SigningHub

Document workflow and digital signature approval.

SigningHub enables organisations to transform paper-based processes into sophisticated digital workflows and to securely sign and seal documents using digital identities, backed up by a legally-reliable audit trail. SigningHub offers high throughput and high availability and is scalable to meet the needs of enterprises of all sizes and Trust Service Providers offering a white-labelled solution.

SigningHub Overview

SigningHub enables efficient, paper-free approval of any business document, agreement, report, request, or package. It supports basic e-signatures, Advanced e-Signatures and EU Qualified Signatures to give document owners complete control over the level of assurance across all use cases.

Highly-granular enterprise-grade controls ensure full **traceability**, **accountability** and **auditability of the document** approval process, while guaranteeing **data integrity** and providing legally reliable **workflow process evidence**.

Ascertia's expertise in public key infrastructure (PKI) technology means that SigningHub can support both in-house PKI systems and publicly trusted trust service providers for cryptographic digital signatures. Multiple deployment options spanning On Premise, Public Cloud, Private Cloud and hybrid options offer customers maximum control over data flows.

Signing keys can be held locally by the signer (e.g. a smartcard or USB token) or in secure cloud-based servers operated by Trust Service Providers that implement the Cloud Signature Consortium (CSC) technical standard for remote digital signing, enabling legally valid digital signatures in jurisdictions across the world.

The fully accessible web interface and fully responsive design makes it easy for anyone to share, view and sign documents 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. Customizable UI elements and colour configurations offer extensive branding controls.

A complete set of APIs means that all SigningHub functionality can be accessed programmatically via integrations with other business applications. has a Restful/JSON API to integrate with existing web-applications.

Key Features

- **PKI Flexibility**: It can use public Trust Service Providers, including EU Qualified certificates, organizational PKI systems, or Ascertia default certificates for different levels of assurance
- **Standards Compliant**: Supports Qualified Remote Signatures with Level 2 Sole Control per the EU eIDAS Regulation,
- **Accessibility**: Complies with Web Content Accessibility Guidelines v2.1 at level AA.
- **Document Standards:** Supports standard document formats including all relevant PDF and PDF/A standards and Microsoft Office formats.
- **High-Availability**: SigningHub is well proven at offering high availability and scales to meet the most demanding business needs.
- **Protection of data:** All documents are protected using AES-256 bit encryption
- **Flexible Deployment**: Can be delivered as an installable product in-house, via Ascertia's cloud service or via one of Ascertia's global Service Providers.
- **Flexible user authentication**: SigningHub provides many authentication options including Microsoft Active Directory, OAuth, SAMLv2, OpenID Connect-based ID providers and many more.
- **Digitally Signed Evidence**: All user operations are made available in a digitally signed report that details all interactions with a document and workflow.

How SigningHub 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.

Workflow Preparation

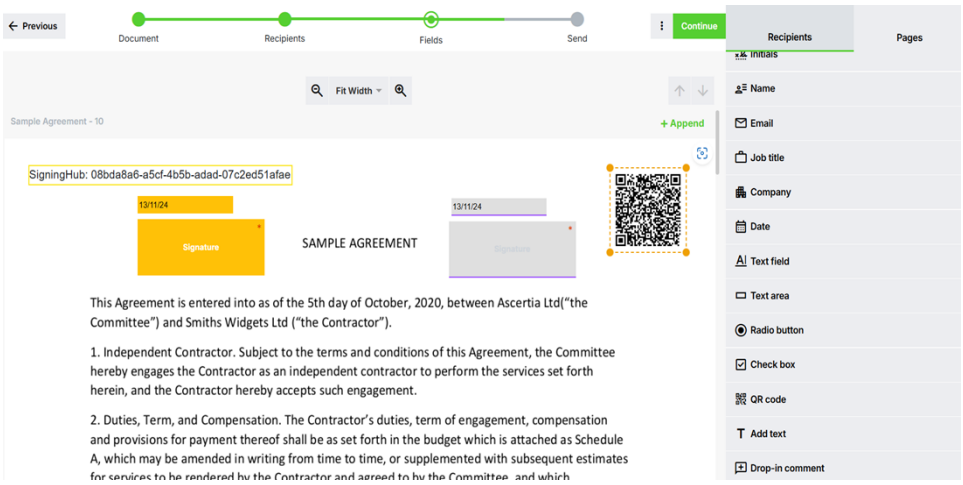
SigningHub supports templates which remember where every signature field and any other object such as initials must be placed, and which permissions must be applied. Now simply “Share” the document to send to other people or groups.

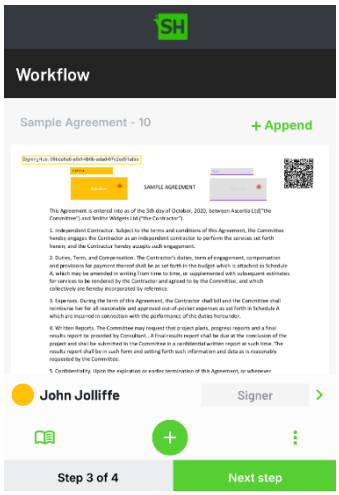
Workflow Management

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.

View and Sign

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.





Standard Integrations

SigningHub integrates with Active Directory, OAuth and SAMLv2 and OpenID Connect (OIDC) 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

Interoperability

SigningHub uses standard PDF PAdES and Word XAdES long-term signatures. This means that signed documents can be checked independently of SigningHub by anyone with the appropriate document reader such as Adobe Reader, 3rd party PDF readers or Microsoft® Word, Office 365 or other compatible software.

Signature Options

Visible signatures can be designed to suit the business need including a personal e-signature image, the user’s name, the time and reason for signing, and the use of corporate logos for branding purposes. Dynamic hand-signature images can be captured on the user’s own device using tablet or mouse movements, or via dedicated compatible signature pads.

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.

Document Security

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 can 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.

Key Differentiators

Organisations can use the Ascertia cloud service, run their own private instance of SigningHub on-premise or leverage one of Ascertia's global Trust Service Providers. In addition they can control their own branding, use their own URLs, and applications can be tightly integrated with SigningHub so that users experience document signing processes within the business application itself.

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

SigningHub is an advanced digital signature workflow platform that supports flexible deployment options and offers multi-tenancy, provides role-based operator access controls and high availability configurations.

Secure web-based management is provided as standard together with advanced management configuration options and detailed reporting.

Supported Operating Systems:

Microsoft Server 2022, 2019, 2016

Supported Databases:

Microsoft SQL Server 2019, 2017, 2016
Oracle 19c
Microsoft Azure SQL Server

Signing Server Support

Ascertia ADSS Server v8.3.6, 8.3.5 and 8.34
Ascertia ADSS Server via CSC 1.0.4.0
3rd Party RSSP via CSC 1.0.4.0
3rd Party RSSP via eID Easy API

Signed by:John Benedict Jolliffe
Signed at:2025-06-26 11:57:01 +02:00
Reason:I approve this document

John JOLLIFFE | Product Manager

About Ascertia

Ascertia provides digital trust for people, devices, data and documents for everybody from individuals to Enterprises and Governments. Ascertia's PKI and digital signature technologies serve a global customer base and partner network via direct and indirect sales channels.

For more info

info@ascertia.com

www.ascertia.com