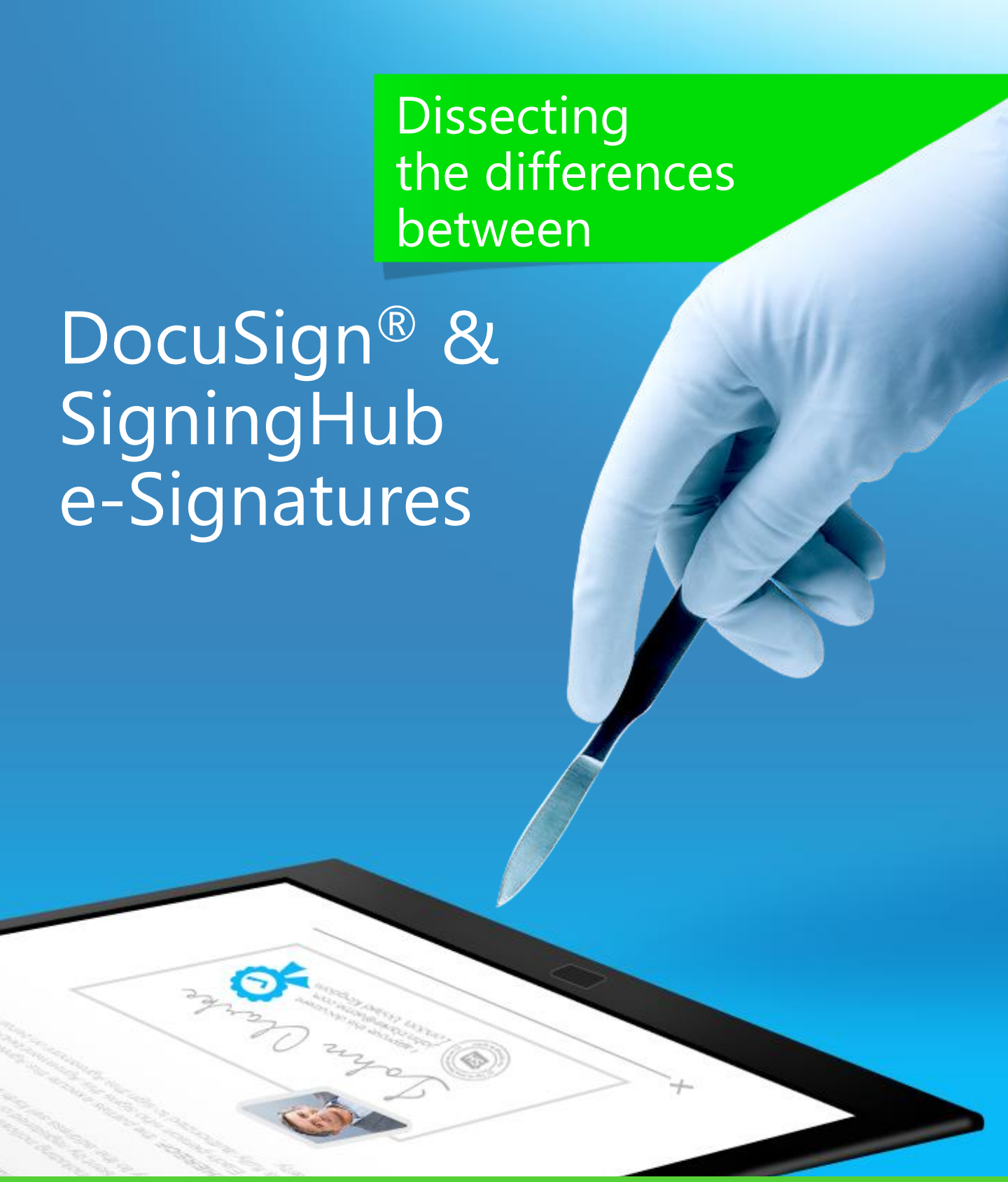
Dissecting the differences between

DocuSign® & SigningHub e-Signatures



What's really inside your e-Signature?

SigningHub

Introduction

What this e-Book delivers

In this eBook we compare the differences in e-Signatures between a document signed using SigningHub and the market-leading provider DocuSign®. The following cloud services were used during this testing:

- DocuSign: https://app.docusign.com/home
- SigningHub: https://web.signinghub.com/Web#/Home

The same Word® document was uploaded to each cloud service in turn and then signed using each service provider's document signing features. The document was then downloaded and the signature verified in Adobe® Reader.

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 for the user 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, how is the user's identity linked to the document and what level of non-repudiation is achieved through the signed document?
- **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. The example signed documents used in this study are also available from Ascertia upon request.

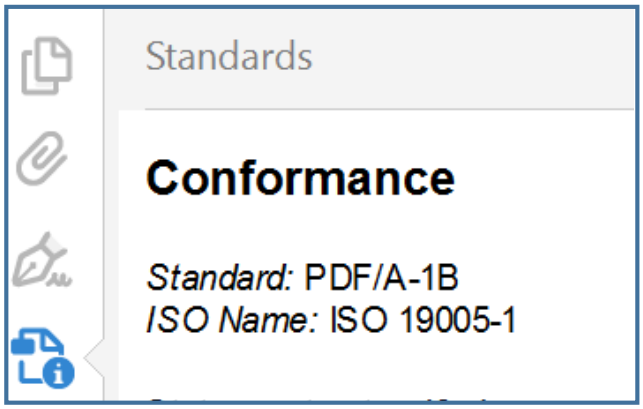
Document Format

DocuSign

DocuSign converts documents to a standard PDF (v1.4) format.

SigningHub

SigningHub automatically converts a broad range of office documents to PDF format and goes a step further to create an enhanced PDF referred to as **PDF/A**. If you open a SigningHub signed document inside Adobe Reader it shows this detail:



PDF/A is an ISO standard (ISO 19005-1:2005) 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.

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 is 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.

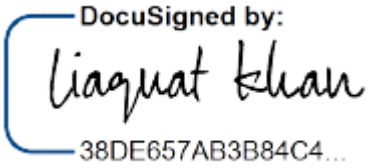
PDF/A format is *strongly* recommended for better security and long-term rendering of signed documents

e-Signature Appearance

An e-Signature appearance is the user's mark on the document to indicate their consent with the document contents. Typically it takes the form of an ink signature image.

DocuSign

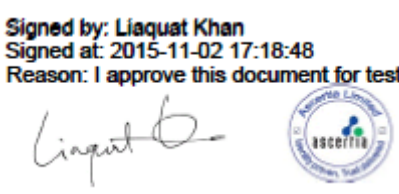
DocuSign supports the use of text-based signatures using fonts which resemble an ink signature. The user can select from a range of styles. DocuSign also provides the option to draw the signature dynamically e.g. on a touch device.



Example e-Signature appearance created using DocuSign text option

SigningHub

SigningHub provides text-based signature appearance as well as drawing options. In addition it also provides a facility to upload a scanned hand-signature image. Furthermore, it allows the use of company logos/seals as a watermark as well as presenting text elements inside the signature appearance which can indicate who signed, when they signed and for what reason.



Example SigningHub signature appearance including text, scanned ink signature image, and company seal

Example SigningHub signature appearance this time only including the signature image

Digital Signature Strength

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 there is a standard definition of the properties of an advanced electronic signature. These are:

- Must be uniquely inked 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:

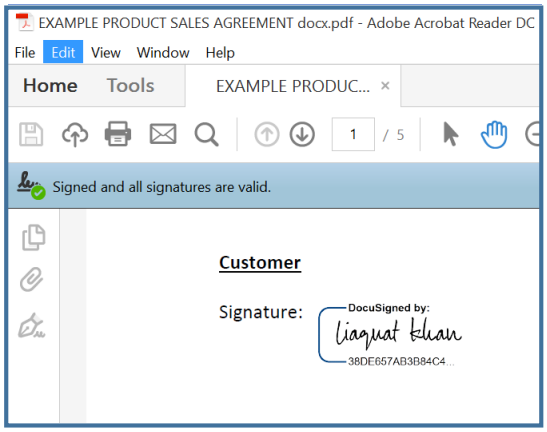
- Who signed it (without any ambiguity), and
- Confirm that no changes were made to the document subsequent to signing

Other jurisdictions follow a similar definition to the EU when describing secure forms of e-signatures.

We will assess the signatures from DocuSign and SigningHub using these requirements of an advanced electronic signature.

Digital Signature Strength - DocuSign

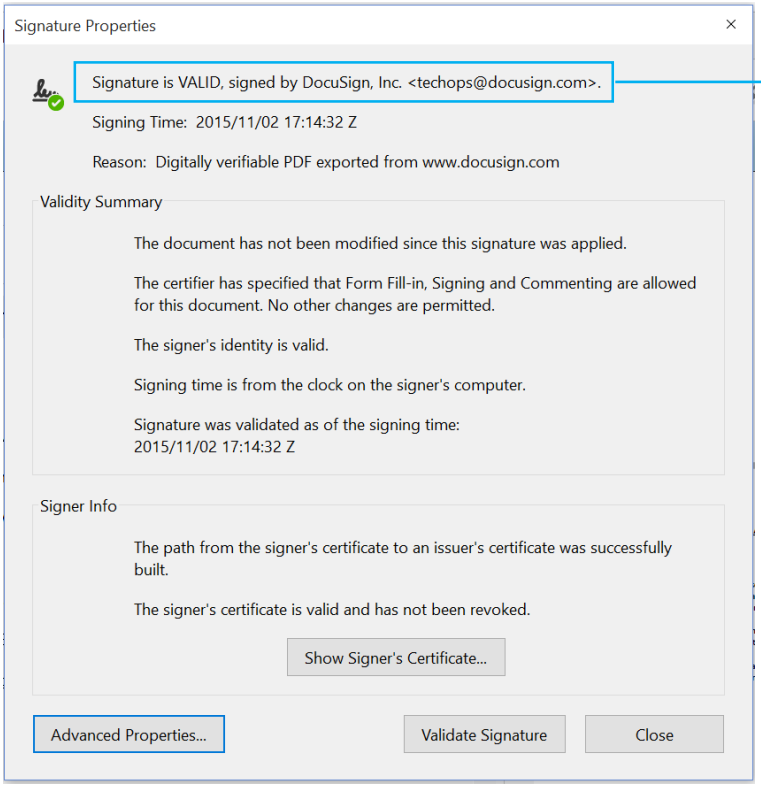
When a signed document from DocuSign is opened in Adobe Reader, the following is shown:



The blue bar shows the document is "Signed and all signatures are valid". At a high-level this sounds encouraging.

However, the e-signature appearance printed on the document **doesn't provide any conclusive proof** as to who actually signed, since this could just be an illegible squiggle. 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:



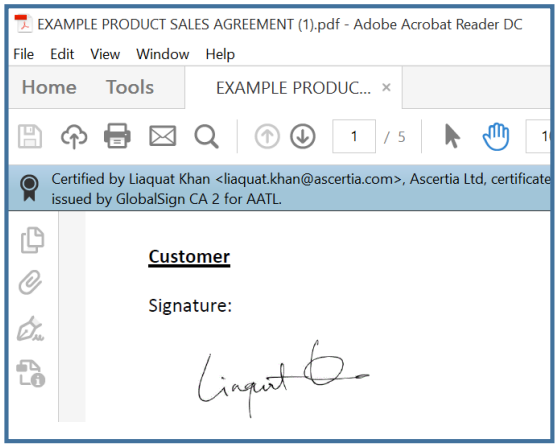
This is a **serious** problem - the signature shows it's signed by DocuSign. <u>This fails to identify the real end-user who actually signed the document.</u>

As the signature is created using one central digital signature key owned by DocuSign, this also fails on the EU requirement *"Created using means that the signatory can maintain under their sole control"*

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

Digital Signature Strength - SigningHub

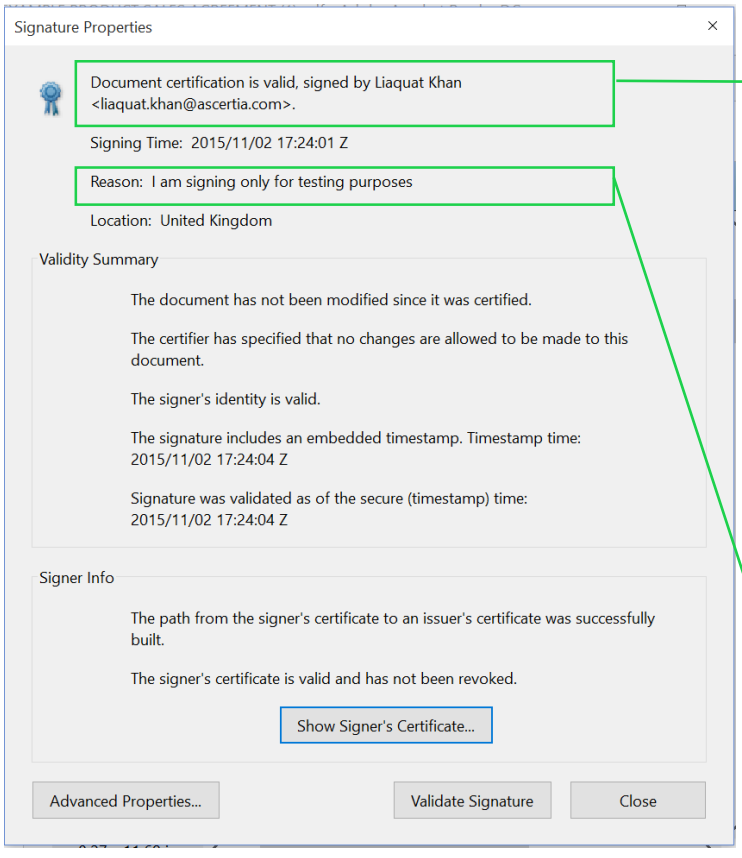
When a signed document from SigningHub is opened in Adobe Reader, the following is shown:



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 (in this case "GlobalSign") who is vouching for the signer's identity. This is a Trusted Third Party which validated the identity and that of the employer.

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



SigningHub clearly identifies the end-user who signed the document. This is possible because SigningHub uses unique signing keys/certificates for every user issued by trusted CAs (as well as its built-in CA).

These keys are under the sole control of the owning 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 possible with DocuSign).

SigningHub also uses secure signature algorithms (SHA256 and RSA2048).

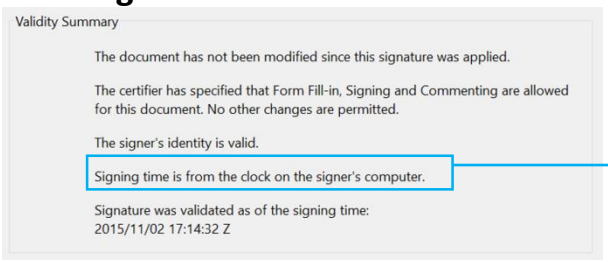
Long-Term Signatures

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. 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.

Let's look at what Adobe Reader makes of DocuSign and SigningHub signatures from a long-term verifiable perspective.

DocuSign



DocuSign does not create e-signatures which will be verifiable in the long-term. It uses the signing time based on the signer's computer, which can't be independently trusted. DocuSign does not embed proof that at the time of signing the signer's digital identity was valid.

SigningHub

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).

It is essential that signed documents are verifiable in the long-term and so standard ETSI PAdES long-term signatures must be used with embedded proofs that allow independent offline verification into the future.

Conclusions

The following table summarises the results of this study:

Property	Purpose	DocuSign	SigningHub
PDF/A Document Format	Can the document format be rendered in the long-term? Does the document format prevent malicious code?	✗	✓
e-Signature Appearances	Can the user's e-signature mark be configured to contain signing time, signing reason, company logos?	✗	✓
Digital Signature Strength - 1	Is the signature linked to the user and the signing key under the sole control of the signer?	✗	✓
Digital Signature Strength - 2	Can any subsequent changes to the document be detected?	✓	✓
Long-term Verifiability of Signed Documents	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?	✗	✓

Check out the other eBooks in this series:

Choosing the Right Type of e-Signature for your business

Key Questions to Ask e-Signature Suppliers

Start using SigningHub Today!

Free Trial

info@SigningHub.com

www.SigningHub.com

Thanks for reading

The SigningHub Team

Useful Links

"How-to" demo videos:
https://www.signinghub.com/how-to-videos/

Integration and API access:
https://www.signinghub.com/website-integration/

Why SigningHub is the most secure way to sign:
https://www.signinghub.com/security/

Buy SigningHub now:
https://www.signinghub.com/buying/pricing-plan-selection.html