cryptoloc

Security technology whitepaper

Cyber threats are listed in the top five global priorities for 2018

According to the Global Risks Report for 2018, cyber risks are in the top 5 of global priorities. The world's increasing interconnectedness and pace heightens our vulnerability to attacks that cause not only isolated and temporary disruptions, but radical and irreversible systemic shocks.

Solutions using our patented Cryptoloc security Technology are at the forefront of secure digital document management.

If cloud-stored information privacy, confidentiality and integrity matter to you, then Cryptoloc is the solution.

The Cryptoloc mechanism provides strong asset and access protection for online document storage.

The Cryptoloc security advantage explained

Cryptoloc technology provides a mechanism for protecting the confidentiality and integrity of documents stored online by integrating Shamir's secret sharing algorithm (RSA), the Advanced Encryption Standard (AES-256) and Rivest-Shamir-Adelman (RSA-4096) Public-Private key cryptography.

Access to online (cloud-hosted) documents can be truly restricted to the owner or persons they authorise, because the cloud host never sees the complete decryption key of any document stored by a document owner. Decryption keys are split and stored by three different parties (the owner, the cloud host and an independent escrow agent).

Assembly of document's decryption key relies on access to a document owner's Private key, and authenticated access to a cloud-hosted Cryptoloc – based solution.

Owners manage access to their own Private key. If the owner of a Cryptoloc – stored document loses their access (e.g. by forgetting the authentication Password to their cloud-hosted Cryptoloc account; or by losing their Private Key), access to their encrypted documents can be restored without compromising the security of the stored documents via the Cryptoloc Escrow Recovery Process.

Cryptoloc Technology Overview

In a Cryptoloc – based solution, document owners use a locally generated private/ public key-pair (4096-bit RSA) to protect the encryption key for each document upload to the cloud. Document owners also use a password authenticated account to access the cloud-hosted Cryptoloc – based solution.

Each time a document is stored, a new random encryption key is generated client-side (i.e. on their local device: PC, smartphone or tablet). Uploading to the cloud via Cryptoloc involves sharing the secret (the encryption key) for each document between each of the three different parties (the document-owner, the cloud-host and an escrow agent). This has the effect of hiding the key material until it is needed to decrypt the document again.

A documents owner's Private Key once generated is only stored locally on their only sign-up device (although it can be transferred to other client devices under the owner's control as required).

A document owner's Private Key is used for decryption of their part of the document encryption key and can also be used for the digital-signing of documents stored in the cloud.

A document owner's Public Key is used to encrypt their part of each document's encryption key and is also used by others to verify the digital signature on a document shared to a third party (see **Cryptoloc-based Document-sharing** below).

Cryptoloc-based Document Upload

DOCUMENT UPLOAD

Step 1 – Document Encryption Key

- Whenever a document owner uploads a document to cloud storage, Cryptoloc first generates three (randomly-generated AES-256) symmetric encryption keys [known as the Primary Document Encryption keys] on the client device. Collectively, these form the document owner's Document Encryption Key (DEK).
- The DEK is used to encrypt the document locally (on the client device) prior to upload.

DOCUMENT UPLOAD

Step 2 – Key Splits

The Primary Document Encryption keys for each document are also duplicated (once again on the client device) so that there are two copies of each one (i.e. six keys). Pairings of two different Primary Encryption keys are then prepared for distribution to each of the three different parities (the document owner themselves, the cloud-hosting organisation and a trusted escrow agent) according to the following scheme:

HOST Keys 0 & 1	OWNER Keys 1 & 2	ESCROW Keys 0 & 2

DOCUMENT UPLOAD

Step 3 – Encryption of the Key-Splits

The pairwise combinations (known as the 'key splits') are encrypted using Public keys of the three different parties prior to upload to cloud storage.

DOCUMENT UPLOAD

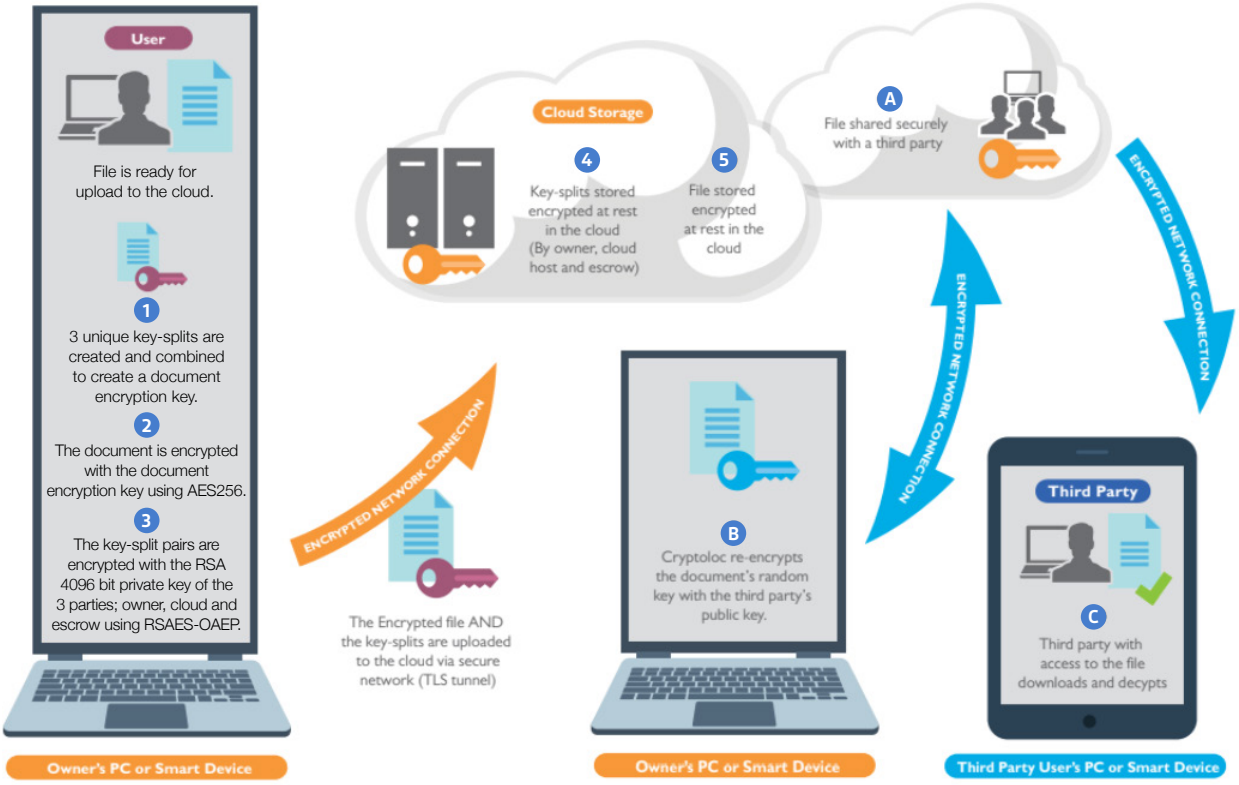
Step 4 & 5 – Upload to Cloud of Encrypted Document and Encrypted Key-Splits

The document to be uploaded (which was encrypted with the DEK) along with the three encrypted key-splits are all uploaded and stored separately on the cloud via Cryptoloc mechanisms.

Each key-split is stored separately under the control of each of the three party's cloud access accounts (the owner themselves, the cloud hosting organisation and a trusted escrow agent).

[Important note: Every new document, even those uploaded by the same user, is stored with a different random DEK]

How does it work?



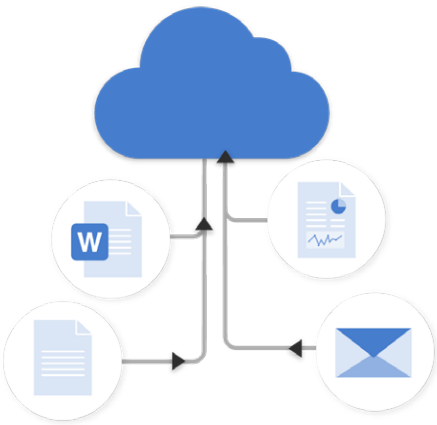
Cryptoloc-based Document download

Whenever a document owner wishes to download a document from the cloud, they must first reassemble the DEK. To do this they must download and decrypt two of the three original key-splits; which yields a copy of the **complete DEK.**

Each Key-split can only be decrypted using the **Private Key** of each one of the three parties involved in the original key-split process. This enables the **Document owner** to decrypt one of the key splits; and the **Cloud storage host** provides access to another key-split based on the owner's authentication when logging-into the Cryptoloc-based cloud storage solution hosted by the Cloud storage host.

With two key-splits, the document owner's local device is used to reassemble the DEK. The DEK is then used by the Cryptoloc-based solution to decrypt the file on the owner's local device.

Cryptoloc-based Document sharing



A Cryptoloc-based solution can enable document owners to grant access to third-party users. If the third-party is a user of the same Cryptoloc-based cloud hosting solution as the owner, then this is achieved by re-encrypting the DEK with the third-party user's Public Key; thereby granting them access to the DEK for the document upon download. Key-splits for access to the document are stored in the third-party's cloud access account until the document owner revokes their access to that document.

cryptoloc
SEND & SIGN

A Cryptoloc-based solution also provides a way for a document owner to securely-share a document to an **external third-party** (i.e. a recipient who has no cloud access account on the Cryptoloc-based solution used by the document owner).

SEND & SIGN

Step 1 – Create a new temporary DEK

The process known as Send & Sign allows a Document owner to request that the system create a temporary DEK for a document (or upload folder*) for a third-party recipient to use to decrypt a copy of a previously-stored document.

(*empty folders can be provided to receive documents from external third-party's as a way to securely share documents supplied by the external party)

SEND & SIGN

Step 2 – Notify the Third-Party

The third-party is notified (usually by email) that a document is available for download. The recipient is prompted to access the Cryptoloc-based cloud solution and confirm that they are ready to download the document.

SEND & SIGN

Step 3 – Confirm Recipient, Download and Decrypt

- When the recipient confirms that they are ready, the Cryptoloc-based solution send them a confirmation code (usually via SMS) which they use to start the download.
- The document is downloaded and decrypted on the recipient's local device (PC, smartphone or tablet).
- The recipient can download the same Send & Sign document multiple times on different devices until the document owner revokes access or until the Send & Sign access time window expires.

Digital Signing and Asset Auditing

Recipients of shared documents (including **users of the same Cryptoloc-based cloud hosting solution and third-party recipients**) can be requested by the document owner to digitally counter-sign a signed-document shared with them.

Digitally-signed documents are hashed and timestamped, enabling them to form the basis of a legal agreement between a document owner and third-party, so long as both parties agree to use the same Cryptoloc-based solution as a platform for their legal agreement.

Access Account Recovery

If a Cryptoloc-based solution account holder loses access to their document storage (either by forgetting their password or losing their Private Key), cryptographic access can be restored to their documents via the 'escrow recovery process'. Once the authenticity of the recover request is established, the account-holders device is used to create a new Public-Private key and the keys-splits for all their documents are regenerated and replace their old key-splits.

Account recovery can be achieved because the escrow agent and the Cryptoloc-based solution cloud host can provide enough information (i.e. two parts of the original document encryption keys (DEK) for each document) to enable the document owner access to their documents.

[It should be noted that even during the recovery process, neither the Escrow agent nor the cloud host have any interactive access to the unencrypted documents of the document owner.

Privacy is maintained because the escrow account is a non-interactive account (it's only function is to invoke the escrow recovery process and stores key-splits for use in recovery) and because the cloud host only provides their key-spits to the document owner as part of the escrow recovery process (in a similar way that to when they provide them to the document owner whenever they authenticate and down-load one of their documents normally].

Secure Communications

Documents stored using a Cryptoloc-based solution are always encrypted on the client device before they are uploaded, and all documents (including decryption key-splits) are securely transmitted using TLS tunnels between client devices and cloud-servers.

Digital Asset Auditing and Document Integrity

A Cryptoloc-based solution automatically stores a new version of every document updated on the cloud. Every document updated becomes a new file stored in the cloud, and each file stored is encrypted with a different random DEK.

Every previous version of a document can be accessed by the document owner, and different versions of the same document can be shared with different third-parties over time as desired.

Cryptoloc-based solution account holders are provided with access to a system-generated audit trail (including time and date stamps), recording the instances all transactions related to each document that store on the cloud. This gives document owners confidence in the integrity of uploaded documents when cloud-storing important and/or confidential documents such as legal agreements, funds transfer records, financial reconciliations, contracts, estate documents, personal records or deeds of ownership of real-world assets. The audit and versioning features of Cryptoloc provide effective 'digital safe-handling' of documents (including those shared with others) with proof of the:

- Chain of custody
- The identity of anyone who accessed (downloaded) a document
- When changes (if any) were made to a document (non-repudiation)
- Verifiable versions of a document at times of upload, update or sharing

The auditing and versioning features of Cryptoloc can also be leveraged to provide some protection from ransomware attacks or the corruption of an owners non-cloud stored documents.

Summary: Why choose Cryptoloc?

- Complete confidentiality, privacy and non-repudiation when signing, sharing and storing documents and digital assets.
- Stored documents are difficult to compromise, and access is securely recoverable.
- Document content cannot be accessed by either the cloud-host or by any malicious intruder even in the unlikely event of a cloud-server breach.
- If the user forgets or loses their login authentication credentials, they may use a recovery process to re-enable access to their account and stored documents.
- The Cryptoloc secure escrow model provides a mechanism by which a trusted, neutral third party, can assist in recovering access to a user's documents. Neither the escrow nor the cloud provider has any access to view the content of any user's documents during the recovery process.

About Cryptoloc

Cryptoloc is an international digital security company providing encryption solutions to secure cloud based information, at rest and in motion. Cryptoloc ensures data confidentiality, authenticity, restricted access and audit controls to keep data privacy, confidentiality and integrity.

Cryptoloc Technology is a patented technology adaptable to any size business across all industry sectors. An international company, Cryptoloc Technology Group has offices in US, UK, JAPAN, SA and Australia.

For more information visit our website where you can arrange to speak to one of our security experts to discuss your organisation's security needs.

WWW.CRYPTOLOC.COM