Your Digital File vs. DocuSign

The Cryptoloc Advantage

Document Security

your Digital file® SMARTER SECURITY

DocuSign®

At-Rest (HDD)

All documents stored on Your Digital File's servers are protected using our patented Cryptoloc technology, securing each file with a unique 256-bit AES key. 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.[1]

Documents stored on DocuSign's infrastructure may be encrypted with 256-bit AES encryption[2], however, this is unclear because, as data is viewed in a web browser, it must therefore be decrypted on DocuSign's servers. This means that DocuSign, not the user, controls the document encryption keys.

In-Flight (TLS)

As documents are protected using Cryptoloc technology, even if the Transport Layer encryption is broken, documents are still protected and can only be decrypted on the client's computer[1]. In addition, we specifically select the highest grade cipher suites and mandate server-side selection of cryptographic cipher protecting user's web access using the strongest available encryption algorithms.

DocuSign espouses *"secure, private SSL 256 bit viewing session"*[2], but does not specify any additional security steps taken.

A security analysis of their login page indicates that they do not even support "Forward Secrecy"[3] [4] with their selection of SSL/TLS ciphers.

Content Confidentiality

your Digital file® SMARTER SECURITY

DocuSign®

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.

Personally Identifiable Information

Users who have not been fully identified cannot directly interact with other users unless they have been explicitly trusted by a fully identified user. Users have full control over whether they are searchable by other authenticated (logged-in) users and even then, only their name, username, position and company is ever displayed to other 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]

[1] Except for SecureShare. We have access to a document's encryption key only at the instant a share is created and or accessed by the recipient. We have access to the document in its complete, unencrypted form only at the instant a recipient downloads the shared document. In contrast, DocuSign has the ability to access the entire, unencrypted document at all times.

[2] Excerpt from the DocuSign Trust Center, "Security Assurance Program" – https://trust.docusign.com/security-assurance-program

[3] Qualys SSL Server Test Results for DocuSign's Login page – https://www.ssllabs.com/ssltest/analyze.html?d=www.docusign.net

[4] As assessed using Qualys SSL Server Test site on Wed, 08 Jul 2015 20:03:47 UTC for the DocuSign Login page, docusign.net (209.67.98.12)

Content Confidentiality

your Digital file SMARTER SECURITY

DocuSign

Document Content

All documents stored on Your Digital File's servers are protected using our patented Cryptoloc technology, securing each file with a unique 256-bit AES key.

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.[1]

"We (DocuSign) ensure the privacy of your legal documents by encrypting them and enacting internal security policies to ensure no employee, even customer support, can view your sensitive documents."[5]

This means that if DocuSign's servers are compromised, by external or internal threat actors, user data is exposed and document confidentiality cannot be guaranteed.

Document Integrity

your Digital file SMARTER SECURITY

DocuSign

Signature Algorithm

RSA-SHA512, RSA public-key crypto with SHA-2 hash, 512-bits. Your Digital File signatures are generated by creating a 512-bit SHA-2 hash of the unencrypted document's "fingerprint" and the current date and time, and applying the RSA digital signature algorithm. This signature is generated using the user's Private Key on their computer.

Unspecified. DocuSign signatures are generated based on a 160-bit SHA-1 hash (a known weak algorithm) and a visual (a.k.a. "wet-ink") signature. All digital signature cryptography is performed server-side.

Client-side Hash Generation

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. DocuSign does not provide this functionality.

Server-side Hash Generation

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, and upon receipt by Your Digital File, are twice hashed, signed and encrypted using the same patented Cryptoloc security algorithms.

SHA-1, 160-bits. DocuSign hashes are calculated server-side using a 160-bit SHA-1 hash (a known weak algorithm). This means a document's integrity is not guaranteed, as documents may be corrupted or altered in transit with no means of detection.

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 on their servers and as such, the integrity of the documents is always in question.

[5] Excerpt from DocuSign, "World-Class Legal Protection" – https://www.docusign.com/how-it-works/legality

Faster Signatures

Q	your Digital file® SMARTER SECURITY	DocuSign®
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.
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 and are at risk of modification if DocuSign's servers are compromised, by external or internal threat actors.
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. No further precautions are necessary as any alteration creates a new version of the document and renders the digital signature void.	Yes DocuSign encourages the insertion of visual signatures and initials on individual pages of electronic documents. This is not necessary when signing using digital signatures. The practice of signing or initialling individual pages is an historic security precaution for the prevention of insertion, removal or alteration after paper documents have been signed.

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 and is used when uploading and signing documents. Our highest level of identity verification confirms each user's identity using the Australian Financial Transaction Reports Regulations[6] (100 point check). Only users with this level of identity verification, users of verified business accounts and users you trust explicitly can sign your documents.

SecureShare recipients' identities are verified through control of both an email address and mobile phone number, which are provided by the user requesting the signature. 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 not controlled by the user.

DocuSign's default identity verification process only requires users to provide a username and password.

[6] Australian Financial Reports Regulations 1990 (Cth) as amended, taking into account amendments up to Human Services Legislation Amendment Regulations 2011 (No. 1), "3 The verification procedure" – https://www.comlaw.gov.au/Details/F2011C00426

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 of which must collaborate to decrypt a document.

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 & authorising, nominating, signing and all permissions require the User's private key).

✓ A Data Legacy service, enabling your data to be accessible to authorised parties in the event you or your business ceases to exist.

Where is your data stored?

Your Digital File's servers are based in ***Australia*** where data is governed by ***Australian law***.

DocuSign currently only has data centres in North America and the European Union.[7]

Data stored on overseas servers is *not* governed by Australian law.

[7] DocuSign Trust Center, System Status – https://trust.docusign.com/system-status/