The benefits of rights management

A guide to Adobe® LiveCycle® Rights Management ES software

Table of contents

1: Background
1: Adobe LiveCycle Rights Management ES
2: Case studies
5: Manufacturing trends
7: Security information
8: Conclusion

This white paper provides an overview of Adobe LiveCycle Rights Management ES software and the benefits rights management can bring to businesses in a range of industries.

Key benefits of Digital Rights Management:

- Protect intellectual property and personally identifying information against accidental or malicious disclosure without impacting productivity or collaboration
- Ensure internal and external recipients have direct access to the latest version of a document, regardless of where or when they need it
- Dynamic policy control so you can change who is authorized to view content no matter where files are located—on websites, CDs, employee laptops, or partners' computers
- Policy control is persistent throughout the information lifecycle as documents are generated and protected on the desktop and server
- Determine who is accessing documents, as well as where and when, speeding communication
- Easy deployment, using ubiquitous and free Adobe Reader® software, and ability to integrate tightly with many other applications, formats, repositories, and authentication mechanisms

Background

Information inside of organizations can take many forms: trade secrets, customer data, manufacturing plans, financial reports, and other proprietary intellectual property. Organizations are interested in maintaining confidentiality and in controlling access and usage of this information. However, they are also mindful that widespread adoption and acceptance only come with seamless user experiences in which security is ubiquitous and unobtrusive.

The mandate to extend communication beyond the traditional centralized organization takes many forms: sharing of manufacturing plans with globally distributed, low-cost suppliers and contractors; delivery of product information and reports to customers and citizens; and sharing of financial materials with distributors, agencies, and partners. There are many risks associated with engaging in these electronic processes. Hackers can break into, modify, or distribute proprietary information. Competitive espionage can encourage employees and individuals to misappropriate secrets. Regulatory requirements and privacy laws dictate how and where information may legally be shared.

Adobe LiveCycle Rights Management ES

Adobe offers an information protection solution that allows organizations to work and collaborate electronically with confidence. This paper provides an overview of Adobe LiveCycle Rights Management ES software and the benefits rights management can bring to businesses in a range of industries.

Protecting sensitive electronic information involves more than basic security and cryptography. The Adobe solution provides end-to-end content protection that respects the owner's intent and mitigates risk while enabling electronic workflows that increase communication. Using solution SDKs, organizations can integrate Adobe LiveCycle Rights Management ES with their existing authentication and authorization infrastructure.

Current approaches to information protection focus on initial distribution or access, for example, encryption during transit (using SSL during web sessions) or file access control lists. Once electronic information has been distributed, protecting confidentiality and privacy is difficult. Organizations cannot dynamically change access rights after initial distribution. In contrast, LiveCycle Rights Management ES solution gives organizations the confidence to engage in sensitive business electronically by providing persistent policy-based protection for your information.

- It controls access by encrypting all information and associating access control with content using industry-standard and government-approved FIPS-140 cryptographic algorithms. And it helps ensure confidentiality and authorization and maintains document integrity.
- Documents and content check in with their managing server to determine authorization, regardless of location. Because the centralized LiveCycle Rights Management ES server must approve access in real time, organizations do not need to be concerned about files that reside on network shares, unprotected websites, or CDs/DVDs that have been distributed. Using a policy lease, offline access can also be more securely managed.
- Persistent access control enables persistent version management. Recipients can be redirected automatically to the latest version of documents whenever they attempt to open an outdated version of a file.
- The solution can optionally maintain a log of access and document usage, providing a full chain of custody.
- Solution SDKs allow integration into existing authentication and authorization infrastructure.

Case studies

This section contains several diverse application patterns in the form of anonymous case studies to promote an understanding of how to deploy information protection. The case studies span multiple industries and workflows and are intended to serve as a starting point for further discussion about the value of assurance in electronic communication.

Highlights

- **Tight integration with enterprise directory/LDAP**—Ease deployments because authentication process is natural for end users, with no burden on IT or support.
- **Authentication SDK to allow custom integration with third-party authentication systems**—Leverage customer's non-LDAP authentication infrastructure, reducing cost to deploy and manage and helping to ensure solution is nondisruptive.
- **Policy-based control**—Allow flexibility in document usage via seven-day lease and IP address restrictions.
- **Fast to customize and deploy**—Use ubiquitous, free Adobe Reader.

Company Q

Company Q is an insurance company with a customer base served through a network of appointed brokers. The business requirement was to provide an easy way for customer account information to be made available to the brokers in a format that would allow them to update and submit to back-office systems.

The Adobe solution replaces an existing system that relied on spreadsheets and addressed the customer's key requirements of securing customer data, controlling user interaction, and conveniently submitting modified data. It was implemented using a combination of solution components from Adobe LiveCycle Enterprise Suite (ES) software to automatically produce intelligent PDF documents, which provide data transport and user interaction via Adobe Reader.

The customer requirements included allowing the document to be searched for specific customer or policy information and re-sorting data by various fields such as customer name and policy number. An important aspect in the design was to allow only certain fields to be updated by the user, so standard controls such as drop-down menus, buttons, and checkboxes are used where possible to simplify and control user input.

The Adobe solution required integration with Company Q's back-end systems from which document production is initiated. The comprehensive application programming interface (API) set available within LiveCycle allowed the development of a custom extension to Company Q's application that calls LiveCycle to populate the intelligent PDF template with data, apply usage rights to activate additional features available within Adobe Reader, and apply security to the document.

Company Q uses a third-party access control solution to centrally control user authentication and access/authorization to their applications. It was essential that the Adobe solution be tightly integrated with it so that user authentication is controlled in the same way as their other applications. The PDF documents also needed to be restricted for use only by certain users within each broker and to expire automatically after a set number of days.

LiveCycle Rights Management ES provides out-of-the-box integration with Lightweight Directory Access Protocol (LDAP) and Microsoft Active Directory implementations to authenticate recipients' credentials. In this case, however, the customer's access control solution does not provide a LDAP interface; instead various APIs are available for external applications. The LiveCycle Rights Management ES SDK allows for this type of integration through custom server-side service provider interfaces (SPIs). In this case, custom SPIs were implemented for user directory, authentication, and authorization so that the Adobe solution was tightly integrated with the customer's access control solution. Tight integration with the existing authentication infrastructure meant that individual brokers were able to engage in more secure communication that did not change their normal workflows—by simply leveraging their existing username and password.

The development of the project involved using Adobe LiveCycle Designer ES software to produce a PDF template with all the required functionality, some development effort to call the Adobe LiveCycle APIs, and integration with Company Q's application access control solution. The implementation was carried out by an Adobe solution partner, and building on an initial proof of concept lasting a few days, the final solution was implemented in a matter of a few weeks. The ubiquity of Adobe Reader helped ensure rapid deployment.

Highlights

- **Native CAD file support**—Share information securely outside of corporate boundary, allowing control over documents regardless of workflow.
- **Authorization SDK for native PLM integration**—Extend boundary of PLM control to documents regardless of whether they are on laptops, on file servers, or in email.
- **Versioning support to simplify management**—Help ensure that only the most recent document is available, regardless of distribution.

Company M

Company M designs and manufactures automotive components for a variety of automobile manufacturers. Most of their design occurs near Detroit, Michigan, in the United States; however, they have centers of excellence in Japan and in the European Union as well. Historically, most of the product manufacturing has been done within North America, but global opportunities and price pressures have forced them to look at outsourcing manufacturing to less expensive providers.

In particular, they have focused on how to manufacture certain price-sensitive components in Asia and assemble them at their plants in the United States. They want to share the relevant product plans with their manufacturing partners and still maintain control over detailed product manufacturing information. They store all of their product documents, including CAD, Word, and Excel files, within Unigraphics Teamcenter. These consist of a mix of CAD and Microsoft Word and Excel documents. When components were manufactured internally, they would grant the manufacturing team access directly to Teamcenter. Now that the manufacturing team spans companies and continents, Company M needs to maintain control beyond the boundary of the product lifecycle management (PLM) system.

Adobe LiveCycle Rights Management ES, however, has provided an effective solution for Company M. The native CAD and other file formats can be shared directly with manufacturing partners, yet access can be controlled via the LiveCycle Rights Management ES server. Through Adobe's Authorization SDK, the rights on the files can be automatically tied to the access assigned in Teamcenter. When a native CAD application is used to open a file, it contacts the LiveCycle Rights Managment ES server, which then consults the PLM system to determine what level of access should be granted. There is no need to create individual policies manually, as the solution automatically detects and enforces the appropriate level of access. This means that Company M can continue to manage access to its repository with confidence that documents distributed outside of the corporate boundary remain secure.

Furthermore, integration with Teamcenter helps ensure that whenever a document is revised, all downstream partners can remain in sync with the latest version. Using the "versioning" capability within LiveCycle Rights Management ES, Teamcenter can make sure policy-protected, older document versions become inaccessible—regardless of where the files reside outside of the PLM system. In fact, if people attempt to open an older version, they can be automatically redirected to the latest version of the document.

Adobe's broad-based approach to the protection of sensitive information enables customers to communicate using high-fidelity, nuanced data in "native" form. Company M can share, on demand, native Microsoft Office and CAD documents that include detailed calculations and product data with confidence that access is restricted and can be revoked at any time.

Highlights

- **Secure offline access**—View protected documents on a laptop with no network access. Authorized users can view only the latest versions of documents while on planes or in the field.
- **Smart card authentication**—Get multifactor authentication, increasing security in high-risk environments.
- **Watermarking**—Help ensure printed documents reference employee name and timestamp of print to keep employees honest, as well as provide a trail of activity.
- **Audit SDK**—View document access usage log data and perform trend analysis.

Company F

Company F is in the aerospace business. They spend large amounts of money in R&D for jet engines. The engines, once built, are brought to aircraft manufacturers to assemble into commercial and military aircraft. A vital part of their business, however, is working with airlines to maintain engine components according to strict government safety standards. Specifically, they send out technicians to the field: to advise customers on how to repair engines, work with government inspectors, and perform maintenance work directly. Part of why Company F has kept much of the R&D work directly within their corporation is that they can maintain profit margins servicing business associated with their designs. Protecting their sensitive information, even as it is distributed to customer sites with field service technicians, is critical.

They have a several-thousand-person organization devoted to field service operations. These technicians are on-site in more than 70 countries worldwide. They need to have a detailed understanding of how the engine parts work and their failure rates, so that they can perform maintenance work for their customers according to strict government standards. The complication is that these employees pose a significant threat to Company F in several ways:

- Given the value of the sensitive information to which they have access, they can reap significant monetary rewards by selling such information while on the payroll.
- Employees can leave to work for a local customer with significant sensitive information in hand.
- In many countries where these aircraft are maintained, the legal system for enforcing the protection of sensitive information is expensive and slow.
- Granting full access to sensitive information without a need to know can violate U.S. export controls.

Using the LiveCycle Rights Management ES solution, Company F can mitigate these threats by providing limited information access to these field employees. They publish their documentation, videos, and CAD drawings as a combined PDF package. Documentation is classified into multiple tiers, and access is granted on a need-to-know basis. This helps to ensure compliance with export controls and enforces existing degrees of trust for field employees. PDF serves as the perfect container of information, as Company F can selectively strip out sensitive data during the classification process.

They protect this PDF document with a policy that grants their employees offline access with a "three-day offline lease." This means that the employees log in to the Company F intranet once every three days and open any protected PDF file. They are then automatically granted access to all field service documents to which they are entitled for three full days. This allows employees to retain access to documentation remotely because they can open documents during these three days without any network access. Yet it helps ensure that if they share a protected document with an unauthorized user, it will automatically be unusable after three days of separation from the corporate network.

The solution is made more effective by leveraging smart card authentication. Company F has configured the login requirement with LiveCycle Rights Management ES to work only with employee smart card badges instead of a simple username/password combination.

Risk is further mitigated by including the employee's username and timestamp on all protected documentation that is printed. This makes documents distributed to employees traceable in an audit. The solution also maintains an access control audit log for every action on protected documents. Individual employees can use the built-in system as well as the extensible Audit SDK to determine document usage trends and take corrective action.

Highlights

- Provide information assurance through a combination of rights management and digital signatures, increasing customers' confidence that their private (banking) data is tamper resistant and remains confidential.
- Leverage existing credentials using the Authentication SDK and minimal development.

Company B

Company B is one of the largest local banks in Singapore, with dozens of branches and hundreds of automated banking centers. As a strongly capitalized commercial bank focusing on this prosperous country, they specialize in a wide range of personal wealth management, commercial banking, corporate and institutional banking, treasury services, and private banking services. They had a pressing business need to increase the operational efficiency surrounding their regularly issued paper-based banking statements. The generation of statements for their wide range of investment products was a time-consuming process that was paper intensive, costly, and not in tune with the increasing environmental consciousness in Singapore. LiveCycle ES solution offerings enabled the bank to move to electronic statements with confidence.

The bank converts their statement data to PDF and uses multiple security solutions within the LiveCycle suite to make sure that the electronically delivered statements are transmitted with integrity, remain confidential, and are verified as authentic. Using Adobe LiveCycle Digital Signatures ES software as a part of their solution allows Company B to digitally sign and certify the statements, giving customers confidence that they have not been altered. The PDF files are protected using LiveCycle Rights Management ES, so only the customer can gain access to the statement.

The entire experience is seamless for the bank's customers. No special software deployment is required, as hundreds of millions of copies of Reader, with built-in rights management client functionality, have been distributed. The bank can be confident that customers will be able to universally open the statements. Customers can acquire their e-statements on demand via web access. They can use Adobe Reader to open their statements, and when they are prompted to authenticate to the system to open their statement, they enter their username and PIN. This was accomplished by writing Java™ code to do a custom integration using the Authentication SDK. It allowed the bank to integrate directly with their user repository and authentication infrastructure.

Highlights

- Enjoy CAD native file support.
- Publish manufacturing documents more securely using Adobe Acrobat®, Reader, and the LiveCycle solution.
- Include 3D data in PDF documents using solutions from Adobe partners Tetra 4D and PROSTEP.
- Share information more securely across a supply chain.
- Use the Authorization SDK for native PLM integration.
- Use versioning support for simplified management, making sure only the latest information is shown.
- Decrease the cost of implementation by automating the solution with manufacturing business process orchestration.

Manufacturing trends

For a while now, manufacturing companies have been required to handle complex data to successfully manage their product lifecycle. This complex data is generally referred to as product information and may include a wide variety of data such as CAD designs, 2D drawings, engineering change orders, parts lists, and so on. This product information is complex due to strong dependencies among these different data sources and more so when it includes 3D geometry with dimensioning and tolerancing annotations. Moreover, the product information set needs to be managed as one synchronized package if it is associated with a product configuration designed for a particular client. Efficiency of communication is critical.

Throughout the lifecycle of a product, from early concept designs to service, product information passes through three major states—Work in Progress (WIP), Released, and Archived—where each state can last from a few days to 50 years. For the last two decades, the manufacturing industry has been shifting from paper to electronic, but more recently, especially in the aerospace and automotive industries, the shift has been more about replacing 2D drawings by a methodology commonly referred to as model-based definition. The essential requirement imposed by this methodology is to eliminate the use of 2D drawings throughout the product lifecycle. While 2D drawings are very cheap to consume, they also lack the clarity required for the more complex products that are manufactured nowadays.

Adobe PDF has been widely adopted in the manufacturing industry. Typically, all 2D drawings are released and archived in PDF or TIFF, and when they are received by suppliers or shop floors, they are immediately printed in multiple copies and distributed across the different groups involved in the manufacturing or assembly process. Inside the OEM enterprise, which usually issues those 2D drawings, the CAD data tends not to circulate outside the engineering team primarily due to the complexity of the data, the cost of the applications to view them, and the skills required to use those applications. Communication, in this case, is usually resolved by sending screenshots or inviting colleagues to a common office where the engineer can control the CAD application and the extended team can focus on the screen. This is clearly far from an ideal solution. Forcing an extended team to focus on a shared session imposes burdens on communication.

With model-based definition come many additional challenges that manufacturing companies are still trying to overcome. For instance, in the effort to shift to this methodology, companies are having to rethink how data is shared and managed both internally and externally during the WIP and Released phases and how it is archived for reuse. There is also a need for non-CAD designers to analyze the data as precisely as possible and collaborate on the data itself and/or any results from the analysis performed. Protecting this data is mandatory given that sensitive information is contained in a collection of CAD files that can be easily repurposed by anybody who has access to them in their native authoring application.

The best solution to address these new challenges is based on PLM systems that provide an environment to create, collaborate, control, and communicate product development and lifecycle information. These systems can more securely manage assets stored internally, granting access to stored documents upon demand and authorization. However, once files are extracted, they remain unprotected and not version controlled.

PLM solutions recommended by CAD and other vendors have gained the most traction with large OEMs and Tier 1 suppliers, leaving the majority of the market that cannot afford multimillion-dollar PLM systems underserved. Not only that, even companies that have implemented a PLM system are still challenged when it comes to opening their PLM environment to thousands of suppliers to give them access to Released data. Indeed, PLM systems are becoming more successful at managing the product lifecycle past the Released state, but they have failed to reach out to all the players involved in the product lifecycle.

Adobe's PDF solutions provide advantages to manufacturers that generate 3D models and the manufacturing processes surrounding them. One of the main reasons that Reader and PDF have been so widely deployed and used is that they are easy to use, they maintain information integrity, and they protect the original document.

Adobe solutions combine desktop and server-based products with 3D PDF technology from industry leaders to help you publish, protect, review, and archive engineering information using PDF files as an essential part of your PLM workflows.

PDF collaboration in PLM workflows

Streamline review and collaboration while protecting propriety manufacturing data as it is shared across the value chain.

1. Design

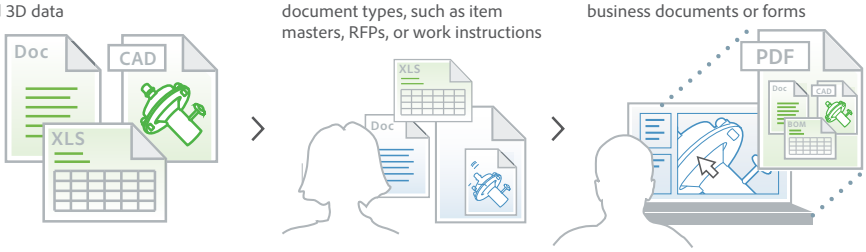
Define a product using multiple document types, including 2D and 3D data

2. Author

Pull data from multiple systems to author manufacturing-specific document types, such as item masters, RFPs, or work instructions

3. Publish to PDF

Convert manufacturing documents to PDF combining 3D data with business documents or forms



Products Used

- Pro/Engineer
- SolidWorks
- AutoCAD
- Microsoft Office

...and many more

- Adobe FrameMaker®
- Anark Core
- Lattice Technology XVL Studio

- Adobe Acrobat Pro
- Adobe LiveCycle PDF Generator ES
- Adobe LiveCycle Forms ES
- PROSTEP PDF Generator 3D for Adobe LiveCycle ES
- 3D PDF Converter from Tetra 4D

4. Protect & control

Apply permissions and/or rights management to PDF documents to control usage, expiration, and revisions outside the firewall

5. Review & approve

Initiate, manage, and track design reviews, enabling anyone with free Adobe Reader to add comments, sign, and save PDF files

6. Archive & retrieve

Convert 3D product data and documents - with comments and approvals - for long term archival in ISO PDF/E and PDF/A formats

Products Used

- Adobe Acrobat Pro
- Adobe LiveCycle Rights Management ES

- Adobe Acrobat Pro
- Adobe LiveCycle Reader Extensions ES
- Adobe LiveCycle Digital Signatures ES

- Adobe Acrobat Pro
- Adobe LiveCycle PDF Generator ES
- PROSTEP PDF Generator 3D for Adobe LiveCycle ES

Coupled with rights management, Adobe solutions allow PLM systems to extend the boundaries of communication and collaboration while protecting CAD data; authorization can extend to files checked out from the PLM environment, regardless of location. Manufacturing companies embracing LiveCycle ES will find that there are virtually limitless ways that authorized users can utilize a portfolio of packaged product information.

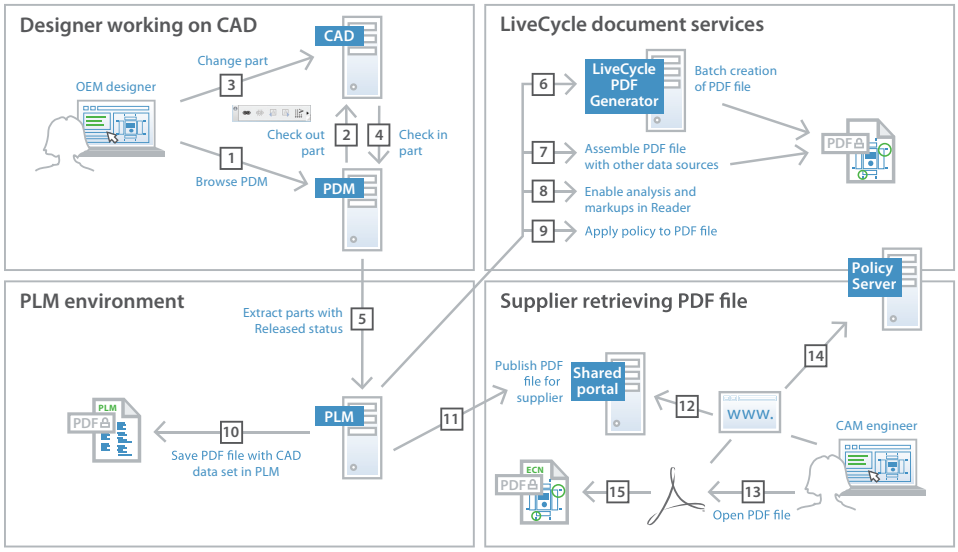
The following workflow illustration highlights the capabilities of the LiveCycle ES platform and how its integration with an existing PLM environment can enhance the Release to Manufacturing process among OEMs, customers, suppliers, and shop floors:

- **Step 1. Generate content**
  Generate content in a variety of formats, including PostScript,® TIFF, text, image files, standard business documents (Microsoft Office word processing files, spreadsheets, and presentations), and multilayered engineering 2D drawings as well as 3D CAD designs of parts and assemblies with 3D annotations and product views.

  Step 2. Convert and combine in PDF
  Convert all product information content including CAD designs with 3D tolerancing and dimensioning annotations, 2D drawings, engineering change orders, and parts lists to PDF by incorporating PROSTEP PDF Generator 3D for Adobe LiveCycle ES into the PLM process. Flexible file submission options include network watched folder, e-mail, web browser, web service, or Java API. PDF files can be combined into a single PDF package to include more information than that contained in the CAD models and drawings.

- **Step 3. Apply document controls**
  Automate the process of encrypting PDF documents, or apply document usage controls using LiveCycle Rights Management ES. PDF files and native CAD files such as Pro/ENGINEER and Microsoft Office files that are maintained in the PLM can have rights management applied to extend the access and usage rights of those files beyond the PLM system.

- **Step 4. Deliver and archive**
  Deliver PDF packages across many channels, including print, fax, e-mail, and web to employees, customers, or suppliers. Or archive PDF files for easy search and retrieval.



Highlights

- Protect your documents with the Adobe encryption module, which is approved for use in the U.S. government via Federal Information Protection Standard (FIPS-140-2) certification.

Security information

LiveCycle Rights Management ES can be used to enforce security policies in documents and other supported formats. It allows content owners to control who has access to sensitive information, audit who has accessed particular files, and dynamically modify access to sensitive information. Using industry-standard security technology to protect sensitive information, it encrypts each file individually using 128- or 256-bit AES symmetric keys, the U.S. government's Advanced Encryption Standard. The module used to encrypt files has been certified to conform to the Federal Information Protection Standard (FIPS 140-2). LiveCycle Rights Management ES is only one component of any security solution, and no security solution provides absolute security. Before deploying, an organization should identify the threats they are trying to block and how the level of protection provided by rights management improves on existing protective measures.

Conclusion

Adobe's mission is to revolutionize how the world engages with ideas and information. Since 1994, with the release of Acrobat 2.0 introducing PDF security and protection, Adobe has been providing information assurance solutions. Our goal is to provide solutions that enable effective communication and collaboration while protecting sensitive information.

With a comprehensive set of desktop- and server-based products and solutions, the LiveCycle ES platform allows authors to control access to documents in a way that fits into existing workflows and communication processes. The benefit for the author is substantial additional control over which documents are accessible, while the impact on consumers is minimized. The solution can tie into existing systems that control authorization and authentication to make the experience of using of rights-managed documents similar to that of using unprotected files. Adobe's products and solutions are based on industry-standard, government-approved security standards and cryptographic algorithms that protect confidential data.

The ubiquity of Adobe Reader makes the cost and effort of deployment minimal. In addition, the flexibility of the PDF format means that many types of data can be shared for electronic collaboration and knowledge transfer.

Effective communication requires that collaboration not be impeded by security or privacy concerns. Protection of sensitive information means that communication can be safely expanded to interorganizational parties worldwide. The combination of information protection and version control can improve operational efficiency in distributed, worldwide collaborations and supply chains, reducing costs and increasing customer and constituent satisfaction.

For more information
www.adobe.com/livecycle

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

Adobe, the Adobe logo, Acrobat, the Adobe PDF logo, FrameMaker, LiveCycle, PostScript, and Reader are either registered trademarks or trademarks of Adobe Systems Incorporated in the United States and/or other countries. Java is a trademark or registered trademark of Sun Microsystems, Inc. in the United States and other countries. All other trademarks are the property of their respective owners.

© 2013 Adobe Systems Incorporated. All rights reserved. Printed in the USA.

91069483 1/13