



G-Cloud 15

Service Definition

SIGNINGHUB DIGITAL SIGNATURE SOLUTION SERVICE DEFINITION

G-CLOUD 15

LOT 2 CLOUD SOFTWARE

Lot 2b Software as a Service (SaaS)

ASCERTIA UK LTD

JAN 2026

Document Version-1.0

Contents

1. Introduction	3
Company Overview	3
Associated Services	5
2. Data Protection	6
3. Using the service	7
Ordering and Invoicing	7
On-Boarding, Off-Boarding, Service Migration, Scope etc.	7
Implementation Plan	8
Service Management	8
Service Constraints	10
Service Levels	10
Outage and Maintenance Management	10
Financial Recompense Model for Not Meeting Service Levels	10
4. Provision of the service	11
Customer Responsibilities	11
Technical Requirements and Client-Side Requirements	12
Development life cycle of the solution	12
After-sales Account Management	13
Termination Process	13
5. Our experience	14
Case Studies	14
Clients	15
Contact Details	15

1. Introduction

Company Overview

Ascertia is a successful global provider of advanced digital signature and electronic identity (eID) validation software solutions, recognised by leading Technology Analysts. Ascertia's products and business solutions focus on enabling high-trust within e-commerce environments through digital signatures and encryption of data at rest. With Ascertia, organisations can confidently complete the transition from paper-intensive processes to fully digital workflows, signing securely across desktop, mobile, and server environments.

Ascertia has a long and established history in the digital signature market and an excellent reputation for delivering products to a wide range of organisations and industries worldwide. Standards compliance and tracking of key standards are fundamental parts of our product strategy. This approach provides customers with long-term investment protection, enabling them to upgrade existing solutions quickly and seamlessly as new releases and features become available. It also underpins the long-term relationships Ascertia has built and maintained with many well-known organisations.

Ascertia adopts a pragmatic and responsive approach to working with partners and customers. Ascertia's strategy is to empower its staff with clear accountability and streamlined communication and approval processes, enabling rapid and effective decision-making. We listen, understand, and act appropriately to ensure the success of our partners and clients.

Value Proposition

SigningHub is a complete solution for document approval workflows, advanced digital signatures and document status tracking. It is designed to optimise how organisations deliver, review, approve and sign their business documents. SigningHub is available as a software product for on-premise hosting as well as a public or private cloud service.

For public sector organisations that require documents to remain valid into the future, SigningHub delivers long-term electronic signatures that are legally compliant and independently verifiable. SigningHub supports all levels of signatures, including EU-qualified signatures.

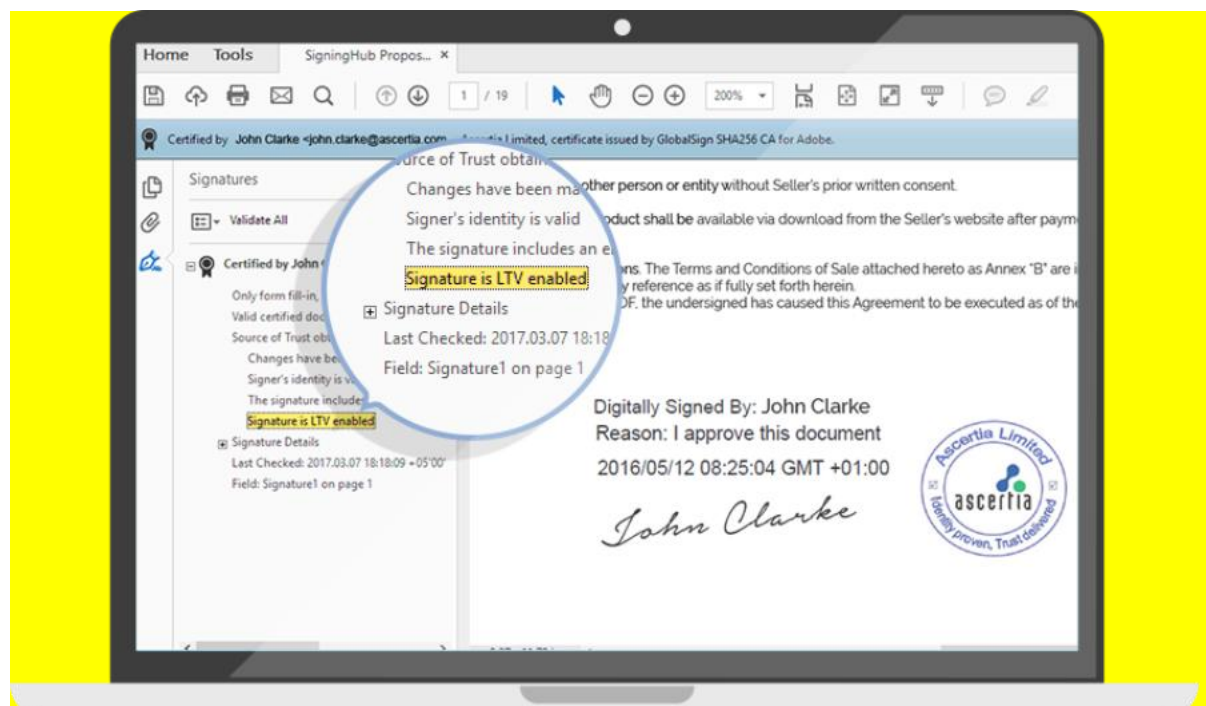
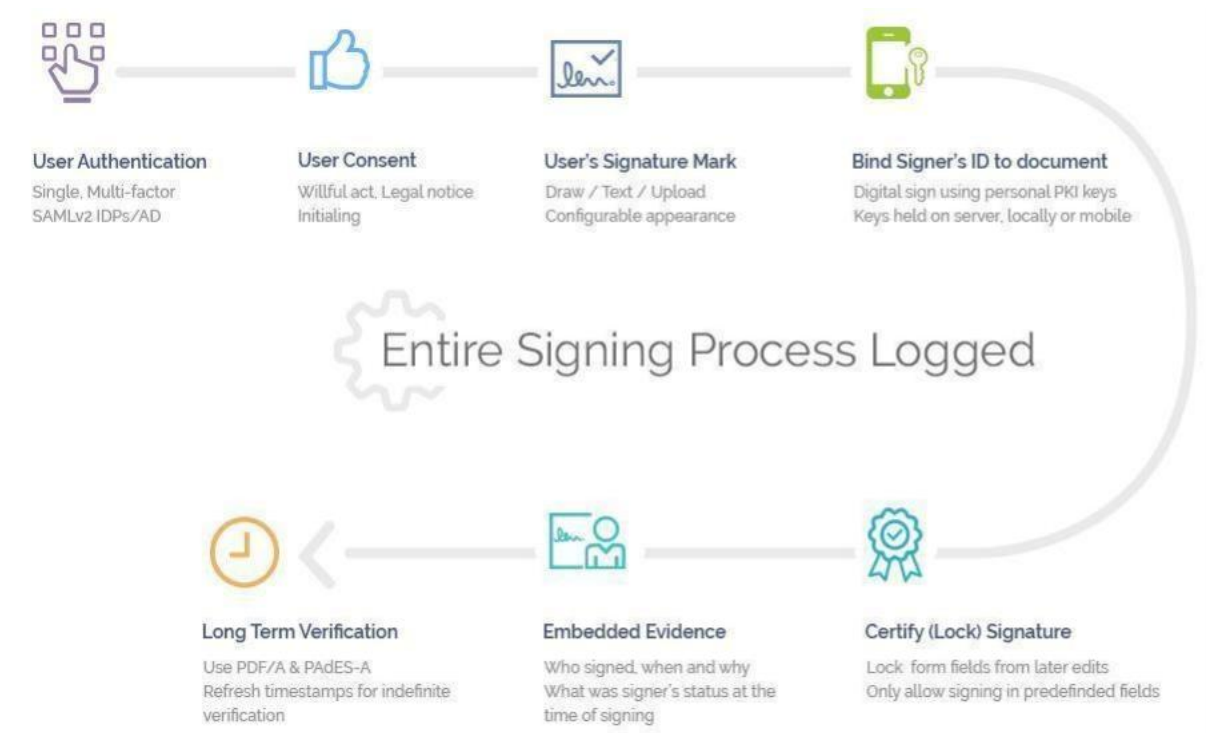
What the Service Provides

SigningHub is a secure digital signature and document workflow solution that enables organisations to eliminate inefficient paper-based processes, delivering significant time and cost savings. Documents can be securely sent to internal or external parties for review and sign-off. The service delivers strong security controls and legally binding signatures, including qualified signatures.

SigningHub allows users to select a document (supporting multiple file formats), upload it and share it with other defined users or groups for review and approval of the contents. Recipients are notified to review the document within a secure and confidential environment and are prompted to apply their digital signature where required. Users can also fill in the pre-existing form fields within the document.

SigningHub provides flexible and automated workflows that support a wide variety of business processes. Workflows can be initiated by any SigningHub user or by integrated business applications,

supporting both human and machine-driven processes. All common document types are uploaded and converted to PDF to take advantage of ISO 32000 and ISO 19005 long-term document preservation features. Visible signature appearances (such as handwritten-signature images, text and company logos/seals) help users easily identify that a document has been signed. Importantly, it is the cryptographic digital signature embedded within the signed document that provides user authentication, data integrity and non-repudiation security services, not just the signature appearance alone.



Current users of the service span a diverse range of industry sectors and organisation sizes. Typical customers are looking for a secure solution, hosted in Europe, compliant with the EU electronic signature standards, supports long-term, document longevity and ensures there is no lock-in proprietary approaches.

Associated Services

All core functionality of the service is available 24/7, including access via the SigningHub web application, APIs, and integrations.

API access is included as part of the service and enables customers to integrate SigningHub into their own systems and workflows. There are no separate bolt-on services required to access core functionality.

The service includes ongoing maintenance, platform updates, security monitoring, and infrastructure management, all of which are handled by Ascertia. Customers are not required to manage or maintain any underlying systems.

Support is included as part of the service, with 24/7 availability for the SigningHub.com platform. Full details of support levels are outlined in our SSP.

2. Data Protection

Information Assurance

SigningHub encrypts all documents using AES (Advanced Encryption Standard) with a 256-bit key as soon as they are received and before they are stored in the database. SigningHub supports database encryption. Each encryption key is unique to the specific SigningHub deployment and is generated dynamically at deployment time. For additional security, SigningHub performs all document hashing itself, ensuring that any cryptographic operation carried out by SigningHub's cryptographic engine is performed only on the document hash rather than the full document. This enables the cryptographic engine to be operated as a managed service where required, an approach used by some partners.

Each SigningHub deployment generates a unique Document Encryption Key (DEK) to protect document data. SigningHub can optionally use an HSM to safeguard the DEK via a Key Encryption Key (KEK) generated and protected by the HSM. This process is managed by SigningHub and its cryptographic engine, with no direct communication between SigningHub and the HSM.

Ascertia's SigningHub Cloud is fully GDPR compliant.

Clients wishing to discuss the use of a high-trust UK data centre, private cloud instance deployment or high-trust Certificate Authorities (CAs) can speak to the Ascertia sales team for guidance. Additional authentication options are also available, including smartcard-based client SSL authentication, Active Directory federated authentication, OAuth, SAML, mobile phone authentication options and other approaches.

Our top priority is protecting your privacy. Ascertia is dedicated to safeguarding your information. Our Privacy Policy is available here: [HTTPS://WWW.SIGNINGHUB.COM/PRIVACY-POLICY/](https://www.signinghub.com/privacy-policy/) which governs the handling of all personal information provided to us.

SigningHub is hosted on a Microsoft Azure server in Northern Europe. User accounts and service plans are managed by dedicated Ascertia staff. No user data is transferred outside the EU.

Data Back-Up and Restoration

Ascertia's SigningHub is hosted by Microsoft Azure, which provides real-time backup of all systems, documents and data.

Business continuity statement/plan

Ascertia's SigningHub Cloud service operates across two separate data centres configured for high availability. Azure SQL database services are used to ensure maximum resilience and availability.

Privacy by Design

Ascertia's SigningHub Cloud is fully GDPR compliant.

3. Using the service

Ordering and Invoicing

SigningHub usage can be purchased on a monthly or annual subscription basis and is available for immediate use. Longer evaluation periods can be arranged by contacting the Ascertia sales team if required. An online shop supports credit card-based purchases for a range of standard plans, with the option to configure custom plans where required. Ascertia's sales team can also discuss specific requirements, manage offline orders, and provide signed electronic invoices.

Availability of Trial Service

Anyone can register to use a free one-month trial account with stated document and signature limits. The Ascertia Sales team can assist with requests for extended evaluation periods to meet specific business needs.

On-Boarding, Off-Boarding, Service Migration, Scope etc.

SigningHub is designed for rapid onboarding, enabling users to register and begin using the service within minutes. Once an account is created, users can upload documents, define signing contacts, apply existing workflow templates or create new ones by positioning signature fields for each signer, and send documents for review and signature.

The SigningHub website includes short demonstration videos (approximately two minutes in length) that explain key features and how to realise business value quickly.

A range of help resources is provided, including online help, a navigation guide, and a "next step" suggestion feature. These can be enabled or disabled within individual user profiles.

Users can off-board from SigningHub easily. All documents can be downloaded or deleted, and signed documents remain verifiable using industry-standard software such as Adobe Reader. Off-boarding can be completed within minutes.

Documents remaining on the system are retained for at least 180 days after they were last opened. Users are notified by email of documents scheduled for deletion, and any documents remaining unopened for a total of 210 days are automatically deleted.

SigningHub provides online document workflow and signing services and is not intended for long-term dormant document storage. All documents are encrypted using AES-256 at the application level and stored as encrypted objects, ensuring secure deletion without the need for overwrite processing or hardware destruction.

Training

Training videos are available on the SigningHub website, and a welcome guide is provided within each new user account. Most customers are able to use the service without additional training.

For integration with existing business applications, RESTful API documentation and source code examples are available on the website. These enable SigningHub to be used either as an extension to modern web applications or as a branded front-end for legacy systems without web-portal capabilities.

Ascertia can provide additional training support where required. Pricing available in our pricing schedule.

Implementation Plan

A detailed implementation plan can be provided on request. The plan is managed using project management software and outlines each step required for successful service onboarding.

Service Management

ITSM alignment statement

Purpose

This document provides external parties with the key elements to understand that Ascertia adopts an IT Service Management approach aligned with the ITIL framework and structured around documented, repeatable, and controlled processes applied across core operations.

Scope

Ascertia implements an operating approach based on strong information and cybersecurity management, demonstrated through voluntary certification (ISO 27001), with continuous assessments conducted in line with the most relevant industrial framework (NIST), and with services managed in line with the ITIL framework. Moreover, Ascertia belongs to a relevant industrial group, and its products are subject to technical regulations and compliance constraints that, together, ensure compliance with all applicable regulations.

While information security governance and risk management are key pillars of the operating approach, IT Service Management practices are applied across the full-service lifecycle, covering service design, transition, operation, and continual improvement. Security (quality, availability, and customer satisfaction) requirements are embedded into service management processes as enabling controls.

The following elements support alignment with the ITIL framework.

- Its staff is continuously trained in managing services and tools.
- The company has an ISMS certified under ISO 27001, which governs information security processes and covers security governance, risk management, incident handling, change management, supplier chain management, and continuous monitoring.
- The security governance model relies on strategic, management, and operational levels and aligns with corporate governance and risk management practices.
- The organisation regularly evaluates its cybersecurity maturity level based on the NIST Cybersecurity Framework (CSF) 2.0. The assessments allow the definition of structured remediation plans and of a multi-year improvement roadmap.
- Continuous monitoring and reporting are in progress.
- Service metrics are implemented.
- The software development lifecycle (SDLC) follows controlled service design and transition practices, including formal code verification, independent quality assurance performed by a dedicated QA team, and separation of duties between development and validation activities.
- Regular Vulnerability Assessment and Penetration Testing (VA/PT) is performed by a specialised team supporting service reliability and risk reduction.

From an IT service management perspective, the organisation has defined and applies Standard Operating Procedures (SOPs), including:

- Incident and Problem Management: Designed to restore normal service operations as soon as possible, while minimising business impact, and preventing occurrences. Incidents are classified, prioritised, and escalated based on impact and urgency, while Problem Management and Root Cause Analysis activities provide structured improvement actions in the continual improvement cycle.
- Change Management: Ensures changes to services and systems are assessed, approved, and implemented in a controlled way, balancing risk, service stability, and the need for enhancements. Additional evaluation includes the possibility of customer disruption.

These processes are consistently applied in everyday operations and integrated with security incident handling, service restoration, and escalation mechanisms.

To summarise, based on the combination of the ISO 27001 certification, the NIST CSF 2.0–based continuous improvement activities, the standardised IT operational procedures, and the controlled service design and transition practices, Ascertia demonstrates an operating model aligned with ITIL 4 practices and consistent with the principles and requirements of ISO/IEC 20000, despite not having formal certification.

ITSM alignment matrix

The following table represents a high-level mapping between ITSM and Ascertia coverage:

Service Governance	Board-approved cybersecurity governance model. Defined roles and responsibilities. Accountability. Integration with corporate governance.
Risk Management	ISO 27001 risk assessment and treatment. NIST CSF 2.0 posture assessments. Risk-based roadmap. Alignment with group-level risk methodology and framework (ERM/COSO, Finance/Company-level controls).
Incident Management	SOP for: incident management; security incident handling integrated with service restoration.
Problem Management	Formal RCA process. Analysis of incidents and control failures to feed improvement actions.
Change Management	SOP for Change Management. Risk-based evaluation of changes aligned with ISO 27001 controls

Service Design & Transition	Controlled SDLC aligned with DevOps principles. Secure coding guidelines based on OWASP. Governed CI/CD pipeline with approval gates. Independent QA. VA/PT.
Monitoring & Event Management	Continuous monitoring of controls. Logging, detection, and periodic reviews.
Supplier Management	Third-party VA/PT performed by specialised providers. Alignment with group-level requirements.
Service Continuity	Security and resilience are embedded in governance and roadmap initiatives.
Continual Improvement	ISO27001 continuous improvement life cycle. NIST CSF 2.0 assessment and remediation plans. Multi-year cybersecurity roadmap. Group-level ongoing monitoring and reporting.

Service Constraints

Software upgrades to the SigningHub Cloud service are first deployed within the SigningHub staging environment. Customers are required to test access to this service and are provided upgrade notifications with a minimum of 7 days' notice for changes to staging.

Service Levels

Ascertia SigningHub is hosted on a high-availability Microsoft Azure configuration across two datacentres, which provides 99.995% uptime.

SigningHub operates at 99.95% with an allowance for one hour of scheduled maintenance every quarter.

Outage and Maintenance Management

SigningHub operates on a high-availability Microsoft Azure platform, providing resilience and scalability. Azure enables rapid performance scaling to ensure the service continues to operate at optimal levels.

Financial Recompense Model for Not Meeting Service Levels

Ascertia will consider any recompense models on a case-by-case basis.

4. Provision of the service

Customer Responsibilities

Users are required to use the service in accordance with the SigningHub Terms of Service, available at: <https://www.signinghub.com/terms-of-service/>. More information below:

Amendment - You are responsible for reviewing the current version of the Customer Agreement periodically. Ascertia may amend this Agreement by (a) posting a revised Customer Agreement on the Ascertia website, or (b) sending information regarding the amendment to the email address you provide to Ascertia. Continued use of the Service will be deemed acceptance of the amended Agreement.

Proper Use - You agree to comply with the terms and conditions of this Agreement and with all applicable local, state, national and international laws and regulations and all Internet regulations, policies and procedures, including all export and other laws regarding the transmission of technical data exported from any country through the Service. You agree that you will not use the Service for illegal purposes, to disrupt the Service, or to distribute content that violates the privacy, intellectual property or other proprietary rights of any third party, or for purposes that Ascertia reasonably determines to be unlawful, obscene, defamatory, harassing, fraudulent, abusive, threatening, harmful, vulgar, or otherwise objectionable. You are wholly responsible for the contents of your transactions through the Service. Your use of the Ascertia service is subject to Ascertia's "Fair Use" policy – see below for more details.

Age - You represent and warrant that you are at least 18 years of age (or, as applicable, the age of majority in the state or province in which you reside), and that you possess the legal right and ability to enter into this Agreement.

Account Registration - You represent and warrant that all of the information you provide to Ascertia is true, accurate and complete, and that you have legal right to use the email address(es) you provide. You agree to keep your information current by updating your account information. You agree to maintain the confidentiality of your account. You are responsible for all activities that occur under your account. If your account remains inactive for more than three months, Ascertia reserves the right to close your account.

Payment Obligations - In the event that you choose to purchase one of the service plans that Ascertia makes available (a "Paid Account"), you agree to pay for using such a Paid Account according to the service plan you select. Payment of your SigningHub account balance is due monthly, yearly or pay as you go in advance and must be made by the credit or debit card you designate, unless you agree a separate post-pay arrangement with Ascertia.

Certain services may be offered in the form of Signature Packs. A Signature Pack grants the Customer a perpetual, non-exclusive right to use the purchased number of signature transactions. Signature Packs do not expire and remain valid until all purchased signature credits have been consumed.

Credit Card Refund Policy - Trial use of SigningHub is available for 5 free signatures and this route must always be used to ensure that SigningHub is acceptable to you before purchasing a service package. If having purchased a service package, you are not satisfied, you may request a refund within 7 days. Once the refund request is made then Ascertia will delete your account plus any data

associated with it and promptly refund the amount paid for the service back to the credit card used for payment, less any credit card operator fees that may be associated with this. Refund requests can be made by email to sales@ascertia.com or by opening a support ticket at <https://ascertia.force.com/partners/login>

NO ADVICE OR INFORMATION, WHETHER ORAL OR WRITTEN, OBTAINED BY YOU FROM ASCERTIA, OR THROUGH OR FROM THE ASCERTIA WEBSITE OR SERVICE, SHALL CREATE ANY WARRANTY NOT EXPRESSLY STATED IN THIS AGREEMENT.

Account Cancellation - If your account is paid-in-full, you may cancel your account and terminate this Agreement at any time. Ascertia recommends printing or copying any important documents because you will lose access to documents, messages or other content contained in your account after cancellation. Ascertia reserves the right to terminate any account that violates the terms of this Agreement.

Communication - You agree that the official time for all transactions using the Service will be the timestamps recorded by the Service's servers. You also agree that all electronic communications or notices sent to the email address you provide to Ascertia, placed in your account, or posted on the Website will be considered "in writing" and received within five (5) business days of its dissemination. Ascertia disclaims all responsibility for all failures in communication caused by failures of third parties to properly process or deliver Ascertia's electronic communications.

Technical Requirements and Client-Side Requirements

SigningHub operates with modern web browsers that support HTML5. Supported browsers include Internet Explorer 9 or later, Chrome version 5 or later, Firefox version 3 or later, Safari version 5 or later, and Opera version 16 or later.

SigningHub supports multiple languages, including English, Dutch, Spanish, French, German, Greek, Latvian, Turkish, and Arabic.

Development life cycle of the solution

Ascertia follows an industry-standard software development lifecycle_process built on agile development principles. Product Managers/Owners define and manage the product roadmap based on market and customer requirements. These requirements are captured as epics and user stories, which are developed into detailed functional specifications used to build the software and drive testing by the Ascertia Quality Assurance team. Software quality and security are at the core of everything we deliver. Ascertia product source code- is maintained in a central, version-controlled repository, and automated testing is executed for every release.

As part of the regular release cycle, the Ascertia development team runs vulnerability scans against products and third-party libraries to identify potential threats and vulnerabilities. These scans are performed at the start of each sprint, and we endeavour to resolve any critical issues discovered within the same sprint where possible.

Automated testing is used extensively for the SigningHub application and forms part of every release cycle.

Ascertia maintains a Security Assurance Response Team who are responsible for reviewing security vulnerabilities that are identified in Ascertia products or associated third party libraries that are shipped as part of Ascertia products. Customers are notified when and if a critical security issue is identified, and immediate remedial action is required.

Updates to SigningHub are announced on the SigningHub website and made available for testing on the staging server prior to deployment on the production servers.

After-sales Account Management

Ascertia provides proactive account management, with an Account Manager and a member of the Customer Success Team assigned to each customer. They act as primary points of contact for queries, support requests, and ongoing account planning.

Termination Process

If an order is given for a longer period, then on termination, Ascertia will refund any unused months that have been paid for. Written notification of termination must be given 30 days in advance if the term of the contract has not been reached.

5. Our experience

Case Studies

We have experience delivering secure, compliant digital signing solutions across both public and private sector organisations. In the public sector, North Yorkshire County Council works with Ascertia to support trusted digital signing processes that improve efficiency while meeting governance and compliance requirements. In the private sector, MD Consents uses SigningHub to manage legally sensitive consent workflows, valuing the platform for its reliability, collaboration, and professional user experience. These examples reflect common challenges around secure document execution, auditability, and ease of adoption, which translate directly to public sector use cases.

[Why North Yorkshire Council works with us | Ascertia | Blog](#)

Case Study: North Yorkshire Council chooses Ascertia to streamline operations

North Yorkshire Council, the authority which governs the English district of North Yorkshire, was looking to streamline processes and maximise cost efficiency. After carefully considering options, the council chose Ascertia's solutions – specifically SigningHub – to manage its document workflows while ensuring legal compliance.

Business need:

As a local government, North Yorkshire Council holds legal compliance and security at the utmost importance. Increasing operational efficiency – from document workflows to record-keeping – is always at the forefront of the decision-making process, too. The council was looking to streamline its processes while maintaining compliance with its legal obligations and water-tight security. A solution that supported remote working and environmental sustainability was also considered.

Solution:

North Yorkshire Council ultimately chose Ascertia due to our area of expertise: simple and secure digital signing. It selected to use Ascertia's SigningHub over other signing applications as its digital signature system to manage its document approval workflows, digital signing and document status tracking. As a result of choosing SigningHub, the council has received "stability and resilience" in turbulent times – namely the global pandemic and its transition to a unitary council in April 2023. North Yorkshire Council noted that with local government reforms at play, there is scope for increased use of our solutions and products in the future – a testament to the Ascertia experience.

Other case studies:

[MD Consents - Why MD Consents uses SigningHub: "Reliable, collaborative, professional"](#)

Clients

Ascertia has Government customers worldwide. In the UK, SigningHub is used by both central government departments and local government organisations. Examples of Ascertia's government customers include:

Ascertia in European Government

Ministerie van Justitie en Veiligheid

KVK WERKT VOOR ONDERNEMERS

OM

Dienst Uitvoering Onderwijs
Ministerie van Onderwijs, Cultuur en Wetenschap

HM Revenue & Customs

Department for Transport

SSC-ICT
Ministerie van Binnenlandse Zaken en Koninkrijksrelaties

HM Land Registry

Vlaanderen
verbeelding werkt

Gedrukt door de Staat
National Treasury Management Agency

CRO COMPANIES REGISTRATION OFFICE
AN OIFIG UIM CHÉILRÚ CUIDEACHTAL

Regeringskansliet

Government of Iceland

Trusted by 20+ Governments

ascertia

CONFIDENTIAL

© Ascertia. All rights reserved.

Contact Details

For further information:

- Consult the service website WWW.SIGNINGHUB.COM
- Email SALES@ASCERTIA.COM
- Telephone:- +44 (0) 800 772 0 442 or +44 (0) 203 633 117