CyStack

Whitepaper

CyStack Locker Password Manager - locker.io

This white paper provides technical descriptions and specifications of CyStack Locker

Version 1.0 - June 2021

About CyStack

Founded in 2017 by a team of security experts, CyStack is now one of the leading cyber-security companies in Vietnam and a member of Vietnam Information Security Association (VNISA) as well as Vietnam Safe Product and CyberSecurity Ecosystem Development Association. CyStack is a partner providing security solutions and services for many large domestic and foreign enterprises.

CyStack's research has been featured at the world's major security events such as BlackHat USA (USA), BlackHat Asia (Singapore), T2Fi (Finland), XCon - XFocus (China)... CyStack experts have been honored by global corporations such as Microsoft, Dell, Deloitte, D-link...

Summary of CyStack Locker's Security Principles

- **Trusted Data Access**: We make sure you can reliably and securely manage and access your confidential data whenever and wherever you need it, whether you are offline or online.
- **Data Viewable to ONLY You**: CyStack Locker is a Zero-Knowledge solution, which means that the data is always encrypted, both on your device and on the CyStack servers, and that no one except you, who hold the Master Password to decrypt everything, can decrypt to see your data.
- **Application of the Best Security Technologies**: CyStack Locker applies the highest security standards to storing and transferring your confidential data. Our designs protect you against malicious attacks such as brute-force or unauthorized data access.
- **Secure Storage Infrastructure**: We currently use the network infrastructure of the world's leading service providers (AWS, Digital Ocean) to store your data; this helps ensure that the system is always safe and stable.
- **Timely Incident Response**: Operating the system 24/7, the CyStack team monitors any abnormalities and responds immediately to any problems.
- **Constant Security Evaluation**: CyStack Locker is implemented with a Bug Bounty program for the world's top researchers to perform constant assessment and penetration testing. Besides, the CyStack team of security experts directly assesses and analyzes risks for the system on a periodical basis to ensure that CyStack Locker is always in the best security condition.
- **Centralized Management**: For businesses, CyStack Locker provides a web-based administration dashboard where administrators can set up security policies, monitor security status, and report. All user activities are logged so that administrators can analyze and evaluate later.

Contents

List of Figures

Overview of CyStack Locker

1.1 Introduction

CyStack Locker is designed to help Users or User Groups manage confidential data, especially logins and passwords. However, to be able to access and decrypt the data in CyStack Locker, users need to memorize ONLY one item. That is their Master Password.

Decrypting user data requires three components: Master Password, Encryption Key and a copy of user encrypted Vault data. Multiple methods can be used to protect each component and each method faces particular threats. By requiring a high level of security in all three components, user data is secured by combining the best features of each. Master Password and Encryption Key are two secret elements for the "two-secret key derivation" process, used in encryption and (data-retrieving) decryption.

1.2 Architecture

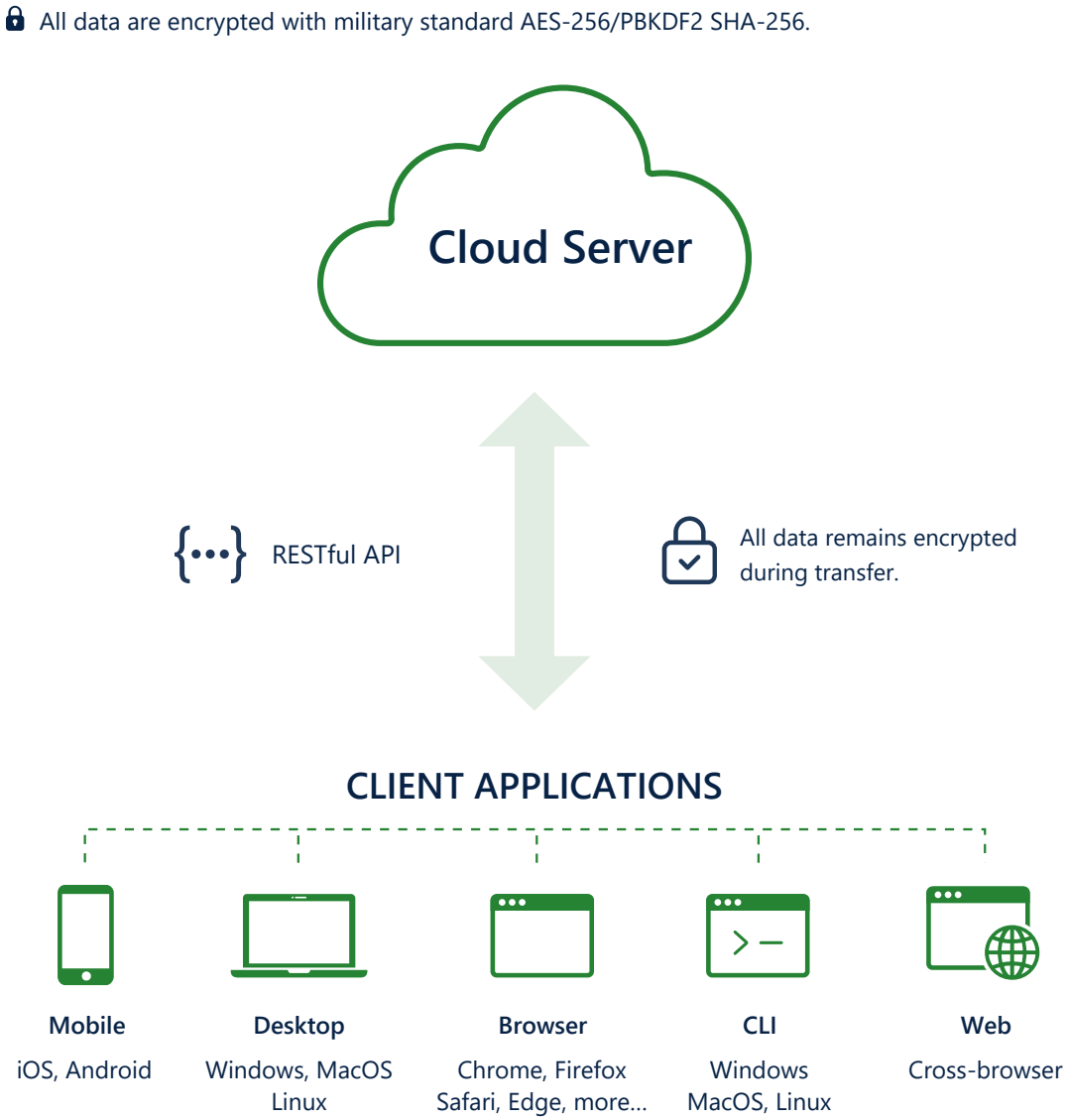

Figure 1: Architecture of CyStack Locker

Security Principles

2.1 Master Password

Master Password is an important secret component in CyStack Locker's "two-secret key derivation" process and is the only item the user needs to memorize for data encryption and decryption.

CyStack recommends that users choose a strong Master Password to ensure safety as well as to prevent common types of password attacks (eg. brute force) performed through supercomputers. CyStack Locker also incorporates a password strength meter that evaluates the Master Password the user is creating and displays a warning. A strong Master Password should comprise a combination of lowercase and uppercase letters, numbers, and special characters so that it is not easily stolen.

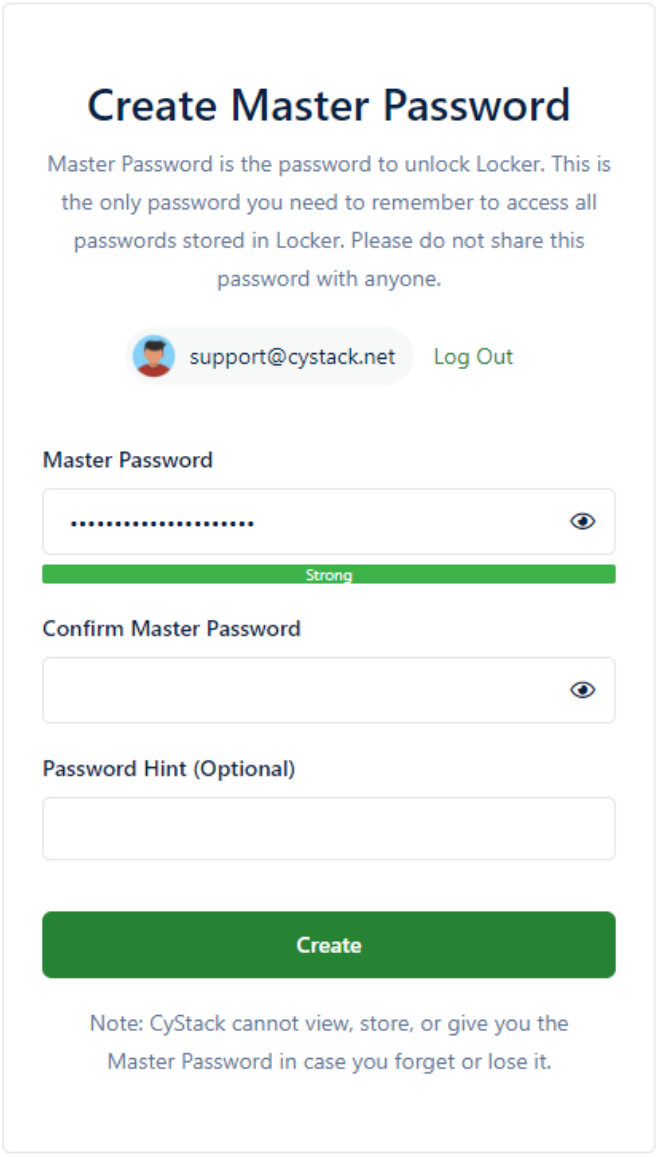

Figure 2: How to create a strong Master Password

2.2 Encryption Key

The other component of the "two-secret key derivation" process, Encryption Key, is generated when a user registers their CyStack Locker account. While there is only one Master Password, which the user needs to memorize, many Encryption Keys are created and used in encryption and decryption processes to access and store data on the CyStack Locker servers. Combining the two components, Encryption Key and Master Password, which have distinctive characteristics but complement each other, ensures a high level of independence as well as security of the data and of the secret keys.

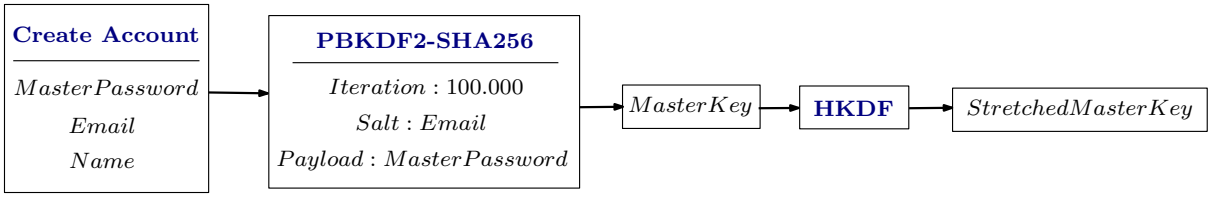

Figure 3: How a Master Key is generated

2.3 End-To-End Encryption

The user's passwords and personal data are secured, with AES-256-CBC Symmetric Encryption algorithm, hash function, and PBKDF2-SHA-256 algorithm. All security keys are created and managed locally on the user's device; all encryption and decryption processes are likewise performed locally. The CyStack Locker servers transfer and store encrypted data only when there is a request to access information.

2.4 Zero-Knowledge Encryption

CyStack Locker cannot know or retrieve the user's passwords or any other confidential data. All data is secured by end-to-end encryption through the user's personal email and Master Password. CyStack Locker does not store and cannot access the user's Master Password or security keys.

2.5 AES-256-CBC Encryption Algorithm

AES-256-CBC (Cipher Block Chaining), the algorithm used to encrypt Vault, is a standard cryptographic algorithm and is used by the US government as well as other government agencies worldwide to protect top-secret data. With proper implementation and strong enough Encryption Key (from the user's Master Password), AES-256-CBC algorithm is proven unbreakable.

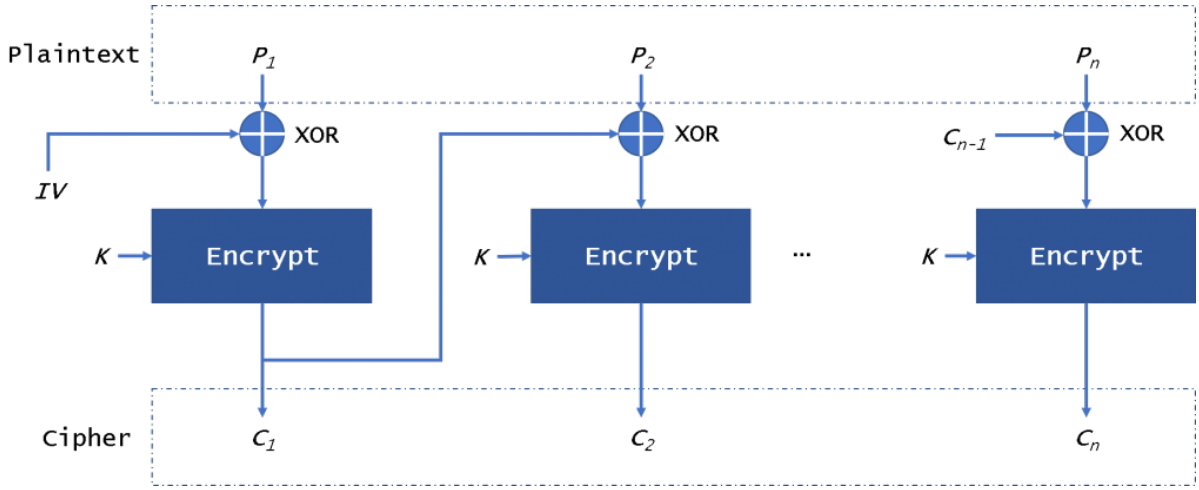

Figure 4: AES-256-CBC encryption

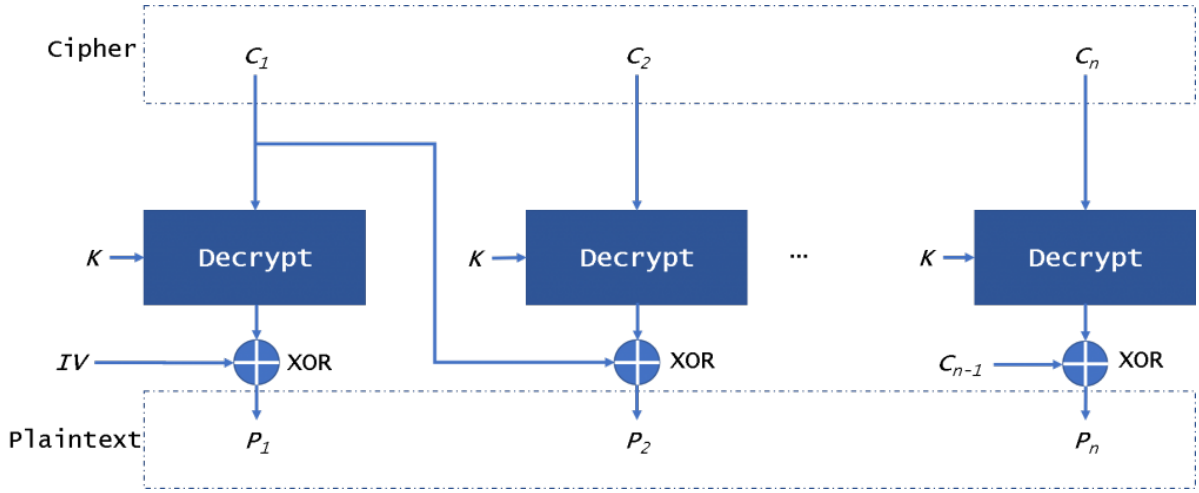

Figure 5: AES-256-CBC decryption

2.6 PBKDF2 Key Derivation Algorithm

The PBKDF2 (Password-based Key Derivation Function 2) SHA-256 algorithm is for generating Encryption Key from the user's Master Password. Before being sent to the CyStack Locker servers, Master Password is encrypted with a random value created by using the user's email address and hashing technique, locally on the user's device. When the CyStack Locker servers receive the encrypted Master Password, the password is encrypted again, with a secure random value (using the CSPRNG security algorithm) and hashing technique, and subsequently stored in the database of CyStack Locker.

The default number of iterations with the PBKDF2 algorithm is 100,001 on the user's device (this can be configured from the account settings), and then an additional 100,000 on the CyStack Locker's servers (for a total of 200,001 iterations by default) before being stored on the servers. Group Key is shared via the RSA-2048 algorithm.

The hash functions used are one-way, which means that no one at CyStack Locker can retrieve them to know the user's Master Password. Even if CyStack Locker is attacked, the user's Master Password cannot be stolen by any means.

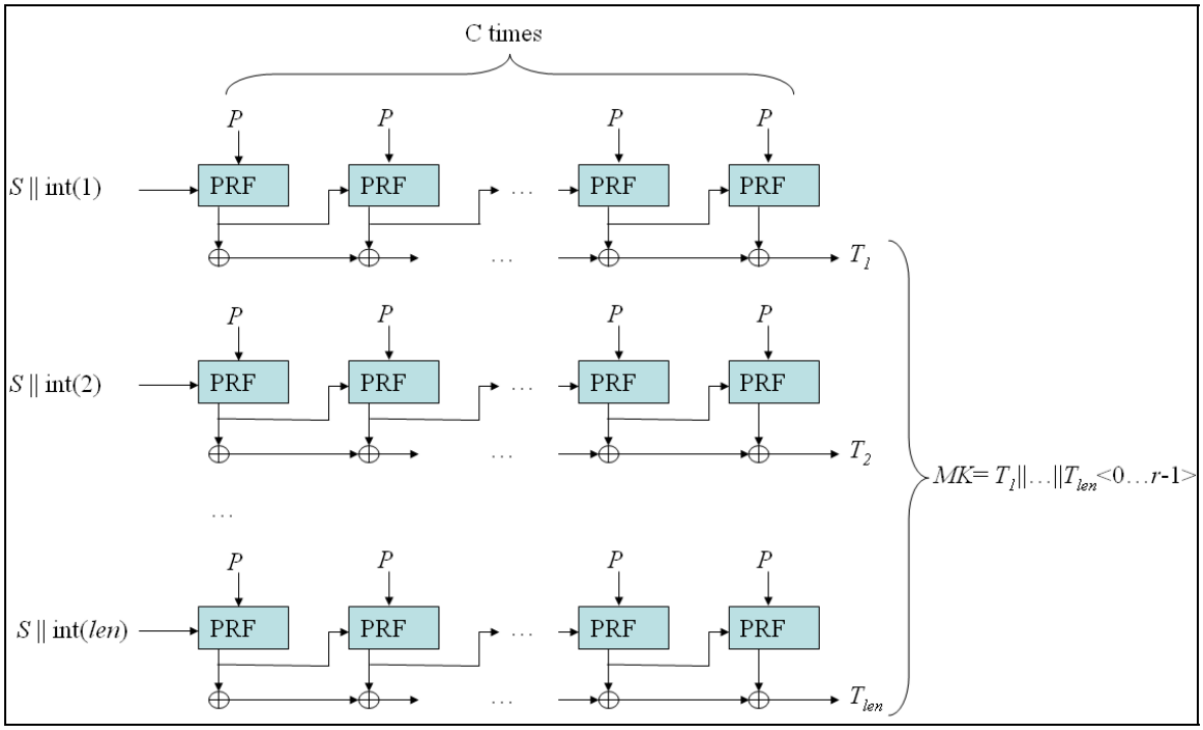

Figure 6: PBKDF2 key derivation algorithm

2.7 RSA Key Pair Generator

An RSA key pair consists of a Private Key and a Public Key. RSA Private Key is used to generate the Digital Signature while RSA Public Key is for verifying the Digital Signature. RSA Public Key is also used in the encryption of the DES or AES algorithms while RSA Private Key is to recover those keys.

The RSA Public Key Generator algorithm is based on the difficulty in solving the "factoring problem". The factorization problem is to find all primes of a given number n. When n is large enough and is the product of several large primes, the problem is considered complicated. For RSA, n usually has at least 512-bits and is the product of two large primes.

RSA-2048. The PKA algorithm can be used to generate pairs of Private Key and Public Key within the secure boundary of the cryptographic coprocessor, given the module size from 512 bits to 2048 bits or 4096 bits. CyStack Locker uses RSA-2048, which has 617 decimal digits (2048 bits) and is the largest of the RSA numbers. RSA-2048 may not be factorizable for many years to come unless considerable advances are made in integer factorization or computational power in the near future.

```
RSA-2048 = 25195908475657893494027183240048398571429282126204032027777137836043662020707
           75955562640185258807844069182906412495150821892985591491761845028084891200728
           44499268739280728777673597141834727026189637501497182469116507761337985909570
           00097330459748808428401797429100642458691817195118746121515172654632282216867
           99875491824224336372590851418654620435767984233871847744479207399342365848238
           82428119816381501067481045166037730605620161967625613384414360383390441495263
           34432190114657544454178424020924616515723350778707749817125772467962926386356
           63732899121548314381678998850404453640235273819513786365643912120103971228222
           120720357
```

Figure 7: RSA-2048

Data Management and Security

3.1 Key Derivation

In CyStack Locker, many Encryption Keys are generated when the user registers a CyStack Locker account, then used in the encryption and decryption of data and keys before being saved on the CyStack Locker servers.

Each CyStack Locker account owns Encryption Key derived from the user's Master Password. The Encryption Key is used to encrypt all data in Vault.

3.2 Encoding Process

CyStack Locker utilizes 256-bit AES-CBC encryption for Vault and PBKDF2 SHA-256 algorithm for generating Encryption Key to protect the data storage.

CyStack Locker always encrypts and/or hashes your data on your local device before sending anything to cloud servers for storage. The CyStack Locker servers are used to store only encrypted data.

Vault can be decrypted only with the key derived from your Master Password. CyStack Locker is a Zero-Knowledge solution, which means that you are the only one who can access the key and decrypt the data in your Vault.

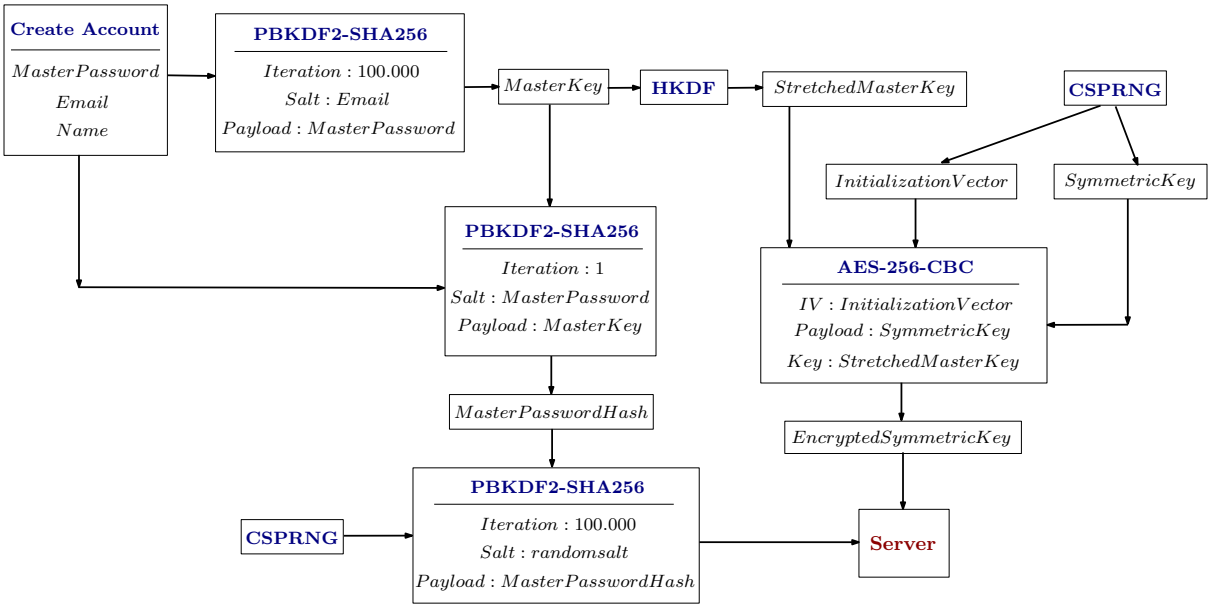

Figure 8: Master Password encryption, Encryption Key and Symmetric Key derivation

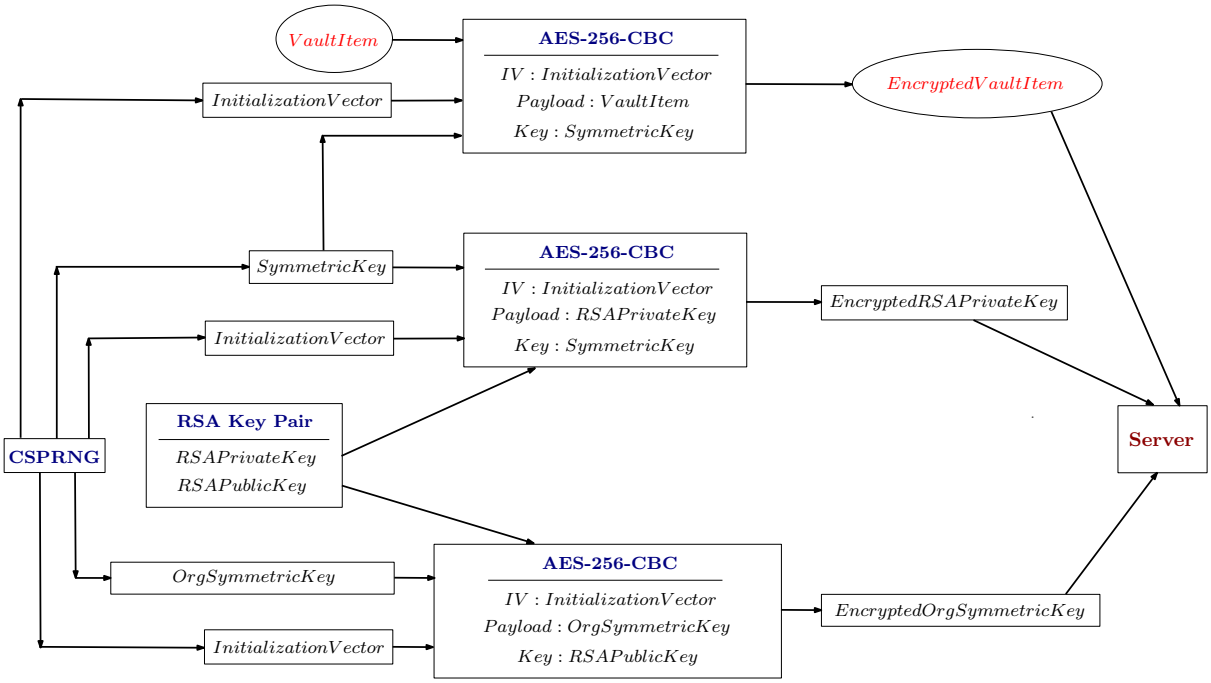

Figure 9: Symmetric Key and Asymmetric Key derivation, then encryption and storage on servers

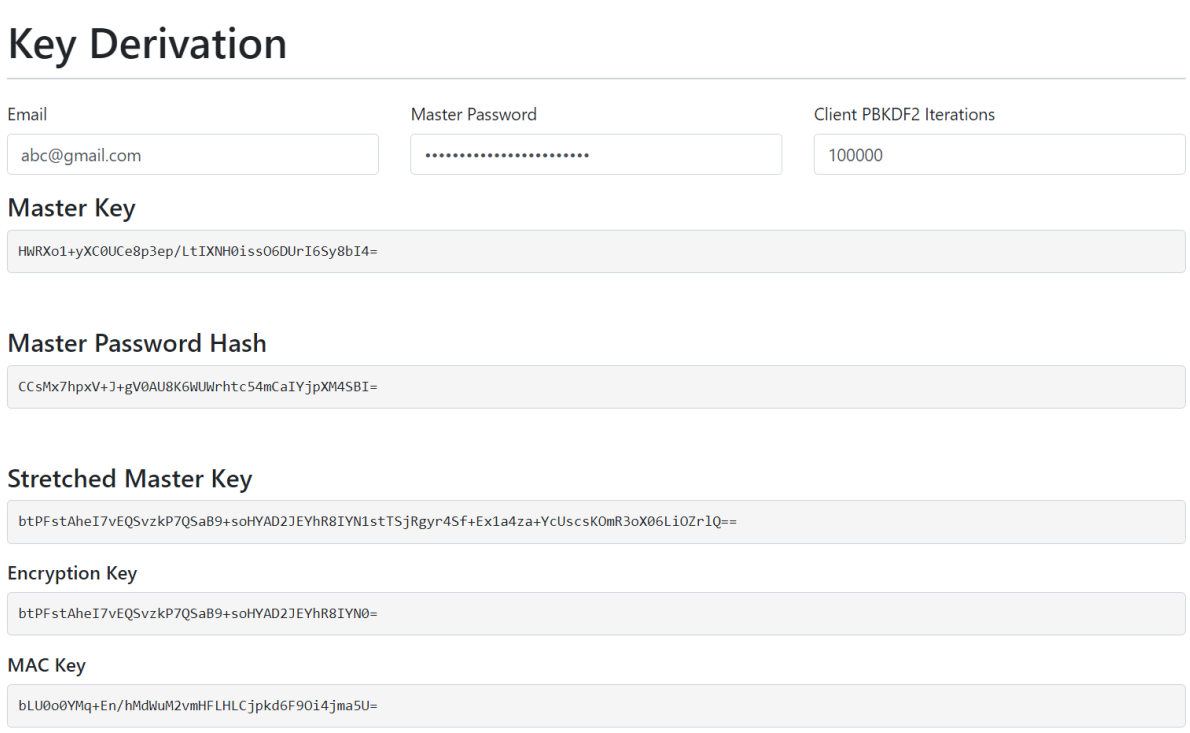

Figure 10: Key derivation in CyStack Locker

3.3 Login and Data Access

First, the user must enter their Email Address and Master Password to log in to their CyStack Locker account.

Next, CyStack Locker uses the PBKDF2 Key Derivation algorithm with a default itineration number of 100,000 to expand Master Password with a random value of the user's email address.

The received value is 256-bit Master Key. A hash of Master Key is sent to the servers when the user creates and logs into their account, and is used to authenticate the user account.

Master Key is then also expanded to 512-bit with the HMAC-based Extract-and-Expand Key Derivation Function (HKDF) algorithm. Encrypted Symmetric Key is decrypted with this Stretched Master Key. Finally, Symmetric Key is used to decrypt the data in Vault

The decryption process is performed entirely on the user's local device because neither Master Password nor Stretched Master Key is stored on or sent to the CyStack Locker servers.

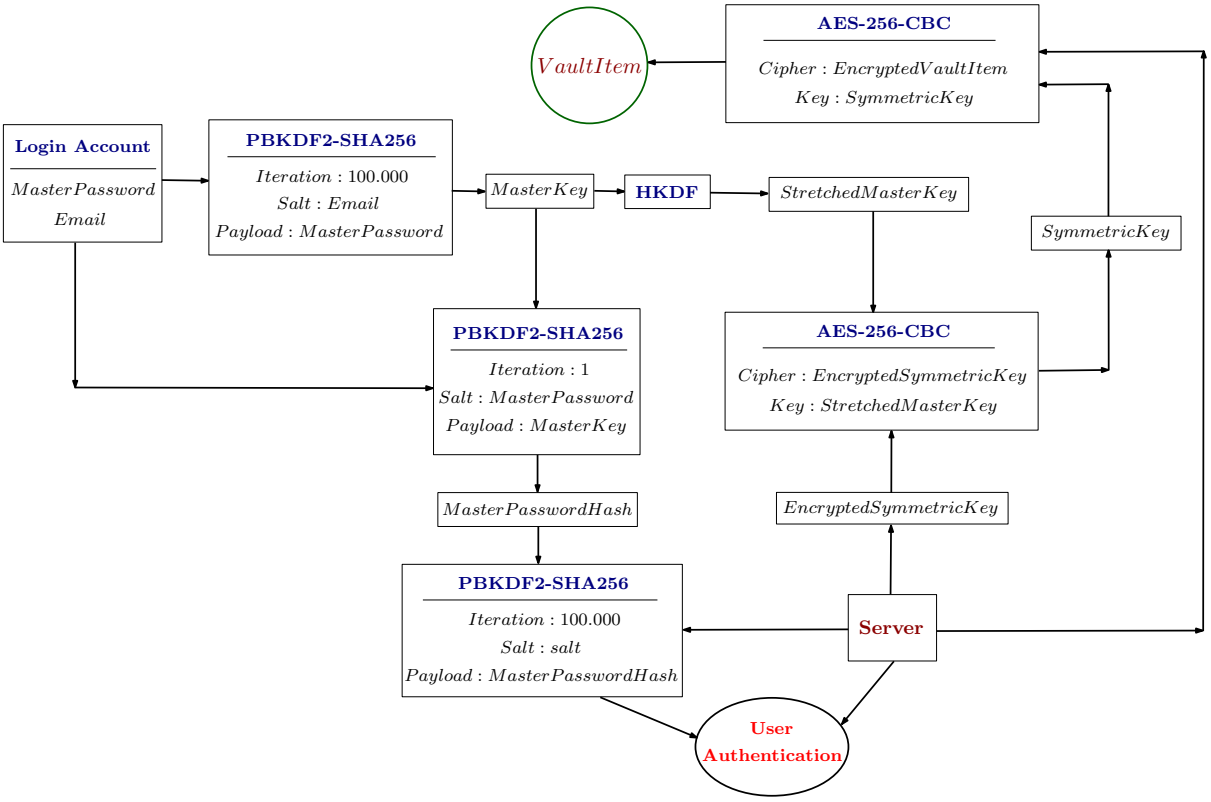

Figure 11: Overview of user login and data access in Vault

3.4 Master Password or Encryption Key Resetting

When changing Master Password, the user also has the option to reset the Encryption Key of the account. Conversely, when changing Encryption Key, the user can also choose to reset

Master Password. The reset process is carried out independently and separately for each element, making it unnecessary for the user to re-encrypt all data in Vault when they change Master Password or Encryption Key, yet ensuring a high level of authenticity and security.

Encryption Key reset is advisable if the user suspects that the previous Master Password has been compromised, or that Vault data in CyStack Locker has been stolen from one of the user devices.

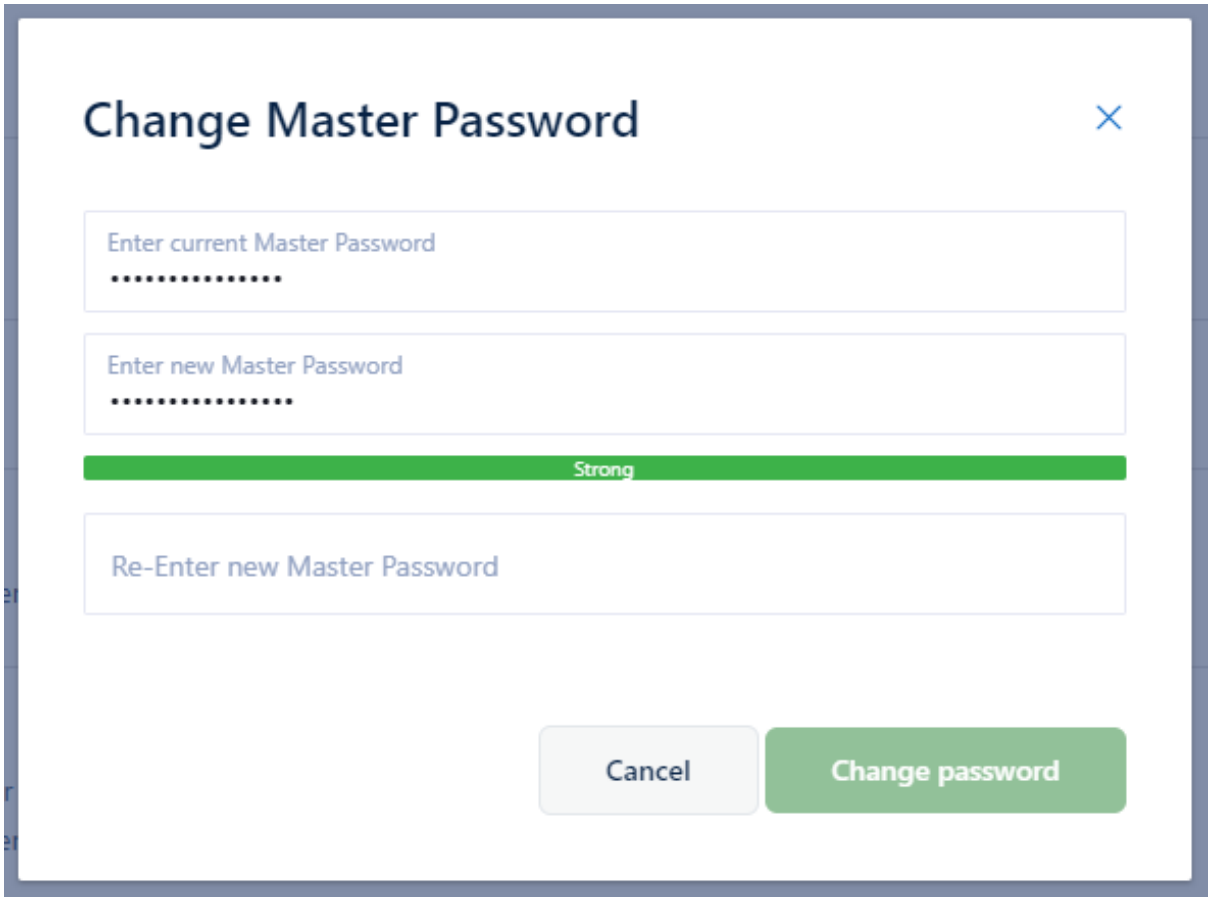

Figure 12: How to change Master Password

Organization Data Access and Sharing

4.1 Organization

In addition to giving the user an option of managing their confidential data with Vault and security keys, CyStack Locker enables them to create Organization for sharing confidential data among group members. An Organization can be a family, a team, a company, or any other type of groups that wants to manage the sharing of confidential data. Similar to the features of personal Vault, information managed and shared within Groups can include Login Data, Identity Data, Card Data and Note Data. Security and authenticity when accessing data in Organization and sharing data among members are ensured with RSA Key Pair, which comprises a Public Key and a Private Key, in the secure format of RSA-2048.

Organization Owner

The user that creates an Organization is referred to as Organization Owner. Organization Owner can invite another user to the Organization to become an Organization Member and share private data in Organization Vault, as long as that user has already registered a Cystack Locker account. Organization Owner can also assign permissions to that Member (User, Manager, Admin, ...) to define and limit their ability to access and manage data in Organization Vault.

Organization Member

After creating a CyStack Locker account, a user can be invited to be an Organization Member in one or many Organizations. After being authenticated and becoming a member of an Organization, the user is authorized to manage access and can request access to data in Organization Vault. Obviously, the user also can create one or many different Organizations where they become Organization Owner, then invite other users to join and share private data in their Organization Vault.

4.2 Organization Data Sharing

When a user registers a CyStack Locker account and would like to share confidential data with other users, the user can create an Organization and invite other users to join as Organization Members. RSA Key Pair, which comprises one Public Key and one Private Key, is generated and used during data encryption and decryption as soon as the user creates the Organization. The user now becomes Organization Owner.

When the user creates an Organization, besides RSA Key Pair which is derived and used, a Symmetric Key (generated earlier when the user registers their CyStack Locker account) and an Organization Symmetric Key are generated through the CSPRNG algorithm. Afterwards,

Organization Symmetric Key is encrypted with the public key from the user's RSA Key Pair, using the AES-256-CBC algorithm. Similarly, the secret key from RSA Key Pair is also encrypted with Symmetric Key, using the AES-256-CBC algorithm. After being encrypted, both keys are stored on the CyStack Locker servers.

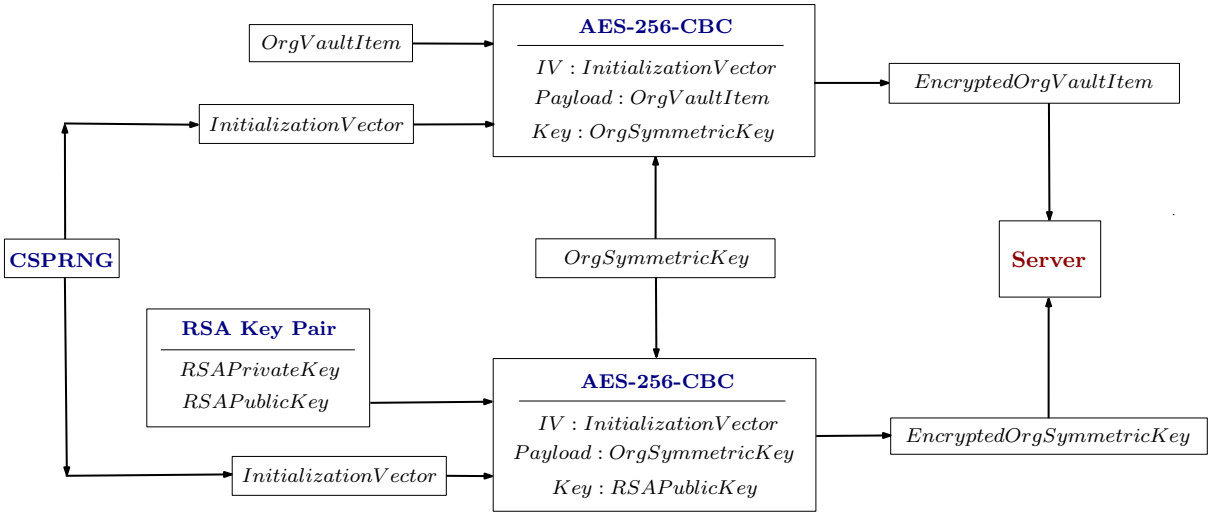

Figure 13: Encryption Key derivation and data storage in Organization

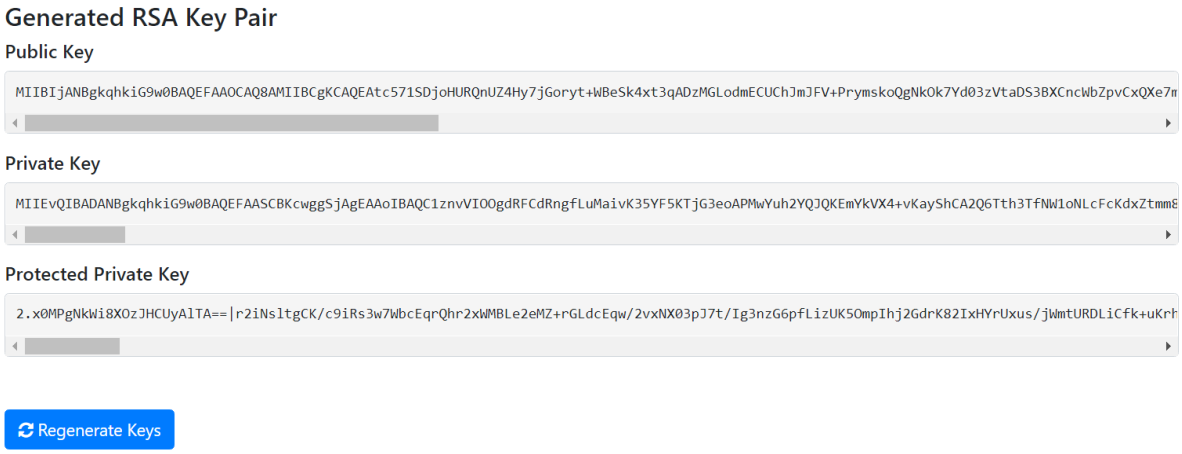

Figure 14: RSA Key Pair derivation in CyStack Locker

Organization Owner can start creating and adding data to Organization Vault, including Login Data, Identity Data, Card Data and Note Data. Then, Organization Vault will be encrypted using Organization Symmetric Key and stored on the CyStack Locker servers.

Organization Owner can invite other users to join Organization as Organization Members to share private data with each other. Confirmed invited users then join Organization as Organization Members under the roles assigned by Organization Owner. Organization Owner needs to authenticate Fingerprint, which serves as the invited users' public key for use in future data encryption, before agreeing to add those users to Organization.

Once every factor is fully authenticated, the users become Organization Members and have access to the data in Organization Vault following their authorized permissions.

Figure 15: List of members in Organization

4.3 Organization Data Access

When a Member in Organization would like to access data in Organization Vault, they can request access to the data through Organization Owner or equivalently authorized members, by submitting their own Public Key to Organization Owner. Organization Owner will now encrypt Organization Symmetric Key with Public Key received from the requesting member, and then send it back to that user. The Member will use their own Public Key to decrypt the received encrypted Organization Symmetric Key, then keep using this key in combination with the encrypted Organization Vault stored on the CyStack Locker servers to decrypt and access the information they want.

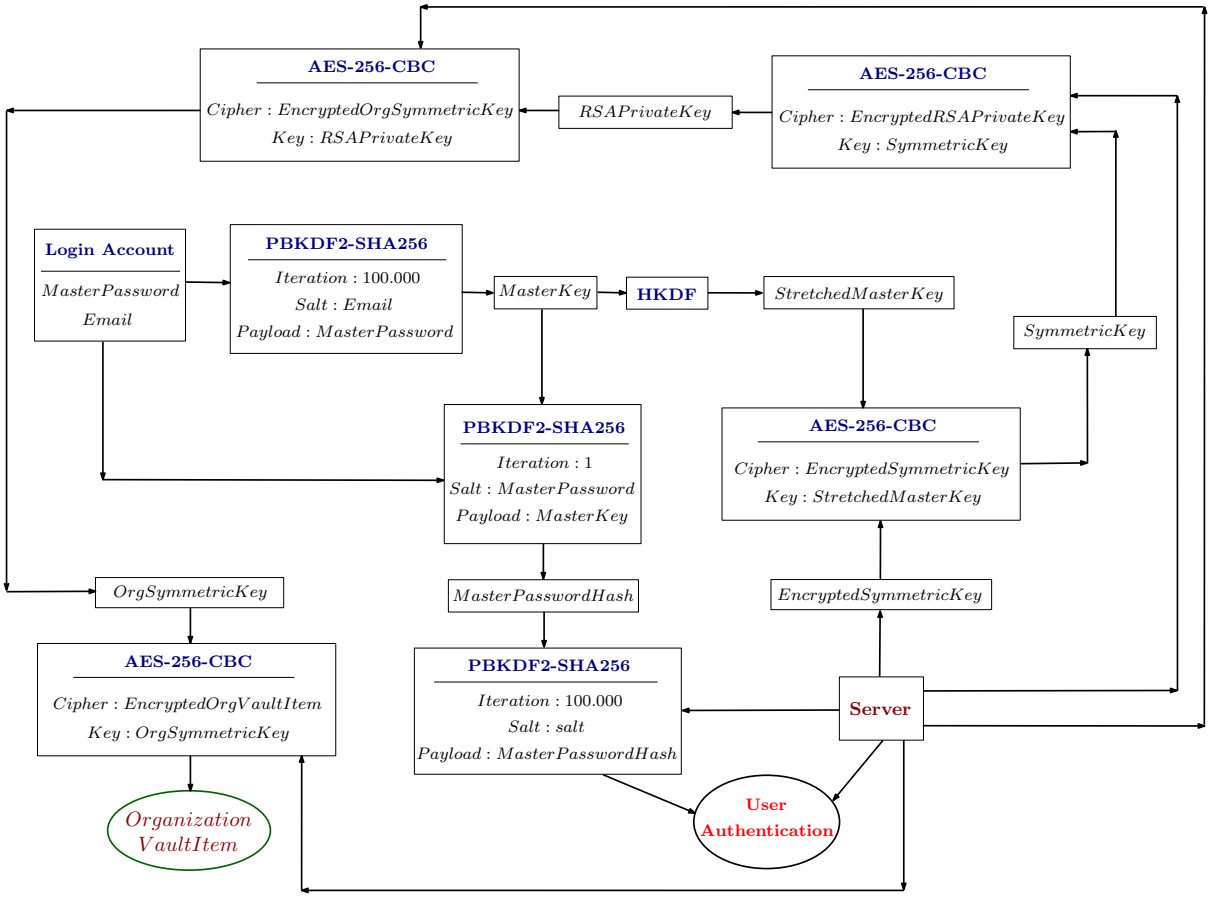

Figure 16: Overview of login and data access in Organization

Network and Data Infrastructure

5.1 Service Providers

CyStack Locker uses cloud server services from some of the world's leading providers for its infrastructure. It is common for these suppliers to meet minimum industry standards such as:

- ISO/IEC 27001: ISO information security management standard
- AICPA SOC 2: AICPA data security standard
- CSA: Cloud Security Alliance cloud service security standard

5.2 Availability

CyStack Locker is designed and built with redundancy for our data centers, minimizing the risk of inaccessibility. Even if the user does not have Internet access, they can still access their data through the copy downloaded on their application.

5.3 Data Storage

CyStack stores user data in the form of files and databases at our trusted storage servers. All the data is encrypted with the user's Master Password. No one, including CyStack's employees, but the user themself can decrypt and access this confidential data.

5.4 Data Backup

We periodically back up user data to the data centers of leading Cloud service providers (AWS, GCP, and Azure) to ensure that even if something goes wrong, the data is still safe.

5.5 Data Transfer

All data is transferred through encrypted communication channels (SSL/TLS), combined with AES-256 encrypted data. With this design, man-in-the-middle attacks are disabled.

Security Assessment

6.1 Master Password

One of the two components of "two-secret key derivation", Master Password, is created and memorized by the user when the user registers a CyStack Locker account. The major limitation of secret data that is memorized and used by humans is the fact that this data can be guessed using algorithms or automatic word guessing systems, based on a set of simple or meaningful word-number sequences (dictionary attack/rainbow table attack).

CyStack Locker has implemented multi-layer protections and multi-way authentication with a high level of security, through AES-256-CBC secure algorithms, hashing technique combined with end-to-end encryption and symmetric - asymmetric key. However, there still exists a high risk that Master Password becomes exposed to the user's clients for various reasons. Besides the user's self-disclosure, it can be hackers' common techniques such as key loggers or malware to infiltrate the user's clients and steal data, or complex algorithms run on supercomputers with high processing speed. Therefore, in addition to warning the user to set a strong enough Master Password to resist attacks, the role of completely unpredictable secret keys and random numbers like Encryption Key is crucial to ensure the security of the user's private data.

6.2 Public Key Verification

Currently, there is no perfect method for users to verify that the Public Key they encrypt data with (Encryption Key) and store on the CyStack Locker servers really belongs to the user they want to share data with. Therefore, when the CyStack Locker servers are compromised or taken over, hackers can provide a fake Public Key to the users to encrypt and successfully execute a Man in the Middle (MITM) attack. As a result, hackers obtain Encryption Key for Vault and can decrypt to access the users' confidential information, without leaving any anomalies for the users to detect or prevent this.

Basically, the threat becomes reality only when a user is invited to Organization and requests access to Vault, but the nature of the attack can be applied in any situation where confidential data (keys, information) is required to be encrypted with someone else's Public Key. There are several possible solutions: the user's Public Key is authenticated by a trusted third party before being encrypted with any data, or the Public Key authentication process is directly and separately performed through a secure communication channel other than that provided by the CyStack Locker servers.

6.3 Security Testing

CyStack Locker is periodically and constantly audited and pentested by:

- Security expert team of CyStack
- Global security community through CyStack Locker's Bug Bounty program on Bug Bounty platform whitehub.net
- Independent security partner of CyStack Locker

All actions are taken to ensure that the system is always in the best security condition and away from attacks.

Conclusion

This technical documentation provides an overview of CyStack Locker's data management and security technology, built to fulfill strict requirements for safety as well as standards of information security management system with constant evaluation and review. CyStack Locker's security solutions, software, infrastructure, and processes are designed to have a multi-layered platform and defense-in-depth, ensuring authenticity and security.

By combining highly reliable security algorithms such as AES-256-CBC, PBKDF2 hash function, together with end-to-end and non-disclosure encryption standards, as well as symmetric and asymmetric encryption keys, the data management and security technology of CyStack Locker offers a comprehensive solution to secure user data, especially passwords and confidential information.