Your Digital File vs. DocuSign

The Cryptoloc® Advantage

Document Security

At-Rest (HDD)

your Digital file® SMARTER SECURITY	DocuSign
All documents stored on Your Digital File's servers are protected using our patented Cryptoloc® technology (industry best practice encryption at-rest is the default). In the unlikely event our servers were to be compromised, the content of all users' documents remain confidential as YDF does not store or have access to client document decryption keys.[1]	Documents stored on DocuSign's infrastructure may be encrypted with 256-bit AES encryption[2] and is therefore decrypted on DocuSign's servers. This means DocuSign likely has access to the document encryption keys.

In-Flight (TLS)

your Digital file® SMARTER SECURITY	DocuSign
Not only does Your Digital File use Cryptoloc® technology to provide industry's best practice Transport Layer (TLS) to protect network communications, but even if a document is intercepted in-flight it can only be decrypted on the client's device (PC, smartphone, tablet) using their private key (RSA 2048-bit) to unlock the decryption key.[1]	DocuSign supports TLS network encryption.

.

Document Integrity

Client-side Hash Generation

your Digital file® SMARTER SECURITY	DocuSign
SHA-2, 512-bits. A hash is calculated twice for each document on the user's computer, once before it is encrypted and again after it is encrypted. These are then signed by the user prior to uploading to Your Digital File to ensure "fingerprint" integrity.	**Not available**. As of this writing, DocuSign does not provide this functionality.

Server-side Hash Generation

your Digital file® SMARTER SECURITY	DocuSign
SHA-2, 512-bits. Your Digital File performs server-side hashing for documents uploaded via SecureShare™. These documents are still protected by transport-layer security (TLS), and upon receipt by Your Digital File, are twice hashed, signed and encrypted using the same patented Cryptoloc® security algorithms.	**SHA-2, 256-bits**. DocuSign hashes are calculated server-side using a 256-bit SHA-2 hash.[3]

[1] Cryptoloc® provides a function known SecureShare™: During a SecureShare™ a user instructs the YDF system access to a document's encryption key at the instant a share is created and/or accessed by the recipient of the shared file. The system access to the document in its complete, unencrypted form only at the instant a recipient downloads the shared document.

[2] https://trust.docusign.com/en-us/trust-certifications/security-assurance-program/

[3] https://support.docusign.com/en/answers/00083753 (2017)

Signature Algorithm

Your Digital File signatures are generated by creating a **SHA-2 512-bit hash** of the unencrypted document's "fingerprint" and the current date and time, and applying the RSA digital signature algorithm. All signatures are generated or verified using the user's Private Key (client-side) on their computer using the user's **RSA 2048 bit private key**.

DocuSign signatures are generated based on a **SHA-2 512-bit** hash. All digital signature cryptography is performed server-side.

Signature Integrity

The hash of the original document is used as the PlainText for all user signatures and validation upon download and decryption.

The hash of the encrypted document is used to verify the document's integrity upon receipt by Your Digital File. This also allows us to continually validate a document's integrity "at rest" and on the client's computer prior to decryption.

All DocuSign hashes are performed server-side and hence the integrity of documents, and their resultant signatures, could be compromised if a server or it's authorised access mechanism are breached.

Content Confidentiality

your Digital file SMARTER SECURITY

DocuSign

Document Content

All documents stored by Your Digital File are encrypted with an AES 256-bit encryption key and then uploaded to the cloud. All files on the cloud are also are protected by our patented Cryptoloc® technology. In the unlikely event our servers were to be compromised, the content of all users' documents remain confidential as we do not store or have access to the complete document encryption keys.

"All eContracts or eDocuments created by our customers when using the DocuSign Signature service is automatically encrypted with an AES 256-bit, or equivalent, encryption key."[5]

This means that if DocuSign's servers are compromised, by external or internal threat actors, user data may be exposed.

Personally Identifiable Information

YDF users cannot directly interact with other users except when they share documents with each other. Even in this case, the only personally identifiable information (PII) available is a user's name and email address (*their username*). Users have full control over whether they are searchable by other authenticated (logged-in) users.

"DocuSign ensures that no personally identifiable information (PII) is displayed to users via email or on our website without the recipient successfully identifying himself/herself through one or more of the authentication options."[5]

Can the system view my documents?

No The Your Digital File system and staff cannot decrypt your documents and view the content. All user documents are always stored in encrypted form on our servers. Documents can only be decrypted on the user's computer.[1]

Yes Documents are decrypted by DocuSign (server side) to support manipulation and web-views.

[1] Exception: SecureShare™: During a SecureShare™ a user instructs the YDF system to access a document's encryption key at the instant a share is created and/or accessed by the recipient of the shared file. The system provides access to the document in its complete, unencrypted form only at the instant a recipient downloads the shared document as authorised by the owner of the file. The complete decryption key created during a SecureShare™ operation is discarded by the system immediately following its usage.

[5] https://trust.docusign.com/en-us/trust-certifications/gdpr/gdpr-faqs/

Faster Signatures

	your Digital file SMARTER SECURITY	DocuSign
Q Can documents be easily signed?	**Yes** Simply upload your document into the system, then share the file, giving the recipient permission to sign the file.	**No** Once documents have been uploaded to DocuSign, signature templates need to be created and added to relevant pages. Recipients need to sign each designated page.
Q Is there a strong audit trail for each signature?	**Yes** Each document signature has a time and date stamped embedded within it. Signatures are created on the client's computer using their own Private Key. These signatures, and the audit trail, cannot be falsified after the event.	**No** While each signature is time and date stamped, the digital signatures are generated on DocuSign's servers may be at risk of modification if DocuSign's servers are compromised, by external or internal threat actors.
Q Does the recipient need to sign all nominated pages in the document?	**No** When a recipient signs a document it is signed in its entirety and **is legally binding as long as both parties agree to trust the YDF platform for their legal or contractual negotiations**. Any alteration of document creates a new version of that document via YDF and renders the digital signature void, so parties must re-sign each new version to continue to their agreement. *A digital signature is cryptographically-tied to the document's current content and is therefore resilient to fraudulent changes to the document following signing.*	**Yes** DocuSign encourages the insertion of visual signatures and initials on individual pages of electronic documents. *This is usually unnecessary when using digital signing because a digital signature is cryptographically-tied to the document's current content and is therefore resilient to fraudulent changes to the document following signing. There may be a process or business requirement for signing each page, but digital signatures render this redundant.*

Superior Signature Authenticity

your Digital file SMARTER SECURITY

DocuSign

How do I know the document was signed by right person?

In addition to a username and password, each user requires a Private Key, which is generated when they sign-up to Your Digital File. A user's Private Key is only ever stored on their computer (client side) and is used when uploading and signing documents.

Once a YDF user has created their access account (username, password and private key) they may upload and digitally-sign documents to share with other YDF users or external parties.

YDF users who mutually agree to trust YDF digital signatures explicitly can digitally-sign each other's documents to verify the integrity of written communications or even in support of contract negotiations using the YDF service.

YDF users can securely also share digitally-signed documents with non-YDF users through the "SecureShare" service. SecureShare recipients' identities are verified through control of both an email address and mobile phone number, which are provided by the user requesting the document. A SecureShare recipient can only access the document through a link sent to their email address and is challenged via an SMS code each time they access and sign a document.

All file encryption keys are located in the DocuSign system (server side) and are therefore not under the direct control of the user.

What if the document is changed after signing?

If the document is altered, all parties to the agreement need to sign the new version of the document. Digital signatures are only valid for the specific version of the document which was signed.

How does Your Digital File deliver Advanced Key Management for maximum information security?

Advanced (Document) Key Management is provided by our patented Cryptoloc® technology and is superior to DocuSign as users' document encryption keys cannot be decrypted by our servers.

- ✓ • Your Digital File's Document Encryption Keys are never stored in a complete form and cannot be decrypted by a single party.
- ✓ • Each Document Encryption Key is made up of three master keys, which are shared between the three parties defined in the system (**user/service/escrow**). Two parties of these parties (**user/service**) must collaborate to decrypt a document for a user or recipient nominated by that user.
- ✓ • Collaboration between the **service** and the **escrow** parties is only used to re-establish access to a user's files should they lose their private key. This collaboration does not result in either party (service/escrow) possessing the decryption keys for a user's files; as the escrow account is not a full-user.

The Cryptoloc® Advantage

- ✓ • Advanced Document Key Management and simplicity of use.
- ✓ • Integrity and validation of all important user actions (all critical user actions such as sharing & authorizing, nominating, signing and all permissions require the User's private key).
- ✓ • A Data Legacy service, enabling your data to be accessible to authorized parties in the event you or your business ceases to exist.

Where is your data stored?

Your Digital File's US servers are based only in **the USA** where data is governed by **US law**.

DocuSign has data centres in North America and the European Union.

Data stored on overseas servers is not governed by US law.