A World-Class Document Workflow and Digital Signature Approval Product

Lawtrust information security solutions

SigningHub

SigningHub enables any organisation to quickly optimise the way they create, share, review, approve and securely sign their business documents.

Electronic Signatures are perfectly acceptable in any form of business agreement and are recognised by most national laws. SigningHub holds and presents documents securely plus cuts time, reduces costs and adds strong controls to minimise signing errors.

Significant cost savings can be made when paper-based processes are moved on-line. For some documents it is vital to ensure **traceability**, **accountability and audit** with clear **legal weight, data integrity** and **individual signed approval** together with easy to access **workflow process evidence**. SigningHub enables quick, efficient on-line approval of any business document, agreement, report, request or package.

SigningHub supports **basic e-Signatures and Advanced E-Signatures**. The best way to prove a document is unchanged from the time of signing is to use cryptographic digital signatures. Organisations need to show that their internal controls are effective and compliant with local legislation and regulations.

Ascertia has offered world-class PKI products for years. SigningHub brings together all of this capability and knowledge to provide the most secure way to sign documents. SigningHub is focused on the high trust, top-end of the market and can use existing national and international PKI schemes, other high trust certificates including those trusted by Adobe Reader and Word for **persistent document security**.

The web interface makes it easy for anyone to sign. Documents can be shared, viewed and signed on any device, anywhere, anytime in a way that suits any approval process. Over 20 languages are supported and others can easily be added or customised.

Why SigningHub?

- A product that can be used in-house, in-country, or via our cloud service
- All documents are protected using AES-256 bit encryption
- It can use Advanced Electronic Signatures, or with high trust certificates with automatic trust in PDF Readers, or other PKIs
- Supports Qualified Remote Signatures with Level 2 Sole Control
- All signing evidence and workflow process evidence is made available in digitally signed documents.
- Long-term PDF digital signatures including timestamps are created
- Supports PDF and PDF/A and Word documents
- Various user authentication options are supported AD, OAuth, SAMLv2
- It helps meets data protection and data residency requirements

How it Works

Upload

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

View and Sign

This image shows a typical view and sign screen. PDF or Word documents are shown within a secure document viewer. Existing signatures are shown with their trust status clearly shown.

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

Initials, form fields, tick boxes and other common document approval features are fully supported.

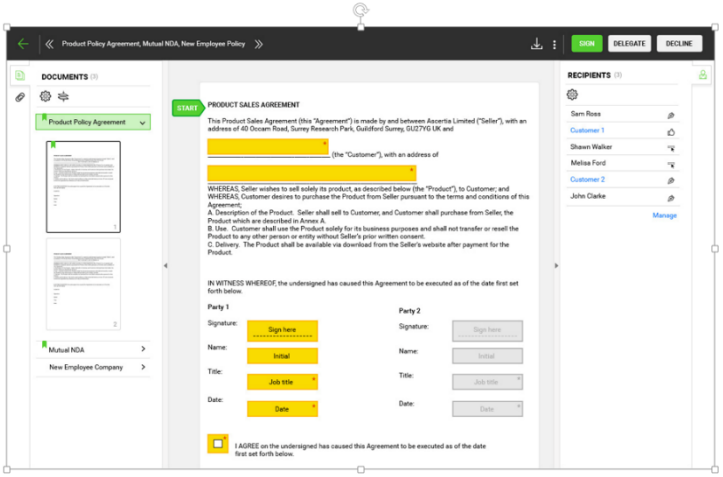
Workflow Preparation

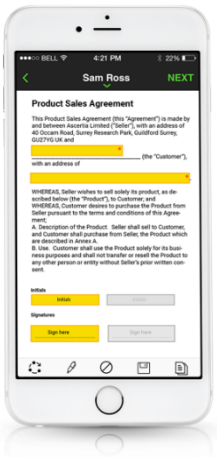
SigningHub supports templates which remember where every signature field and any other object such as initials must be placed and also which permissions must be applied. Now simply “Share” the document to send to other people or groups.

Workflow Management

Each recipient is notified when their action or approval is required. They view each document within the SigningHub secure viewer and click to sign the signature field reserved for them. The next signer is notified and the workflow continues.

Document View & Sign Screen



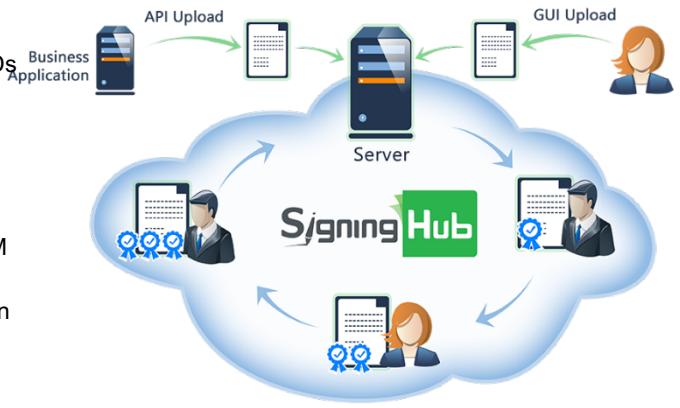


Key Features

Key Differentiators

Organisations can use the cloud service OR run their own private copy of SigningHub on-premise or in-country, they can control their own branding, use their own URLs, applications can be tightly integrated with SigningHub so that users believe that viewing and signing is a standard part of the business application itself.

SigningHub always creates long-term signatures and existing high trust eIDs and other certificates can be used. A solution option for Qualified Remote Signatures with Level 2 Sole Control is available.



Standard Integrations

SigningHub integrates with Active Directory, OAuth and SAMLv2 identity providers. Cloud drive integration is provided. SharePoint, Dynamics CRM and Salesforce apps are available. Other applications can be quickly integrated using the SigningHub Restful/JSON API. Contact us to check on the status of an available integration with your applications.

Fully Interoperable

SigningHub uses standard PDF PAdES and Word XAdES long-term signatures. This means that signed documents can be checked by anyone with Adobe Reader other PDF readers or for Word documents Word 2013 or Office 365 other compatible software.

Visible Signature Options

Visible signatures can be designed to suit the business need. We recommend a personal e-signature image be included as well as the user's name and the time and reason for signing. Any number of appearances can be created and use including the use of corporate logos for branding purposes. Dynamic hand-signature images can be captured using tablet or mouse movements.

Strong Security and Workflow Process Evidence

SigningHub encrypts all documents using AES-256 before storage in the database. All web-sessions use SSL/TLS v1.2 encryption. All digital signature use SHA-256 and RSA 2048 or stronger, with trusted timestamps to ensure strong signing time evidence. The document owner can set the access rights for each collaborator. These include rights (or restrictions) to download the document, print the document, as well as to set and enforce embargo dates for accessing and viewing the document.

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 and their IP address. SigningHub controls the signing process so that users can only sign when it is their turn and only in their assigned signature fields. A long-term signed Workflow Evidence Report is available to capture all details of the workflow process actions. This PDF is able to be exported to ensure that all relevant information can be retained within the business application, or within a document management system. This is vital with using a cloud service.

Workflow Templates

Often documents are shared with the same people, same permissions and signed in the same places. All of these details can be saved within a workflow template and can be automatically applied to other documents that need to be processed in the same way.

For further information refer to www.signinghub.co.za

SigningHub Standards Compliance

Signature Formats	PDF, PDF/A and Word 2013 signatures, including PAdES & XAdES long-term signatures
Platforms for clients	Any modern HTML5+ desktop or mobile browser
Server Host Machine(s)	Windows Server 2012 and R2 with SQL Server 2012, 2014
HSMs (Host Machine)	Options for Gemalto/SafeNet, Thales nShield, Utimaco, plus Azure & AWS HSMs
PKI standards	All relevant PKI standards are supported, SSL/TLS v1.2, AES-256 bit document encryption
Back-end Interfaces	A Restful/JSON API, plus certificate checking using OCSP, CRL over LDAP/S and HTTP/S

LAWtrust
Web: www.lawtrust.co.za
Email: info@lawtrust.co.za
Tel: +27 (012) 676 9240

Lawtrust information security solutions