Security White Paper

VERSION 3.1
10 AUGUST 2018

Contents

General Security Principles

Master Password

To ensure the security of an account, it is essential that users choose a strong master password for their Vaulteq account. The master password should be long and unique, with a mix of character types; it directly impacts the overall security of the data as other encryption keys are generated from this password.

Derived Key

Master Password which is first derived with 10k rounds of PBKDF2 with the account name as salt. The Derived Key is used to encrypt the Encryption Key and to create the Authentication Hash.

Private Encryption Key

A random generated Elliptic-curve key pair of 32-bytes is created. The Private Key is encrypted with AES-GCM-256 and the Derived Key as the key. The Private Encryption Key is used to Decrypt your Encrypted Vaults.

Public Encryption Key

This is the public key everyone can use to encrypt data. It is part of the Elliptic-curve key pair. Only the owner of the Private Encryption Key of the pair is able to decrypt the encrypted data. This key is used by team members to encrypt shared vaults.

Authentication Hash

SHA512 Hash is made from the Derived Key. The Authentication key is used to authenticate with the Vaulteq API.

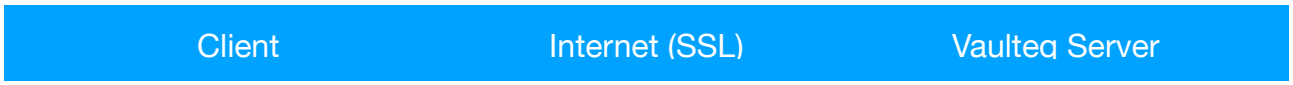
Access Token

When authenticated a unique access token is stored on the device. This token is used during the communication with the Pawr server. This ensures an extra level of security. ea. When a device is lost this token can be used to block all access.

Device Key

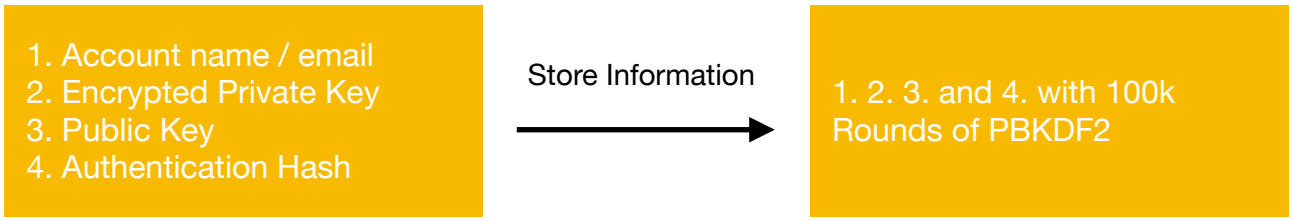
For each unique combination of location and device (App, Extension or Console) a device key is generated and coupled to an access token. Devices can be managed to allow two-factor authentication.

Communication



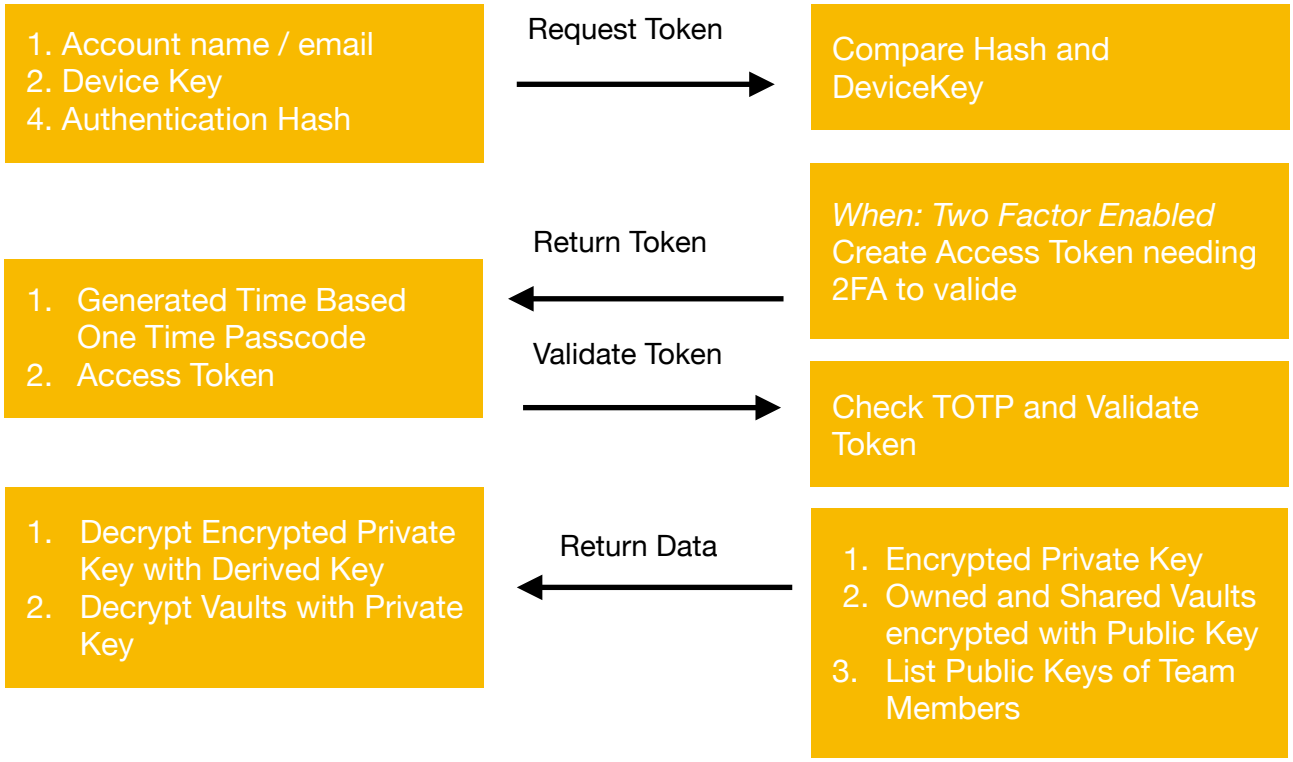
Account Registration

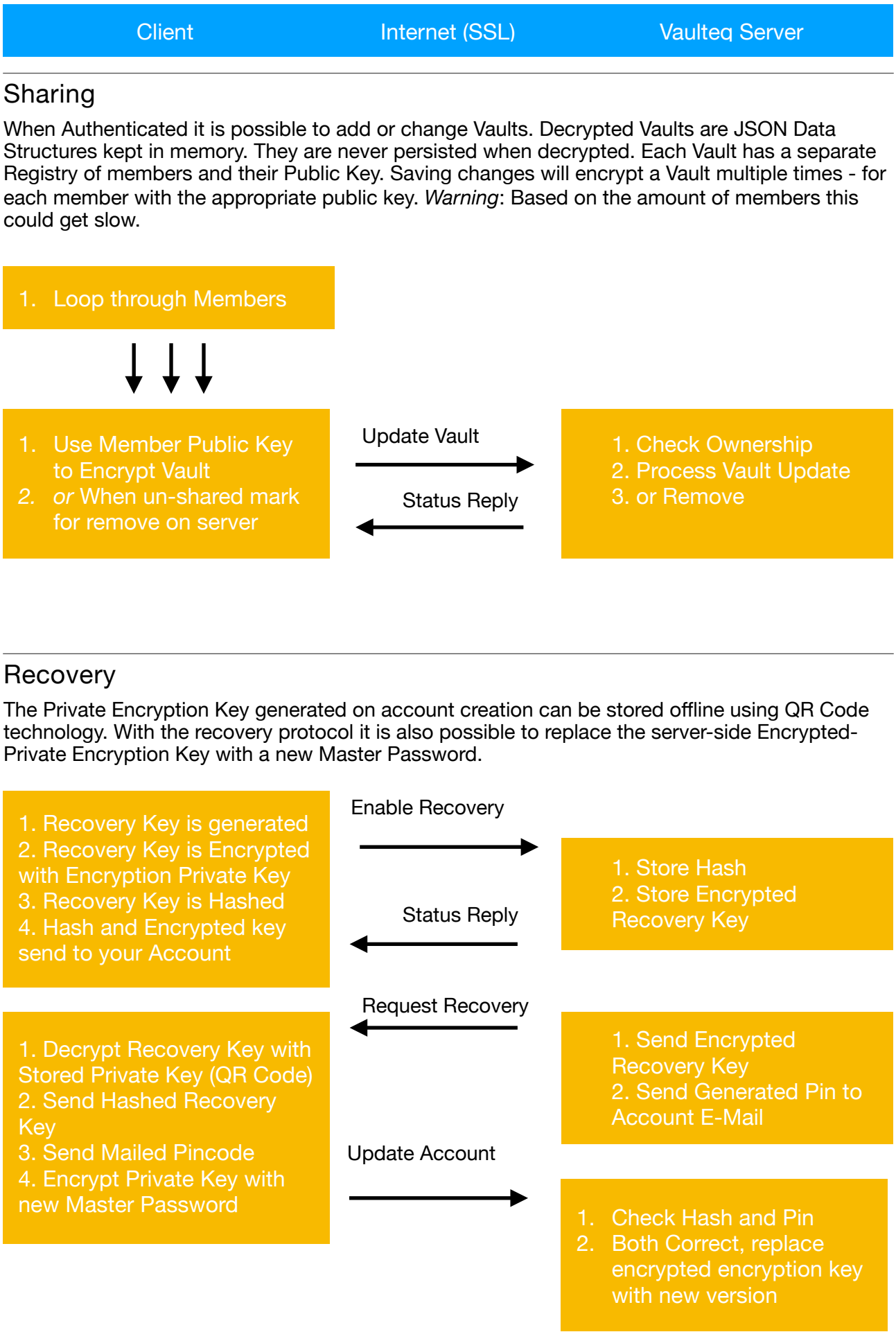
When the account is created an Elliptic-curve key pair is generated on the Client. The Private Key is encrypted with the Master Password. The master password never leaves the Client.



Authentication

After the registration it is possible to request an Access Token. The Master Password is always needed for an Authentication since it is never persisted or stored in memory. Without the Master Password it is impossible to Decrypt the Private Key to get access to the Vault contents. When 2FA is enabled for a device key the Token needs to be validated first.




Client
Internet (SSL)
Vaulteq Server
Sharing
When Authenticated it is possible to add or change Vaults. Decrypted Vaults are JSON Data Structures kept in memory. They are never persisted when decrypted. Each Vault has a separate Registry of members and their Public Key. Saving changes will encrypt a Vault multiple times - for each member with the appropriate public key. Warning: Based on the amount of members this could get slow.
1. Loop through Members
1. Use Member Public Key to Encrypt Vault
2. or When un-shared mark for remove on server
Update Vault
Status Reply
1. Check Ownership
2. Process Vault Update
3. or Remove
Recovery
The Private Encryption Key generated on account creation can be stored offline using QR Code technology. With the recovery protocol it is also possible to replace the server-side Encrypted-Private Encryption Key with a new Master Password.
1. Recovery Key is generated
2. Recovery Key is Encrypted with Encryption Private Key
3. Recovery Key is Hashed
4. Hash and Encrypted key send to your Account
Enable Recovery
Status Reply
1. Store Hash
2. Store Encrypted Recovery Key
Request Recovery
1. Decrypt Recovery Key with Stored Private Key (QR Code)
2. Send Hashed Recovery Key
3. Send Mailed Pincode
4. Encrypt Private Key with new Master Password
1. Send Encrypted Recovery Key
2. Send Generated Pin to Account E-Mail
Update Account
1. Check Hash and Pin
2. Both Correct, replace encrypted encryption key with new version

Security

Protection

A. Two-Factor Authentication can be enabled to increase the account protection.
B. Access Tokens are limited to one day of usage. Their expiration can be monitored in the Console.
C. Each authorised device can be managed from the Console. A device can be blocked permanently or untrusted to force two-factor.
D. Vaults and the Master Password is never persisted unencrypted and only decrypted into memory for the duration of application usage.

Attack Prevention

A. Brute Force the Authentication API with the account name. After 10 incorrect authorisation keys the account is locked and an email is send to the account holder with instructions to unlock the account.
B. All Vaulteq communication is done through HTTPS to prevent Man In The Middle Attacks.
C. Master Password never leaves the Client rendering MITM attacks obsolete.
D. AES-GCM-256, when used with a strong Master Password. The Master Password is protected with PBKDF2.

Type of brute force attack	**AES 256 (*)**	**AES 256 with PBKDF2 with 10000 iterations (*)**
4 million terms dictionary	2,8 seconds	**21 hours**
Alphanumerical(small caps + digits) password of 7 characters	15,7 hours	**48,6 years**
Alphanumerical(small caps + digits) password of 8 characters	23,6 days	**1751,3 years**

(*)Time to get the password on a Xeon 1.87 GHz (4 cores)