in a variety of form factors and are typically small enough to be carried in a pocket or purse. In most cases, a PIN or password may be required for two-factor authentication. Users may also use software tokens stored on a computer, PDA, or mobile phone. Software tokens are considered weaker than hardware tokens, as they may be more easily compromised. However, logging on to a device to enable a software token is easy, and there is nothing physical to carry.

Roaming credentials are another option, either for users with multiple computers, who may have been issued separate sets of certificates and private keys on each computer, or those that need to log in and sign on as mobile users. Roaming credentials let users access their private key anywhere they can obtain Internet access. It is potentially easier to implement and manage, while still secure and transparent to users.

A typical use case might involve a doctor signing for a prescription while on the road. A roaming ID allows signers to simply authenticate to the credentials server using an existing login mechanism such as username/password, one-time password token, or Kerberos SSO, in order to sign a document. Once created, roaming ID–based signatures function exactly as hardware-based signatures do in Acrobat or Reader.

Scenario 3: Desktop signing for digital signatures



Advantages—With PKI-based trusted credentials, the level of assurance is typically higher than that of electronic signatures protected only by a password. Integrity of the documents is maintained via standards-based digital signatures, so there is potential for archiving within regulatory guidelines and better interoperability outside of an organization's borders. Therefore the solution is typically used for both internal and external applications.

Adobe products feature industry-leading support for PKI standards, FIPS-validated cryptographic modules, NIST test suite validation, and JITC/SAFE/IdenTrust certification, all of which combine to provide a powerful, dependable, and interoperable digital signature solution.

For the roaming credentials option, no client PKI or software is required on the desktop. Roaming credentials are generally easier to deploy than hardware or software PKI credentials because of the server-based architecture, central administration, and lack of tokens.

Disadvantages—There is often additional cost and complexity when implementing client-based PKI, though managed services can help reduce deployment and management burdens. For software tokens, the solution is somewhat less secure than hardware tokens due to keys being resident on the client computer. For the roaming credentials option, users must be online to sign, and additional server infrastructure and IT resources are required.

Regulatory considerations—PKI solutions like SAFE-BioPharma can help provide high assurance and compliance with regulations (such as the FDA's 21 CFR Part 11).

"Signed by Adobe" solution components—A typical solution includes Acrobat, Reader, and/or LiveCycle ES products such as Adobe LiveCycle Forms ES, LiveCycle Digital Signatures ES, LiveCycle Reader Extensions ES, and LiveCycle Process Managment ES. A complete solution is typically deployed in conjunction with Adobe partners that provide identity management and PKI. Note that to enable signing in Reader, you must use Acrobat 8 Professional or LiveCycle Reader Extensions ES software to create and enable the document for signing. For the roaming credentials option, a complete solution is typically deployed in conjunction with Adobe partners. For a current list of Adobe security partners, visit the Adobe Security Partner Community online at *http://partners.adobe.com/security*.

Customer use case: The Government of Belgium

Belgium is one of the first countries to institute an electronic identification (e-ID) card initiative for citizens, although governments worldwide are considering similar initiatives. In 2009, all Belgian citizens over 12 years old will be required to carry an e-ID containing a digital certificate, making this the country's largest e-government initiative.

The e-ID enables the government to move from costly, error-prone workflows for processing citizen paperwork to digital transactions. Of utmost importance to the initiative's success is ensuring that digital information submitted by citizens remains secure from submittal through processing. They also needed to enable citizens to use nonproprietary, freely available software to complete, sign, and submit personal information.

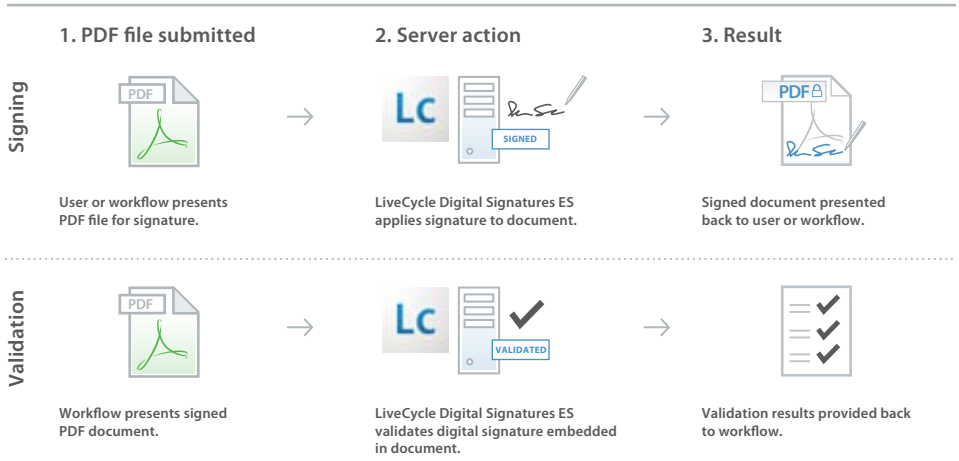
Belgium decided to use Adobe LiveCycle ES solutions to help ensure that digital information submitted by citizens to the government remains secure. Through this implementation, they were able to reduce reliance on paper processes, expand citizen and business access to government services, and reduce government operating costs.

Scenario 4: Simple server signing

A simple server signing scenario uses LiveCycle Digital Signatures ES and server-side certificates from a third party to sign a PDF document. The end user may submit the signed document manually or through a specified workflow. Once it is submitted, the LiveCycle server uses these certificates to apply a signature (commonly a certification signature) to the document. The server then presents the user with a signed PDF file.

Another scenario might involve an organization which receives dozens to perhaps thousands of signed PDF documents. LiveCycle Digital Signatures ES can be inserted into a workflow to validate documents in bulk and then route the valid documents to the next step in the workflow.

Scenario 4: Simple server signing



Customer use case: Penn State University

The registrar's office at Penn State University receives more than 120,000 transcript requests a year. Requests come in by mail, by fax, or through a web portal submission system. Approximately 25% of the requests are urgent, with alumni needing transcripts sent by overnight mail for a job interview or to meet a graduate school application deadline.

Penn State officials were also concerned about an ongoing issue: the proliferation of fake diplomas and falsified transcripts worldwide. Annual sales of false documents are estimated at more than US $100 million worldwide. The falsified transcripts have become so advanced that they include watermarks, metallic strips, and other identifiers that make it more difficult for organizations to verify the authenticity of Penn State documents and transcripts.

To fend off these growing concerns, Penn State decided to implement a certified electronic transcript solution using Adobe LiveCycle products. Penn State students and alumni can log on to the school's extranet using their assigned passwords to order these transcripts and enter the mailing or e-mail addresses of the people to receive the transcripts. The system pulls student information from the school's mainframe applications and places it in the transcript template. LiveCycle Forms ES then automatically generates a transcript in Adobe PDF, which in turn is certified by LiveCycle Digital Signatures ES using a high-assurance GeoTrust CDS digital credential stored on a hardened SafeNet Hardware Security Module (HSM).

The final secured electronic transcript is placed on an FTP server for downloading by specified recipients. As transcripts are downloaded, the student or alumnus making the request is notified by email.

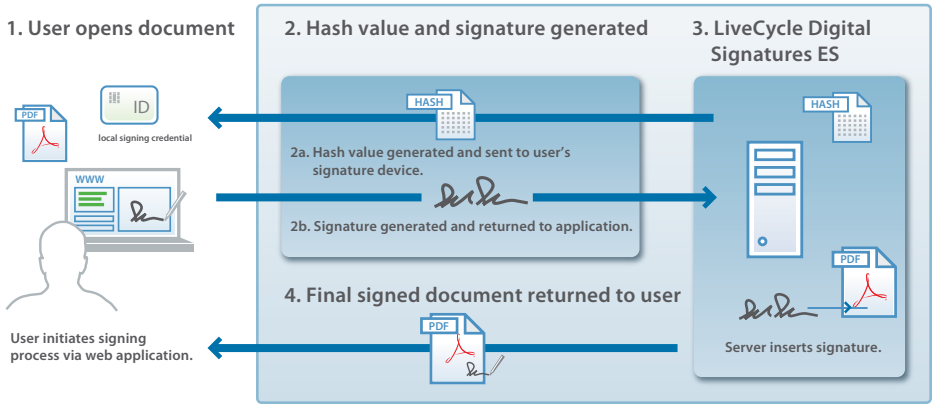
"This process addresses many important steps," says James Wager, assistant vice president for student enrollment. "We know the PDF files are secure and authenticated and that recipients can easily open the files using free Adobe Reader software. At the same time, built-in tracking and notification in our web portal eliminate questions about when transcripts were sent and if they were received. It's a terrific solution."

When recipients open a certified PDF transcript in either Adobe Reader or Acrobat, the certification signature is automatically validated and trusted. This assures any recipient that the transcript came from Penn State and that its contents have not been changed.

Scenario 5: Server signing using local credentials

This type of digital signature implementation allows the signer to log on to a web user interface and sign documents using a local PKI credential. In this scenario, users can "bulk sign" a batch of documents or sign a document from within a web portal rather than in Acrobat or Reader. The web user interface simply presents a list of documents that the user needs to approve. Specifically, users can view the document in Reader but then can sign the document by clicking a button in the web user interface, which brokers the signing to the client. In the background, the server creates a hash value and sends it to the signer's computer via an ActiveX or Java™ applet. The hash value is then signed using the user's private key and sent back to the server to be embedded in the document. This scenario can be implemented using either hardware or software tokens on the client.

Scenario 5: Server signing using local credentials



Advantages—The solution offers central configuration at the server, so there are no issues or dependencies on Reader versions or configurations. Reader 7 and later software can validate signatures automatically in scenarios where the documents were signed by the server. Another advantage of server signing is that it can easily integrate with existing core business processes to sign as part of a bulk workflow.

Disadvantages—The system is initially more expensive and may be less flexible and provide lower assurance because documents are being viewed in a browser or list when they are signed.

Regulatory considerations—PKI solutions such as SAFE can help provide assurance and compliance with regulations like the FDA's 21 CFR Part 11. SAFE-BioPharma is the nonprofit association that created and manages the SAFE-BioPharma digital identity and signature standard for the pharmaceutical and healthcare industries.

"Signed by Adobe" solution components—A full solution from Adobe typically includes LiveCycle Digital Signatures ES and may include LiveCycle PDF Generator ES and LiveCycle Process Management ES software. A complete solution is typically deployed in conjunction with Adobe's ecosystem of partners to provide identity management and PKI. For a current list of Adobe security partners, visit the Adobe Security Partner Community online at *http://partners.adobe.com/security.*

Customer use case: Procter & Gamble

Procter & Gamble (P&G) has one of the strongest portfolios of brands, including a variety of prescription and over-the-counter medicines. The company develops many of these treatments in partnership with outside drug research specialists. The process of discovering new medical treatments involves a constant exchange of information among clinicians, researchers, quality control staff, marketing specialists, and dozens of other internal staff and external partners. In addition, P&G works closely with government regulators to ensure that products meet stringent safety and efficacy criteria.

A primary challenge is, of course, that only a small percentage of treatments ever make it to market, making it essential that everyone involved in product development can quickly and efficiently create and review research and development information. As a result, many biopharmaceutical companies seek to automate manual processes involving paper.

P&G uses Adobe solutions as part of its eLab Notebook program to streamline the creation, management, review, approval, and signing of a large volume of research and development information. After data is collected and Adobe PDF files are sent for review, recipients who need to sign the file can do so digitally using LiveCycle ES. The eLab Notebook solution uses LiveCycle Digital Signatures ES to apply the signatures to research documents that are compliant with the SAFE-BioPharma standard. The automated system also helps support regulatory compliance through the use of digital signatures that comply with the SAFE-BioPharma standard.

An initial study of anticipated savings from the eLab Notebook initiative estimates an overall productivity gain of 5%. However, actual productivity realized by the solution for some early adopters is approximately 10%, translating to as much as four hours per week of time for each researcher. This savings—combined with a projected 7% productivity gain due to the ability to more easily and reliably reuse knowledge across experiments—adds up to millions of dollars in savings per year for the company.

Summary

Different electronic signature technologies can solve a variety of use cases across industries. The following table highlights the inherent tradeoffs to each approach. In general, the higher the level of assurance required, the higher the total cost of ownership of the solution. Many options are available through Adobe and its partners, and we can help you map the appropriate solution to your set of challenges. The right combination of technologies can help your organization unlock the value of an electronic signature solution and begin to realize the tremendous benefits of closing the loop on online business processes. This is not a market where one size fits all. Adobe recognizes the need to deliver a portfolio of best-of-breed technologies that include the right mix of cost, assurance, and overall risk management to meet corporate objectives. No other vendor can provide the depth and breadth of solutions that organizations require, based on a proven, ubiquitous set of core technologies that companies of all sizes in all geographies have come to trust.

Electronic and digital signature methodologies comparison

Technology scenario	Assurance level provided	End-user provision of digital identities required	Desktop hardware required	Server required	Server database required
Electronic signatures—click to sign	Low to medium	No	No	Yes	Yes
Electronic signatures—signature image	Medium	No	Yes	No	No
Digital signatures—desktop signing	Medium to high	Yes	Maybe*	No	No
Digital signatures—server signing	Medium	No	No	Yes	Yes†

* Hardware is required for smart cards, not for software IDs or USB tokens.

† Digital identities must be server managed.

Adobe

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

95011606 10/08