

Adobe® Acrobat® 4.0

Adobe Acrobat 4.0 and Digital Signatures

An increasing number of organizations are using innovative technologies such as Adobe Acrobat software to help make the transition between paper and digital forms of document distribution. Using Acrobat software to convert paper-based documents and electronic forms to compact, universally readable Adobe Portable Document Format (PDF) files not only makes information more accessible and manageable, but also promotes a streamlined office document workflow. In particular, the annotation features found in Acrobat 4.0 greatly improve office document review and mark-up, a cooperative process integral to many enterprise workgroups.

Recognizing the need for the highly controlled review of electronic documents in many sensitive environments—including legal, financial, and government applications—Adobe has engineered Adobe Acrobat 4.0 to include full support for digital signatures. Digital signatures authenticate and safeguard information by allowing authors and key personnel to “sign” electronic documents with a unique electronic signature that identifies the person who applied it as having read, reviewed, or contributed to the document’s creation. A digital signature can also verify that a document has not been altered since it was sent. The support for digital signatures adds significant value to Acrobat 4.0 software, enhances the productivity of internal and external workgroups, and increases document security in any organization.

Digital signatures defined

When users need to authenticate a paper-based document, they do so by applying their handwritten signature, with a writing instrument, to an actual paper page. This authentication can have important business implications—for example, a signature can seal a contract, approve an expense report, or validate a performance review. Electronic documents, including Adobe PDF files, pose a unique problem—they can’t be “signed” by hand, but they often require the same level of authentication as paper documents. Digital signatures were developed to address this dilemma.

A digital signature encodes an electronic document with an encrypted unique signature that positively identifies the person who applied the signature. Digital signatures can be implemented as a stand-alone tool or integrated into enterprise networks. While a relatively new technology, digital signatures have found numerous applications in diverse fields; they are essential in any application that requires reliable authentication of electronic documents. One of the best-known uses of digital signatures can be found in the burgeoning area of electronic commerce (eCommerce) where clicking a button at the end of a Web site-based consumer purchase replaces the handwritten signature of a traditional credit-card transaction. But digital signatures are also quickly becoming an integral part of many organizations’ document review processes—in any environment where one or more people have to “sign-off” on electronic documents, digital signatures are an essential tool.

Two basic models for digital signatures exist today: key-based signatures and biometric signatures. Key-based signatures attach an encrypted unique signature to a document that verifies who signed the document, when it was signed, and other user-determined information. Key-based systems can also control access to a document, allowing only certain persons holding certain keys to read or modify the document. Because key-based signatures are often officially registered with a Certification Authority (see next section), they provide both identification and nonrepudiation, which are both important when signing legal documents. Biometric signatures also employ an encrypted algorithm but additionally incorporate a digital representation of an actual handwritten autograph. Sophisticated data about the movement of the pen during signature (the “inscription event”) is attached to the digital signature, including the speed of pen movement as well as the relative positioning of curves, loops, lines, crosses, and other orthographic features.

Regardless of whether a digital signature is key-based or biometric, it serves generally the same purpose. It confirms the identity of a person who has read or altered a document. Both kinds of signatures can also be used in conjunction with other enterprise security technologies to provide authentication and privacy protection in large networks. Adobe SelfSign, which is included with Acrobat 4.0 software, employs key-based signatures; supported third-party applications include a range of key-based and biometric solutions.

The role of a Certification Authority

Located either inside or outside an organization, a Certification Authority (CA) is an objective third party that validates the authorship of a digital signature. After gathering significant documentation from the owner of a digital signature, the CA issues the individual a certificate for signing documents. Only that user has the password that allows access to material protected by the certificate. Every time the user attempts to access protected material within an electronic document, the password is checked against the CA's database to validate the user's signature. Not all digital signature technologies rely on CAs—for example, the Adobe SelfSign plug-in is a “self-trust” model that lets users create their own certificate to be shared with others at their discretion. And biometric technologies are often employed without CAs, under the assumption that “biological behavior” provides adequate evidence of signature origin—at least as much as traditional paper signatures provide.

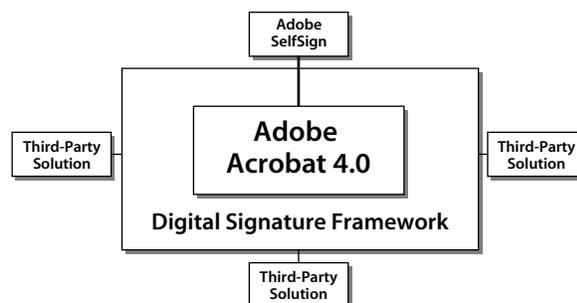
Digital signatures in the office document workflow

Organizations of all sizes are discovering the value of “going digital.” First, by converting office documents to Adobe PDF files—which preserve the look and feel of any original document and can be read from any computer—these organizations make information much more accessible to people who need it. Adobe PDF files can be e-mailed, posted to an intranet server, or made part of a Lotus Notes database, creating an extremely efficient distribution system for important documents. Many of these documents, including financial information, white papers, legal documents, and external communications, require extensive review and mark-up by internal and external workgroups, and the powerful annotation tools found in Acrobat 4.0 help streamline the review process considerably. (For more information, see the Adobe white paper “Acrobat 4.0 and Office Document Review and Mark-up,” which is downloadable from www.adobe.com/acrobat.) The support for digital signatures found in Acrobat 4.0 software complements this process perfectly, both by allowing the authentication of Adobe PDF files directly from within the Acrobat application and by showing what changes have been made to an Adobe PDF file between signatures.

Adobe Acrobat 4.0—The digital signature framework

Some digital signature technologies employ stand-alone applications to authenticate electronic documents such as Adobe PDF files. With the digital signature framework found in Acrobat 4.0 software, you can take advantage of integrated plug-in versions of many of these technologies, including solutions from Adobe and several third-party developers. This integration allows you to easily make digital signatures an integrated part of your Adobe PDF-based office document workflow.

Adobe SelfSign provides an ad hoc out-of-the-box digital signature capability for users who do not require a scalable identification model. Third-party solutions address a variety of business needs, and some technologies include Entrust Technologies, VeriSign, PenOp, Coastek, Silanis Technology, Communication Intelligence, Digital Applications, and Seal Systems.

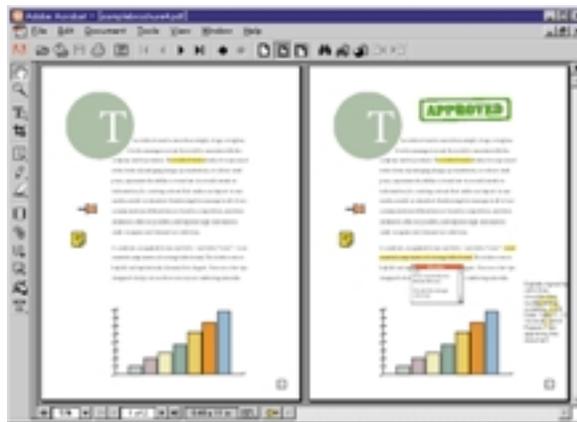


The digital signature framework found in Adobe Acrobat 4.0 employs an open plug-in architecture to accommodate solutions from Adobe and several third-party providers.

Seamless integration enhances functionality

Because the digital signature framework is based on an open architecture, the various supported technologies are accessible directly from within the application. Simply choose the Digital Signature tool from the Acrobat toolbar to apply your key-based or biometric digital signature to any Adobe PDF file. This seamless integration not only eliminates the need to switch between Acrobat and stand-alone digital signature applications, but also enhances overall functionality by providing Document Compare, support for multiple signatures, and form field integration.

- **Document Compare**—When it is used alone, the new Document Compare feature found in Acrobat 4.0 streamlines the document review process; when it is combined with seamless support for digital signatures, it further improves version control and increases document security. Document Compare lets you open two or more Adobe PDF files in tiled windows for side-by-side on-screen comparison of different versions of a document. More importantly, the feature lets you “rollback” among versions of a document to see what changes have been made between digital signatures. Acrobat software highlights any changes for easy comparison and author identification, and all the changes can be summarized for at-a-glance review.



- **Multiple signatures**—You can apply as many different signatures to a PDF file as necessary. This is important in situations where you might want to combine several digital signature technologies to authenticate, restrict access to, or secure a document in multiple ways.
- **Form field integration**—You can directly apply digital signatures to signature-specific form fields, making the authentication of documents, such as expense reports, much more efficient. Additionally, this enhanced functionality makes working with Acrobat forms extremely easy.

Improving authentication in many environments

Using digital signatures in an office document workflow can be an essential authentication strategy for many types of organizations. Within corporations, accounting departments can electronically obtain the multiple signatures required to authorize expense report reimbursement, and human resources departments can use digital signatures to authenticate repetitive document sets, such as benefits applications and tax forms. Legal firms can impose high-level version control on volatile documents such as contracts and living wills, tracking small but important changes and instantly identifying the authors of content alterations.

Many health care industries—from insurance companies to hospitals to pharmaceutical manufacturers—gather countless signatures for documents that require authentication and/or input from doctors, administrators, and other professionals. Attaching digital signatures provides a high level of security for such sensitive documents and can increase productivity where very large numbers of documents must be authenticated. For example, the U.S. Food and Drug Administration requires the authentication of thousands upon thousands of documents during the drug approval process. In each of these examples, the integration of digital signatures with the Document Compare feature found in Acrobat 4.0 lets key personnel not only confirm whether changes have been made between signatures, but also ensure document integrity and promote accountability among reviewers of important documents.

Regardless of whether you're in charge of approving expense reports or developing a promising new drug, the digital signature support found in Acrobat 4.0 software can help improve productivity in environments where one or more persons must authenticate electronic documents. And distributing your authenticated documents in Adobe PDF has its own rewards—you reduce the cost and time associated with traditional delivery methods, such as interoffice mail, fax, or express services; you decrease the likelihood that the documents will be lost or filed incorrectly, a major cause of lost productivity in organizations today; and because electronic distribution eliminates the need for hard copies, you reduce the consumption of toner and paper, which is an economic as well as environmental benefit.

Adobe Document Solutions—Making the most of your information

As large organizations transfer more documents electronically, they are looking for tools and solutions to update and refine inefficient, paper-based processes such as document authentication and security. By offering universal access to any document through Adobe PDF, as well as powerful support for digital signatures, Adobe Acrobat 4.0 software is the perfect choice for organizations that wish to increase efficiency and productivity. But improving document authentication is only part of the Acrobat story. Together, Adobe Acrobat and Adobe PDF form the foundation of Adobe Document Solutions—an integrated way of creating, sharing, and reviewing documents—to help you make the most of your information. Innovative technologies such as Adobe Acrobat Capture® software and Adobe PostScript® 3™ complement Acrobat software and Adobe PDF to provide a powerful solution that enables your enterprise to see the greatest return on its information assets.

For more information about Acrobat, Adobe PDF, and other Adobe Document Solutions, visit the Adobe Web site at www.adobe.com/acrobat.

Other resources:

Third-party partners

The Web sites of our third-party digital signature partners provide a wealth of information regarding digital signatures and other security technologies:

- Entrust Technologies—www.entrust.com
- VeriSign, Inc.—www.verisign.com/product/acrobat/index.html
- PenOp, Inc.—www.penop.com
- Silanis Technology Inc.—www.silanis.com
- Communication Intelligence Corp.—www.cic.com
- Digital Applications, Inc.—www.digapp.com