cryptoloc

Cryptoloc for Registry Whitepaper

The bold task of making a user accessible registry

A registry is a collection of all the official records relating to someone or something. Businesses and Governments maintain multiple registries that are core to the success and function of their departments. These may vary from a registry of suppliers to a registry of births, deaths, and marriages.

As we move to a paperless society, large collections of valuable metadata are an increasingly valuable target for cyber criminals.

The Privacy Act states that any entity must take active measures to ensure the security of the personal information they hold. In the case of large registries, the risk mitigation process has historically been to remove the registry from online access. This process requires that all modifications to the registry must be completed only by internal resources with access to the offline system. The pitfalls of an offline, or largely access-restricted, system include the overheads required in managing and maintaining the most up-to-date information.

The ability for users to directly access and maintain their own information in a registry has many advantages. It empowers the user to retain a sense of ownership of their data and ensure that it is up to date. This can capture many more accurate registry entries whilst adding little to no overhead costs. Until now, this capability came at the cost of security and an increased risk of cyber-attacks.

Cryptoloc technology enables accessible, online data registries without compromising security, privacy or adding expensive resources.

The Cryptoloc security advantage explained

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

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

Assembly of decryption keys relies on access to the owner's private key and an authenticated access to a cloud-hosted Cryptoloc-based solution.

Owners manage access to their own information. If the owner of a Cryptoloc-stored document loses their access – by forgetting their authentication password to their cloud-hosted account, for instance, or by losing their private key – access to their encrypted information can be restored without compromising the security of the documents via the Cryptoloc Escrow Recovery Process.

A Cryptoloc technology registry

In a Cryptoloc registry, each participant has ownership of their registry entry and can grant or revoke access to third parties as required. Every file uploaded to the registry has a complete audit trail, and the owner can view all activity associated with their data.

A Cryptoloc registry requires every user to complete a 100 point identification check to the standards specified in the Anti-Money Laundering and Counter-Terrorism Financing Act 2006. This combination of a verified user account, multi-factor authentication and the use of distributed unique private key splits ensures that information cannot be intercepted or decrypted by anyone other than the intended parties.

With a focus on the user experience, a Cryptoloc registry enables users to have complete control and knowledge that their information is up to date, correct and safe.

Embracing the power of a platform creates flexibility, accessibility and reduces the maintenance and upkeep of a registry. Giving power to the customers to own and maintain their own data creates a sense of confidence and ownership of the system, increasing acceptance and ongoing usage.

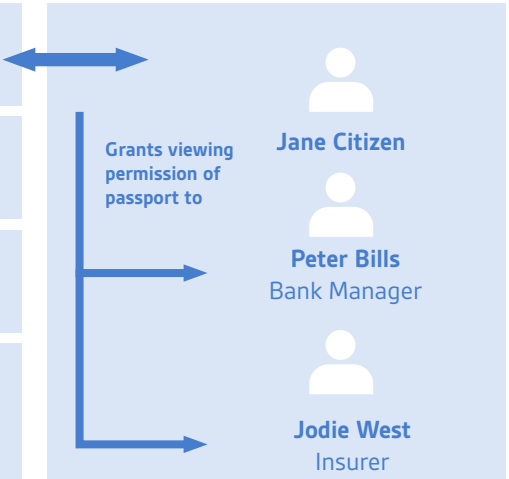
Likewise, department employees have verified registered accounts with specific access controls and can assist in traditional ways to upload and maintain documents on behalf of the registry record owner.

How does it work?

Each user has control of only their registry entry and all actions and versions are captured in a complete audit trail.

Jane Citizen	Passport Driver's Licence	Birth Certificate Marriage Certificate
Jack Wilson	Birth Certificate	Student Card
Steve Roberts	Birth Certificate Driver's Licence	Death Certificate Marriage Certificate
Anne Brown	Proof of Address Driver's Licence Power of Attorney	Will NDIS Healthcare Card
Bob Jones	Passport Driver's Licence	Medicare
Joe Smith	Builder's Licence Driver's Licence	Birth Certificate

Timestamp	Description	System User
15-11-2020 12:32pm	File: Builder's Licence.png Uploaded	Jane Doe, Department of Registries
15-11-2020 12:33am	File: Passport.png Uploaded	Jane Doe, Department of Registries
15-11-2020 12:35pm	File: Birth Certificate.png Uploaded	Jane Doe, Department of Registries
01-02-2021 10:22pm	File: Builder's Licence.png New Version Uploaded	Jack Done, Builders Licensing Association
02-02-2021 8:28pm	File: Builder's Licence.png Downloaded	Joe Smith
02-02-2021 8:28pm	File: Builder's Licence.png Shared to Jill Renovating Customer	Joe Smith
04-02-2021 8:01am	File: Builder's Licence.png Downloaded	Jill Barnes, Renovating Customer



Timestamp	Description	System User
01-02-2019 12:32pm	File: Passport.png Uploaded	Jane Citizen
12-02-2019 05:20am	File: Passport.png Downloaded	Jane Citizen
12-02-2019 05:24pm	File: Passport.png Shared to Bank Manager	Jane Citizen
12-02-2019 10:02pm	File: Passport.png Downloaded	Peter Bills, Bank Manager
18-06-2020 4:28pm	File: Passport.png new Version Uploaded	Jane Citizen
18-06-2020 5:14pm	File Passport.png Share to Insurer	Jane Citizen
20-06-2020 2:17pm	File Passport.png Downloaded	Jodie West, Insurer

How does the security work?

DOCUMENT UPLOAD

Step 1 – Encrypting the information

Whenever a user uploads a document to the registry, Cryptoloc first generates three random symmetric encryption keys, meaning that each piece of information uploaded has unique encryption. Collectively, these three keys form the user's Document Encryption Key (DEK). The DEK is used to encrypt the document locally (on the client device) prior to upload.

Step 2 – Key Splits

The document encryption keys for each document are duplicated (once again on the client device) so that there are two copies of each one (i.e. six keys). Pairings of two of the three encryption keys are then prepared for distribution to each of the three different parties (the user themselves, the registry hosting organisation, and a trusted escrow agent) according to the following scheme:

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

Step 3 – Encryption of the key splits

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

Step 4 – Upload to registry of encrypted document and key splits

The information to be uploaded (which was encrypted with the DEK) along with the three encrypted key splits are all uploaded and stored separately on the registry via Cryptoloc mechanisms. Each key split is stored separately under the control of each of the three party's registry access accounts (the user themselves, the registry hosting organisation, and a trusted escrow agent).

Step 5 – Granting another user access

Users can securely share their information with third-party users. If the third-party is a user of the same registry solution as the owner, then this is achieved by re-encrypting the DEK with the third-party user's Public Key. Key splits for access to the document are stored in the third-party's registry account until the document owner revokes their access to that document.

DOCUMENT DOWNLOAD

Step 6 – Reassemble the DEK to decrypt

The user in the Cryptoloc registry has two out of the three parts of the decryption key to decrypt the file (keys 1 and 2). The registry host has the missing third key (keys 0 and 1). This enables the user to reassemble the three parts of the DEK using their authenticated registry host account.

Step 7 – Decrypt the information

The DEK segments and information is all downloaded and decrypted locally on the user's device, ensuring that they cannot be intercepted and viewed in transit.

Digital Signing and Asset Auditing

Recipients of shared documents (including users of the same Cryptoloc-based registry 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 registry as a platform for their legal agreement.

Access Account Recovery

If a Cryptoloc-based registry 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-holder's device is used to create a new Public-Private key and the key splits for all their documents are regenerated, replacing their old key splits.

Account recovery can be achieved because the escrow agent and the Cryptoloc-based registry 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 – its only function is to invoke the escrow recovery process and store key splits for use in recovery – and because the cloud host only provides their key splits to the document owner as part of the escrow recovery process.

Secure Communications

Documents stored using a Cryptoloc-based registry 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 registry automatically stores a new version of every document updated on the registry. Every document updated becomes a new file stored in the registry, 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 registry account holders are provided with access to a system-generated audit trail (including time and date stamps), recording all transactions related to each document stored on the cloud. This gives document owners confidence in the integrity of uploaded confidential documents such as legal agreements, contracts, estate documents, personal records or deeds of ownership. The audit and versioning features of Cryptoloc provide effective digital safe-handling of documents, including those shared with others, with proof of:

- 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 owner's non-registry stored documents.

Why choose Cryptoloc?

- Complete confidentiality, privacy and non-repudiation when signing, sharing and storing documents and digital assets.
- Stored documents cannot be compromised, and access is securely recoverable.
- Document content cannot be accessed by either the registry-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.
- Placing customers in control of their own data creates a sense of confidence and ownership of the system, increasing acceptance and ongoing usage.
- Increased flexibility and reduced cost of registry maintenance, data entry and traditional security costs.

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