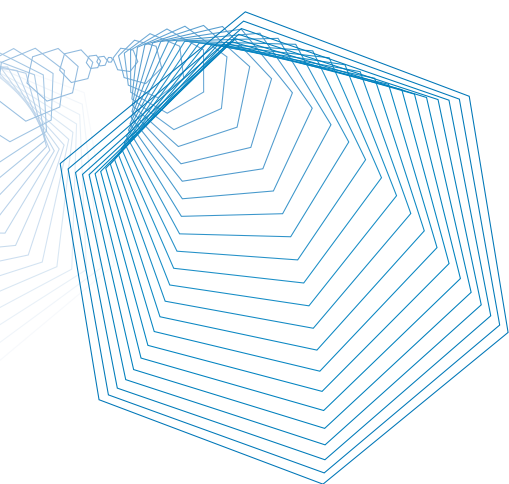


Adobe® LiveCycle™ Document Security

Enhance security of sensitive information automatically from the server

Many essential business processes involving employees, customers, partners, and constituents are not fully automated because of security concerns. But how do you automate these key processes with the assurance that documents maintain their authenticity, integrity, and confidentiality?



ADOBE LIVECYCLE DOCUMENT SECURITY:

- Ensures document authenticity, integrity, and confidentiality
- Safeguards information beyond the network
- Helps you meet regulatory requirements
- Reduces cost of protecting information
- Lets you leverage existing infrastructure investments to integrate with public key infrastructures
- Enhances document security throughout the information lifecycle

Automate business processes—more securely

Adobe LiveCycle Document Security enables your business to bring more paper-based processes online by providing digital signature and encryption capabilities in a server environment. With Adobe LiveCycle Document Security, essential business processes that used to rely on expensive and time-consuming paper-based documents and physical delivery can be more securely automated, thereby increasing your employee productivity and customer satisfaction.

- Digitally sign and certify PDF files
- Validate digital signatures
- Encrypt and decrypt documents
- Integrate with a Hardware Security Module (HSM) for added security and performance

Adobe LiveCycle software is built on a common server architecture based on Java 2 Platform, Enterprise Edition (J2EE) and XML, allowing for easy integration into enterprise infrastructures by providing Java application programming interfaces (APIs) and support for Web services protocols. Adobe LiveCycle is optimized for IBM® WebSphere® software and can be deployed on JBoss application servers.

Bring critical processes online

Adobe LiveCycle Document Security provides digital signature and encryption capabilities in a server environment, eliminating the need for someone in the organization to manually open each file and add or verify digital signatures.

With Adobe LiveCycle Document Security, enterprises can process Adobe PDF documents with digital signatures from leading third-party vendors to enable large volumes of certified documents in batch (or bulk) on the server. Before a transaction is processed, Adobe LiveCycle Document Security checks whether a document has been altered and was really approved by the correct person—validating the authenticity and integrity of content, as well as the signer's digital identity.

Meet regulatory requirements

With Adobe LiveCycle Document Security, enterprises can now incorporate electronic forms and documents into processes that already exist in core enterprise systems. When Adobe LiveCycle Document Security receives a PDF document, it opens the document and validates it based on the signature status. This feature extends processes beyond the firewall to customers, partners, and constituents, while meeting corporate and government regulations for protecting the security and privacy of electronic information sharing.

Leverage existing IT investments

For organizations that have deployed a public key infrastructure (PKI), Adobe LiveCycle Document Security provides encryption and decryption capabilities. Documents that are automatically generated can be encrypted for distribution and encrypted documents that have been submitted can be automatically decrypted, ensuring the document content will not be accessed by unauthorized parties. These capabilities enable enterprises to leverage existing

SYSTEM REQUIREMENTS

Microsoft® Windows Server™ 2003

- Intel® Xeon™ processor at 2.8GHz or faster, or equivalent processor
- 2GB of RAM (minimum)/two CPUs
- Swap disk space: 30GB minimum; 7,600 rpm drives
- 350MB of available hard-disk space for installation
- CD-ROM drive

IBM AIX 5L™

- IBM POWER4™ processor at 1.7GHz or faster, or equivalent processor
- 2GB of RAM (minimum)/two CPUs
- Swap disk space: 30GB minimum; 7,600 rpm drives
- CD-ROM drive

Red Hat® Enterprise Linux® AS 2.1

- Intel Xeon processor at 2.8GHz or faster, or equivalent processor
- 2GB of RAM (minimum)/two CPUs
- Swap disk space: 30GB minimum; 7,600 rpm drives
- 350MB of available hard-disk space for installation
- CD-ROM drive

Sun™ Solaris™ 8 or 9

- Sun UltraSPARC III at 1.2GHz
- 2GB of RAM (minimum)/two CPUs
- Disk space: 30GB; 7,600 rpm drives
- 350MB of available hard-disk space for installation
- CD-ROM drive

Web Application Server/OS

- WebSphere 5.1 on Windows Server 2003
- WebSphere 5.1 on AIX 5L
- WebSphere 5.1 on Red Hat Enterprise Linux AS 2.1
- WebSphere 5.1 on Solaris 8 and 9
- JBoss 3.2.2 on Windows Server 2003
- JBoss 3.2.2 on Red Hat Enterprise Linux AS 2.1

FOR MORE INFORMATION

To learn more about Adobe LiveCycle Document Security and the complete line of Adobe LiveCycle products, please visit www.adobe.com/products/server/securityserver/main.html.

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

Adobe, the Adobe logo, Acrobat, Adobe LiveCycle, and Reader are either registered trademarks or trademarks of Adobe Systems Incorporated in the United States and/or other countries. Intel and Xeon are trademarks or registered trademarks of Intel Corporation or its subsidiaries in the United States and other countries. AIX 5L, IBM, POWER4, and WebSphere are trademarks of International Business Machines Corporation in the United States and/or other countries. Linux is a registered trademark of Linus Torvalds. Microsoft and Windows Server are either registered trademarks or trademarks of Microsoft Corporation in the United States and/or other countries. Red Hat is a trademark or registered trademark of Red Hat, Inc. in the United States and other countries. Solaris and Sun are trademarks or registered trademarks of Sun Microsystems, Inc. in the United States and other countries. All other trademarks are the property of their respective owners.

© 2004 Adobe Systems Incorporated. All rights reserved. Printed in the USA.
95003818 8/04

technology investments in PKI and smart card solutions to provide enhanced security. Adobe LiveCycle Document Security also provides bulk digital signature capabilities on PDF using HSMs for highly secure cryptographic functions.

Key features

- Provides enterprises with the ability to digitally sign and certify PDF files on a server
- Validates digital signatures
- Enables the encryption and decryption of documents
- Features integration with a HSM for added security and performance

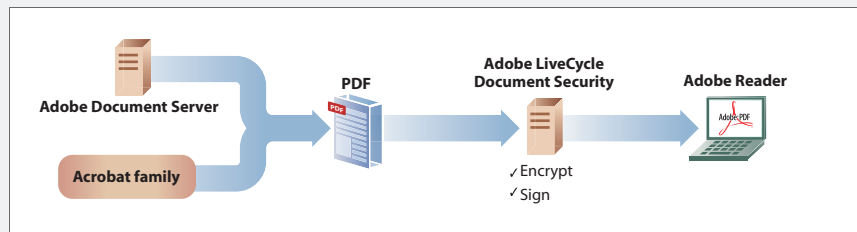


Figure 1: Certified Document Publishing

The diagram offers a simplified view of the certified document publishing capabilities of Adobe LiveCycle Document Security in an enterprise environment (examples include an investment bank report or a government hearing transcript):

1. In this workflow example, a PDF document is created using Adobe Document Server. [Note: The PDF document also can be generated from the Adobe Acrobat® family of products or Adobe LiveCycle Forms.]
2. To preserve the integrity and authenticity of the document, Adobe LiveCycle Document Security digitally signs the document. Adobe LiveCycle Document Security then sends the document to the recipient.
3. The recipient opens the document in Adobe Reader® software to validate the digital certificate.

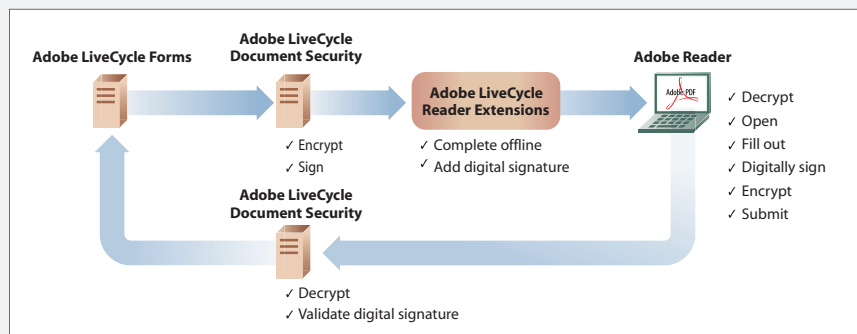


Figure 2: Secure Information Processing

This diagram shows a simplified view of the secure information processing capabilities of Adobe LiveCycle Document Security in an enterprise environment (such as for clinical trials):

1. In this round-trip workflow example, a PDF form is created using Adobe LiveCycle Forms. If prepopulated with information, the PDF form may also be encrypted before being sent to Adobe LiveCycle Document Security.
2. Adobe LiveCycle Document Security digitally signs and encrypts the form.
3. Adobe LiveCycle Document Security then sends the form to Adobe LiveCycle Reader Extensions to apply usage rights. These usage rights include completing the form offline, as well as signing, certifying, and authenticating forms using industry-standard technologies and PKIs. The form is then sent to the recipient to open or decrypt with a smart card or other PKI solution and Adobe Reader.
4. Once received and opened in Adobe Reader, the recipient completes the required information, then digitally signs the form—and if it arrived encrypted, re-encrypts the form—and submits it back to the Adobe LiveCycle Document Security.
5. Before a transaction is processed, Adobe LiveCycle Document Security decrypts the data and determines whether the form has been altered and was approved by the correct person—validating the authenticity and integrity of content, as well as the signer's digital identity. It then passes the information back to Adobe LiveCycle Forms to extract the data from the form to enter into or update the appropriate enterprise systems.

