

Analizando las
diferencias entre las
firmas digitales

DocuSign® & SigningHub



¿Qué es lo que contiene realmente
una firma digital o electrónica?

SigningHub

Introducción

En este documento se comparan las diferencias de las firmas digitales de documentos firmados utilizando SigningHub y DocuSign®. Los siguientes servicios en la nube fueron utilizados para realizar esta prueba:

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

El mismo documento Word® fue subido a cada uno de los servicios de firma en la nube, cada uno a la vez y luego fueron firmados utilizando cada uno de los servicios y funcionalidades disponibles. El documento luego fue bajado y las firmas verificadas en Adobe® Reader.

Los siguientes aspectos fueron analizados durante esta prueba:

- **Formato del Documento:** ¿El documento es transformado a un formato seguro de manera previa a su firma?
- **Apariencia de la Firma Digital:** ¿Qué opciones se encuentran disponibles para el usuario de manera que pueda utilizar la misma forma de su firma manuscrita en el documento?
- **Robustez de la Firma Digital:** ¿De qué manera el documento se bloquea después de firmar de manera que no puedan ser realizados cambios? ¿De qué manera la identidad del firmante se liga al documento? ¿Qué nivel de no repudio se logra a través del documento firmado?
- **Verificación de Largo Plazo:** ¿Pueden las firmas de los usuarios ser verificadas en el largo plazo?

Cada aspecto de los arriba mencionado está cubierto en una sección separada de este documento. Una muestra de los documentos firmados utilizados en este estudio también se encuentra disponible en Ascertia y pueden solicitarse.

Formato del Documento

DocuSign

DocuSign transforma los documentos al formato estándar de PDF (v1.4).

SigningHub

SigningHub automáticamente transforma un amplio rango de documentos de Office a formato PDF y va un paso más allá transformando el formato a los documentos PDF a **PDF/A**. Si un documento firmado por SigningHub se abre desde Adobe Reader se mostrará el siguiente detalle:



PDF/A es un formato estándar ISO (ISO 19005-1:2005) especializado para la preservación digital de documentos electrónicos. PDF/A se diferencia de PDF al no permitir características que no sean adecuadas para la firma segura y el archivo de largo plazo.

De manera específica PDF/A requiere que:

- Que las fuentes se encuentren completamente incrustadas en lugar de que estén disponibles a través de links dinámicos. Esto garantiza la representación del documento firmado en el largo plazo y evita que las fuentes sean cambiados en el futuro.
- Está prohibido JavaScript y otros contenidos ejecutables. Esto evita que un código malicioso que pueda estar dentro del documento, cambie la vista del documento para el usuario al momento de firmar. Esto es esencial para lograr *What You See Is What You Sign (WYSIWYS)*, lo que se ve es lo que se firma, un importante requisito de seguridad para evitar el no-repudio.

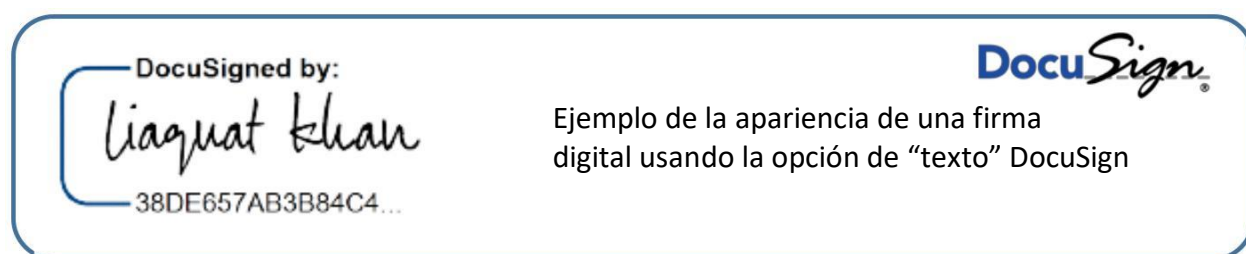
El formato PDF/A es ampliamente recomendado para un mejor nivel de seguridad y representación al largo plazo de los documentos firmados.

Apariencia de la Firma Digital

La apariencia de una firma digital corresponde a la firma del usuario en el documento que indica su consentimiento a los contenidos del mismo. Típicamente tiene el formato de la firma manuscrita en papel.

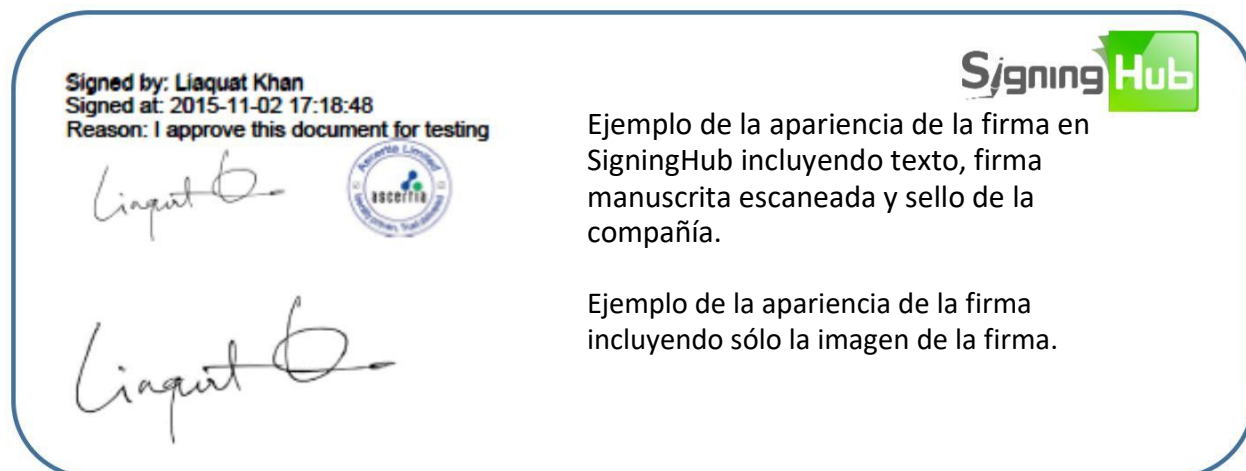
DocuSign

DocuSign soporta el uso de firmas basadas en textos, utilizando fonts que asemejan la firma en papel. El usuario puede seleccionar dentro de un amplio rango de estilos. DocuSign también provee la opción de dibujar la firma de manera dinámica, por ej. A través de un dispositivo touch.



SigningHub

SigningHub permite el uso de firmas con apariencia basada en texto así como también las que son "dibujadas". Adicionalmente provee la facilidad de subir una firma manuscrita escaneada. Más aún, permite el uso de logos y sellos de la empresa u organización como un sello de agua, así como la incorporación de textos en su interior, con información respecto de quien firmó, cuando firmó y por qué razón.



Robustez de las Firmas Digitales

Un documento firmado debe tener ciertas propiedades de seguridad inherentes para que resulten útiles para su uso en el mundo de negocios, así como proveer de evidencia legalmente aceptable en el caso de ser requerida por la justicia.

Este tipo de firmas a menudo se le denomina “firmas electrónicas avanzadas”. En la Unión Europea (UE) existe un estándar que define las propiedades de la firma avanzada, éste incluye:

- Deben estar vinculado al firmante de manera única
- Deben ser capaces de identificar al firmante
- Creada a través de mecanismos que el firmante pueda mantener bajo su control único.
- Vinculada de tal manera a los datos a los cuales se encuentra relacionada que cualquier cambio posterior en ellos pueda ser detectado.

Cualquiera debe ser capaz de verificar un documento firmado en términos de:

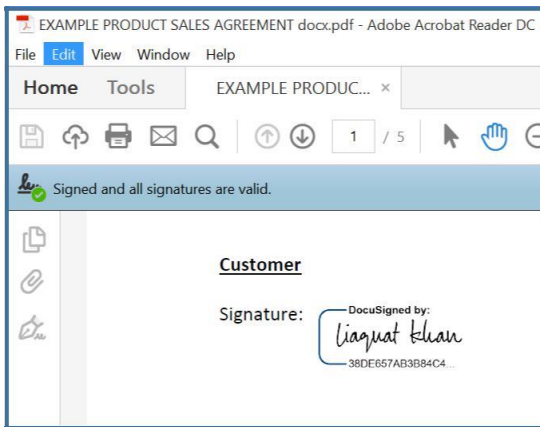
- Quién lo firmó (sin ninguna ambigüedad), y
- Confirmar que no se han realizados cambios después de que el documento fue firmado

Otros países o jurisdicciones siguen definiciones similares a los de la Unión Europea cuando describen formatos seguros de firmas digitales.

Realizaremos a continuación un análisis de las firmas digitales en DocuSign y SigningHub usando los requerimientos definidos para las firmas electrónicas avanzadas.

Robustez de las Firmas Digitales - DocuSign

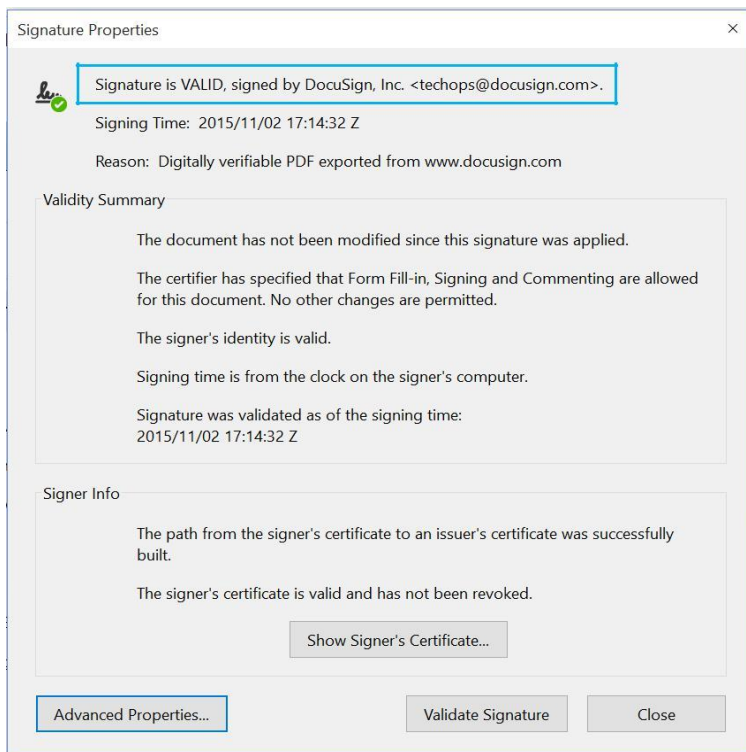
Cuando un documento firmado en DocuSign es abierto en Adobe Reader, la siguiente información se muestra:



La barra azul muestra que es documento se encuentra “Firmado y todas las firmas son válidas”.

Sin embargo la apariencia de la firma en el documento **no es una prueba concluyente** de quien, dado que se trata ya que esto podría ser un garabato ilegible. También puede haber muchos usuarios con el mismo nombre lo que hace difícil determinar quien realmente firmó.

Con una firma en DocuSign, la apariencia de la firma digital no es clickeable para su análisis. El diálogo de propiedades de la firma de Adobe Reader Signature no obstante puede ser abierto y muestra lo siguiente:



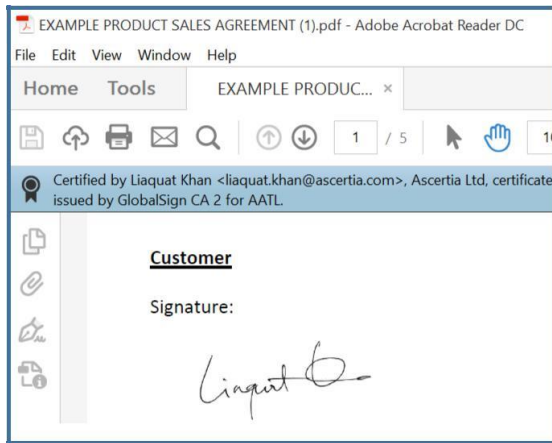
Este es un problema serio, la firma muestra que ha sido firmado por DocuSign, pero falla en identificar el usuario final real que firmó el documento.

Dado que la firma se crea a través de Claves de firma central en DocuSign no Cumple con los requisitos de la UE “Creada usando medios que solo el firmante tiene control de manera exclusiva”

DocuSign provee protección a la integridad del documento ya que el documento es firmado utilizando algoritmos robustos (SHA256/RSA2048) y cualquier cambio posterior al documento será detectado.

Robustez de la Firma Digital - SigningHub

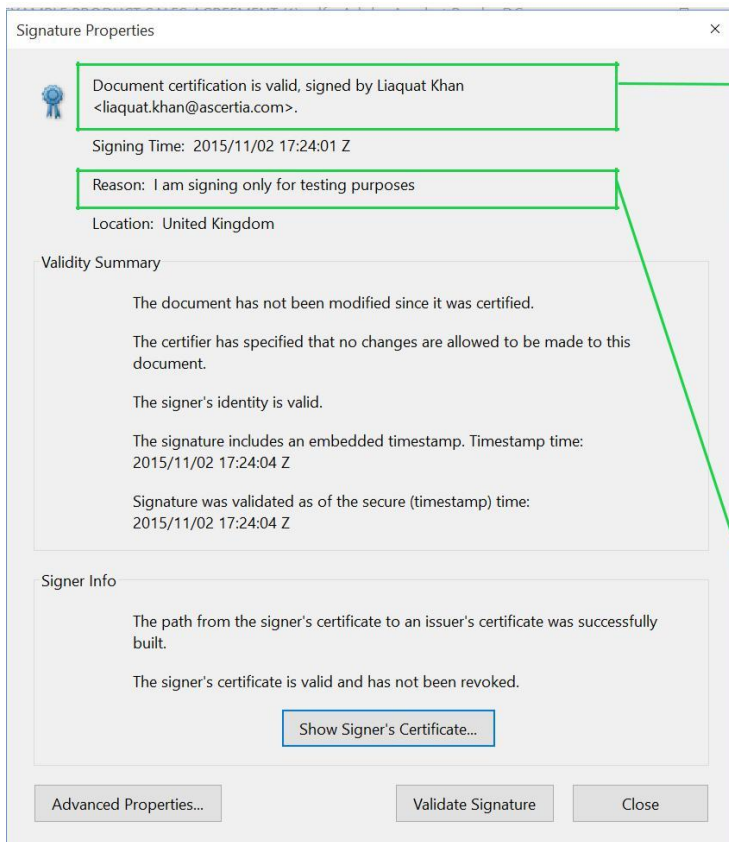
Cuando un documento firmado por SigningHub se abre en Adobe Reader, la siguiente información aparece:



Con SigningHub, la barra azul muestra quien firmó el documento (incluyendo su dirección de correo) y quien es su empleador, en este caso Ascertia Limited.

Va un paso más allá al mostrar la Autoridad Certificadora (en este caso "GlobalSign") que está avalando la identidad del firmante. Es un tercero de confianza que validó la identidad del empleador y al empleador.

Con SigningHub, al hacer click en las firmas digitales Adobe Reader de manera inmediata presenta la siguiente información:



SigningHub identifica claramente al usuario que firmó el documento. Esto es posible porque SigningHub usa claves de firma/certificados únicos para cada usuario, los que son emitidos por CAs confiables (así como incorporados en la CA).

Estas claves están en posesión y control único del usuario que es el dueño, así nadie más puede crear firmas en lugar del titular.

El documento además es "certificado" – este es un tipo especial de firma PDF que evita la incorporación de cualquier contenido por ej. Comentarios o anotaciones. Finalmente es posible que el firmante defina en su firma, la razón de ella (que no parece posible de realizar con DocuSign).

SigningHub además utiliza algoritmos de firma seguros (SHA256 and RSA2048).

Firmas de Largo Plazo

Los documentos en el mundo de la empresa, el gobierno, las organizaciones necesitan ser verificables por meses y años en el futuro.

Para lograr esta condición se requiere de una firma avanzada digital habitualmente denominada como firma de verificación en el largo plazo.

El formato estándar para ello es conocido como ETSI PAdES. Los documentos firmados con firmas de largo plazo incluyen sellos de tiempo que pueden ser verificados de manera independiente para probar cuando fueron firmados.

También contienen pruebas de confianza respecto de que el certificado digital del firmante era válido al momento de la firma.

Revisemos lo que hace Adobe Reader a las firmas digitales en DocuSign y SigningHub desde la perspectiva de la verificación de las firmas de largo plazo.

DocuSign

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.

The signer's identity is valid.

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

Signature was validated as of the signing time:
2015/11/02 17:14:32 Z

A blue box highlights the text "Signing time is from the clock on the signer's computer." with a blue arrow pointing to the right.

DocuSign no crea firmas que puedan ser verificables en el largo plazo. Utiliza para registrar el momento en el que el documento fue firmado la fecha del computador del usuario, lo que no permite la independencia en la fuente de confianza. DocuSign no incrusta evidencia de prueba que permita validar que al momento de la firma la identidad digital era válida.

SigningHub

Validity Summary

The document has not been modified since it was certified.

The certifier has specified that no changes are allowed to be made to this document.

The signer's identity is valid.

The signature includes an embedded timestamp. Timestamp time:
2015/11/02 17:24:04 Z

Signature was validated as of the secure (timestamp) time:
2015/11/02 17:24:04 Z

A green box highlights the timestamp information with a green arrow pointing to the right.

SigningHub crea firmas de largo plazo de acuerdo al estándar (PAdES). Así también incrusta un sello de tiempo confiable emitido por una autoridad acreditada (Time Stamp Authority -TSA). SigningHub también incorpora pruebas respecto a la validez de la identidad del firmante en el momento de su firma (a través de información CRLs/OCSP).

Es fundamental que los documentos firmados puedan ser verificables en el largo plazo, por ello es necesario utilizar el estándar ETSI PAdES que incrusten en la firma pruebas de evidencia que puedan ser verificadas por entidades independientes en el futuro.

Conclusiones

La siguiente tabla resume las conclusiones de este estudio:

Propiedad	Objetivo	DocuSign	SigningHub
Formato del Documento PDF/A	¿Puede el formato del documento ser utilizado en el largo plazo? ¿El formato del documento evita código malicioso?		
Apariencia de la Firma Digital	¿Puede ser configurada la apariencia de la firma del usuario, la fecha de la firma, la razón, el logo de la empresa?		
Fortaleza de la Firma Digital (1)	¿Se encuentra la firma ligada al usuario y las llaves de firma bajo el solo control del firmante?		
Fortaleza de la Firma Digital (2)	¿Es posible detectar cualquier cambio que se haga al documento una vez firmado?		
Verificación de Largo Plazo de los Documentos Firmados	Puede la firma ser verificada de manera independiente en los siguientes meses o años? ¿Contiene la firma una prueba independiente de la fecha en que se firmó del estado del firmante al momento de la firma?		