

## Dissecting Differences between SigningHub™ & DocuSign® e-Signatures

Acme Inc. (the "Customer"), with an address of 40 Occam Road, Surrey Research Park, Guildford, Surrey, GU27YG UK and  
this Product Sales Agreement (this "Agreement") is made by and between Seller and Customer, as described below (the "Product"), to be sold solely to the Customer, with an address of 40 Occam Road, Surrey Research Park, Guildford, Surrey, GU27YG UK and  
Seller wishes to sell solely its Product, as described below (the "Product"), to be sold solely to the Customer, with an address of 40 Occam Road, Surrey Research Park, Guildford, Surrey, GU27YG UK and  
Customer shall purchase the Product from Seller pursuant to the terms and conditions of this Agreement, and shall not resell, lease, license, or otherwise use the Product for any other purpose or for any other person or entity without Seller's prior written consent.  
WHEREAS, Seller desires to sell to Customer, and Customer desires to purchase from Seller, the Product, as described below (the "Product"), to be sold solely to the Customer, with an address of 40 Occam Road, Surrey Research Park, Guildford, Surrey, GU27YG UK and  
Customer shall purchase the Product from Seller pursuant to the terms and conditions of this Agreement, and shall not resell, lease, license, or otherwise use the Product for any other purpose or for any other person or entity without Seller's prior written consent.  
WHEREAS, Seller desires to sell to Customer, and Customer desires to purchase from Seller, the Product, as described below (the "Product"), to be sold solely to the Customer, with an address of 40 Occam Road, Surrey Research Park, Guildford, Surrey, GU27YG UK and  
Customer shall purchase the Product from Seller pursuant to the terms and conditions of this Agreement, and shall not resell, lease, license, or otherwise use the Product for any other purpose or for any other person or entity without Seller's prior written consent.  
A. Description of the Product: The Product is a software application that allows users to create and manage digital signatures.  
B. Use: Customer shall use the Product to create and manage digital signatures.  
C. Transfer: The Product shall be available via download from the Seller's website after payment and Conditions of Sale attached hereto as Annex A.  
D. Terms and Conditions: The Terms and Conditions of Sale attached hereto as Annex A are incorporated into this Agreement and shall govern the use of the Product.  
IN WITNESS WHEREOF, the undersigned has caused this Agreement to be executed and signed by its duly authorized representative on the date first set forth below.

John Clarke  
Signed By: John Clarke  
Signed Date: 12/05/2020 10:28:00 UT  
Reason: I approve the document  
Sign Here



## Introduction & methodology

In this updated eBook we compare the current differences in e-signatures between a document signed using Ascertia's SigningHub solution and provider DocuSign®. Both products have evolved and developed since we first reviewed them in 2015, so we felt it was time to revisit the comparison.

We used each company's free trial cloud service for the comparison:

**SigningHub:** <https://web.signinghub.com/Web#/Home>

**DocuSign:** <https://app.docusign.com/home>

We generated a sample contract document for signing in Word® and uploaded this to each cloud service for signing using each service provider's document signing functionality. The document was then downloaded and the signature verified in Adobe® Acrobat Reader DC (2020).

We also generated an example identity 'Flo Voges' and company 'Growth Engine' for testing purposes.

### The following aspects were assessed during this study:

- **Document format:** Is the document converted to a secure format before signing?
- **e-Signature appearance:** What options are available to the user in making their e-signature mark on the document?
- **Digital signature strength:** How is the document locked after signing so that no further changes can be made?
- **Identifying the signer:** How is the user's identity linked to the document and what level of non-repudiation is achieved through the signed document?
- **Timestamps:** What timestamp details are available and are there any issues with them?
- **Long-term Verifiability:** Can the user's signature be verified in the long-term?

Each of the above aspects is covered in a separate section of this eBook.

## Definitions of electronic & digital signature levels

Anyone new to this area can be easily confused about what constitutes an electronic signature and how different types of e-signatures compare in terms of evidential power and legality.

At a basic level any mark on an electronic document can be used to capture the signer's intent to approve or accept the contents of that document. The form of the "mark" or how it was created is not important. What is important is proving who made the mark and that the document was not changed subsequently.

### CLICK TO SIGN SIGNATURES

- › These include tick boxes, e-squiggles, scanned images, and typed names
- › No cryptographic protection of the document
- › Do not provide strong evidence of who signed or even protect the document from subsequent change.

### BASIC ELECTRONIC SIGNATURES

- › Immediate signing, no user registration or login required
- › Document signed and protected with server held signing key or e-Seal only
- › May or may not include a trusted timestamp
- › The signer's identity is not verifiable directly from the signed document.

### ADVANCED ELECTRONIC SIGNATURES (AES) or DIGITAL SIGNATURES

- › Uses unique PKI signing key per user
- › Strong user authentication, the user's identity is cryptographically bound with their signature
- › Provides strong non-repudiation - show exactly who signed the document
- › Supports secure remote signing.

### QUALIFIED ELECTRONIC SIGNATURES (QES) or DIGITAL SIGNATURES

QES provide the highest level of legal recognition & acceptance by providing the benefits of AES plus the following:

- › Formal registration process for the user to verify their identity by a qualified Certificate Authority (CA)
- › Relies on Government recognised CAs only
- › Cross-border use under EU eIDAS Regulation.



# Signing tests and results

An e-Signature appearance is the user’s electronic mark on a document to indicate their consent with the document contents. Typically, it takes the form of an ink signature image, or a text-based facsimile of it.

## Signing methods and e-Signature appearance – text, draw, upload, logo & stamp

### SigningHub – Signing options

Offers options to use:

- > Use your initials
- > Text based signature (using one of a selection of fonts)
- > Draw your signature (with your fingertip or a stylus)
- > Upload a signature (a scan of your real hand-written signature).

Additionally, you have the option to add the following elements to the document template:

Initials, Name, Email, Job title, Company, Date, Text field (e.g. reason for signing), Text area, Radio button, or Check box.

**SigningHub** - This is a view of the completed and signed document showing the signees’ e-signatures:

**FIELDS**

- Electronic Signature
- Initials
- Name
- Email
- Job Title
- Company
- Date
- Text Field
- Text Area
- Radio Button
- Check Box


**ACCEPTANCE OF PROPOSAL**  
Please indicate your acceptance of this proposal by signing and dating this document and returning it to ABC Construction & Landscaping Ltd. Thank You.


Name \_\_\_\_\_

Signed \_\_\_\_\_

Dated \_\_\_\_/\_\_\_\_/\_\_\_\_

**Signed by: Flo Voges**  
Signed at: 2020-08-28 14:58:13 +00:00  
Reason: Witnessing Flo Voges





*NOTE All names are fictitious and are not intended to represent real people or companies. This is a sample agreement only and has no legal standing in the UK or any other country.*



# Signing tests and results

## DocuSign – Signing options

Offers options to use:

- > Use your initials
- > Text based signature (using one of a selection of fonts)
- > Draw your signature (with your fingertip or a stylus)
- > Option to upload a hand-written signature (this has to be done in your account Signature settings)
- > Option to save multiple signatures (useful if you need to sign using different versions of your signature, e.g. formal and informal, or with and without a title).

Additionally, you have the option to add the following elements to the document template:

Initials, Stamp, Date, Name – First / Last, Email, Job title, Company (e.g. company name), Text field (e.g. reason for signing), or Check box.

**FIELDS**

- Signature
- Initial
- Stamp
- Date Signed

---

- Name
- First Name
- Last Name
- Email Address
- Company
- Title

---

- Text
- Checkbox

**DocuSign** - This a view of the completed and signed document showing the signee's e-signature:

**ACCEPTANCE OF PROPOSAL**  
Please indicate your acceptance of this proposal by signing and dating this document and returning it to ABC Construction & Landscaping Ltd. Thank You.

Name

Signed \_\_\_\_\_

Dated

**DocuSigned by:**  
  
FAT7326E8ED8043F...

**DS**

**DocuSigned by:**

*NOTE All names are fictitious and are not intended to represent real people or companies. This is a sample agreement only and has no legal standing in the UK or any other country.*



## Signing tests and results

### DocuSign – other signing options:

- **DocuSign’s ‘eNotary’** remote online signing service allows the inclusion of the notary’s official stamp or logo (as above). It also requires signees to present a second form of identification via video link, and for that ID process to be recorded.
- **Draw a new Signature** - Under signing settings you can select an option that requires each recipient to draw a new signature for each signature or initial filed, as this is required for certain legal and financial documents.



## PDF formatting

### SigningHub – PDF formatting

SigningHub automatically converts a broad range of office documents to PDF format more specifically PDF/A which allows long-term archival.

If you open the SigningHub signed document inside Adobe Reader DC it shows the below detail:

Signatures

Validate All

- > Certified by SigningHub Digital Witness <support@ascertia.com>
- > Rev. 2: Signed by SigningHub Digital Witness <support@ascertia.com>

If you then open the Information icon it shows the Standards used by SigningHub:

Standards

**Conformance**

Standard: PDF/A-2A  
ISO Name: ISO 19005-2

Status: not yet verified

**OutputIntent**

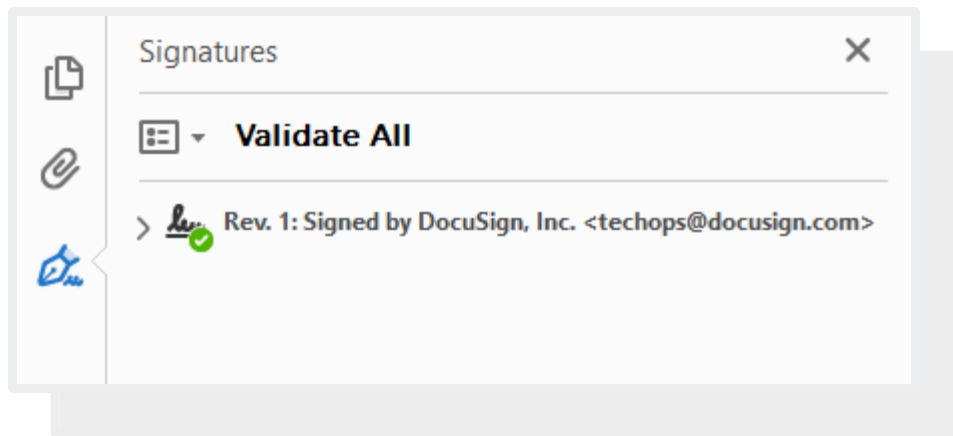
Identifier: Custom  
Info: sRGB IEC61966-2.1



## PDF formatting

### DocuSign – PDF formatting

DocuSign converts documents to a standard PDF format (version 1.5 – Acrobat 6.X). This was checked using the Adobe Signature Panel and Document Properties. DocuSign does **NOT** appear to convert them to the more secure PDF/A standard, the **'Standards' option simply does not display** in Acrobat Reader DC for the DocuSign document – see below:



### Why does this matter?

PDF/A is an ISO standard (ISO 19005-1:2005 OR ISO 19005-2) format of PDF specialised for the digital preservation of electronic documents. PDF/A differs from PDF by disallowing features ill-suited to long-term archiving and secure signing, such as font linking (as opposed to font embedding) and encryption.

PDF/A formatting ensures a document can be reproduced precisely whatever the software being used. This is because all the information needed to display the document is embedded within the file, meaning your PDF/A documents are safe, accessible and secure for the long term.





## PDF formatting

There are several levels of PDF/A format: PDF/A-1b, PDF/A-2b, PDF/A-3 and PDF/A-4 each with increasing levels of document format support and conformance.

In particular PDF/A requires:

- Full embedding of fonts rather than dynamic font linking. This ensures the long-term rendering of signed documents and prevents dynamic font changing in the future
- JavaScript and other executable content are forbidden. This prevents malicious code inside the document changing the user's view of the document when signing. This is essential for meeting What You See Is What You Sign (WYSIWYS), an important security requirement for achieving non-repudiation.

**PDF/A format is strongly recommended for better security and long-term rendering of signed documents.**



## Digital signature (AES or QES) strength comparison

A signed document needs to have some inherent security properties in order to be useful for real business use and to provide evidence which will be legally acceptable in a court.

Such signatures are often termed “**advanced electronic signatures**”. Within the EU’s eIDAS standard there is a standard definition of the properties of an advanced electronic signature. These include:

- Must be uniquely linked to the signer
- Capable of identifying the signer
- Created using means that the signatory can maintain under their sole control
- Linked to the data to which it relates in such a manner that any subsequent change of the data is detectable.

This means anyone should be able to easily verify a signed document in terms of:

- Who signed it (without any ambiguity), and
- Confirm that no changes were made to the document subsequent to signing

Other jurisdictions around the world follow similar definitions to the EU when describing secure forms of e-signatures.



# Digital signature (AES or QES) strength comparison

## Assessment

We wanted to assess how the document was locked after signing so that no further changes can be made, how the user's identity is linked to the document, and what level of non-repudiation is achieved through the signed document?

### Question – How was the document locked after signing?

**Answer** – Once the document is signed using a digital signature it becomes locked and any further changes will invalidate the signature. When viewing the document in a PDF viewer such as Adobe Reader it will validate the document and the signature and if the document has changed the signature will not be valid and a message displayed saying so.

### Question – How was the user's identity linked to the document?

**Answer** – Advanced Electronic Signatures (AES) and Qualified Electronic Signatures (QES) provide the highest levels of trust and assurance because these use unique signing keys for every signer. This directly links the user's identity to the signed document such that anyone can verify it on their own using an industry standard PDF reader (Adobe Reader for example). Furthermore, as the signer has sole control of their unique private signing key this ensures non-repudiation.

### SigningHub vs DocuSign:

- The ability to create e-signatures and digital signatures is standard in SigningHub functionality
- E-signatures are standard in DocuSign but digital signatures are not
- DocuSign does offer the option of advanced electronic signatures but to make use of the functionality a paid for add-on in addition to the plan cost is required called Standards-Based Signatures. After purchasing a plan, DocuSign need to be involved to add Standards-Based Signatures to allow the use of advanced electronic signatures.



# Digital signature (AES or QES) strength comparison

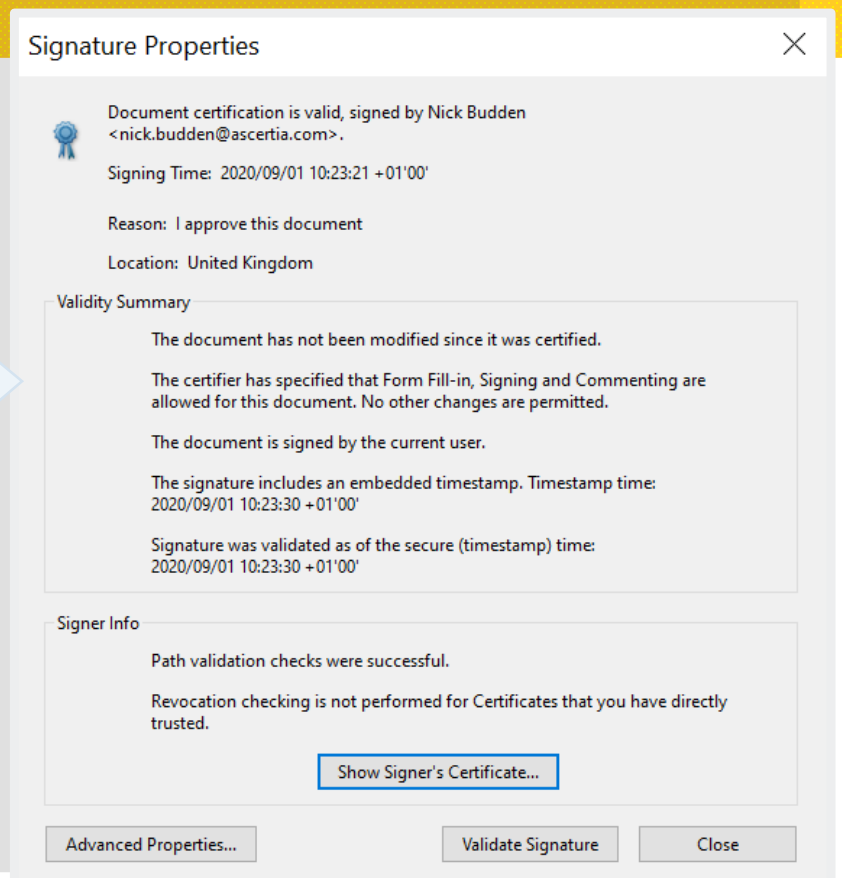
## SigningHub - Digital signature strength

When a signed document from SigningHub is opened in Adobe Reader DC you see the following:



With SigningHub, the blue bar clearly shows who signed the document (including their email address) and who their employer is, in this case Ascertia Limited. It goes a step further by showing the Certificate Authority who is vouching for the signer's identity.

With a SigningHub signature, the e-Signature mark is clickable, in this case Adobe Reader shows the following dialog:





## Digital signature (AES or QES) strength comparison

### **SigningHub clearly identifies the end-user who signed the document.**

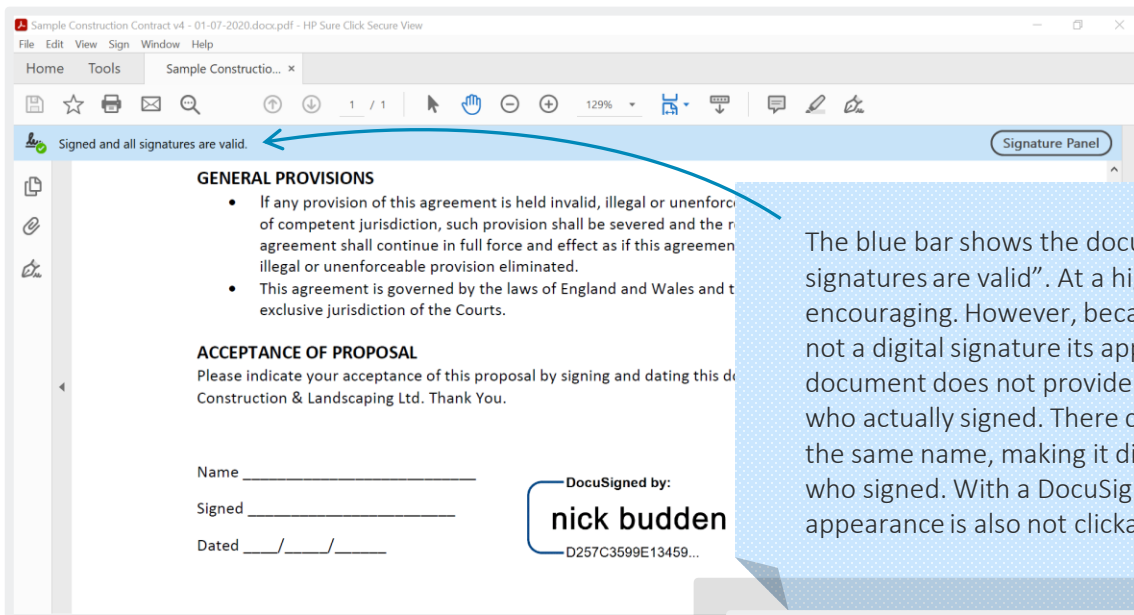
This is possible because SigningHub uses unique signing keys/certificates for every user. These keys are under the sole control of the user, therefore no one else can create the signatures on behalf of the user. The document is also “certified” - this is a special type of PDF signature which prevents the addition of any further content e.g. comments, annotations etc. Finally, it is also possible for the signer to define in the signature the reason why they are signing (which seemed not to be possible with DocuSign). SigningHub also uses secure signature algorithms (SHA256 and RSA2048).



# Digital signature (AES or QES) strength comparison

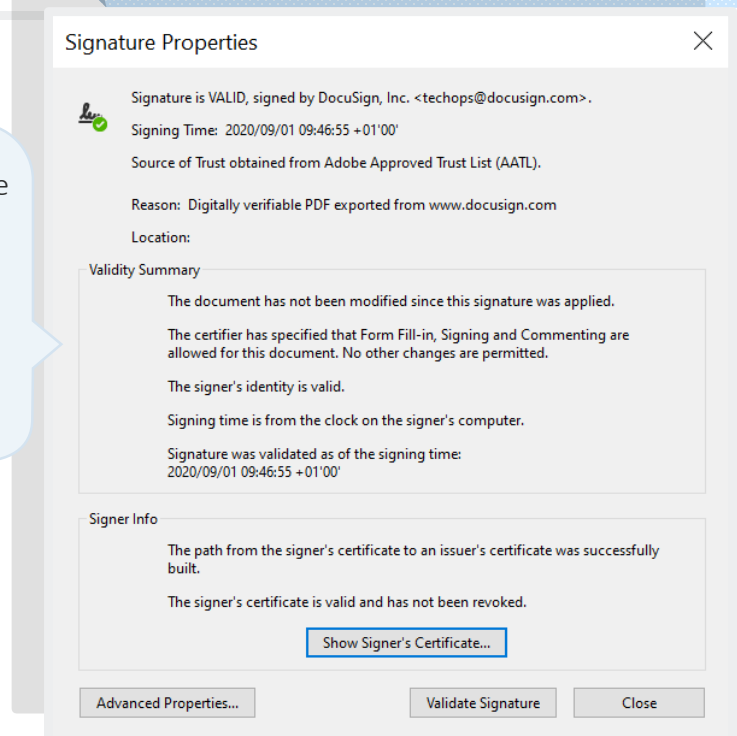
## DocuSign - Digital signature strength

When a signed document from DocuSign is opened in Adobe Reader, the following is shown:



The blue bar shows the document is “Signed and all signatures are valid”. At a high-level this sounds encouraging. However, because this is an e-signature and not a digital signature its appearance printed on the document does not provide any conclusive proof as to who actually signed. There could also be many users with the same name, making it difficult to determine exactly who signed. With a DocuSign signature, the e-signature appearance is also not clickable.

The Adobe Reader Signature Properties dialog can however be opened from the left-hand panel and this reveals the following:





## Digital signature (AES or QES) strength comparison

### DocuSign - Digital Signature Strength *(continued)*

Due to the fact that it is an electronic signature, the signature shows it is signed by DocuSign, but this fails to identify the real end-user who actually signed the document.

In the above screenshot it is also indicated that form fill-in, signing and commenting are allowed for this document. It also indicates that the Signing time is from the clock on the signer's computer. This has a significant impact as this allows the user to change the time of his computer before signing and the changed time will be the time indicated on the signature. In contrast, SigningHub makes use of a timestamping authority which means the time on the signature is from an independent time source.

DocuSign does however provide document integrity protection as the document is signed using strong algorithms (SHA256/RSA2048) so any subsequent changes to the document will be detected.

As mentioned earlier, DocuSign does offer the option of Digital Signatures but to make use of the functionality a paid-for add-on in addition of the plan cost is required called Standards-Based Signatures. After purchasing a plan, DocuSign need to be involved to add Standards-Based Signatures to allow the use of Advanced Electronic Signatures.

### Digital signature strength comparison – other questions

#### Question – What levels of authentication are required?

**Answer** – Both SigningHub and DocuSign enabled the trial to go ahead after simply requiring an active email and mobile phone number for account activation. When moving to full versions both SigningHub and DocuSign offer authentication using various identity providers.

#### Question – Non-repudiation and confidence?

**Answer** – SigningHub's 'Workflow Evidence Report' and DocuSign's 'Certificate of Completion' both provide detailed and comprehensive reports, which provide a lot of supporting evidence to verify the signing process.



# Signature and document integrity

## Signature integrity:

### > Who really signed it?

When using digital signatures, the signature is generated using the private key belonging to the user performing the signing operation. The user has sole control of the private key and so only the user can perform the signing operation.

### > Was it the recipient, or someone else?

When using digital signatures, the signature is generated using the private key belonging to the user performing the signing operation. The user has sole control of the private key and so only the user can perform the signing operation. The user cannot deny signing because they have sole control over the private key offering non-repudiation.

### > Is the signature linked to the user and the signing key under the sole control of the signer?

By using PKI certificates and keys the signing key becomes the sole control of the signer by using hardware devices such as an appliance for remote signing, HSM, smartcard/Token or a software solution.

### ***Proof of identity (additional proofs required) See Question / Answer above.***

Both SigningHub and DocuSign offer authentication using various Identity providers before performing a signing operation using a digital signature.

It should be noted that Digital Signatures in DocuSign requires adding the Standards-Based Signatures add-on.

## Document integrity:

### > Could it have been altered since signing?

The Adobe Reader DC 'Signature Properties' shows that both the SigningHub and DocuSign documents have not been altered since signing.

### > Both **SigningHub & DocuSign** show the same 'Validity Summary' information:

#### Validity Summary

The document has not been modified since this signature was applied.

The certifier has specified that Form Fill-in, Signing and Commenting are allowed for this document. No other changes are permitted.

### > Can any subsequent changes to the document be detected?

Yes, for both SigningHub and DocuSign this can be demonstrated by: If you make changes to the document and then view it in Adobe Reader, it will indicate that the document signature is invalid.





## Timestamps

Adding a 'timestamp' to an electronically or digitally signed document adds an extra layer of security, by recording the date and time when the document was signed by each person.

Knowing when a document was signed could be important if any legal disputes arise at a later date.

Examples of this could include the question of whether an NDA was in force at the time of information disclosure, the price of a commodity at a particular time, payments due on the supply of goods or services from a particular starting point.

From a legal and security point of view its clearly essential that the actual date and time of signing cannot be disputed at a later date, and that documents signed in different timezones can be accurately compared.

### Trusted Timestamps

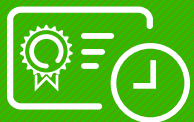
It is not enough to take the timestamp from the signee's computer or device since these times can be easily manipulated.

For a trustworthy timestamp the time used should be based on **Coordinated Universal Time (or UTC)**, and the timestamp itself should be provided by a trusted and independent third party, known as a **Timestamping Authority (TSA)** that uses **Public Key Infrastructure (PKI)** technology to supply the timestamp, so that the timestamp cannot be manipulated by the user.

Trusted Timestamping means you can be confident that the timestamp is accurate, cannot be manipulated, that documents signed in different countries/timezones can be compared, that the time and date reference can be independently verified, even after the expiry or revocation of the signer's digital credentials and that the signature will still be valid in years to come.

### Definition of a Timestamp:

Data in electronic form which binds other electronic data to a particular time establishing evidence that these data existed at that time.



## Timestamps

### SigningHub – Timestamps

When viewing the Signature Properties in Adobe Reader DC for SigningHub you see the following message:

The signature includes an embedded timestamp. Timestamp time:  
2020/09/01 10:23:30 +01'00'

Signature was validated as of the secure (timestamp) time:  
2020/09/01 10:23:30 +01'00'

SigningHub uses a trusted timestamp and therefore negates the possibility of tampering with timestamps applied to any signature/document.

### DocuSign – Timestamps

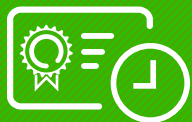
When viewing the Signature Properties in Adobe Reader DC for DocuSign you see the following message:

Signing time is from the clock on the signer's computer.

Signature was validated as of the signing time:  
2020/09/01 09:46:55 +01'00'

DocuSign does not create e-signatures with timestamps that can be trusted. It uses the signing time based on the signer's computer, which cannot be independently trusted. DocuSign does not embed proof that at the time of signing the signer's digital identity was valid.

DocuSign does however offer the option of a verifiable timestamp for their digital signatures (but not for their electronic signatures), but only as a paid-for extra.



## Long-Term Verifiable Signatures (LTV)

### Business documents need to be verifiable months and years into the future

To achieve this requires a special type of advanced e-signature, referred to as a **Long-Term Verifiable Signature (LTV)**. A standard format is known as ETSI PAdES\*.

Documents signed with a long-term signature include embedded, independently trusted **timestamps** to prove when the document was signed.

They also contain independently trusted proof that the **signer's digital certificate was valid** at the time of signing.

### SigningHub – LTV

SigningHub creates standard long-term signatures (PAdES). It embeds secure trusted timestamps from an independent Time Stamp Authority (TSA). SigningHub also embeds proof that the signer's digital identity was valid at the time of signing (CRLs/OCSP info).

SigningHub also comes with a **complete built-in PKI** including CA, OCSP/CRL and TSA Services. Alternatively, SigningHub can rely on any external PKI whether its enterprise, national, public, or global CA.

It is essential that signed documents are independently verifiable in the long-term and therefore PAdES long-term signatures must be used with an embedded timestamp that allows long-term verification.

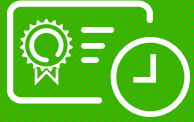
SigningHub supports the following LTV signature formats:

For PDF documents:  
PAdES (including PAdES-X-Long and PAdES-A)

For XML documents:  
XAdES (including XAdES-X-Long and XAdES-A)

For any other document format:  
CAdES (including CAdES-X-Long and CAdES-A)

Even with a long-term signature there are risks that over time the underlying cryptographic algorithms may become weak or the TSA certificate may expire. In such cases SigningHub supports the embedding of further timestamps protected under stronger algorithms. A chain of timestamps therefore can help protect the document for perpetuity.



## Long-Term Verifiable Signatures (LTV)

### DocuSign – LTV

DocuSign eSignatures and Digital Signatures are now LTV enabled.

DocuSign digitally seals all PDF documents that are downloaded from the DocuSign platform with a certificate issued by Entrust. This means that when validating the document, it is validating the certificate used for the digital seal. The sign-time is captured inside the PDF Document and the PDF Viewer will validate the signature using all the details that are contained directly inside the PDF. As mentioned before, the signing time is captured from the user's computer's clock and is therefore manipulatable.

DocuSign say "If you downloaded your document prior to LTV ramp up, you may have a yellow warning. It does not mean that the underlying document and electronic signatures affixed to the document are invalid. Re-downloading the document will affix a new DocuSign digital seal". This will only work whilst you remain a DocuSign customer of course.

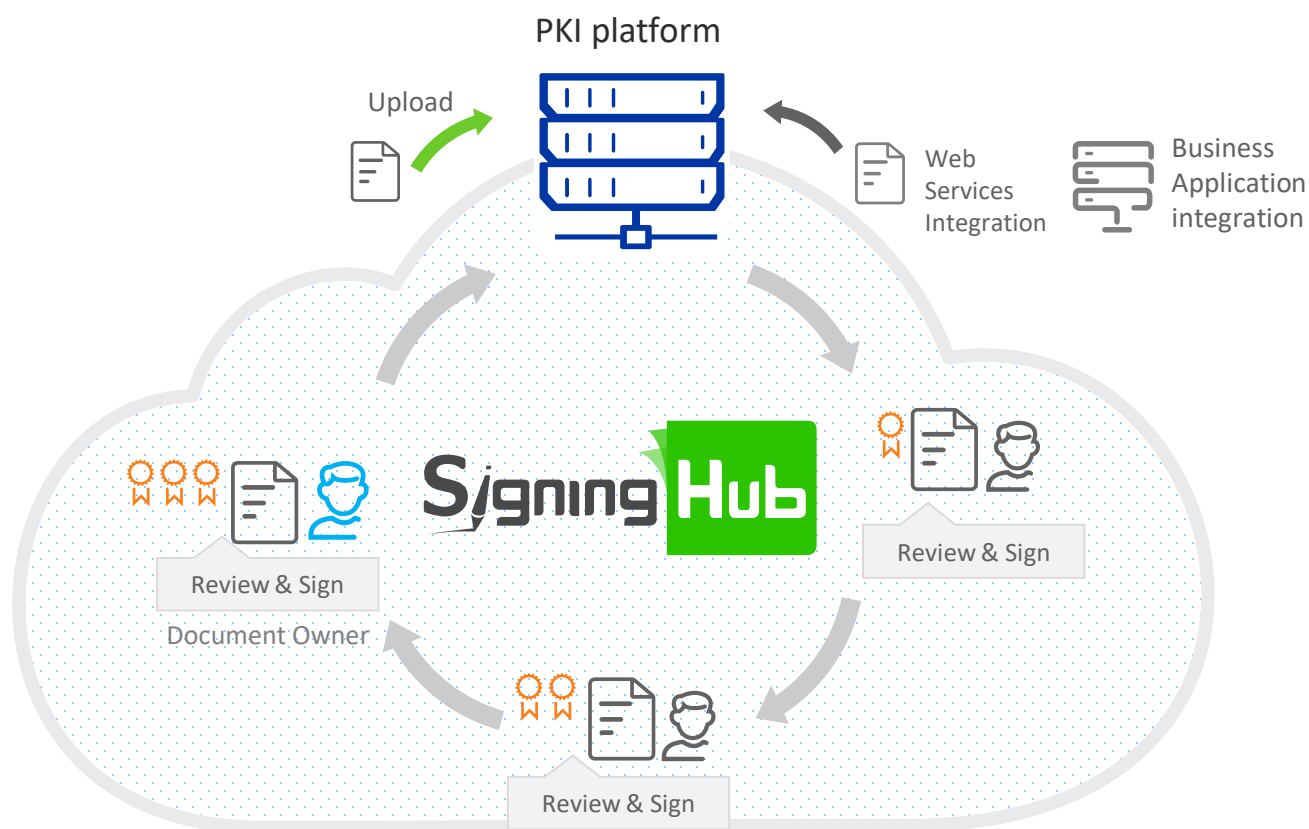
**\*See** [https://www.etsi.org/deliver/etsi\\_en/319100\\_319199/31914201/01.01.01\\_60/en\\_31914201v010101p.pdf](https://www.etsi.org/deliver/etsi_en/319100_319199/31914201/01.01.01_60/en_31914201v010101p.pdf)



## Workflow processes

### SigningHub - Workflow

Allows creation of workflow templates that define who the signatories are, in which order they must sign, where in the document the signature should be placed, their access permissions, legal notices, initials fields, form field assignments and all other low-level parameters associated with the signing process. End-users can then simply select these workflow templates to automate the document preparation stage instead of manually preparing the document each time.



### DocuSign - Workflow

Lets you specify and order any number of signers. Assign recipients different roles and access beyond signing permissions. Route documents to multiple users in serial, parallel and mixed sequencing to fit your ideal process. Require users to sign one by one or allow them all to sign at the same time.



## Standards compliance

The **eIDAS** Regulation aims to make e-business easier and more trustworthy across Europe. It provides rules for legal certainty and technical interoperability for electronic identities and e-signatures and the Trust Service Providers (TSPs) that offer these services.

In 2007 the international standardization organisation OASIS drew up a set of standards for 'Digital Signature Service Core Protocols, Elements, and Bindings'.

This standard defines the basic functionality for the creation (SignRequest /-Response) and validation (VerifyRequest /-Response) of CMS- and XMLDSig-compliant signatures. This has since been extended to cover time stamping, code signing, entity seals, signature verification, signature creation devices and a host of other details.

In 2016 the **European Standard 'ETSI EN 319 142-1'** was published on Electronic Signatures and Infrastructures (ESI) and PAdES digital signatures. It is intended cover digital signatures supported by PKI and public key certificates and aims to meet the general requirements of the international community to provide trust and confidence in electronic transactions.

For more information on 'ETSI EN 319 142 please see:

[https://www.etsi.org/deliver/etsi\\_en/319100\\_319199/31914201/01.01.00\\_30/en\\_31914201v010100v.pdf](https://www.etsi.org/deliver/etsi_en/319100_319199/31914201/01.01.00_30/en_31914201v010100v.pdf)

### SigningHub - eIDAS compliance update

SigningHub meets both the eIDAS Regulation and the ETSI/CEN standards for creating and verifying eSignatures and eSeals, as well as for certificate issuance, validation and timestamping. SigningHub supports all three levels of signature, however it has been specifically designed for organisations that demand the high-trust offered by advanced and qualified eSignatures.

SigningHub does not provide the same services as a Qualified Trust Service Provider (QTSP), rather it is our customers and partners who provide these services, using our technology.



## Standards compliance

### SigningHub - eIDAS compliance update (*continued*)

SigningHub supports **eIDAS compliant advanced long-term digital signatures** using unique keys for every single one of its users.

SigningHub offers **Bulk signing** of PDF, XML and other documents such as invoices, reports, statements, etc.

- using Qualified or AATL or other high trust certificates
- using OASIS DSS web services or fast HTTP/S APIs
- using high level DotNet or Java APIs
- using Auto File Processor watched folder client
- using Secure Email Server

eIDAS Requirement	SigningHub Compliancy
Uniquely linked to the signer	Users are provided with individual signature keys, or can use unique keys sourced from a trusted third-party Certificate authority (CAs)
Created using electronic signature creation data that the signer can, with a high degree of confidence, use under their sole control	User signing keys can be held in a centrally held/cloud-based Hardware Security Module (HSM)/SAM Appliance (Conforming to SCAL2), or locally by the user on a separate smartcard, or USB token. In all cases the user is securely authenticated before access to their signing key is allowed.
Capable of identifying the signer and linked to the signed data in such a way that any subsequent change in the data is detectable	SigningHub creates long-term advanced signatures which contain all the embedded evidence to prove who signed, why they signed, when they signed, and what they signed.

For more detailed information on how SigningHub and the Ascertia 'ADSS Signing Server' enable ETSI PAeS, XAdES, and CAdES compliant signatures please see our datasheet here:

<https://www.ascertia.com/Downloads/datasheets/ADSS-Server-datasheet.pdf>



# Standards compliance

## DocuSign - eIDAS compliance update

DocuSign now offers eIDAS compliant Advanced and Qualified digital signatures.

DocuSign France is a registered Trust Service Provider (QTSP) on the EU Trust List as of June 2018, for the following:

Premium Cloud signing CA:

- > Qualified certificate for electronic signature
- > Qualified certificate for electronic seal
- > Qualified timestamp

DocuSign Standards-Based Signatures for the European Union		
DocuSign’s EU Standards-Based Signatures Portfolio, with Compliant Standards*		
Express Signature “for everyday, global transactions”	EU Advanced Signature “for everyday, global transactions”	EU Qualified Signature “for everyday, global transactions”
Embedded Standards	Embedded Standards	Embedded Standards
X.509 PKI (Digital Certificate and Signature Technology)	X.509 PKI (Digital Certificate and Signature Technology)	X.509 PKI (Digital Certificate and Signature Technology)
RFC 5280 – PKIX	RFC 5280 – PKIX	RFC 5280 – PKIX
ISO 32000-1	ISO 32000-1 LT	PADES B-LT
PADES B-B	ETSI EN 319 411-1	ETSI EN 319 411-2 QCP-n-qscd (Qualified Electronic Signature)
ETSI EN 319 142	ETSI EN 319 421	ETSI EN 319 421
FDA 21 CFR Part 11**	Adobe Approved Trust List	Adobe Approved Trust List
		EU Trusted List Service Provider (TSL) 3 Qualified Signature Creation Device
*Qualified Signature is currently available via integrations with 3rd party TSPs. **Configurable Option		

To make use of Express, EU Advanced and EU Qualified Signature functionality in DocuSign an additional cost product called Standards-Based Signatures is required. The product is not a standard offering in DocuSign and if required DocuSign would have to be engaged to setup the product.





# Internal, remote & on premises signing

## **SigningHub - Ascertia ADSS SAM Appliance**

Designed specifically with Qualified Trust Service Providers (QTSPs) in mind, the Ascertia ADSS SAM Appliance enables remote signing services to be set up and offered to customers. Together with Ascertia's SigningHub and ADSS Server products, QTSPs are now able to provide fully hosted remote signing services or hybrid solutions.

Ascertia's ADSS SAM Appliance was the first product to achieve Common Criteria EAL4+ certification against the eIDAS ETSI EN 419241 standard and the EN 419 241-2 Protection Profile with Level 2 Sole Control. It's a high performance 1U hardware appliance that meets FIPS 140-2 Level 3 criteria.

Seamless integration with Ascertia's SigningHub and ADSS Server products – it can be used to generate, protect and process all user signing keys. It can use software crypto, a software HSM simulator or a PKCS#11 HSM.

## **DocuSign Signature Appliance**

The DocuSign Signature Appliance is a hardware appliance for on-premises or hybrid deployment of electronic signatures and storage of digital signature certificates. It streamlines the signature process, and helps you maximize compliance with regulations.

## **DocuSign Security Appliance**

The DocuSign Security Appliance is a software application for managing DocuSign eSignature encryption keys in a data centre. As an add-on to DocuSign eSignature, it delivers all the benefits of our cloud application, plus the security assurance of storing encryption keys behind a firewall, separate from encrypted documents.



## Internal, remote & on premises signing

### **DocuSign PrivateServer HSM - End of Life**

Also known as DocuSign HSM Appliance (“HSM Appliance”), and its related services and contracts.

### **What is happening with HSM Appliance?**

DocuSign is exiting the HSM business and, as a result, HSM Appliance comes to the end of its life cycle, including End-of-Sale, End-of-Support, and End-of-Life. DocuSign will make best efforts to assist customers with the migration to other HSM offerings of their choosing.

What are the dates for End-of-Sale, End-of-Support and End-of-Life, and what happens at each date?

- End-of-Sale is January 1, 2021. The SKU will be retired and DocuSign will no longer sell the HSM Appliance.
- End-of-Support is July 1, 2022. DocuSign will no longer provide support, service engagements, bug fixes, or patches. **IMPORTANT:** If you have a subscription that ends after this date, DocuSign will continue to provide maintenance and support until the subscription expires.
- End-of-Life is December 31, 2023. The product will be considered fully retired upon this date.



## Comparison table

eIDAS Requirement	SigningHub Compliancy	DocuSign	SigningHub
<b>Electronic Signature types supported</b>	Basic Advanced or Digital AES Qualified or Digital QES	Yes Yes Yes	Yes Yes Yes
<b>Internal Signing</b>	Can you support internal signing by the user organisation?	Yes	Yes
<b>Remote Signing</b>	Can you support remote signing by multiple users at multiple locations?	Yes	Yes
<b>Tamperproof throughout the workflow</b>	Can a document be signed at each stage of a workflow?	Yes	Yes
<b>Document Integrity</b>	Is document integrity maintained?	Yes	Yes
<b>Signature Integrity</b>	Is the signature integrity maintained?	Yes	Yes
<b>Timestamps - 1</b>	Can the timestamp be verified for electronic signatures?	No, it is taken from the user's device (and can therefore be set by the user)	Yes
<b>Timestamps - 2</b>	Can the timestamp be verified for digital signatures?	DS offer eIDAS compliant timestamps as a paid for extra	Yes
<b>Future Proof</b>	Can you prove that a signature was valid at time of signing?	Yes, but documents signed before DocuSign enabled LTV will need to be signed again to have LTV functionality	Yes

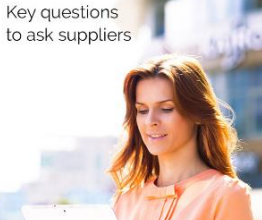


## Comparison table

eIDAS Requirement	SigningHub Compliancy	DocuSign	SigningHub
<b>PDF/A Document Format</b>	Can the document format be rendered in the long-term? Does the document format prevent malicious code?	No – PDF/A not used	Yes
<b>e-Signature Appearances</b>	Can the user's e-signature mark be configured to contain signing time, signing reason, company logos?	Yes	Yes
<b>Digital Signature Strength - 1</b>	Is the signature linked to the user and the signing key under the sole control of the signer?	Yes, but only if using the Standards-Based signature add on	Yes
<b>Digital Signature Strength - 2</b>	Can any subsequent changes to the document be detected?	Yes	Yes
<b>Long-term Verifiability of Signed Documents</b>	Will the signature be independently verifiable in the months and years to come? Does it contain independent proof of signing time and signer's status at time of signing?	Yes, but documents signed before DocuSign enabled LTV will need to be signed again to have LTV functionality	Yes



## Check out the other eBooks in this series



### Check out the other eBooks in this series at:

- > Choosing the Right Type of e-Signature for your business
- > Key Questions to Ask e-Signature Suppliers
- > eIDAS eSignatures & eSeals
- > Why you need to move to SHA2 at every level
- > 6 Common Threats to your signed documents
- > How different high trust industries benefit from e-Signatures.

<https://www.signinghub.com/ebooks/>

**Start using SigningHub Today!**

### Useful Links

**"How-to" demo videos:**

<https://www.signinghub.com/how-to-videos/>

**Why SigningHub is the most secure way to sign:**

<https://www.signinghub.com/security/>

**Integration and API access:**

<https://www.signinghub.com/website-integration/>

**Buy SigningHub now:**

<https://www.signinghub.com/buying/pricing-plan-selection.html>

[info@SigningHub.com](mailto:info@SigningHub.com)

[www.SigningHub.com](http://www.SigningHub.com)

**Thanks for reading  
The SigningHub Team**