C2 Backup Security White Paper

Last updated: Nov 16, 2022

Table of Contents

Executive Summary

Backing up your data has become essential when it comes to keeping it safe, especially in the event of a disaster. However, with the amount of data, duplicated files, and the number of devices we use growing every day, performing regular backups may become an arduous task. Furthermore, how can you ensure that your data remains safe and secure during backup or restoration? This is where C2 Backup comes into play.

C2 Backup is Synology's cloud-based backup solution that comes built-in with a number of convenient features. With just one backup task for your entire device, you can back up your files, applications, and system configurations on a regular basis. With **cloud service backups**, you can also back up and restore items in Microsoft 365. C2 Backup also offers a variety of recovery options, including downloading specific files or folders from the **C2 Backup Recovery Portal** or restoring your entire device using the **C2 Backup Recovery Wizard**.

Your data safety in the cloud is our top priority, so we've made sure that with C2 Backup, your data are encrypted on the client side through the use of military-grade encryption technology, keeping your data secure and protected during backups, in storage, and during restorations.

This white paper provides an overview of C2 Backup, as well as detailed explanations of the processes for encryption, data security, and more.

Introduction

C2 Backup is Synology's cloud-based backup solution with comprehensive data protection for devices and Microsoft 365 services. With C2 Backup, you can back up and restore not only your entire device, including your documents, photos, and videos, but also your app and system configurations and Microsoft 365 services, all while resting assured that your data is always secure.

Key security principles

C2 Backup is Synology's solution for backing up and restoring your device data. This white paper explains how this is done in a secure way. C2 Backup utilizes a similar approach to security that has been implemented in other C2 services, namely, that we can best protect your secrets by not knowing them.

Privacy by design

It is impossible to lose, use, or abuse data that one doesn't possess, so our systems have been designed with an effort to reduce the amount of sensitive user data that we are able to access. This concept is utilized throughout the entire system, such as our inability to acquire or store your C2 Key during authentication. This means that there is no way that we could know your C2 Key, and if we don't know your C2 Key, we don't own your data.

You own your data

C2 Backup is designed to make sure that only **you** have access to your data, which is encrypted locally during storage. On top of that, our utilization of **end-to-end encryption** and **client-side encryption** keeps you and your data as safe as possible from anyone looking to gain access.

Designed for transparency and trust

When it comes to our service usage data collection methods, Synology strives to be as open and transparent as possible. Your permission will always be required when we collect any of your service usage data. On top of that, our team takes pride in their efficiency to react when investigating, verifying, resolving, or mitigating reports of any bugs or vulnerabilities with our products.

Protection on C2 services

To avoid users having to remember a number of encrypted passwords, C2 services have developed and implemented a single encryption key, known as the **C2 Encryption Key (C2 Key)**. This encryption key is used across all C2 services (except C2 Storage).

Your C2 Key is not stored by any means on the Synology C2 server, therefore the only person who knows it is whoever has access to your Synology C2 account. Also, since this C2 Key will be used to decrypt all of your stored encrypted data, we suggest that you use a key that is strong, easy to remember, and follows our C2 Key requirements. If you happen to lose your C2 Key, Synology C2 will not be able to retrieve your encrypted data. Thus, it is critical that you keep your C2 Key as safe and secure as possible.

Synology C2 services provide the maximum possible security for your encrypted data by using the C2 Key to derive, encrypt, and decrypt all cryptographic and Derived Keys.

C2 infrastructure

Physical location

We currently operate data centers worldwide. All users are ensured that their data is hosted in the location of their own choice. For example, our EU-based data center allows business customers to comply with European data protection laws. New locations may be added in the future, however, this will not affect existing clients or their data. For more information about our data center locations, please visit our official website. Please see Synology C2 services' Terms of Service, Privacy Statement, and Data Processing Agreement for more details on legal guarantees.

Site security

Synology data centers have passed rigorous inspections for strict security procedures and physical safety features, and meet Synology's high standards for incident response and access restrictions. Synology monitors employee access to its storage locations and implements different mechanisms to ensure data durability and fault-tolerant storage. With your data security in mind, the architecture of Synology C2 data centers aims to ensure that no valuable data will be lost. For more details, you can refer to the **Data Durability** section of this white paper.

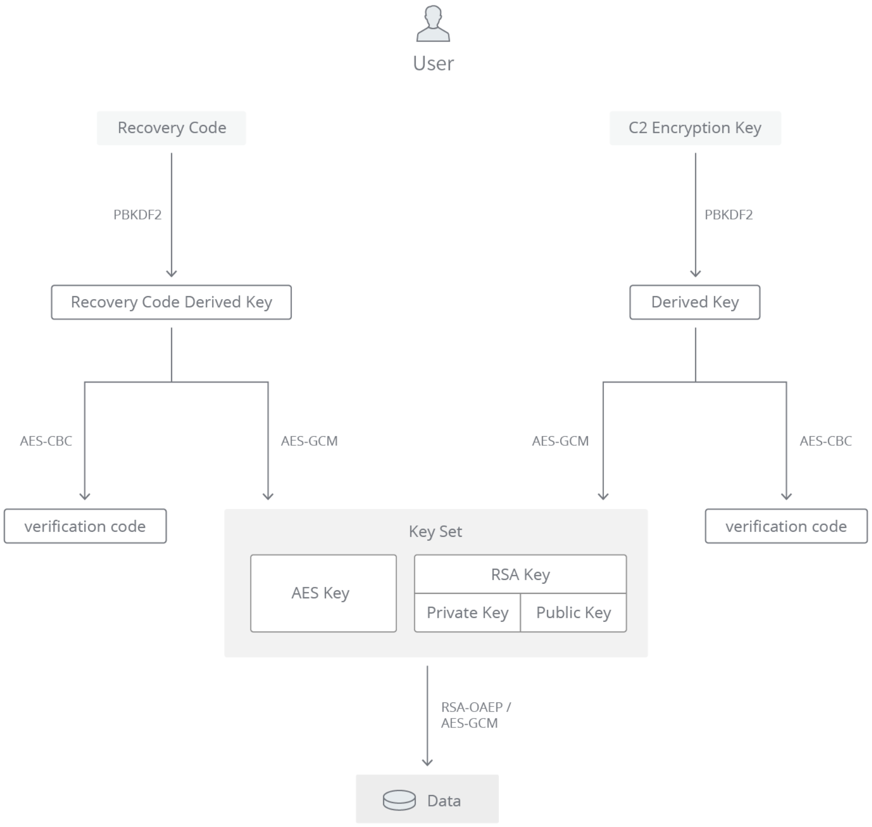
C2 Backup Encryption Methods

Encryption technology

Synology C2 services use two different types of encryption technology to protect the **data in transit** between the sender and the recipient, along with the **data-at-rest** that is stored on the cloud and the C2 server.

- **AES (Advanced Encryption System) Encryption**: A symmetric type of encryption that uses the same cryptographic keys for encryption and decryption, so the sender and recipient must both use the same key to keep a private information connection.
- **RSA (Rivest–Shamir–Adleman) Encryption**: An asymmetric type of encryption that uses a Key Pair that consists of the Public and Private Keys (Secret Key). Content that is encrypted by the Public Key can only be decrypted by the Private Key. As a result, keeping the Private Key confidential is necessary to ensure your data safety.

C2 Encryption Key data structure



The **C2 Encryption Key (C2 Key)** is provided by the user, and the AES-256-CBC encryption is derived from the encryption key through the PBKDF2 derivation function to reduce vulnerabilities of brute-force attacks.

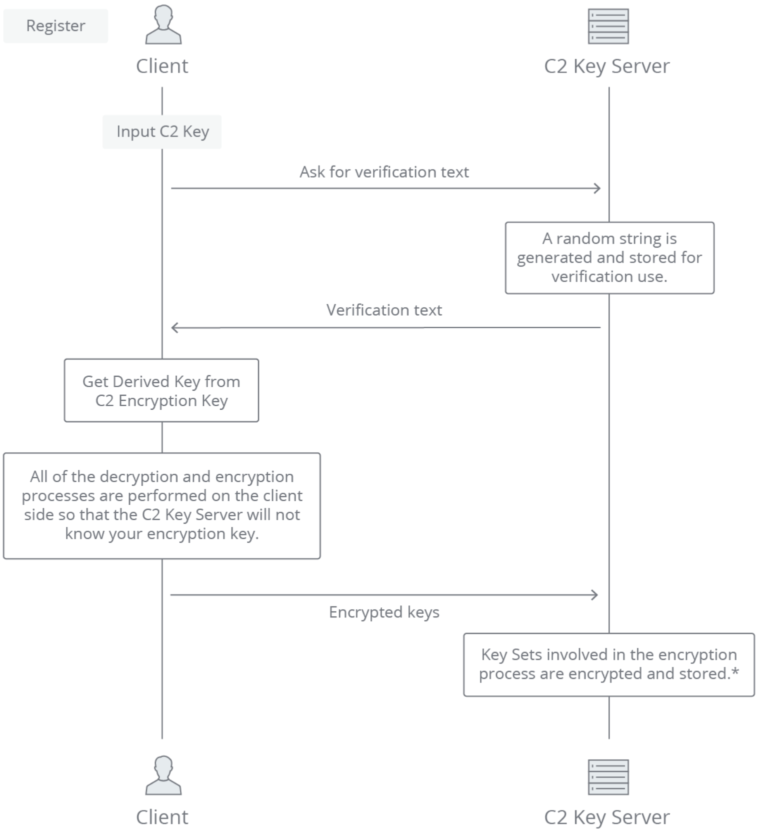
The **Derived Key** is used to encrypt and decrypt **verification codes** through **AES-256-CBC encryption**. Since the C2 Key server should not know about the encryption key, the verification for the encryption key is done by testing the ability to decrypt an encrypted verification code.

The Derived Key is also used to encrypt and decrypt the **Key Set (RSA Keypairs and AES Keys)** through **AES-GCM encryption**.

C2 Encryption Key registration and verification

C2 services have been designed with your security and data safety in mind, keeping your data protected when stored on our servers. To do this, we have implemented the use of an encryption key mechanism, the **C2 Encryption Key (C2 Key)**, to which only the user themselves has access. During first-time setup, you will need to set up your own C2 Key.

Registration


Register
Client
C2 Key Server
Input C2 Key
Ask for verification text
A random string is generated and stored for verification use.
Verification text
Get Derived Key from C2 Encryption Key
All of the decryption and encryption processes are performed on the client side so that the C2 Key Server will not know your encryption key.
Encrypted keys
Key Sets involved in the encryption process are encrypted and stored.*
Client
C2 Key Server

* The Public Key is not encrypted, since it will be used when performingfile transfers between users.

On the C2 Encryption Key setup page, you will be requested to register your C2 Key. Since this key will be used during encryption across all of your C2 services (except C2 Storage), please make sure to choose a key that is strong, memorable, and follows our C2 Key requirements.

After you have input your encryption key, your client will send a request to the C2 Key server to generate and store a random string in the form of a **verification code**. This will be used to test the ability of the client to decrypt the encrypted verification code later on. This makes it possible for the C2 server to verify your identity **without** needing to save your C2 Key.

Once the verification code has been generated, it is sent to your client to generate the RSA Key, AES Key, and Derived Key, along with the encryption of said keys. All of the decryption and encryption processes are performed on the client end, so the C2 Key server remains unaware of the encryption key.

After the client has encrypted the corresponding keys and verification codes, they are then sent back to the server to store the user metadata, encrypted verification code, Private Key, Public Key, and AES Key. Once your registration has been successfully completed, the Recovery Code, Derived Key, and the Verification Key will be generated and encrypted on the client end. Make sure to download or save your Recovery Code so that you can perform recoveries if needed in the future. The Recovery Code utilizes the same registration method as mentioned above when performing a recovery of your C2 Key.

Verification

If you have already registered your C2 Key and wish to access your encrypted data, you must input your C2 Key into the C2 Backup portal to begin the decryption process. After entering your C2 Key, the Derived Key will be generated for decrypting the encrypted verification code on the client end. Then, the client will send a request to the C2 Key server to verify the verification code.

Once verified, the Public Key, encrypted Private Key, and encrypted AES Key will be sent to the client to be decrypted, and will then be used to decrypt the encrypted service keys obtained from the C2 server. By keeping the encryption and decryption processes on the client end, the C2 server is unable to retain any knowledge of your C2 Key or gain access to your encrypted data. Once the encryption and decryption processes are completed, you will be able to access your data in C2 Backup.

Changing of encryption keys

If you use the same password for C2 Key as you do for other accounts, we recommend that you change your C2 Key to something else to limit the possibility of a data breach. You can change your C2 Key in your account settings in the C2 Backup Portal. Once you input your old C2 Key, your client will submit a request to the C2 Key server to pre-verify the user metadata and the encrypted verification code. After the old C2 Key is verified, the old Key Sets will be decrypted via the old Derived Key and a confirmation code will be sent to your client.

Once the confirmation code has been confirmed by the C2 Key server, you will be able to input your new C2 Key. When you do this, the new Derived Key, AES Key, and RSA Key Pair will be generated, and the old Key Sets will be re-encrypted via the new Derived Key to complete the encryption process. All previously stored data will be re-encrypted, and a new Recovery Code will be generated, meaning that the old recovery code will no longer be valid. This entire process may take some time to complete.

Creation of a Recovery Code and C2 Key recovery

Encryption key recovery allows you to restore access to C2 services by resetting your C2 Key and recovering your encrypted data stored on the C2 server. In order to use this function, however, you must have already downloaded or stored and have access to the **Recovery Code** that was automatically generated during the setup of your C2 Key. Make sure to keep your Recovery Code safe, since the C2 server does not keep your C2 Key and the only method to retrieve it is with your Recovery Code, which is encrypted and stored on the C2 server and can only be decrypted using the Recovery Code's Derived Key.

Creation

Your **Recovery Code** is automatically generated once you have completed the registration of your C2 Key. You can download and store this code somewhere safe in case you forget your C2 Key. After C2 Key setup is complete, your client pre-registers the Recovery Code by sending a request to the C2 Key server to generate a random string in the form of a verification code. Once the process is complete, the C2 Key server stores the user metadata and the verification code. The verification code is then transmitted to your client after the generation of the Recovery Code and derivation of the Recovery Code's Derived Key.

Your client will use the Recovery Code's Derived Key to encrypt the verification code and Key Set (Private Key and AES Key only). Your client will then use this Derived Key to encrypt the Recovery Code. After this encryption is complete, the client will send a request to accept the encrypted verification code, encrypted Private Key, Public Key, encrypted AES Key, and encrypted Recovery Code. Once accepted, the C2 Key server will store said keys along with the user metadata. Once the entire process is complete, the Recovery Code will be ready to save or download.

Recovery

When you need to recover your C2 Key, you will be asked to first enter your **Recovery Code** and then create a new C2 Key. Upon entering the Recovery Code, its Derived Key will be generated and the user metadata and verification code will be retrieved from the C2 Key server. The encrypted verification code will be sent to your client for decryption via the Derived Key that was generated by the Recovery Code. Your client will then send a request to verify the verification code and generate a random string in the form of a confirmation code, which is then stored along with the user metadata.

Once the verification process is complete, the C2 Key server will send the confirmation codes, the old Key Sets (derived via the old Derived Key), and the new Verification Key to your client. You will then be asked to set up your new C2 Key, which will be used to derive the Recovery Code's Derived Key. When you do this, a new Recovery Code Derived Key, AES Key, and RSA Key Pair will be generated, and the old Key Sets will be re-encrypted via the new Recovery Code Derived Key to complete the encryption process. Similar to the registration process, after the C2 Key has been set up, all of your data will be re-encrypted and a new Recovery Code will be automatically generated, all of which may take some time. At this point, make sure that you download or save your Recovery Code for future recoveries.

Upon creation of the Recovery Code, your client will encrypt the RSA Key Pair and AES Key using the new Recovery Code Derived Key, which then also encrypts the new verification code and re-encrypts the old Key Sets. The client will then ask for the C2 Key server to allow and verify the user metadata along with the encrypted keys mentioned above. Once validated, your new C2 Key and Recovery Code will be ready to use, and your encrypted data will be accessible via the new C2 Key.

Notes:

- A new Key Set will be created each time you register, change, or recover your C2 Key. All old Key Sets will be re-encrypted after the C2 Key has been changed or recovered.

C2 Backup User Data Protection

Encryption of your backup data

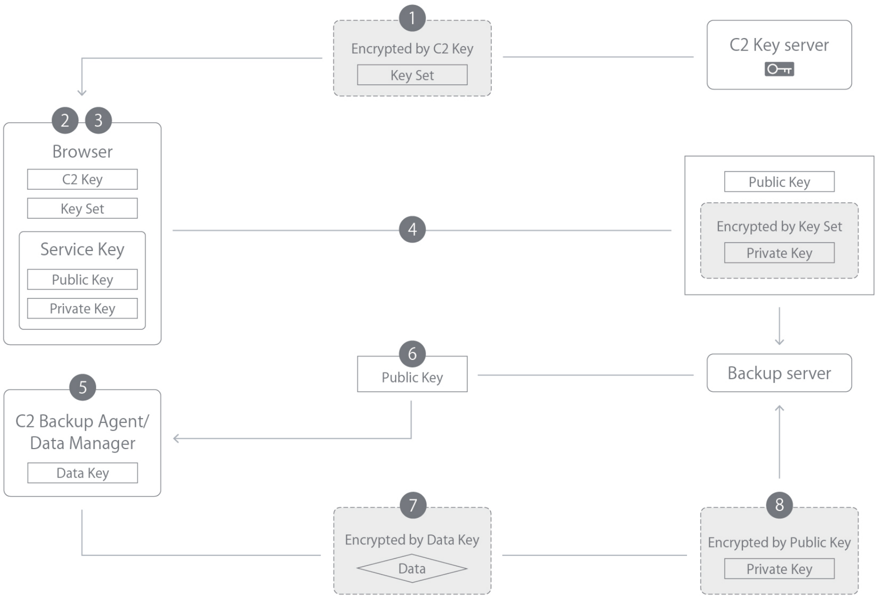
Since the primary purpose of C2 Backup is to keep your backup data completely secure on the C2 server, we have ensured that decryption can only be performed by the user.

In order to do this, our system was designed in such a way that your regular backups are automatically encrypted, and must be decrypted using your C2 Key whenever you need to recover your data. This is done through the use of asymmetric encryption. However, in order to boost performance times and encrypt your backups as effectively as possible, we have also introduced the usage of symmetric encryption, resulting in the **hybrid cryptosystem** as explained in this section.

C2 Backup utilizes three layers of encryption keys: the C2 Key Set, the Service Key, and the randomly-generated Data Key. All backup data are encrypted using the **Advanced Encryption Standard (AES)** in **Counter Mode (CTR)** using a 256-bit randomly-generated Data Key. The AES 256-bit algorithm is well-known as an impenetrable, military-grade encryption, and has even been approved by the U.S. National Security Agency for the encryption of top-secret information.

For device backups, the Data Key is randomly generated by the **C2 Backup agent** desktop utility; whereas for Microsoft 365 backups, the Data Key is randomly generated by the **Data Manager**, which handles the data between the Microsoft server and the C2 server. The Data Key is then encyrypted by the Service Key's Public Key using 4096-bit RSA. This approach utilizes asymmetric encryption, which means that the keys used to encrypt and decrypt your Data Keys are different. The Service Key is also randomly generated and its Private Key is encrypted via your C2 Key Set, guaranteeing that only you will have access to your C2 Backup data.

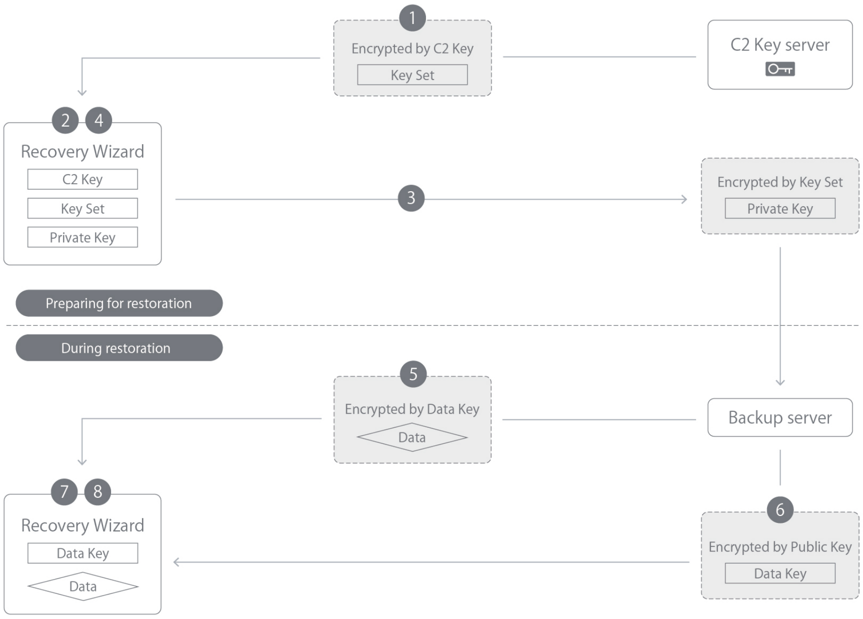
When backing up a device or a Microsoft 365 service, the Data Key will be randomly generated and temporarily saved to the memory of the C2 Backup agent or Data Manager, then used to encrypt your backup data. The Data Key will then be encrypted via the Service Key and transferred along with the backup data to be stored on the **Backup server**, which is the server dedicated to backup storage in C2 Backup.



1. Upon signing in to C2 Backup for the first time, the encrypted Key Set is retrieved from the C2 Key server.
2. The user enters their C2 Key, which is used to decrypt the Key Set.
3. The Service Key (Public Key and Private Key) is randomly generated in the browser.
4. After the Private Key is encrypted by the C2 Key Set, it is sent along with the Public Key back to the C2 server.
5. The C2 Backup agent or Data Manager randomly generates a Data Key, which will be used to encrypt the backup data.
6. The Service Key's Public Key is retrieved from the Backup server.
7. The backup data is encrypted via the Data Key and then uploaded to the server.
8. The Data Key is encrypted via the Service Key's Public Key and then uploaded to the Backup server.

Entire device restore

C2 Backup offers bare-metal backups and restorations through the creation of recovery media, allowing you to easily safeguard your entire device. With the C2 Backup Recovery Media Creator, you can create recovery media that can be used later on to restore your device. When executing a restore with the **C2 Backup Recovery Media Creator**, you must first enter your C2 Key to decrypt your data. Your encrypted data, the Data Key, the Service Key's Private Key, and the Key Set will then be retrieved, and your C2 Key will be used to decrypt the Key Set, the Private Key, and the Data Key. Then, your backup data will be decrypted by the Data Key and the restoration process will begin. This method employs **end-to-end encryption**, which means that all of your data is encrypted and decrypted on the client side, ensuring that the C2 server never has access to your encrypted data.



Preparing for restoration

1. The encrypted Key Set is retrieved from the C2 Key server.
2. The user enters their C2 Key, which is used to decrypt the Key Set.
3. The encrypted Private Key of the Service Key is retrieved from the Backup server.
4. The Key Set is used to decrypt the Private Key.

During restoration

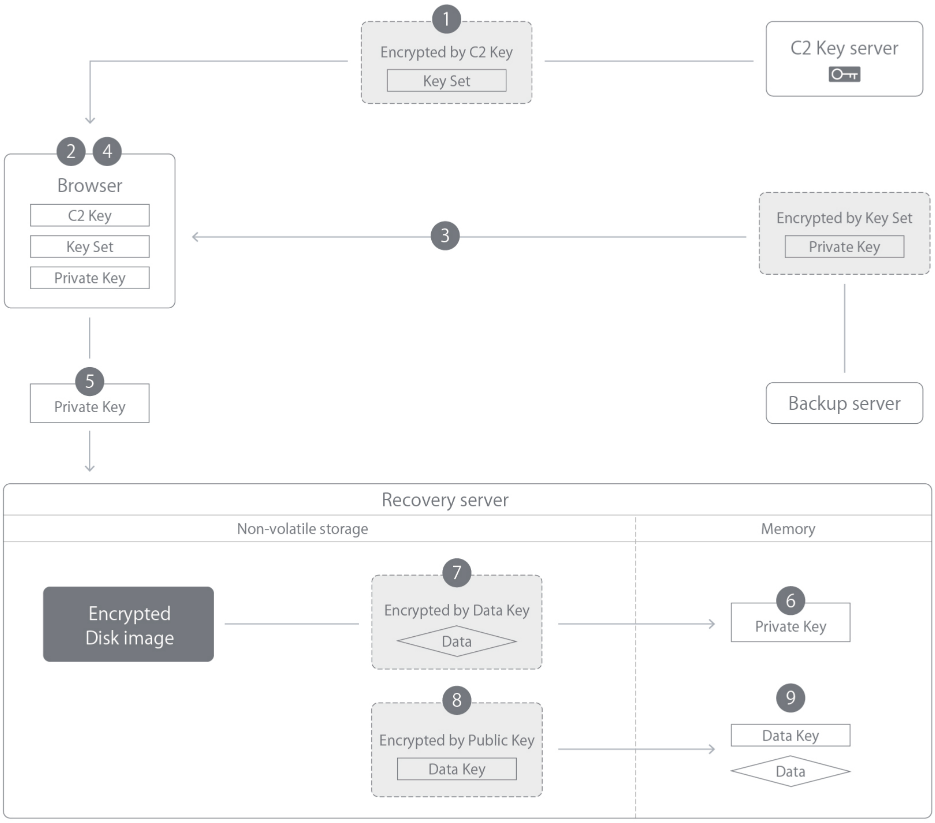
1. Data is restored from data chunks, which requires the corresponding Data Keys.
2. The corresponding Data Key is retrieved and then encrypted by the Public Key.
3. The Data Key is decrypted via the Private Key.
4. The data is decrypted by the Data Key.

Restore with the Recovery Portal

With the **C2 Backup Recovery Portal**, you can download specific files to your device or restore a Microsoft 365 service. The C2 Backup Recovery Portal performs **client-side encryption** during backup, meaning that the data is unreadable before entering the server or network. File restorations are performed only through the **C2 Backup recovery server**, whereas Microsoft 365 service restorations are performed through the **cloud service backup server**, both of which are sub-servers within C2 Backup.

Restore files to your device

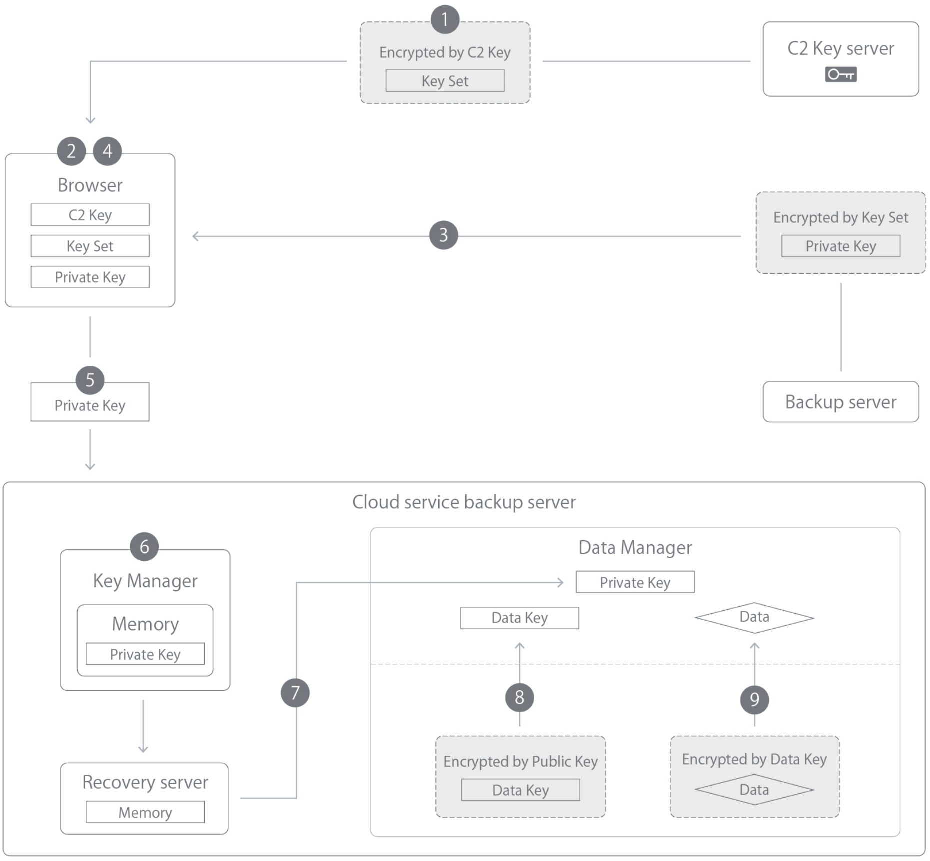
For file restorations, your backed up image must be mounted on the C2 server in order to access specific files from the **C2 Backup Recovery Portal**. Upon starting a restoration, you must enter your C2 Key, which will then be used to decrypt the Service Key's Private Key. This Private Key will then be transferred back to and mounted on the **C2 Backup recovery server**. The corresponding Data Key of the required data chunk will be decrypted on the serverside in order to decrypt the required data. However, to keep your data safe, the decrypted Private Key, Data Key, and restoration data are only cached temporarily in the server's volatile memory. Furthermore, if there is no request from your browser for more than 10 minutes, the disk image will be automatically unmounted, and the decrypted keys will be destroyed. Once your restoration data has been decrypted in the server's memory, your data will be available for download in the C2 Backup Recovery Portal.



1. The encrypted Key Set is retrieved from the C2 Key server.
2. The user enters their C2 Key, which is used to decrypt the Key Set.
3. The encrypted Private Key of the Service Key is retrieved from the Backup server
4. The Private Key is decrypted via the Key Set on the device.
5. The Private Key is sent to the C2 Backup recovery server.
6. The Private Key is temporarily stored in the memory of the C2 Backup recovery server.
7. After the C2 Backup recovery server mounts the encrypted backup disk, it will identify the Data Key required for the data chunk the user needs.
8. The C2 Backup recovery server retrieves the encrypted Data Key, which is then decrypted by the Private Key.
9. The data is decrypted via the Data Key.

Restore a Microsoft 365 service

When restoring or previewing a Microsoft 365 service in the **C2 Backup Recovery Portal**, you must enter your C2 Key into your browser, which will then be used to decrypt the Service Key's Private Key. The Private Key will then be transferred to the **Key Manager**, which handles all of the keys within the **cloud service backup server**. All of the keys in the Key Manager are cached temporarily in volatile memory and will be destroyed if there are no restore tasks or requests from your browser for more than 10 minutes. The **Data Manager**, which handles the data between the Microsoft server and the C2 server, will then request the encrypted data from the C2 Backup recovery server and the Private Key from the Key Manager. Both the encrypted data and the Data Key will be decrypted in the Data Manager and restored to the destination. At this point, items that you wanted to restore will be restored to the Microsoft server, and items you wanted to preview will be previewed in the C2 Backup Recovery Portal.



1. The encrypted Key Set is retrieved from the C2 Key server.
2. The user enters their C2 Key, which is used to decrypt the Key Set.
3. The encrypted Private Key of the Service Key is retrieved from the Backup server.
4. The Key Set decrypts the Private Key.
5. The Private Key is sent to the Key Manager of the cloud service backup server.
6. The Private Key is temporarily stored in the Key Manager's volatile memory.
7. Upon receiving the restore request, the C2 Backup recovery server takes the Private Key and passes it to the Data Manager.
8. The Data Manager retrieves the encrypted data and the encrypted Data Key.
9. The Private Key decrypts the Data Key, which is then used to decrypt the data.

Other required data

Outside of your backup data, certain additional information will be necessary to utilize the full functionalities of C2 Backup and to maximize your user experience. For example, the name and IP address of your device will be required for device management, and your username and email address will be required for the associated cloud services. When using Microsoft service backups, additional information such as your email subjects, senders' email accounts, and other unidentifiable metadata will be required to enable the **Log** feature and the **search tool** in the C2 Backup Recovery Portal. All of this information is protected with disk encryption and stored in Synology's Data Centers, which have undergone rigorous inspections for strict security protocols and physical safety measures, as well as meeting Synology's high standards for incident response and access limitations.

Conclusion

Synology puts security and privacy first when designing its services, giving customers full control over their data, even in the public cloud. Synology C2 services follow industry best practices by encrypting data during storage and transmission using two global standards.

You can keep your data safe with Synology C2 Backup by staying on top of data backups using a single device or Microsoft 365 service backup task. Along with being able to back up your data, you can also browse it or restore it, all while keeping your data safe and secure with state-of-the-art encryption technology.