

# DocumentSign™ - Compliance with CFR 21 Part 11

Certified Document Services (CDS) provides a cost effective PDF digital signing solution



## Who needs to be aware of CFR 21 Part 11?

Pharmaceutical stake holders such as drugs manufacturers, medical device manufacturers, biotechnology companies and biologics developers together with any enterprises regulated by the FDA need to be aware of the requirements for CFR 21 Part 11 compliance. In the competitive world of life sciences it is crucial to benefit from the efficiencies offered by electronic communications. If your organization is involved in clinical trials, virtual office communications and the movement of any sensitive electronic information including medical device quality control records or any type of electronic submissions to the FDA, then you need to carefully consider this important federal regulation.

## CFR 21 Part 11 Background

Part 11 was developed in response to the soaring costs associated with managing the distribution, storage, and retrieval of records used in conjunction with the FDA. Additionally, security concerns surrounding wet ink signatures surfaced as it became apparent these signatures including the content they were attesting to could be easily falsified. Title 21 of the Code of Federal Regulations; Electronic Records; Electronic Signatures (21 CFR Part 11) outlines the standards for use of electronic records and signatures in FDA-regulated activities, including clinical trials and pharmaceutical manufacturing. Part 11 in particular applies to records in electronic form that are created, modified, maintained, archived, retrieved, or transmitted under any records requirements set forth in Agency regulations. Part 11 also applies to electronic records submitted to the Agency under the Federal Food, Drug, and Cosmetic Act (the Act) and the Public Health Service Act (the PHS Act), even if such records are not specifically identified in Agency regulations

CFR Electronic Signature and Records Requirements	Areas CDS can help Organizations comply
11.10 Controls for Closed Systems	
11.30 Controls for Open Systems	
11.50 Signature Manifestations	
11.70 Signature/ Record Linking	
11.100 General Requirements	
11.200 Electronics Signatures Components and Controls	
11.300 Controls for Identifications Codes/ Passwords	

## Which Versions of PDF reader support Certified Document Services?

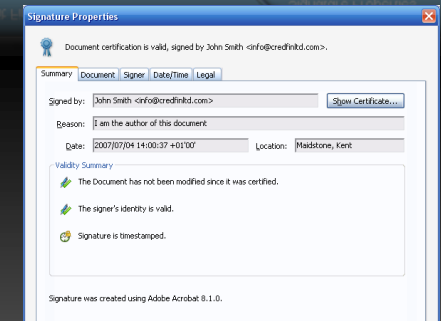
The technology to recognise inherently trusted digital signatures incorporated into PDF documents first appeared with version 6.0. The blue security bar was introduced with version 8.1 of the product suite (including the free reader) to ensure a greater level of visual impact and therefore a higher level of trust and assurance than the previous versions.

## How it works...

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, on-line certificate status protocol (OCSP), and time-stamping details that become the foundation for strong authentication, data-integrity and non-repudiation of the transaction.



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.**

# DocumentSign™ - Who benefits from CDS

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



### Manufacturer and Design:

Architecture, Engineers, and Construction (AEC) professionals benefit from CDS with faster design collaboration, more efficient and less expensive electronic document storage, and stronger protection via tamper evident engineering and product documentation as documents are exchanged among customers, partners, contractors, and building departments.

### Education

More and more educational institutions are increasing student and alumni satisfaction as universities and colleges disseminate sensitive documents like transcripts and admissions letters electronically in a fraction of the time and costs seen with their paper equivalent.

### Government

CDS supports both local and federal government initiatives including the Government Paperwork elimination Act helping reduce costs, enhance citizen accessibility to government information, and reduce unnecessary environmental waste while at the same time providing high assurances to its citizens that the information is legitimate.

### Financial Services

Industry best practices coupled with government imposed regulation like Sarbanes-Oxley make CDS an attractive option as a thorough audit of the signature properties are embedded in the document itself. Well after the Digital ID expires, the signature characteristics are preserved providing relying parties strong authentication of both the organization and individual or role that signed the PDF, whether the content is still intact, and the exact date and time of the transaction as determined by a RFC 3161 compliant time-stamp.

### The Notarial and Legal professions

CDS provides unequalled support of trusted documents in multiple languages. This alone facilitates increased cross border transactions as both sides are able to interrogate the authenticity of a document in their local language; *the ideal solution for e-Notarization.*

### 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.



### Solution Highlights...

**PersonalSign™ Pro Digital ID** for Adobe PDF is a desktop solution designed for individuals and organizations with low volume requirements. Authors can certify PDFs using Adobe® Acrobat® or Adobe® LiveCycle® solutions and a GlobalSign DocumentSign™ Digital ID securely stored on a cryptographic device. For low volume requirements this is a SafeNet FIPS 140-1 level 2 USB token. *(highlighted below)*

**DepartmentSign Digital ID** for Adobe PDF is an automated PDF digital signing solution designed for organizations with medium volume requirements. A role-based credential e.g. 'Marketing Department' is issued and its corresponding private key securely protected on a SafeNet FIPS 140-1 level 2 cryptographic device such as a Luna® PCI HSM (Hardware Security Module)

**CorporateRA Digital ID** for Adobe includes two options for the Enterprise to manage the full life-cycle of Digital IDs issued under their organization name. i.e. Individual signing USB tokens or central-based credentials for either role-based signings or server held individual Digital IDs. Distributed implementations involve providing organization administrators (acting as the organization registration authority) a bulk shipment of Safenet USB tokens which work in conjunction with Acrobat Standard/Professional/3D. Centralized, server-based implementations work with SafeNet hardware security modules (optionally sold) that are highly integrated with Adobe's LiveCycle Enterprise Server suite. The net result is a highly automated solution with robust signing functionality..



*SafeNET iKey™ 2032 USB Cryptographic security comes as standard for all PersonalSign and PersonalSign professional solutions – Portable/Flexible/Reliable*

For more details on being safe online with DocumentSign contact GlobalSign: [www.globalsign.com](http://www.globalsign.com)

[support@globalsign.com](mailto:support@globalsign.com)

US: 866 511 5035

UK: +44 1622 766766

EU: +32 16 89 19 00

JP: +81 03 5728 1551