

# A<sup>TM</sup>DOCS<sup>TM</sup>

cloud-based document workflow and digital signature approval

Online document viewing and signing for internal and external users with full tracking of the business document approval process

Individual user keys and certificates are used to create advanced digital signatures on PDF and PDF/A documents

Available as a commercial cloud service and also as a software product for local deployment - you choose!

Organisations can now quickly optimise the way they create, transmit, review, approve and sign their key business documents using ADocs from Ascertia.

Substantial cost savings can be made when paper based processes are moved full on-line including print and send costs as the costs of searching and re-sending. For certain documents **traceability, accountability** and audit with clear **legal integrity** and **individual signed approval** are vital. Indelible digital signatures enable the on-line approval of any business documents such as agreements, orders, reports, insurance, expenses etc. Organisations need to show that their internal controls are effective and compliant with local legislation, regional directives and market expectations. And increasingly they need to demonstrate their commitment to the environment.

ADocs provides (or uses existing) e-IDs to create **advanced digital signatures** for persistent document security. The interface is intuitive and makes it easy for busy managers that want to use a system without being baffled by technology. ADocs provides a simple to use, document sharing, viewing and sign-off solution suited to any approval process. It cleverly implements industry standard advanced digital signature security to enable sign-off from anywhere!

## Why use ADocs?

- ➔ Use it as an internal or external cloud service product
- ➔ It's simple to register and easy to use via a web-browser
- ➔ Meets EU Qualified Signature requirements and creates [long-term PDF standard digital signatures](#)
- ➔ It uses unique signing keys for each person and supports existing CAs, TSAs or offers internal options
- ➔ Supports PDF and PDF/A documents - other document formats can be converted to PDF/A
- ➔ Central signing keys can be authorised using strong OTP authentication sent via SMS to a user's mobile phone
- ➔ Implements real-world scenarios such as group signing, delegated signer, document recall etc

## How it Works

### Upload

Log-in and upload your documents to ADocs. Documents can be in PDF or converted to PDF from various other formats. PDF/A is also supported for long-term rendering and accessibility.

### Prepare and Send

Prepare a document by positioning each user's signature field in the desired order and location. Define any restrictions such as local save, local print, date embargos (or just use an existing template), now simply "send" the document.

### Review and Sign

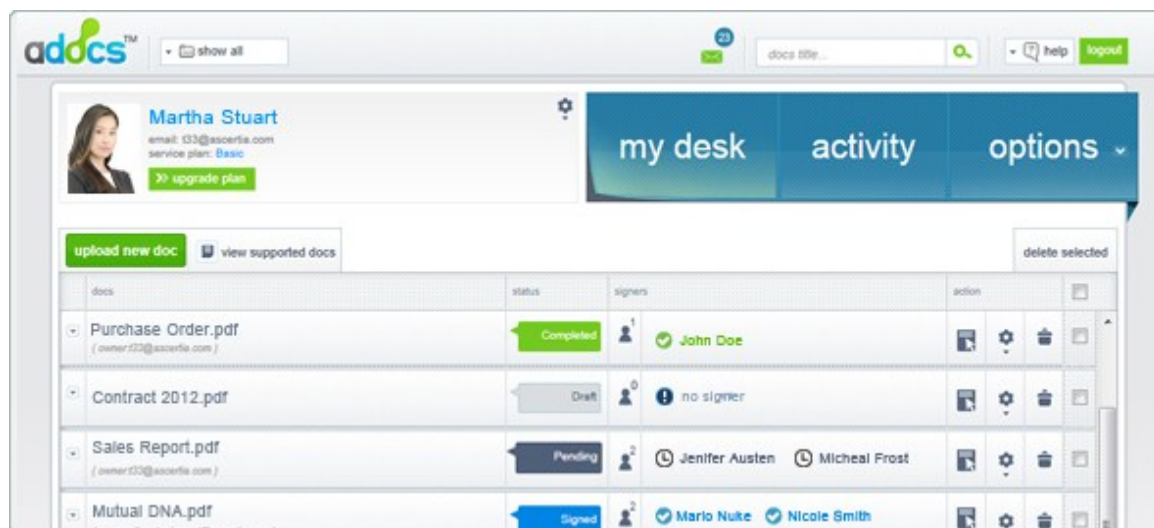
Each collaborator is notified when their approval is required. They review documents within the ADocs secure viewer and click to sign the signature field reserved for them. The next signer is notified and the workflow continues.

### my desk overview

This screenshot shows a user's ADocs "my desk". Multiple documents can be seen with their current status showing.

Documents are shown within the secure document viewer. Existing signatures are shown with their trust status clearly shown.

Document owners can review the status of documents sent for others to review and approve.



## No Local Software

ADocs is a web-application and so users do not need to install or manage any local software. All that is needed is a standard web browser and an Internet connection, now users can view, sign and verify any document, from anywhere, at any time.

## Management

ADocs manages multiple end users as part of the internal or service offering. For commercial service use ADocs includes an e-commerce module that can charge users (or enterprises) on a monthly, quarterly or annual basis.

## Fully Interoperable

ADocs uses standard PDF PAdES signatures including Certify signing. This means that signed documents can be verified by anyone with the freely available Adobe® Reader. Each user has a unique signing key and certificate held securely within ADocs or locally on a smartcard or USB token or software store. All X.509v3 and eID certificates can be used.

## Visible Signatures

Each user can configure a personal signature appearance to be stamped on the document at the time of signing. Administrators can optionally set corporate logos for branding. Dynamic hand-signature images can be captured using tablet or mouse movements. Ascertia Docs controls the signing process so that users can only sign when it is their turn and only in their assigned signature fields.

## Data Leakage Protection (DLP)

Good DLP features are provided within the system and document viewer. All documents are AES-256 bit encrypted in the database. All connections are over encrypted SSL/TLS sessions. The document owner can set the access rights for each collaborator. These include rights (or restrictions) to download the document, print the document, set and enforce embargo dates for viewing the document.

## Document Tracking

All document actions are recorded and these include the upload time, the time it was shared, when it was viewed and by whom, when it was signed and by whom. Each revision of the document can be saved and viewed by the document owner if required

## Share Profiles

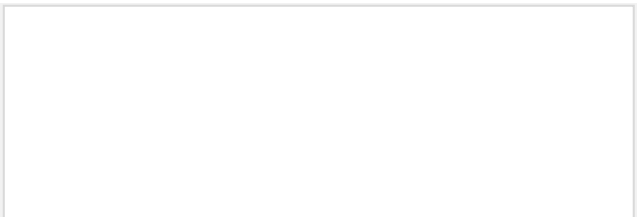
Often documents are shared with the same people and signed in the same places. Instead of defining the document sharing process each time, you can save these configurations as share profiles and automatically apply them to future documents that need to be processed using the same approval process. For detailed list of features and see: [www.ascertia.com/Products/ADocs.aspx](http://www.ascertia.com/Products/ADocs.aspx)

# Key Features



ADocs Standards Compliance	<b>Signature Formats</b>	PDF & PDF/A Signatures, including PAdES Long-Term Signatures
	<b>Platforms for clients</b>	Windows & Unix/Linux – Browser support includes IE 7+, FireFox 3+, Chrome, Opera
	<b>Server Host Machine(s)</b>	Windows 2003 and 2008 (32-bit and 64-bit) with SQL Server 2005 & 2008 (and Express)
	<b>HSMs (Host Machine)</b>	HSMs are supported - PCI or network HSMs from SafeNet and Thales nCipher
	<b>PKI standards</b>	PKCS#7, PKCS#11, PKCS#12, RFC 5280, SSL/TLS
	<b>Back-end Interface</b>	OCSP (over HTTP/S), LDAP/S and HTTP/S for CRL Retrieval, OASIS DSS

**Ascertia Limited**  
**Web:** [www.ascertia.com](http://www.ascertia.com)  
**Email:** [info@ascertia.com](mailto:info@ascertia.com)  
**Tel:** UK: +44 1256 895416  
 US: +1 508 283 1890



Try it **FREE** here:  
<http://www.SigningHub.com>