SigningHub – Release Notes

This document provides a high-level description of the new features in each release of SigningHub.

SigningHub 8.0	October 2021

<u>New Features</u>

- Cloud Signature Consortium (CSC) (SHE-19859, SHE-22601, SHE-22743)
    - SigningHub now supports the Cloud Signature Consortium (CSC) v1.0.4.0 API protocol. This enables administrators to configure any Remote Signing Service Providers (RSSP) that is compliant with the 1.0.4.0 API for signing documents.
- Signature and Signature Label updates (SHE-29239)
    - "PAdES Part 2" PKCS#7-LT signatures have now been replaced with "PAdES-B-LT" ETSI compliant signatures. In addition, "PAdES Part 4" labelling within SigningHub has now been updated to "PAdES-B-LTA" for adhering to the current ETSI standards.
- Levels of Assurance for Digital Signatures (SHE-18526, SHE-27176, SHE-25398, SHE-7392)
    - The Document Owners can now mandate for the minimum Level of Assurance against the certificates used for digitally signing documents. Recipients will be able to sign the documents with only those certificates that comply with the Level of Assurance configured by the Document Owner.

      Within the Document Viewer, the "Electronic Signature" and "Digital Signature" signature field types have been merged into a single field, called the "Signature". The Level of Assurance can be specified against the signature field. Supported Levels of Assurance include: Electronic Signature, Electronic Seal (eSeal), Advanced Electronic Seal (AdESeal), Qualified Electronic Seal (QESeal), Advanced Electronic Signature (AES), High Trust Advanced Signature (AATL), Qualified Electronic Signature (QES).

      For customers operating SigningHub internally or in territories outside of the EU, administrators can define their own friendly names and abbreviations for the Levels of Assurance, which will replace the default names and abbreviations.
- Microsoft Azure Active Directory and Office 365 on Mobile Apps (SHE-23722)
    - Enterprise administrators can now configure Microsoft Azure Active Directory and Office 365 authentications while signing a document on the mobile web and native apps (Android and iOS).
- ECC & ECDSA Signature Algorithm (SHE-28956)
    - SigningHub now supports ECDSA based certificates.
- Bulk Signing in Mobile Web and Native Apps (SHE-28899)
    - SigningHub users can now perform Bulk Signing using mobile web and native apps (Android & iOS).
- TSAs for Document and Signature Timestamp (SHE-26549)
    - Administrators can configure separate Timestamp Authority (TSA) servers for signature and document timestamping.

<u>Improvements in this Release</u>

- Certification Profile and Witness Signatures (SHE-22339)
    - The term "Witness signing" has been deprecated. All signing profiles previously configured for witness signing have now migrated to certification profiles. The default level of assurance for these profiles is eSeal. It is recommended to follow the upgrade guide or involve support team to avoid any confusion.
- PKCS#1 Raw Signatures (SHE-24927)
    - SigningHub now works with the centralised implementation of PKCS#1 to support multiple RSSPs via the CSC protocol. Signing Profiles in ADSS should now be configured to support PKCS#1.

- PDF/A Standard Compliance (SHE-27353)
  - SigningHub now retains document compliance to PDF/A standards for PDF/A compliant documents.
- Database Performance (SHE-25590)
  - Improvements have been made to deal with unnecessary refresh token generation. SigningHub now only generates against an authentication request if the previously generated refresh token has been expired.
- Document Locking (SHE-25100)
  - The Signing Server and Signing Service Profile ID for ADSS Server has been replaced with a Signing Profile under the Workflow Evidence Report and Document Settings (Lock PDF Fields) in SigningHub Admin configurations.
- Fonts and Signature Appearances (SHE-27171)
  - The option to manage fonts and Signature Appearances have moved from Signing Profiles to Service Plans to enable centralised management. SigningHub Admin can now configure a Service Plan to allow only selected signature appearances for Enterprises. Enterprise Owners and Enterprise Admins can further configure Enterprise Roles to allow only one or multiple signature appearances for Enterprise Users.
- Workflow Evidence Report (SHE-22638)
  - The Workflow Evidence Report now includes details of both third-party authentication and authenticated user to provide better visibility.
- Smartcard and USB Tokens for XML Signing (SHE-22561, SHE-22561)
  - XML signing can now be done using local smartcards or USB tokens, server held keys including Advanced and Qualified Remote Signing or via CSC signing services.
- Workflow Completion Report and Webhooks Configurations (SHE-25064)
  - Workflow completion report and Webhooks configurations are now available in one place under enterprise advanced settings.
- Multiple certificates for Remote Authorization (SHE-22744)
  - SigningHub allows ADSS Server generated signing certificates to be imported for a given user by a suitably authorised system admin. A system administrator can import multiple certificates for a user using a friendly capacity name.
- Resetting Password for a CSP User (SHE-27631)
  - SigningHub now allows resetting CSP user passwords at ADSS Server without requiring additional user authentication prompts.
- Displaying National Identity Number in the Signature Field and Appearance (SHE-19085)
  - National ID's can now be displayed in the reason field of the signature.
- Accessing Documents via Integrated Business Application (SHE-28013)
  - Document signers can now access the Document Viewer being prompted for login credentials while accessing SigningHub using an integrated business application.
- Document Signing Authentication for Signers (SHE-26425)
  - The Document Owners can now enter the mobile number of each signer separately for OTP authentication. "Document-level user authentication"" field has been renamed to "Document Access Authentication".
- Workflow Comments using RESTful APIs (SHE-24753)
  - The SigningHub REST APIs now allow a Document Owner or a recipient to add a comment to the workflow. The API also allows access to existing comments in a workflow.
- Enterprise Branding (SHE-20471, SHE-22686)
  - Enterprise Admins can now control the logo used in a custom enterprise roles signature. Custom logos are independent of the company logo.

- o Enterprise Managers can now control how enterprise users manage their signature logos. An enterprise signature logo image appears as part of the signature appearance, independent of the company logo.
- Controlling Signing Methods via Enterprise Roles (SHE-23109)
    - o Signing methods for web browsers and mobile apps are now controlled through the same configuration settings under the Enterprise Roles.
- Displaying Signature TimeStamp Policy ID under SigningProfiles (SHE-26682)
    - o SigningHub now provides the flexibility to configure separate TSA (TimeStamp Authority) Servers for document signature and document TimeStamp Policy IDs within signing profiles.
- Managing Permissions for Enterprise Guest Users to Change Signing Location (SHE-24096)
    - o This release provides Enterprise Admins with an option to allow or restrict the enterprise and guest users to change their default geographical location while signing the documents.
- Performance Improvements
    - o This release brings several performance improvements in different areas of SigningHub including Document Viewer, Enterprise Branding, management of SigningHub Contacts and Groups, Document Listing, document management, Enterprise user management, cache management, reports, third-party integrations, and signature fields
- Cleaning Document Logs after Generating Workflow Evidence Report (SHE-27838)
    - o System administrators can now configure the Service Plans to clean the Workflow History following the generation of the Workflow Evidence Report.
- Relocated the "Next Recipient" information under the Workflow Details Dialog (SHE-27177)
    - o Performance improvements have been made for the Documents listing page, recipient information is now displayed in workflow details instead of Documents Listing. To access the workflow details an icon is used in place of the three dots.

        The "next-signer" parameter in the GetPackages API response has been deprecated and has a static value of the empty string. In the next release, the "next-signer" parameter will be no longer available.
- Controlling Visibility of the "Start New Workflow" Option on Documents Listing (SHE-29281)
    - o Enterprise Admins can now configure the Document settings of an Enterprise Role to hide or show the "Start New Workflow" option on the Documents Listing page in the More Options menu.
- Displaying Legal Entity Identifier (LEI) Information on Signature Verification Result (SHE-21488)
    - o Where a certificate used for document signing has an LEI (Legal Entity Identifier) set as an extension, the LEI information now appears in the signature verification dialog in SigningHub, the LEI information in the verification dialog also provides a link to the LEI information at Global Legal Entity Identifier Foundation (GLEIF).
- Importing SigningHub E-Seal Certificate from ADSS Server (SHE-28471)
    - o SigningHub can now automatically fetch the eSeal certificate from ADSS Server using the Certificate Alias.
- Data Validation on Text Fields (SHE-26452)
    - o Document Owners can now require specific information to be provided by signers in documents based on data validation that is specified in a new text field option. The new "Validation" dropdown replaces the "Required" checkbox.
- OAuth2.0 Connector (SHE-24400)
    - o SigningHub Administrators can now create a connector for any third-party authentication provider that uses OAuth2.0 authentication protocol.

Discontinued Features

- Removed Default Service Plan (e-Signing Users) (SHE-26106)
    - The default Service Plan that used to be assigned to an unregistered user by the application now has been removed completely from Global Settings. Now an unregistered user will follow the document owner's Service Plan and assigned Enterprise Role (when document owner is an individual user then only service plan is applicable).
- Removed the "Next Signer" Parameter from GetPackages API (SHE-27177)
    - The "next-signer" parameter in the GetPackages API response has been deprecated and has a static value of the empty string. In the next release, the "next-signer" parameter will be no longer available.

SigningHub Product Compatibility

SigningHub is compatible with the following Ascertia Products.

Product	Version(s)
Go>Sign Desktop	6.9
SigningHub Mobile SDK – Android	8.0
SigningHub Mobile SDK – iOS	8.0
SigningHub (iOS)	8.0
SigningHub (Android)	8.0
ADSS Server	6.9.0.0

Compatibility with Earlier Versions of ADSS Server

SigningHub 8.0 is compatible with the 6.8.0.6 and 6.7.0.8 versions of ADSS Server except for the following features that are not supported.

ADSS Server 6.8.0.6
- Reset password for a CSP user without user authentication (SHE-27631)   - Automatic download of the eSeal certificate from ADSS Server for provided Certificate Alias (SHE-28471)
ADSS Server 6.7.0.8
- Reset password for a CSP user without user authentication (SHE-27631)   - Automatic download of the eSeal certificate from ADSS Server for provided Certificate Alias (SHE-28471)   - Cloud Signature Consortium (CSC) Signing (SHE-19859)

For further details contact us at sales@ascertia.com or visit www.ascertia.com

*** End of Document ***