GlobalSign
GMO INTERNET GROUP

Create trusted digitally signed documents

Replace paper-based workflows with document signing certificates for Adobe AATL

Create trusted documents with AATL

GlobalSign's PDF Signing solution allows authors to create PDF and Office files that automatically certify to the recipient that the author identity has been verified by a trusted organization. Adding a digital signature is the virtual equivalent to sealing a document and adding a wet ink signature. Recipients are assured that the document is authentic, comes from a verified source, and the contents have not been tampered with since being digitally signed.

Business Benefits

- Enable secure electronic document workflows
- Included timestamping services support time sensitive document transactions and audit trails
- Meet compliance requirements on digital signatures
- Ensure document integrity and authorship
- Save time and resources over paper-based workflows

Deployment Options

The Adobe AATL Certificate Policy requires certificates to be stored on FIPS-compliant hardware, such as a SafeNET iKey token or Hardware Security Module (HSM). GlobalSign offers a variety of deployment options to support the needs of all organizations, small to large.

Token-based

Ideal for individuals and organizations who need to digitally sign a moderate amount of PDF documents (<5,000/year) or do not use an automated PDF generation solution.

Hosted HSM

Ideal for organizations using automated PDF generation software, such as Adobe LiveCycle, Ascertia DSS, Eldos Secure Black Box, or iText Java/C Sharp, to generate and manage large volumes of documents that do not have the desire, internal PKI knowledge, or capacity needs to warrant owning and operating their own HSM.

On-premise HSM

Ideal for organizations using automated PDF generation software, such as Adobe LiveCycle, Ascertia DSS, Eldos Secure Black Box, or iText Java/C Sharp to generate and manage large volumes of documents that have the desire and internal support to operate and manage their own HSM.

Digitally Signed PDFs

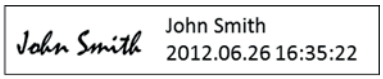
GlobalSign's document signing certificates allow you to add certifying and approval signatures to PDFs.

Certifying Signatures

Adding a certifying signature to a PDF means you are the author of the document, have finalized its contents, and want to secure it against tampering after it has been distributed. Certified documents display a blue ribbon across the top of the document containing the signer's name and the Certificate issuer - a clear, visual indicator of document. authenticity and authorship.

Approval Signatures

Approval signatures expedite an organization's approval procedure by capturing the electronic approvals made by individuals or departments and embedding them within the actual PDF. Signatures can be customized to include an image (e.g., your physical signature or official seal) and various signature details (e.g., signing location, date, reason for signing).



Digitally Signed Office Documents

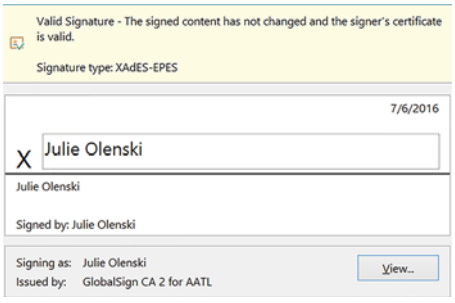
Microsoft supports two types of digital signatures - visible and non-visible.

Non-visible

Non-visible signatures are used when you need to provide document authenticity, integrity, and origin assurances, but don't need a visible signature line. Documents with a non-visible signature display a red ribbon in their task bar.

Visible

Visible digital signatures appear as a signature line, similar to a physical document. This method is commonly used when you need multiple users to sign documents like contracts or other agreements



Contact us for more information about document signing certificates.

www.globalsign.com | sales@globalsign.com