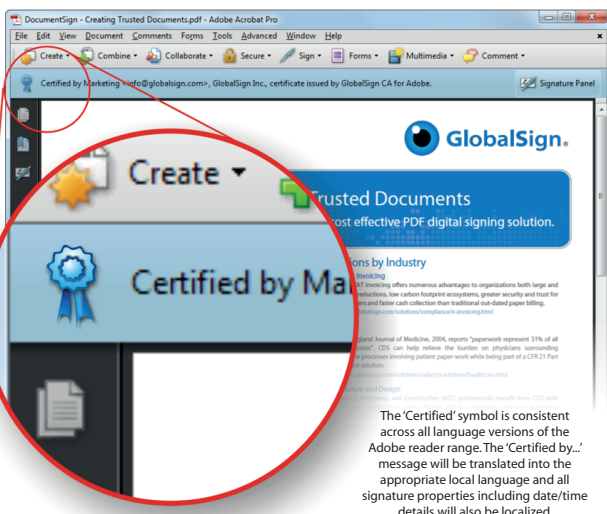# GlobalSign®

PDF Signing for Adobe CDS - PAdES - Best Practice - Timestamping
Certified Document Services (CDS) provides a cost effective PDF digital signing solution.
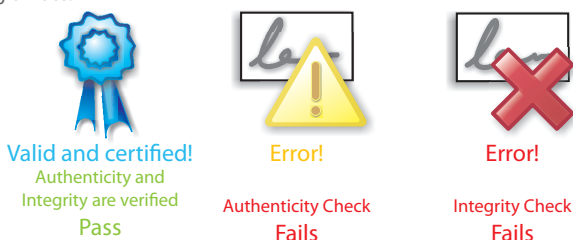
How to create trusted documents with CDS

Certified Document Services (CDS) is a service which is enabled by the Adobe Root Certificate Authority and was introduced into the Adobe® Acrobat® product range supporting SHA-256 from version 7.0 onwards. CDS empowers document authors to digitally sign Portable Document Format (PDF) files, using an industry standard X.509 digital certificates chained to the Adobe Root Authority to allow automatic validation of authenticity of the author using the free Adobe Reader software. No additional client software or configuration is required.

A major advantage to any organization with stakeholders in multiple countries, is the built-in international language support within the PDF reader itself. Available in over 30+ languages, Adobe Reader ensures a consistent digital signature experience worldwide. CDS was designed specifically to enable any organization providing documents to large and disparate recipients, who may be in multiple countries, to increase the assurance level of the document. The document's integrity and authenticity are digitally preserved by the addition of the CDS signature to the PDF. Document authors are able to increase this assurance level without requiring recipients to deploy additional processes - it simply works, ensuring an effective ROI through a vast reduction in the investment normally associated with supporting a proprietary security system.

The 'Certified' symbol is consistent across all language versions of the Adobe reader range. The 'Certified by...' message will be translated into the appropriate local language and all signature properties including date/time details will also be localized.

Following a thorough verification of the 'Applicant' requesting a PDF Signing for Adobe CDS certificate, GlobalSign will issue a 'pickup' link which allows a certificate to be generated and securely stored on a SafeNet® hardware cryptographic device. Authors can digitally certify PDFs using certificates "chained" up to the trusted Adobe Root. Recipients simply need to open the document using the Adobe free reader to instantly verify the authenticity and integrity of the document. Adobe's simple to interpret "Blue Ribbon, Yellow Warning Triangle, and Red X" trust messaging allows even novice users an easy to understand method to determine if the document is legitimate.

Valid and certified!
Authenticity and Integrity are verified
Pass

Error!
Authenticity Check
Fails

Error!
Integrity Check
Fails

For more information about GlobalSign solutions, please call 603-570-7060 or 877-775-4562

Visit www.globalsign.com for more information

International Standards and Best Practice

Security through obscurity does not suit delivery of products and/or services to a mass market via the Internet. The Internet itself is a generic service, where as PKI (Public Key Infrastructure) is a highly suitable security service for the Internet and delivering trusted documents.

Whilst 800M+ users worldwide have access to the Adobe PDF reader, is PDF not a proprietary standard? The answer is no, in that PDF is an International Standards Organization (ISO) standard (ISO 32000-1) and equally importantly the signature mechanisms built into Adobe Acrobat, Reader and LiveCycle ES conform to a European Standard. ETSI/ESI Technical Standard (TS) 102 778, better known as PAdES (pronounced with either a long or short a), highlights how the digital signature format described in ISO 32000-1 meets the needs of the 1999 EU Signature Directive.

Part 1: "PAdES Overview - a framework document for PAdES"
Part 2: "PAdES Basic - Profile based on ISO 32000-1" (Best Practice)
Part 3: "PAdES Enhanced - PAdES-BES and PAdES-EPES Profiles"
Part 4: "PAdES Long Term - PAdES-LTV Profile"
Part 5: "PAdES for XML Content - Profiles for XAdES signatures"

This document you are viewing conforms to Part 2 and as best practice embeds a copy of the certificate used to sign the document, the status of the certificate (via a Certificate Revocation List) and also a digitally signed Timestamp. All versions of Acrobat reader can use the Timestamp (including expired timestamps) to effectively allow the trust status of the document to last as long as the underlying cryptographic technology is secure.
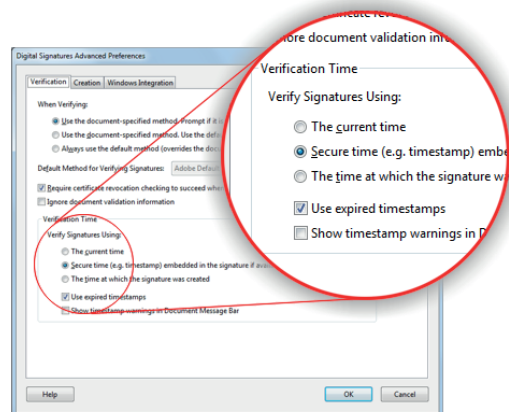
The SafeNet Range (USB & HSM)

GlobalSign's PDF Signing for Adobe CDS Certificates are usually provided with either a SafeNet iKey 4000 (SHA1 capable) or a SafeNet iKey 5100 (SHA256 capable). As an extension of smart card technology both keys plug into any USB port to provide strong portable user authentication without the need for costly reader devices. Certificates installed on to either token ensure regulatory compliance with the FIPS 140-2 Level 2 requirements of the Adobe CDS program.

For organizations with high volume signing requirements or the need for automation, GlobalSign is able to provide a HSM (Hardware Security Module) in either PCI, PCI(e) or Network attached. In addition, GlobalSign's ePKI (Enterprise PKI) solution is available for companies that require multiple digital identities. The ePKI platform is a simple, easy to use web-based portal for non-technical managers with around the clock access for issuing and managing Digital IDs. All Digital IDs are issued from pre-vetted legal identities (Certificate Profiles) ensuring that proper audit trails are in place for true transparency. Full Digital ID management features (issuance, renewal, reporting and revocation) are accessible 24/7 – essential for organizations operating globally and often with temporary resources or partnerships.