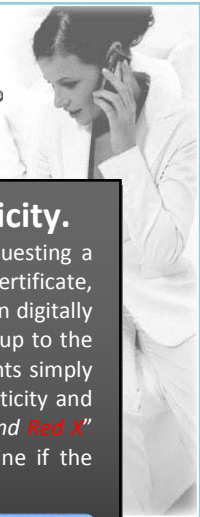


DocumentSign™ - Certifying and Signing Options

Digital IDs for the Adobe PDF Platform: Certified Document Services (CDS)



Certified Document Services

Certified Document Services (CDS) is one of the services enabled by the Adobe root certificate authority. CDS enables document authors to sign Portable Document Format (PDF) files, using standard digital certificates, which automatically validate when authors are using free Adobe® Reader® software. No additional client software or configuration is required.

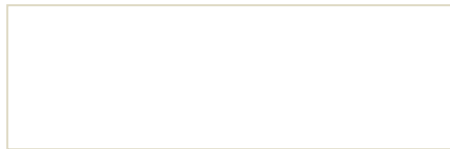
CDS was designed to enable organizations and individuals who publish high-value documents to large and disparate recipient groups to increase the assurance level that the document's integrity and authenticity are preserved. By adding a CDS signature to a PDF file, document authors can increase this assurance level without requiring recipients to deploy additional software.

Which Versions of PDF reader support Certified Document Services?

The technology to allow digital signatures to be incorporated into PDF documents first appeared with version 5.0 of the Adobe Acrobat Reader product. The blue security bar was introduced with version 8.1 of the product suite (including the free reader) to ensure a greater level of visual impact and therefore a higher level of trust and assurance than the previous versions.

To Certify or to Sign?

By way of illustration, this document features two digital signatures. The first signature applied to the document was a **certification** signature where the author of the document attested to the accuracy of the content. An **approval** signature is shown in the box below:-

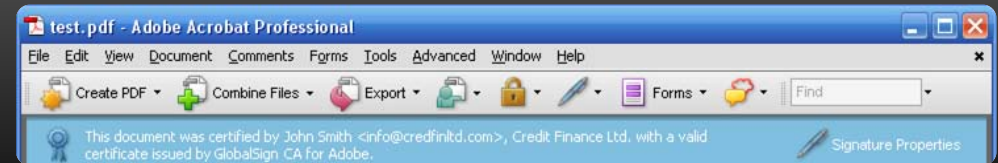


As an example document flow, the original document could have been counter signed by several parties in alternative organizations as part of an approval process.

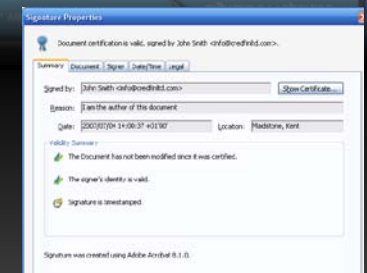


Certification Signatures – The initial indication of authenticity.

Following a thorough verification of both the individual and / or the organization requesting a DocumentSign digital ID, GlobalSign will issue the digital ID in the form of a Digital Certificate, securely stored and protected on a SafeNet® hardware cryptographic device. Authors can digitally certify PDFs (desktop and server-based solutions available) using certificates “chained” up to the trusted Adobe Root. Approval signatures may also be applied at a later stage. 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, Question Mark, and Red X*” trust messaging allows even novice users an easy to understand method to determine if the document is from a legitimate source.



By clicking on the signature properties, recipients can view additional information, such as signing certificate details including information about the certificate policy, signer’s contact information, Certificate Revocation information via embedded Certificate Revocation List (CRL) details and time-stamping information which are the foundation for strong authentication, long term validity, data-integrity and non-repudiation of the signature. Enterprises no longer need to fear their brand and reputation are at risk in the event a legitimately authored PDF is maliciously modified and falsely re-circulated under their name.



Modified/Changed
Potential issue!



Unknown Author
(Revoked, Expired or non trusted Digital ID)
Potential issue!



Certified
Trusted

Remember! For the highest assurances of who created a document, look for the Blue Security Bar and Blue Rosette.