Adobe® LiveCycle®
Digital Signatures ES

Best practices to streamline your business

The last mile problem

As organizations have moved to all-electronic processes and are focused on building customer loyalty with a compelling web presence, there is still one aspect of business that remains on paper. Approvals and sign-offs continue to rely on handwritten signatures on paper, whether it is a business-to-consumer (B2C), government-to-consumer, or business-to-business (B2B) process. Thus, signature collection activity has earned the unenviable position of being the last component that must be completed to enable a process to be truly automated and online.

In the physical world, agreements are executed with a wet ink signature. The relying party has often built appropriate trust relationships and chain of custody in the business process over a period of time. In today’s economy with global reach, businesses are focused on improving efficiencies. That includes executing sales faster, closing purchase orders quickly, and getting management approval on the latest project with the click of a button. The process of printing and faxing; signing, scanning, and e-mailing; or printing, signing, and mailing documents has a number of weak links when time is a precious commodity. How do you know the contract sign-off in Bora-Bora is really being executed by an authentic party?

Digital signatures have several advantages over wet ink signatures:

- An independent third party asserts the authenticity of the signer, so you know the contract agent has been vetted by the registration authority.
- Documents are authentic.
- Digital signatures provide assistance in nonrepudiation to combat the pesky “Not I” syndrome.
- Digital signatures help close deals faster by offering quick turnaround on contracts, applications, purchase orders, and sales orders.
- Digital signatures eliminate printing by keeping transactions and documents completely online.

Compliance

In the United States, the Gramm-Leach Bliley Act (GLBA), Health Insurance Portability and Accountability Act (HIPAA), and Sarbanes-Oxley (SOX) have given corporations a reason to rethink their long-term record retention strategies. By storing all documents and transactions online with digital signatures when required, these corporations can improve their compliance score on yearly audits and lower the cost of compliance going forward. Archiving and finding information on particular subjects is greatly simplified when records are electronic, and electronic records speed searches and take up less physical space. Signing relevant contracts and documentation digitally provides additional evidence that is usually expected by good corporate governance principles.
As you might expect, the higher assurance does come at a cost: the cost of establishing the organizational policy and infrastructure surrounding digital signatures and the cost of enabling signers and relying parties to digitally sign documents.

With return on investment (ROI) as the key driver, organizations must naturally look for synergies in their identity management practices that enable business workflows for authentication and single-sign-on purposes as well as for document signing. Enterprises that use best practices have found positive ROI results from their projects.

The legal and regulatory environment

Electronic signatures and digital signatures

There are several international, national, and local directives in place that provide businesses with the much-needed assurance that an electronically signed document has the same level of admissibility as legal evidence. Electronic signatures are a broader concept than digital signatures and include artifacts as diverse as a digitized image of a wet ink signature and even e-mail headers. Digital signatures, on the other hand, are based on the well-known public key cryptography principles.

A click-through agreement on a portal could be considered an electronic signature, as long as the authenticity of the signer can be proven with appropriate audit logs and the document integrity is maintained. Naturally, this experience can be moved up the assurance scale either by hooking up a signature pad to the signer’s application and providing the ceremony and the cryptographic protection (optionally) or by using a digital ID stored on a token or Smart card that is hooked up to the device or application used for signing.

Not all signatures are equal

All signatures are not created equal. At the lowest end is what the market today calls the click-through signature, which is what we are subject to when installing new software on a computer in the form of an End-User License Agreement (EULA). Users are forced to scroll down to indicate that they read the material and then proceed after performing an action such as clicking a checkbox.

This strategy works well if the problem being addressed is to record a sale. This operation tries to establish the context that the user was actively engaged in the installation process. However, there is no active identity management of the user other than linking the user to a license activation code, a credit card number, or some other attribute. Establishing nonrepudiation is a matter of establishing the activity with the help of several external systems. This is a classic electronic signature model.

The next level in establishing a truly electronic process is a business process model that hinges on a re-authentication of the approver. This type of process involves preserving the audit logs of the authentication to serve as nonrepudiation evidence for the approval or rejection of a transaction.
For example, consider a scenario in which a supervisor needs to review the quality level of a batch of drugs in an application. Once she has reviewed it, she can approve or reject the batch based on quality control tests. Instead of deploying a digital signature solution, this company may determine that the act of accepting or rejecting batches of drugs is more valuable to the business case. Hence, a re-authentication of the supervisor’s credentials (which could be as simple as entering a PIN or password) might be a sufficient risk mitigation strategy. Such a deployment may be justified if the value of the asset, as determined by the need to meet the regulatory and compliance requirements, proves to be lower than the cost of deploying a high-assurance solution. This is an electronic signature solution. It is slightly more secure than the click-through method if strong identity management practices are used to provision users into this system. The LiveCycle Platform provides a strong foundation to build a system that meets these electronic signature requirements. Capabilities such as identifying and authenticating users and logging their actions on documents routed for their approval are native in LiveCycle ES.

Some deployment models are hybrid in nature. For instance, an account opening process in a bank typically involves capturing reference signatures of the account holders. This then involves an in-person activity where the account holder actually signs on an electronic signature pad. Adobe partner and vendor products are available to provide strong cryptography, adding to the integrity and authenticity of the digitized image of the signature captured by the electronic pad. Processes in certain industries, such as life sciences and financial services, require long-term retention of data and documents—some for 20 years or more. In those situations, as the business redesigns its long-term storage and record-retention policy, the legal aspects of preserving the document authenticity and chain of custody become important. LiveCycle ES Update 1 provides new capabilities in content management. LiveCycle Designer ES together with the functionality in LiveCycle Content Services ES can deliver the foundation for the hybrid model.

Electronic signatures unleash their full potential when orchestrating several of the services offered by the LiveCycle Platform. Digital signatures in particular provide the high assurance of authenticity and integrity that is required in some customer workflows. Adobe Acrobat, Adobe Reader, and LiveCycle Digital Signatures ES also address questions that surround long-term preservation of signatures when crypto–based digital signatures are used for signing.

Frequently cited regulations
The U.S. Electronic Signatures in Global and National Commerce (or ESIGN) Act was passed in 2000 (www.ftc.gov/os/2001/06/esign7.htm) and provides the basis of giving electronic signatures the same legal effect as a handwritten signature. It provides the necessary foundation for building the legal framework for legal admissibility of electronically signed documents. The American Bar Association has provided guidance on the technology and legal aspects of this topic at www.abanet.org/scitech/ec/isc/dsg-tutorial.html.

The U.S. Food and Drug Administration regulation 21 CFR Part 11 (www.fda.gov/cder/guidance/5667fnl.htm) provides a broad guidance for scope and application of electronic signatures in electronic records. It covers a wide technology range, including password-based authentication as a form of electronic signature at one end and Smart card–based digital signatures at the other end. The spirit of the regulation ensures authenticity and integrity of the quality assurance process and other life science processes surrounding not only drug trials and submissions but also access to patient and participant records and so forth. An approval or rejection of a transaction is considered an electronic signature. Heavy emphasis is placed on the security and audit measures for the systems and processes surrounding the capture of the electronic signature. Thus, audit trails capturing the signature or approval event add sophistication for a signature-based workflow.

Signatures and Authentication for Everyone (SAFE) is a bio-pharma association (www.safe-biopharma.org) focused on developing technology standards that meet their industry requirements. Adobe products, including Adobe Reader, Adobe Acrobat, and Adobe LiveCycle Digital Signatures ES, are SAFE-certified products. You can obtain more information on this topic at www.adobe.com/lifesciences/safe.html.
The European Commission in 1999 first provided the much needed regulatory framework for accepting electronic signatures as legally equivalent to handwritten signatures in the form of Directive 1999/93/EC (http://portal.etsi.org/esi/Documents/e-sign-directive.pdf). This directive recognizes three classes of signatures:

- General electronic
- Qualified electronic
- Enhanced electronic

Although all of them are equally enforceable and cannot be denied legal effect, the qualified and enhanced electronic signatures offer higher assurances of security at the operational level. Several standard organizations in Europe have published both the legal and business overview of the directive as well as the technical guidance on this subject. More information is available at www.ict.etsi.org/EESSI_home.htm.

**Streamlining business processes**

**SOA and PKI**

Service Oriented Architecture (SOA) has been endorsed by businesses because it provides the ability to add on incremental process improvements and extensions while limiting the exposure of these new investments. Adobe LiveCycle ES (Enterprise Suite) is an SOA platform for customer engagement applications that include electronic documents and process management to automate workflows involving documents (see Figure 2). The Digital Signatures service can be added easily to new or existing LiveCycle ES based applications to conquer the last mile problem in going truly electronic.

LiveCycle Digital Signatures ES enables users to:

- Publish certified documents that can prove the authenticity and integrity of the document
- Control the changes that are permitted in documents as they flow through a business process with a certification signature
- Validate signatures on documents before moving to a document management system

Aside from the direct tangible benefits of investing in LiveCycle Digital Signatures ES, businesses can also extend the ROI on existing investments in public key infrastructure (PKI) and associated key management hardware.
Certified documents

A certifying signature is a digital signature in every sense of the term. It provides both document authenticity and integrity just as an approver signature provides. Two key attributes distinguish it from the regular approval signature:

- It has to be the first signature on the form or document.
- By virtue of it being the first signature, the signer can control the changes that are permitted to the document throughout the business process.

Typically, a certifying signature is placed by the form designer or publisher to indicate the origin of the form to the relying communities. There are three permission modes that are associated with the certifying signature:

- No changes are permitted which could be used for press releases, government policy statements, and so on.
- Form fill-in and signatures are permitted—such as in the case of a purchase orders, in which you fill in the order details and sign it.
- Form fill-in, signatures, and annotations are permitted—which can be used by notaries certifying signatures. In addition to signing, notaries may also choose to add a comment regarding their attestation.

Visible or invisible certification

LiveCycle Digital Signatures ES, much like Acrobat and Reader Extensions can place a visual representation of the certification on forms or keep the certification invisible. In both cases, the relying party sees a blue certification ribbon in the document message bar if the certifying signature is valid.

Figure 3 is an example of a visible certifying signature where there is enough space in the document to hold the signature. An invisible signature is not visible on the document itself, but users can inspect its properties in the signature panel of Adobe Reader or Acrobat.

When an invisible signature is applied, there is no visible signature block in the document or the form itself that represents the certification. The signature panel of Adobe Reader or Acrobat provides access to the signature properties.

With LiveCycle Digital Signatures ES, Adobe recommends applying invisible certifying signatures. Visible certifying signatures require the ability to save a snapshot of the document, and they are not currently supported for dynamic XML Forms Architecture (XFA) forms.
Document signatory control
Business processes are dynamic, and the flow of the document is controlled by the application logic or, if applicable, the rules engine responses to the current state and events in the business. If a clinical trial quality control submission must be approved by five independent signatories, the signatory (or approver) attributes should be set dynamically when each individual signs. This eliminates costly mistakes in hard coding signatories to signature blocks and enables businesses to control the signatories by their role instead of by their name.

Traditionally, these signature properties are controlled by what Adobe technology calls seed values. LiveCycle Designer enables a form or document template author to define these settings when the document is created. It can also be useful to define some broad principles such as using a specific issuing certificate authority (CA) or a certain class of certificates with a specific policy Object Identifier (OID). At runtime, as application logic or the business rules engine dictates, LiveCycle Digital Signatures ES is able to set further attributes such as a requirement that only one of three known members can sign. These specific member certificates are associated with the signature field validation.

Tip: LiveCycle ES Service Pack 1 enables you to set these attributes to existing signature fields instead of only when adding new signature fields.

This capability is typically used when an enterprise wishes to dynamically control the number of signatories and the signer in operations such as Standard Operating Procedure (SOP) controls or a complex business contract with several internal approvers.

Long-term preservation of signatures
One of the key competitive advantages of Adobe signature solutions is that it allows the signer to embed the revocation information at the time of signing. This capability alone enables the relying party to validate the signature long after the signer certificate has expired or been revoked.

Tip: The Sign and Certify operations in LiveCycle Workbench enable the process designer to set the process property of Embedding the Revocation Information at the time of signing. Be sure to check this setting when designing the process.

Certificate lifecycle management is complex, and the risk involved in accepting digital signatures is two-fold:

- Ensuring that the signer is authentic and his private key has not been compromised at the time of signing
- Treating documents that are signed at a future date when the signer’s certificate has expired or been revoked due to a compromise

The risk in the first issue can be managed by ensuring that the private key is issued using secure vetting and by using enrollment processes provided by the PKI infrastructure that LiveCycle Digital Signatures ES and Adobe Reader and Acrobat rely on.

The second issue can be minimized (and nearly eliminated) by allowing the relying party to inspect the document validity when signing it.

Validating signatures
In this scenario, the LiveCycle Digital Signatures ES service acts as the gatekeeper of all in-bound documents headed to the document management system. Before the documents are saved and linked to other intellectual property within the enterprise, LiveCycle Digital Signatures ES validation services are used to capture the validity of these documents.

LiveCycle ES Service Pack 1 provides the ability to list revocation information and other verbose information on signature validity of signatures. If long-term record retention and meeting compliance directives are critical, a static PDF file should be generated (flatten the form to a document such that there is no interactivity) and the signature validity details should be appended to the document before archiving. (Note that the term archiving does not refer to the PDF/A standard.)
LiveCycle Digital Signatures ES can verify both certifying and approval signatures that are applied individually or on the desktop. Furthermore, on the desktop the signature could have been applied using the default signature handler in Adobe Acrobat or Adobe Reader or by using third-party plug-ins. (Note that third-party plug-ins must be implemented in accordance with the signature specifications defined in the PDF reference.)

Tip: LiveCycle Digital Signatures ES can also be used to validate XML data signatures that may have been applied to form data (authored via LiveCycle Designer ES) during form submission.

**Use case scenarios**

There are a few basic patterns of document workflows that include digital signature–based approvals.

**Internal form approval workflow**

LiveCycle ES services are used to build a form dynamically on the server. This form is subsequently routed via LiveCycle Workspace ES to enable form fill-in or digital signature–based approvals. This workflow relies on the digital signature capability that is available in Adobe Reader. These forms can be static or dynamic XML forms. Note that LiveCycle Workspace ES cannot route documents.

This scenario is best suited for an internal approval workflow that requires approval from one or more employees. Employees are expected to log into LiveCycle Workspace ES to track their Task List and complete their document approval tasks.

This scenario uses the client–side digital signature services (Adobe Reader signature capabilities). It is important to note the new Adobe Reader 9 signature usability and validation changes.

A nuance in this workflow is distributing a form that has a certifying signature. The certifying signature is applied by LiveCycle Digital Signatures ES. In this workflow, LiveCycle Digital Signatures ES is a component of the solution deployed.

**Certified form workflow**

A government-to-citizen service for renewing drivers’ licenses or a B2C transaction that includes a funds transfer require proof for the applicant or customer that the form is authentic and has not been tampered with. The form available on the website must be a certified form. That certification is performed on the LiveCycle Platform when the recipient downloads the form or when the system sends the recipient the form via e-mail. Recipients must fill in data and apply their signature before returning the form to the business or agency. The form can be submitted to a website or e-mailed back to a specific contact after the signature is captured in Adobe Reader.

**Step 1: Authoring in LiveCycle Designer ES**

The form author uses LiveCycle Designer ES to lay out the form and create an XFA or XML Data Package (XDP) file to persist the template. By default LiveCycle Designer 8.0.1 or later saves the form as a dynamic PDF file that is compatible with 8.0.1 or later.

Tip: To enable a form to be signed or certified, that form must be rendered to PDF on the server or client. If the form is always being generated on the fly with data and is completely dynamic, it conflicts with the “what you see is what you sign” and “what you signed is what you saw” principles that are the core tenets of a corner-to-corner digital signature. This is quite different from the expectation surrounding a data signature in which the data alone is being signed—not the visual representation of the form.

Tip: For performance reasons, scripts should not be used if XFA constructs are available. For example, if users are creating a table that enumerates the data on a page, they should create a sub-form and associate data with it. Any post-signing scripts that change the form data should be avoided because they cause the form state to change from being a non-shell to a shell PDF file. Post-sign validation scripts might result in changes in the document, which change the signature status. Also note that signature fields should be ideally created beforehand for a dynamic form. Adding a signature field dynamically to a signed document could impact the size of the document.
Step 2: Activities on LiveCycle Workbench ES and administration

The following are activities and administration tasks that are performed on LiveCycle Workbench ES:

- Using the XDP template: In this case, the XDP template must be merged with data using the LiveCycle Forms ES render service. Non-shell (PDF-rendered) documents should be created for signing.
  Tip: Use LiveCycle Designer 8.0 or later and save the file as a 7.0-compatible dynamic form.
- Certify: For certification, the credential must be added in Trust Store. The credential can be stored either in a Hardware Security Module (HSM) such as SafeNet Luna SA or nCipher nShield or in the LiveCycle ES Trust Store component. In the latter case, the private key is in the LiveCycle ES database. Certification method in Workbench is present under Processes > Digital Signatures > Signatures: 1.0 > Certify PDF. Adobe recommends using invisible certification, if possible. LiveCycle Digital Signatures ES enables invisible certifying signatures to be placed in a static form or document.
- Extend Adobe Reader: This is the task of enabling certain features such as form fill-in and signing in Adobe Reader. The document must be certified before features such as form fill-in and signing can be enabled for Adobe Reader because Adobe PDF only recognizes the first signature as a certification signature. The process of enabling a form for Adobe Reader is actually just creating a digital signature that is similar to a code signing signature. The document or form can now be sent to the next signer or approver through e-mail, a watched folder, or a task in LiveCycle Workspace ES.

Step 3: User signing in Adobe Reader

The user fills in the data and signs the form or document. Adobe recommends that no unsigned changes should be added after signing. Any unsigned changes have the potential to invalidate the signature or convert the form from non-shell to shell, thereby disabling the LiveCycle Digital Signatures ES service capabilities.

The user submits the form using the Submit button (in LiveCycle Workspace ES), e-mail, or a watched folder.

Changing a form workflow

How do you determine the number of signatories and route forms appropriately?

An easy extension of the internal form approval workflow is: What if the business rules determine that there must be more approvers than the form was originally designed for?

Tip: A best practice is to design the form with the maximum number of signatories that could be possible. You can then activate them from their hibernating state as the business rules dictate.

Modify Signature Field API, which can modify the seed value and field locking rules of a signature field, must be used. This API is available in LiveCycle ES Service Pack 1 in LiveCycle Workbench ES under Processes > Digital Signatures > Signatures: 1.1 > Modify Signature Field.

LiveCycle Digital Signatures ES is used to validate approval signatures placed by individuals to whom the form was routed (either via LiveCycle Workspace ES or any ad-hoc manner such as e-mail).

Validating digital signatures

A G2C or B2B application that receives signed applications or form submissions might have a reason to validate the signatures on these forms.

LiveCycle Digital Signatures ES provides an API getSignatureStatus() that returns one of the following validity states: VALIDANDUNMODIFIED, VALIDANDMODIFIED, INVALID, or UNKNOWN.

The signature status verifies two elements—signer validity and document integrity. If the signer validity is undeterminable or invalid, the document integrity information is not provided.
Tip: When validating digital signatures on the server, it is important that field locking rules associated with digital signatures in the form are enforced and any violation produces an invalid signature. Adobe recommends using LiveCycle Digital Signatures ES to validate signatures on AcroForms and XML forms that do not have any field locking capability designed into them.

LiveCycle Digital Signatures ES applies a notary-like signature, which is another approval signature attesting to the fact that the service validated the inbound signatures on the form or document.

Stamping inbound forms
There are business processes that require an inbound form or application to be stamped on arrival. In this case, a signature service to apply a signature that indicates receipt of an application or a counter signature after having validated incoming signatures might use of LiveCycle Digital Signatures ES capabilities.

Tip: LiveCycle Digital Signatures ES can sign AcroForms and static XML documents, but it cannot sign dynamic XML forms.

To design forms to enable LiveCycle Digital Signatures ES workflows, Adobe recommends using static XML forms.

Ensure you have a static XML form
In general, there are two ways that you may have prepared your form for use in Acrobat or Reader: You may have saved it as a PDF file from Designer and opened it in Acrobat or Reader, or you may have saved it as an XDP file from Designer and rendered it on the server using LiveCycle Forms ES before opening it in Acrobat or Reader.

Saving a PDF file from Designer
When you author a form in LiveCycle Designer ES, there are different save options: XML Form (XDP), Adobe Static PDF Form, and Dynamic PDF Form.

1. Save the form as an Adobe Static PDF Form.
2. Choose File > Form Properties > Defaults Tab, and select Override Default Rendering. Then select Acrobat 8.0 (Static) PDF Form. This prevents LiveCycle Forms ES from generating a dynamic XML form by default for your form template authored in Designer.

Using an XDP file
Some business processes merge data from a data source into an XML template to render forms in Adobe Reader. This is accomplished by saving an XDP file from Designer ES and using LiveCycle Forms ES to render the XDP file as a form that can be opened in Acrobat or Reader. The XDP file itself has no notion of being static or dynamic. Instead, this is enforced at the time of rendering on the server by LiveCycle Forms ES. The following steps ensure that the process is operating on a static XML form:

1. Pass the XDP file and any XML data you wish to merge as input to the LiveCycle Forms ES renderPDFForm operation with all the default settings.
2. Change the Render At Client setting to No. This means that the server must always generate a permanent PDF rendition within the form, thus making it a static XML form.

Now the output from LiveCycle Forms ES will be suitable to use for the full range of functionality used by LiveCycle Digital Signatures ES.
Validating signatures on electronically submitted documents
You need a business process to validate all signatures in electronically submitted documents, such as registration forms submitted to the Chamber of Commerce.

Verification of both certified and recipient signatures is possible. As mentioned earlier, post-signing changes should not be done.

The verify method in Workbench is present under Processes > Digital Signatures > Signatures: 1.0 > Verify PDF Signature.

The verification information may be used in further processing.

**LiveCycle Digital Signatures ES configuration**
This section provides an overview of the LiveCycle ES components that are involved in defining a LiveCycle Digital Signatures ES process and the best practices surrounding it.

Within LiveCycle Workbench ES, there is a Process Design perspective and a Process Design tool. The digital signature process author must have a LiveCycle Workbench set up on a client machine that connects to the LiveCycle server.


Drag-and-drop methods from the Services view and the Properties tab can be used to configure each of the methods. These methods can be connected using routes, which can also be made conditional.

Variables can be created for the process and provided as inputs and outputs of the methods. And XPaths of these variables can be used to access inner values (in the case of complex types).

**Securing the signing keys**
The LiveCycle ES application user must have adequate permissions to invoke Sign and Certify operations. Specific permissions are required for signatures operations to be invoked successfully. These permissions can be added using the LiveCycle Administration Console at Home > Settings > User Management > Users and Groups. The available roles are Services User and Trust Administrator. The permissions associated with these roles are Certificate Read, Credential Read, CRL Read, and Service Invoke.

The Trust Store must hold the certificates to build the chain and the signing keys.

The Trust Store can be accessed in the Administration Console at Home > Settings > Trust Store Management. The signing keys can be either held in the LiveCycle ES database as local credentials or provisioned into a Hardware Security Module (HSM).
Adding local credentials

PFX or P12 files are credentials that reside on a filesystem. They can be imported into LiveCycle ES (see Figure 4). During the import process, these are identified by an alias that the user must specify. It is important to use a meaningful alias because it will be used later for signing or certifying operations.

Figure 4. Importing local credentials.
Adding HSM credentials

There are situations when signing credentials are stored on a Hardware Security Module (HSM). These credentials are accessed using PKCS#11 interfaces that are supplied by the HSM vendor. PKCS #11–based credentials can be accessed by configuring profiles in the Trust Store. The profile name referenced in the administration interface is the same as the alias name that you specify using the vendor configuration tools. Security partners providing HSMs that are known to work with LiveCycle Digital Signatures ES are nCipher and Safenet. Note that other PKCS #11–compliant HSMs might also be functional. The certificate of the private key that is being referenced in the HSM should be provided when defining its profile (see Figure 5) along with slot information.

Figure 5. Referencing a credential in a Hardware Security Module.
Specifying the trust anchors for signature validation

Trust anchors and intermediate certificate authorities (ICAs) must also be imported into the Trust Store to enable chain building at the time of signing and validation. The administration interface is as shown in the figure below.

Figure 6. Specify trust anchors.

Trust anchors may be trusted for various operations, such as certified documents or regular signatures. The level of trust will affect the signature validity status.

Tip: ICAs must not be trusted for anything. Trusting an intermediate CA certificate prevents chain building to occur completely and thereby could result in no revocation information being included in the signature at the time of signing.

Obtaining digital certificates
Adobe signature solutions can use any X509v3 digital certificates issued by a CA. Enterprises can choose to host their PKI in-house (using an Entrust CA, Microsoft CA, or any other CA) if their goals include two-factor authentication with certificates for employees, contractors, and perhaps even vendors. In this scenario, end users can also participate in digitally signing documents in Adobe Reader or Adobe Acrobat.

The other option is to buy the digital certificates from vendors such as VeriSign or Thawte. Adobe also offers a Certified Document Service (CDS) program (www.adobe.com/security/partners_cds.html). The CA vendors that participate in this program issue either an individual certificate or an organization certificate. The primary advantage of using certificates in this
program is that it eliminates out-of-band exchange of the trust anchor in order to validate a signature at the recipient end. The CDS certificates chain up to an Adobe root CA. Adobe customers should approach the participating vendors for purchasing any such certificates.

Adobe security partners
Adobe has cultivated strong relationships with several security vendors that offer a wide variety of solutions, including electronic signature pads, smart cards, tokens, and HSMs. A comprehensive summary of the security partner offerings is available at http://partners.adobe.com/public/developer/security/index_security_partners.html.

Conclusion
LiveCycle Digital Signatures ES along with forms enabled for Adobe Reader provide a strong platform to solve the last mile problem in going all electronic in business processes. Adobe Reader enables third party-vendors to plug in a functionality that provides a ceremonial process to signing by using electronic signature pads. The plug-in architecture enables the LiveCycle ES platform to offer a wider array of electronic signature choices to customers. These choices range from a click-to-approve signing functionality to a high-assurance PKI-based signing infrastructure with hardware tokens for citizens, employees, and perhaps even consumers.

Further reading
- Gartner, Inc. Electronic Signature Suites and Services Mature, Gregg Kreizman and Kristen Noakes-Fry, 2/6/08 (to access or purchase this document, go to www.gartner.com.)