nCrypted Cloud

470 Atlantic Avenue
Boston, MA 02210
tel. (617) 520-4120

NCRYPTED CLOUD TECHNICAL OVERVIEW OF ENCRYPTION AND KEY MANAGEMENT

nCryptedCloud key management and sharing system is a patent pending Enterprise level security system with the ease of use of a consumer product. nCryptedCloud key management system was designed with security and privacy in mind. It protects all of your cloud-based files while giving you the flexibility to share files with other users of your choice, with a mandate of ease to use for the end user.

All Topics

- How nCryptedCloud Protects your files
- How nCryptedCloud "Multi-Identity" works
- How the User Personal Key (UPK) works
- How the User Recovery Key (URK) works
- How the Organization Recovery Key (ORK) works
- How nCryptedCloud "Share Securely" works
- Separating your keys and your data, why it's important
- Examples

How nCryptedCloud protects your files:

nCryptedCloud uses a Zip format to contain your data. Using Zip format for your encrypted files provides users with the assurance that their data can always be recovered using any standard Zip tools. The Zip format is a well-known format and can be decrypted by many other standard tools. Long-term storage of encrypted files in custom file formats is a risk. To decrypt your files you will need to have the software available and running. By using Zip format for long-term storage, you can use any standard Zip utility to decrypt your data as long as you have the password.

nCryptedCloud uses AES-256 encryption to protect your data that is stored in the Zip container. This is currently the industry standard that is used to protect data from brute force attacks. Zip format supports AES-256 encryption natively. By using the Zip format encryption, nCryptedCloud assures that you can always decrypt your files even with standard Zip tools.

nCryptedCloud generates a unique password for each encrypted file using our patent pending key management system. By using a unique password for each file, nCryptedCloud assures that all of your data is secured and safe from brute force attacks.

If an attacker were to gain access to the password for a single file, they would not be able to access any other encrypted files.

With nCryptedCloud all encryption and decryption is performed on the client. The unique passwords used to encrypt your files are never stored in the cloud.

nCrypted Cloud

470 Atlantic Avenue
Boston, MA 02210
tel. (617) 520-4120

How nCryptedCloud "Multi-Identity" works:

nCryptedCloud uses a patent pending "Multi-Identity" management system. This allows users to maintain multiple identities in a single account. When files are encrypted the Recovery Key that is used is connected to a specific identity. By associating the recovery information with a specific identity it allows the user to separate their personal data from their corporate data. This separation allows users to leave a company and maintain all their personal data, while assuring the corporation that the user no longer has access to corporate data.

How the User Personal Key (UPK) works:

When a user enrolls in nCryptedCloud we use PBKDF2 (Password Based Key Derivation Function 2) to generate a User Personal Key (UPK) for you by using specific information from your account and password. The UPK is used to protect specific information and is never transferred to nCrypted Cloud's server. This way only *you* can re-create the UPK by entering your account and password.

How the User Recovery Key (URK) works:

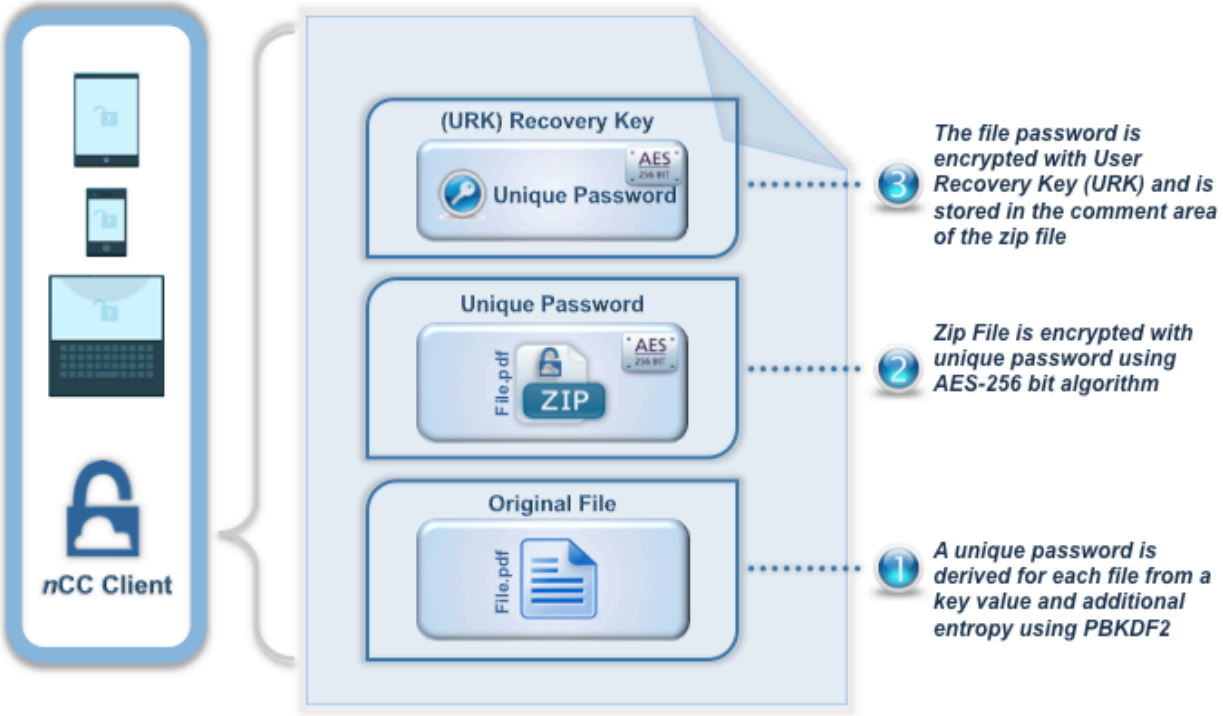
When you enroll in nCryptedCloud we also generate a Public/Private Key for your account. This key is called your User Recovery Key (URK). The URK is stored locally in a file called the "KeyStore." The "KeyStore" is protected using an operating system method, so no one can gain access to your keys. Your URK is then sent to our servers and stored in an encrypted format. When a file is encrypted, we encrypt the unique password for the file with your URK, and store that in the comment area of the Zip file. This way you can always recover the password with your Recovery Key.

With nCryptedCloud's "Multi-Identity" system, we generate a unique URK for each identity you have. This allows us to separate the data that is protected with your UPK and your URK.

nCrypted Cloud

470 Atlantic Avenue
Boston, MA 02210
tel. (617) 520-4120

NCRYPTEDCLOUD RECOVERY KEY USAGE DIAGRAM



For the free version of our software we maintain the URK for you, so that you can always get back your data. **In the paid version we give you two options: not storing your URK on our servers, or storing your URK (encrypted with a passphrase) on our servers.** With either of these options you will be responsible for backing up your URK or remembering your passphrase. If you lose your URK or forget your passphrase you will be unable to read or open your encrypted files.

How the Organizational Recovery Key (ORK) works:

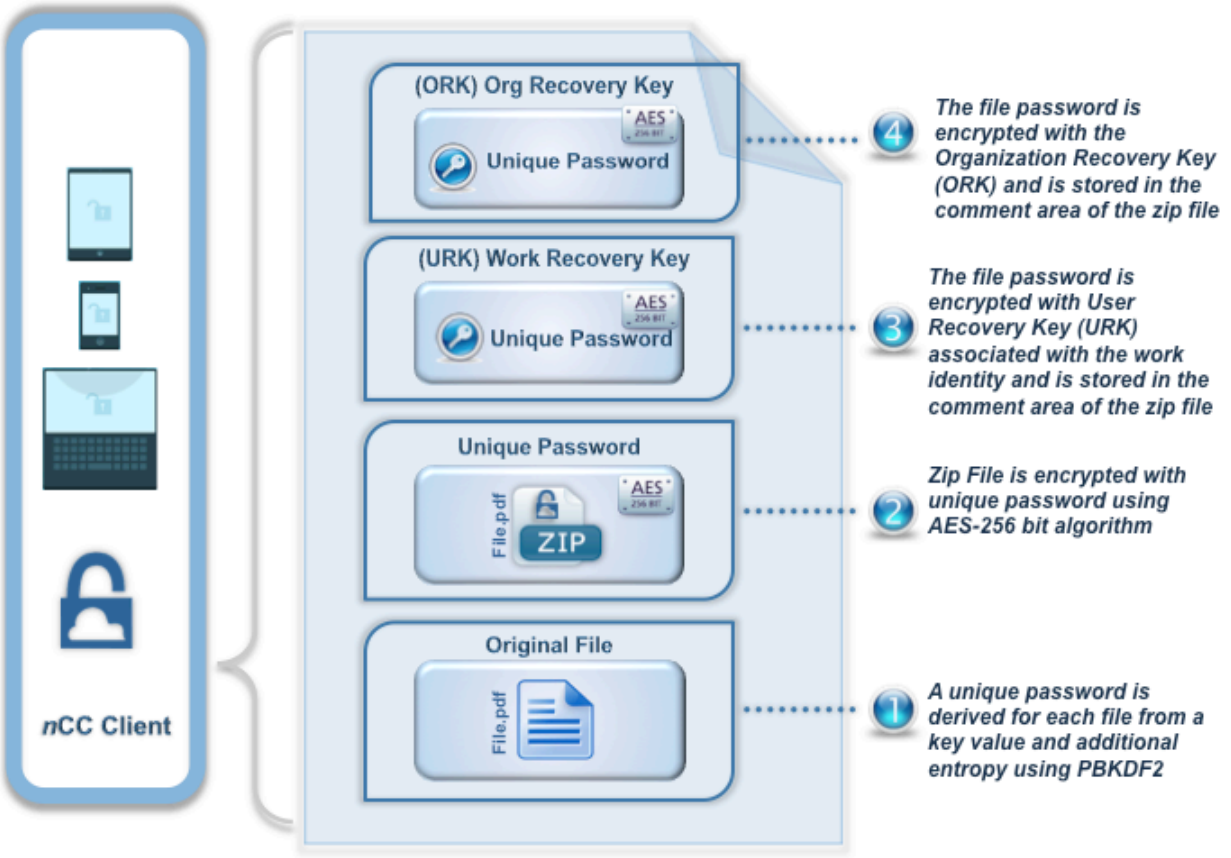
When you enroll your corporation in nCryptedCloud, we generate an Organizational Recovery Key (ORK). When users encrypt data with their corporate identity we also encrypt the unique password with the ORK. This allows an organization to always recover corporate data that was encrypted by its employees. Because the ORK is not used in file encryption performed with your personal identity, the corporation has no access to any personal data you have encrypted.

When an employee leaves the company, the organization can disable the user's corporate identity from the nCryptedCloud admin portal, and the user will no longer be able to decrypt work files, but will maintain full access to any of his/her personal files.

nCrypted Cloud

470 Atlantic Avenue
Boston, MA 02210
tel. (617) 520-4120

NCRYPTEDCLOUD ORGANIZATION RECOVERY KEY DIAGRAM



How nCryptedCloud "Share Securely" works:

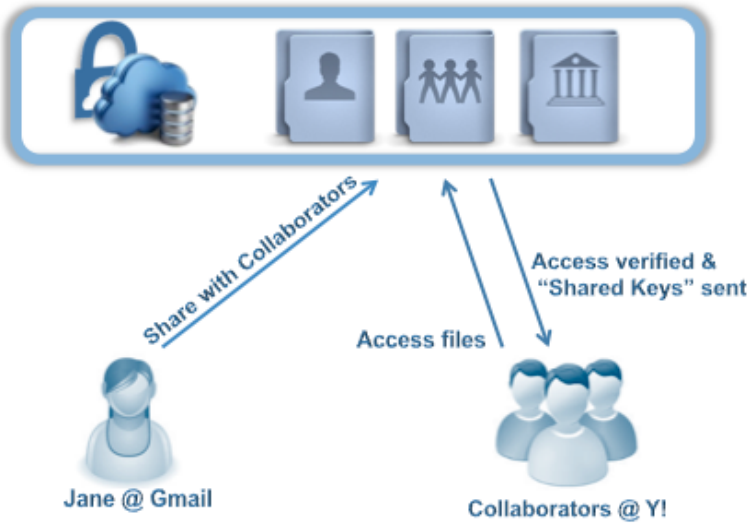
nCryptedCloud uses these same methods to implement an enterprise ready security and collaboration platform. Having your data secure is the first great step in maintaining your privacy, or your company's compliance with industry regulations. But not being able to easily share your data or collaborate with others would mean that employees would not readily adopt this technology. nCryptedCloud takes the hassle out of sharing encrypted documents with others.

To easily facilitate the sharing of files, nCryptedCloud uses a slightly different method of key management that allows us to control who can access your files. When you select a folder for "Secure Sharing," nCryptedCloud generates a unique symmetric key for the folder. This key is stored on our server and in your local key store. When you place a file in this folder, nCryptedCloud generates a unique password with which to encrypt the data. The "Recovery Record" for a shared file contains the unique file password encrypted with the owner's URK.

Once a user's access to a folder has been removed, nCryptedCloud then deletes the symmetric key from their local key store and they can no longer decrypt the files in the shared folder.

470 Atlantic Avenue
Boston, MA 02210
tel. (617) 520-4120

NCRYPTEDCLOUD "SHARE SECURELY" DIAGRAM



1 Jane @ Gmail shares folders with collaborators.
2 When collaborators access the files the sharing status is verified, and "Shared Keys" are sent to decrypt files .
3 Client caches key for offline access, or keys are deleted if shared status is invalid.

Separating your keys and your data, why it's important:

An important thing to remember is that nCryptedCloud servers do not store your data. This means that, even in our free version, we cannot decrypt any of your data since we do not have access to it. Likewise Dropbox, or your cloud storage provider, cannot decrypt your data because they do not have access to your keys. Your UPK and your URK are never stored on Dropbox or any other cloud storage provider. This separation of data and keys is a very important point. It's what makes nCryptedCloud the best choice to protect you data.

470 Atlantic Avenue
Boston, MA 02210
tel. (617) 520-4120

EXAMPLES

Encrypting and Decrypting Private Files:

Encryption:

1. Create a secure unique password.
2. Encrypt the plaintext data using AES-256 Zip encryption.
3. Encrypt the file password with the nCryptedCloud User Recovery Key (URK).
4. Store the encrypted password in the encrypted Zip file.

Decryption:

1. Decrypt the encrypted file password using the user's private key.
2. Decrypt the encrypted data using the file password.

Shared File encryption:

1. Bob wants to share some documents with other users.
2. Bob encrypts his files using nCryptedCloud “Share Securely” method.
3. nCryptedCloud creates a unique key for the folder and stores it locally on Bob’s machine.
4. nCryptedCloud sends the key to our server, and it is encrypted and stored on our server.
5. All the files in the shared folder are encrypted with unique passwords which are derived from the symmetric folder key value and additional entropy.
6. The file password is also encrypted with the Bobs URK.
7. The encrypted file password and symmetric folder key ID are stored with the encrypted data in the Zip file.
8. Bob shares the folder with Sue and Joe.
9. Sue receives the shared folder request from Bob and accepts the request.
10. When Sue needs to access the files on her machine, nCryptedCloud verifies that Sue has access to the folder key and distributes it to her.
11. If Bob removes Sue’s access to the folder, the folder key is removed from Sue’s local key store and she can no longer decrypt the files.

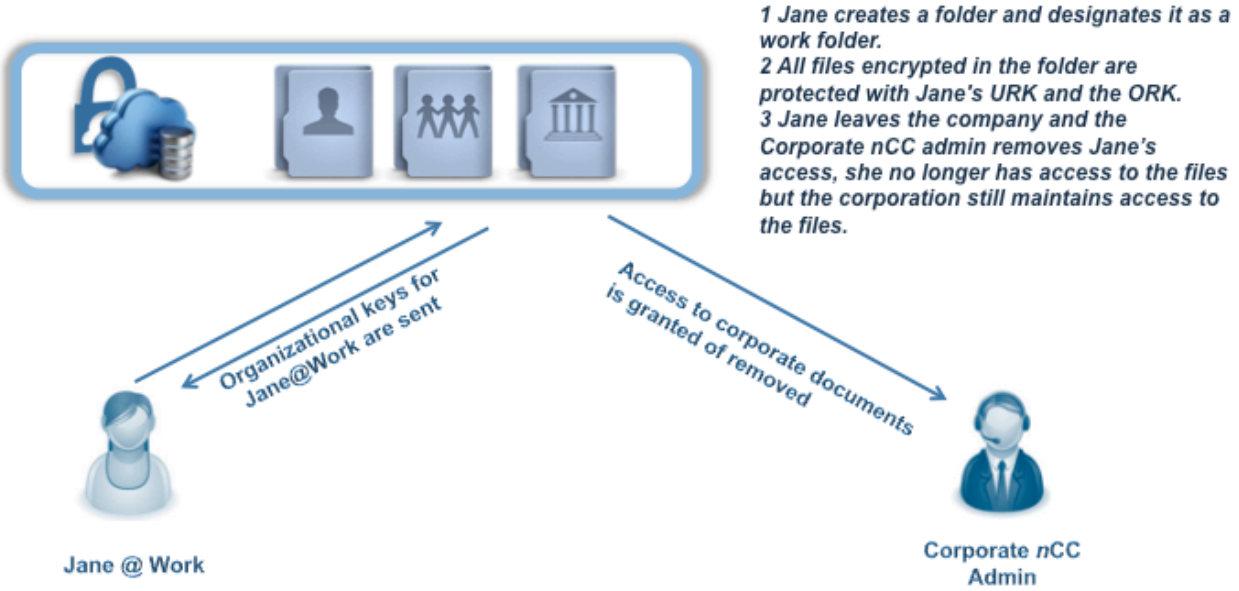
nCrypted Cloud

470 Atlantic Avenue
Boston, MA 02210
tel. (617) 520-4120

Organization Folder Encryption:

1. Jane created a folder and designates it as a corporate work folder.
2. Jane adds files to the work folder.
3. All the files in the work folder are encrypted with unique passwords.
4. The file password is encrypted with Jane's URK for her organization identity.
5. The file password is encrypted with the ORK .
6. The encrypted passwords are stored with the encrypted data in the Zip file.
7. If Jane leaves the organization access to her ORK is removed, and she can no longer decrypt the files in this folder.

ORGANIZATION FOLDER ENCRYPTION DIAGRAM



nCrypted Cloud

470 Atlantic Avenue
Boston, MA 02210
tel. (617) 520-4120

Organization Shared Folder Encryption:

1. Jane wants to share some documents with other users.
2. Jane creates a work folder and adds some files to it.
3. Jane encrypts her files using nCryptedCloud "Share Securely" method.
4. nCryptedCloud creates a unique key for the folder and stores it locally on Jane's machine.
5. nCryptedCloud sends the key to our server where it is encrypted and stored.
6. All the files in the shared folder are encrypted with unique passwords that are derived from the symmetric folder key value and additional entropy.
7. The file password is also encrypted with the Jane's URK for her organization identity.
8. The file password is encrypted with the ORK.

9. The encrypted file passwords and symmetric folder key ID are stored with the encrypted data in the Zip file.
10. Jane shares the folder with Sue and Joe.
11. Sue and Joe receive and accept the shared folder request from Jane.
12. When Sue needs to access the files on her machine, nCryptedCloud verifies that Sue has access to the folder key and distributes it to her.
13. If Jane removes Sue's access to the folder, the folder key is removed from Sue's local key store and Sue can no longer decrypt the files.
14. If Jane leaves the organization, access to her URK is removed, and she can no longer decrypt the files in this folder.

ORGANIZATION SHARED FOLDER ENCRYPTION DIAGRAM