KEEVO

Keevo Multi-Factor / Multi-Signature Authentication System for Secure and Convenient Digital Identity and Virtual Asset Management

(version 1.1.4)

Introduction

Blockchain decentralized computing platforms are a nascent, highly disruptive technology with many potential applications, use cases and benefits which are growing rapidly. Crypto currencies, like Bitcoin, Bitcoin Cash, Etherium and others, are one of the first use cases for blockchain technology and are also growing significantly. These crypto currencies are virtual assets and means of digital stored value that leverage blockchain technology to enable users to securely own and easily transfer them anonymously and without the need for a 3rd party intermediary like a bank or central government. At the core of each blockchain use case is a user's digital identity or private key, usually a hexidecimal-based 64 character string of numbers and characters. These private keys are used to securely "sign" transactions such as sending or receiving a virtual asset like Bitcoin from one user to another and recording and validating the transaction on a highly secure and immutable blockchain.

While there are many benefits to this new type of database and decentralized compute platform, there are currently many frictions (pain points, unmet needs and latent desires) for users who are trying to securely and conveniently manage their private keys and virtual assets. Significant security breaches of internet-based software (SW) wallets which hold users' private keys online, large heists of crypto currency being held by online exchanges on behalf of users and other hacks and lost/stolen digital identities on various blockchain platforms are being reported with growing frequency, size and scale.

As a result, hardware (HW) wallets -- like Ledger Wallet's Nano S, X or Ledger Blue, Trezor's Model 1 and Model T, ShapeShift's KeepKey and others -- which hold a user's private keys on an "air gapped" device enable more secure transactions, have grown in popularity. And, while HW Wallets are indeed more secure than most SW Wallets, all of them still require users to keep a randomly generated pseudonym or seed phrase which needs to be written down on a piece of paper and then securely stored separate from the device. Seed phrases are 12 to 24 words which need to be entered in a specific order. These seed phrases can then be used by the user -- or any person who gets access to the seed phrase -- to recreate the private key being stored on a Wallet. Once any user is in possession of this private key, they can then “sign” transactions and transfer ownership of the crypto currency and virtual assets associated with and owned by that private key to any other key. The intent of these seed phrases is to let users restore their HW wallets in the case where their original device becomes inoperable for some reason or is lost or stolen. However, managing and keeping paper seed phrases safe is incredibly cumbersome, unreliable and inherently insecure. In fact and to our mind, the need for paper pseudonyms completely negates any security provided by the HW technology in the wallet devices themselves. Lastly, none of these HW or SW wallets or online exchanges currently offer a good solution to securely transfer virtual assets to beneficiaries and to do so without sharing any private keys or account information.

Keevo’s novel Multi-Factor / Multi-Signature Authentication (MF/MSA) system, Keevo’s HW Wallet and unique business model combine to solve these frictions and create what we believe is the world’s most secure AND convenient way to manage your digital identity and virtual assets for your and your named beneficiaries on any blockchain platform.

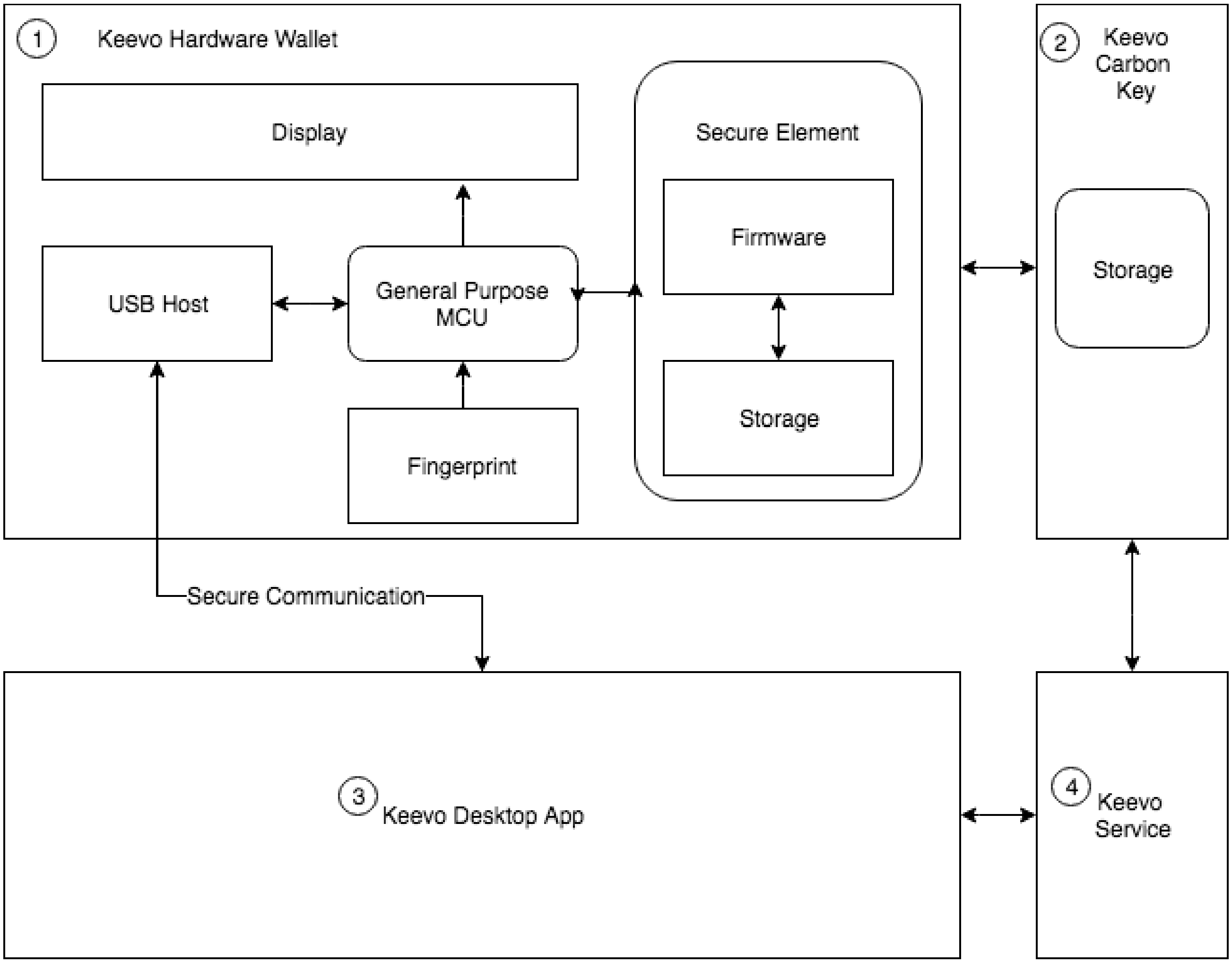
Our (MF/MSA) system is at the heart of this secure, convenient and flexible solution.

- As a start, MF/MSA enables the Keevo Wallet to offer the only four factor authentication (“4FA”) solution in the market.
- In addition to two standard factors which include a password or PIN (“something the user knows”) and the device itself (“something a user has”), the Keevo Wallet also employs a user’s biometric fingerprint and technology (“something unique to an individual user”) to encrypt and decrypt private keys.
- As such, the Keevo Wallet with 4FA is the only HW wallet on the market that does not require a paper seed phrase to restore broken/stolen/lost devices. We call this, “Paperless” Recovery” and it’s core to our invention and unique in the marketplace.
- MF/MSA also enables Keevo to offer the world the first native beneficiary solution tp transfer virtual assets in a highly secure, private and still decentralized manner.
- And, we have several other features and benefits that leverage this MF/MSA system to enable even further security and convenience enhancements, future multi-level authentication approaches for enterprises and multi-party networks, among other valuable applications.

Key Components

As outlined below, there are four main components to the Keevo solution:

1. The Keevo Hardware (HW) Wallet or Device
2. The Keevo Carbon Key
3. The Keevo Desktop App
4. The Keevo Service



The Keevo Hardware Wallet

The Keevo HW Wallet houses the core security components of the Keevo solution. Key elements include the following:

1. 2.8” TCP LCD Display
2. Fingerprint sensor
3. USB port
4. Secure and General Purpose MCUs
5. Secure Element where firmware and kernel are stored

The Keevo Device is an air-gapped HW Wallet which securely stores the user's encrypted private keys. It also provides a display which enables the user to setup their digital identify and create their private keys, register with the Keevo service, and manage their virtual assets on the blockchain. The Keevo HW Wallet also connects to the Keevo Carbon Key and Desktop App via a secure communication framework.

The Keevo Carbon Key

The Keevo Carbon Key contains a secure memory element and is used as an independent factor and backup of the user's information for custodianship. The memory unit includes encrypted information from the user and their potential custodians.

The Keevo Carbon Key can be used to restore a user's HW Wallet and recover their secure private keys if any of the following occur:

- The Keevo HW Wallet is lost, stolen or becomes inoperable, or
- A user forgets their password, or
- A user is unable to enter his or her fingerprint

The Keevo Desktop App

The Keevo Desktop App is a downloadable software application which enables users to easily and conveniently manage their public keys and virtual assets including functionality such as checking balances and ownership associated with their digital identify, seeing the value of commonly held crypto currencies like Bitcoin based on third party exchange information, transferring virtual assets like crypto currency to other user's public addresses, etc. The Keevo Desktop App is a highly secure solution, but is still connected to the internet. As such, the communication protocol between the HW Wallet Device and the Desktop App will not allow for tampering of the Keevo Device.

The Keevo Premium Plus Service

Users do not need to register and pay for the Keevo Premium Plus Service, but doing so would provide them with many additional benefits. For users who opt in, register and pay for the Keevo Service, they will receive even more security, convenience and many other potential benefits to manage their digital identity and assets.

At its core, the Keevo service will provide users the ability to securely transfer to Keevo and rely upon Keevo to securely store their Keevo Carbon Key. This protects their information in an encrypted manner so no one, not even Keevo, can make any use of their data.   This service also enables users to easily retrieve and restore their digital identity and private key in the case of misfortune, such as losing their HW Wallet Device or if it becomes inoperable for some reason The Keevo service will also enable users to designate and initialize beneficiaries. These will be additional user identities who will encrypt the Keevo Devices (HW Wallet Device and the Keevo Carbon Key) with individual factors such as a PIN and Fingerprint. In this case and upon certain verifiable circumstances (such as death of the user), the Keevo service can provide beneficiaries with a user's Keevo Carbon Key and the ability to retrieve the user's private key and restore/reset the key and designate new beneficiaries.

As part of our vision, the Keevo Service will also include many other potential solutions and benefits for registered users. These benefits could include, but are not limited to some of the following …:

- Enhanced and extended Keevo HW Wallet Device warranties
- Discounts for replacement and upgrade device purchases
- Insurance cover for identity theft and/or loss of digital assets
- Access to buy and send Keevo Gift packages (e.g., bundled Keevo HW Wallet and Keevo Carbon Keys with pre-loaded crypto and Keevo Service registrations)
- Access to and ability to participate in Keevo-to-Keevo loans and interest-bearing HODL savings accounts
- Discounted or free exchange services for crypto currency trading
- Additional digital asset solution beyond crypto currencies -- e.g., photo storage, tickets, government issued IDs, digital records management, etc.
- Other services
- ...

MF/MSA Core Concept

Keevo's Multi-Factor / Multi-Signature Authentication system is based on Shamir's secret sharing algorithm (which is essentially an application of the Lagrange polynomial). But, Keevo's MF/MSA then introduces a second tier or multiple additional tiers of factors as/when needed.

The core concept in MF/MSA is to require k out of n MF/MSA to authenticate and validate a transaction. Given a Master Key (note as Key_0, master key can be considered as a seed phrase or private key of all cryptocurrencies), we divide this Key_0 into multiple factors: F_1, F_2, ... , F_n. Each factor is unique and independent. A factor could be any type or category of keys.

For example, a Factor (F_n) could be any of the following …:

- F_1 a Device like the HW Wallet Keevo Device
- F_2 a second type of Device like the Keevo Carbon Key
- F_3 a type of biometric data like a fingerprint (series of vectors, images, …)
- F_4 another type of biometric data like an optical scan or facial image
- F_5 a defined user's (e.g., the Keevo Wallet owner) password or PIN (e.g., a 6 or more alpha-numeric string) as inputted by the defined user
- F_6 another defined user's (e.g., the Keevo Wallet owner's named custodian) password or PIN (e.g., a 6 or more alpha-numeric string) as inputted by the defined user

- F_7 a defined GPS lat-long ring-fenced set of coordinates which much be read and entered by a given device (e.g., the 10 meters within the defined center of the user's home or specific location as captured by the user's Keevo HW Wallet Device upon initialization).
- F_n any number of other types of defined factors

That said, having any one factor alone, e.g., F_1 or the HW Wallet Keevo Device as in the example above, cannot reveal or decrypt the data from any other factor. Any k of these factors will be able to reveal the master key Key_0. More specifically and in the initial Keevo use case, we will employ the following 4 Factors:

- F_1: Keevo device, it serves as one factor itself
- F_2: User's PIN, custodian's PIN (encrypted and stored in carbon key)
- F_3: User's fingerprint, custodian's fingerprint (encrypted and stored in carbon key)
- F_4: Carbon Key, carbon key is served as an independent factor

In our initial MF/MSA implementation, any 3 out of 4 of these Factors (from F_1 to F_4 will be required to decrypt the Master Key_0 and sign a transaction.

Note: we are only using 3 out of 4 factors and keys in our first implementation. Over time, this MF/MSA approach can and will introduce any number of new factors,(e.g, another type of carbon key detachable/connected device or another type of biometric information or another type of user, etc). And, we might also introduce new factorial rules (e.g., 6 out of n). And while these type of k out of n MF/MSA Factor rules are controlled by Keevo at the outset, we might enable our community of developers using our platform to define their own k out of n MF/MSA factors and rules.

In addition, we could introduce factors that include a second layer of key sharing encryption. For example, F_5K_1, F_5K_2, F_5K_3 where 2 out of 3 key sharing is required for a single F_5. While not the only use case and benefit from this type of key factor organization, it would be decentralized while still having hierarchical approval rights (for example within a large enterprise or multi-level/multi-locational organization). For example, an enterprise could define the CEO as F_5 where she or he alone can authenticate and executed a transaction, but where each SVP who reports to the CEO can also have an F_5 key factor (e.g., F_5K_i for SVP 1 ,F_5K_{ii} for SVP 2, and so one) and where at least n number of SVPs are required to sign and be authenticated in order to decrypt and retrieve the F_5 key and sign a transaction. .

In our Keevo initial use case and by way of a practical example, below are several examples of when/how an owner of a Keevo HW Wallet and subscriber to the Keevo service could use Keevo to need to sign and execute transactions:

- If a user wants to send Bitcoin which they own with their Private Key stored on Keevo, they would just need to use their Keevo HW Wallet Device, enter their PIN, and fingerprint. These 3 out of 4 factors (k out of n) would be enough to decrypt the Master

Key_0 so they can sign the transaction. Said another way, the user would not need the 4th Factor, the Carbon Key, to decrypt the Master Key.

- If a user loses their Keevo HW Wallet and wants to restore their Master Key on a new Device, the Keevo service would send the user a new "blank" HW Wallet Device along with the user's Carbon Key which the Keevo service has in its secure storage vault. The user would then connect their own personal Keevo Carbon Key to the new Keevo HW Wallet Device and enter their PIN and fingerprint. Again, these 3 out of 4 factors (k out of n) would be enough to decrypt the Master Key_0 so they can sign the transaction. In this case, the transaction would be to create a new F_1 for the new HW Wallet Keevo Device. Said another way, with the Carbon key and their other two factors, the user could restore a new HW Wallet Keevo Device.
- If a user forgets their Keevo HW Wallet PIN, they can request the Keevo service to send them their Keevo Carbon Key which the Keevo service has in its secure storage vault. The user could then connect their own personal Keevo Carbon Key to their Keevoe HW Wallet Device and scan their fingerprint. Again, these 3 out of 4 factors (k out of n) would be enough to decrypt the Master Key_0 so they can sign the transaction. In this case, the transaction would be to create a new PIN or F_2 for the HW Wallet Keevo Device and Keevo Carbon Key. Said another way, with the user's Keevo HW Wallet Device, the Keevo Carbon key and the user's fingerprint (any 3 out of 4 factors), the user can restore and re-set the 4th Factor, their PIN.
- If someone steals a user's HW Wallet Keevo Device (F_1), the thief could still not sign any transaction as they would not have either the user's PIN, biometric or Keevo Carbon Key.
- If the Keevo Service tried to recreate the user's Master Key_0 by somehow using the Keevo Carbon Key that we have in our vault storage, we couldn't because we wouldn't have 2 of the user's other Factors (the Keevo HW Wallet Device, the user's PIN or the user's biometric keys) to decrypt the signatures for those factors.
- If a user -- who has registered with the Keevo service and setup a beneficiary -- dies, the Keevo service will follow certain agreed upon procedures to document and validate the user's death (e.g., log in as the custodian using certain identification information and providing valid proof of a user's death like an apostilled original copy of the original user's death certificate) and then enable the beneficiary to access/use the HW Wallet Device and sign transactions.

- More specifically, the Keevo service would …:
  - Validate the user's death
  - Authenticate the beneficiary and their contact information.
  - Transfer and include the beneficiary's encrypted data onto the Keevo Carbon Key
  - Send the Keevo Carbon Key to the beneficiary

    - The beneficiary can then connect the Keevo Carbon Key to any Keevo HW Wallet Device to recover the Master Key_0 and reset all the factors using their two Factors -- their PIN (F_2K_2) and their biometric information (F_3K_2)
    - Upon resetting the factors, the beneficiary will then become the new owner of the Master Key. They will be able to reset the PIN (F_2K_1) and enter their biometric information as (F_3K_1).
    - The beneficiary will also be prompted to register for the Keevo Service upon which time they can also initialize and set up their own beneficiaries and utilize the Keevo Service to securely store and retrieve their Keevo Carbon Key.
- These are just a few example use cases. There could be many others. The below sections will lay out other user flows and key use cases in more detail.

Keevo Device Setup and Initialization

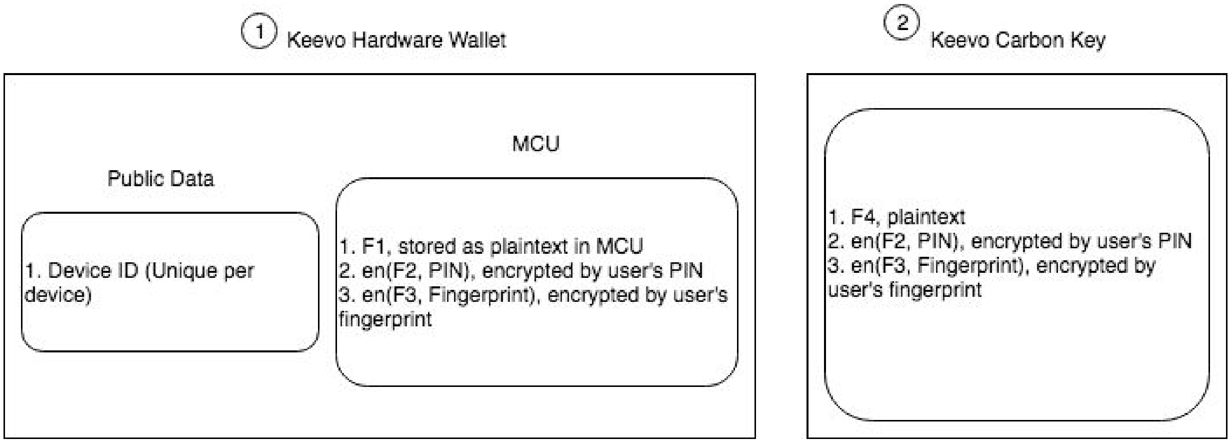
When receiving the Keevo HW Wallet Device and Keevo Carbon Key for the first time, users will be guided through a setup and registration process. At this time, users will initialize both HW Devices and setup their other Factors and beneficiaries. This section will describe the user flows and functionality provided during this initialization process.

Initialization flow for users who purchase the Hardware only

This is the initialization flow and underlying operations for users who only buy the Keevo HW Wallet Device and decide not to opt in to and register for the Keevo Service. In this case, certain factors are not created and certain keys are not encrypted (e.g., Carbon Keys).

1. The user Connects their Keevo HW Wallet Device to their laptop or another power source
2. The secure MCU in the the Keevo HW Wallet Device will generate a random number. This will be the Master Key_0
3. Once the Master Key_0 is generated, the secure MCU in the Keevo HW Wallet Device will also generate four additional factors: F_1, F_2, F_3 and F_4. As in the example above, these Factors will be for the Keevo HW Wallet Device Factor (F_1), the user's PIN Factor (F_2), the user's Fingerprint Factor(F_3), and the Keevo Carbon Key Factor (F_4).
4. Users will then be guided through a UI and process to input their PIN and fingerprint.
5. The user's PIN will be used to encrypt F_2, so we will have $encrypt\ (F_2, PIN)$
6. The user's Fingerprint data will be used to unlock an enclave which stores an encrypted F_3 , so we will have $encrypt\ (F_3, Fingerprint)$
7. The Keevo UI will then present the user the benefits and cost of the Keevo service and will offer the user the opportunity to register for the Keevo service

8. If the user opts NOT to register for the Keevo Service, the UI will continue to guide the user through the process to set up, encrypt and save their information on the Keevo Carbon Key. The first step in this UX will be to connect the Keevo Carbon Key to their Keevo HW Wallet Device. The UX will then inform the user of the following steps 8 & 9 and will also let the user know when the process is complete and they can disconnect the Keevo Carbon Key from the Keevo HW Wallet Device.
9. All of this encrypted user information along with the Keevo Carbon Key Factor (F_4) will be stored securely on the Keevo Carbon Key.


1 Keevo Hardware Wallet
Public Data
1. Device ID (Unique per device)
MCU
1. F1, stored as plaintext in MCU
2. en(F2, PIN), encrypted by user's PIN
3. en(F3, Fingerprint), encrypted by user's fingerprint
2 Keevo Carbon Key
1. F4, plaintext
2. en(F2, PIN), encrypted by user's PIN
3. en(F3, Fingerprint), encrypted by user's fingerprint

Initialization flow for users who purchase the Keevo Hardware Wallet AND register for the Keevo Service

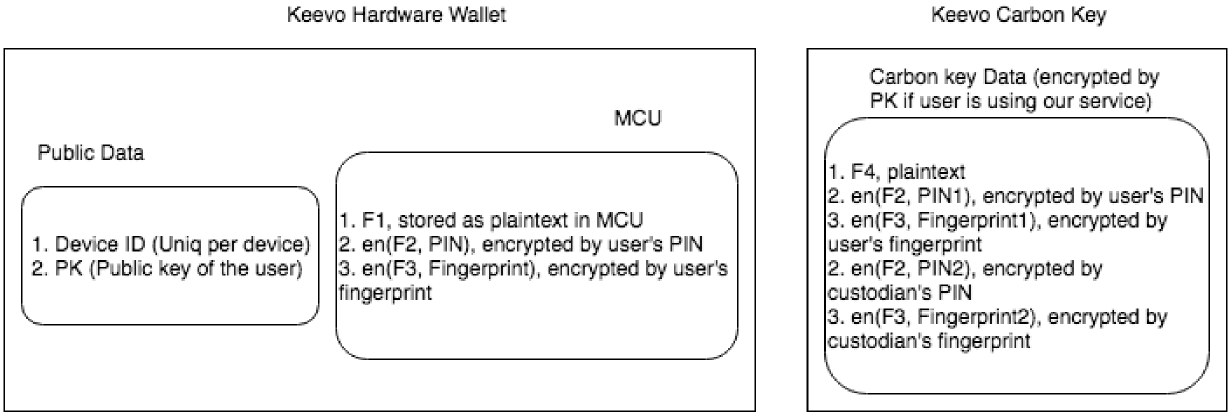
This is the initialization flow and underlying operations for users who buy the Keevo HW Wallet Device and then also opt-in and register for the Keevo Service. In this case, certain additional UI/UX flows are followed which create other factors and keys which are encrypted (e.g., custodian beneficiaries).

1. The user Connects their Keevo HW Wallet Device to their laptop or another power source
2. The secure MCU in the Keevo HW Wallet Device will generate a random number. This will be the Master Key_0
3. Once the Master Key_0 is generated, the secure MCU in the Keevo HW Wallet Device will also generate four additional factors: F_1, F_2, F_3 and F_4. As in the example above, these Factors will be for the Keevo HW Wallet Device Factor (F_1), the user's PIN Factor (F_2), the user's Fingerprint Factor(F_3), and the Keevo Carbon Key Factor (F_4).
4. Users will then be guided through a UI and process to input their PIN and fingerprint.
5. The user's PIN will be used to encrypt F_2, so we will have $encrypt\ (F_2, PIN)$

6. The user's Fingerprint data will be used to unlock an enclave which stores an encrypted F_3 , so we will have $encrypt\ (F_3, Fingerprint)$
7. The Keevo UI will then present the user the benefits and cost of the Keevo service and will offer the user the opportunity to register for the Keevo service.
8. If the user opts in for the Keevo Service, the UI will then guide the user through the process to register for the Keevo Service
   - User would be prompted to download the Keevo Desktop App
   - When desktop app is opened, user can see a login/signup page
   - User starts signup and Know Your Customer (KYC) process
     i. User enters email, name, address, phone number
     ii. User sets password for his/her account
     iii. User enters three security questions
     iv. Keevo will verify the email and phone by sending email and message
     v. User account is created
     vi. (Optional) Keevo ask user to enter/upload other KYC items, e.g. Social security number or driver's license/passport etc.
     vii. User enters credit card information for his/her account
     viii. User reviews his/her information and confirms subscription with the Keevo service
     ix. Keevo service website will generate a public/private key pairs for the user
     x. Keevo service website will send back the public key to desktop app
   - The Desktop App will ask user to connect the HW Wallet Device to the laptop, this step will be skipped if it's already connected
   - Desktop App notify HW Wallet Device the user is subscribed with the service, and send the corresponding public key to the device
   - Upon receiving the public key from desktop app, the device will keep the public key in it and will use it to encrypt the carbon key data later on.
9. After the user registers for the Keevo Service, they will be guided through an offer to set up a Custodian for the Keevo Service. If a user wants to have a beneficiary, they need to provide complete KYC information, i.e. the Beneficiary's social security number, home address, picture of their passport and/or driver's license and number, etc.
10. The Beneficiary will be asked to sign up for an account in Keevo as well. But their account type will be as a Beneficiary and is under the user's account. The signup flow for Beneficiaries will be the same as for the user except they do not need to setup payment information.
11. Once a Beneficiary's account is setup, the Desktop App will guide the custodian to enter PIN2 and fingerprint2. When the Beneficiary enters this information, the Keevo HW Wallet will generate $encrypt(F_2, PIN2)$ and $encrypt(F_3, Fingerprint2)$ accordingly
12. Once the user completes the Beneficiary UX, all of this encrypted user information along with the Keevo Carbon Key Factor (F_4) will be stored securely on the Keevo Carbon Key. More specifically the encrypted factors that will be stored on the Keevo Carbon Key include the following:

   - $encrypt(F_2, PIN)$
   - $encrypt(F_3, Fingerprint)$
   - $encrypt(F_2, PIN2)$
   - $encrypt(F_3, Fingerprint2)$

   The data will be encrypted by the user's public key (note as $PubKey$) and then stored on the Keevo Carbon Key.
13. The Keevo Desktop App notifies the user the backup process is done
14. The Keevo Desktop App will then guide the user through a process to create and print out a shipping label to add to their self-addressed envelope. The UI will then guide the user to disconnect their Keevo Carbon Key, secure it safely in the Keevo self-addressed return envelope and affix the shipping label so the user can send their Keevo Carbon Key to the Keevo cold vault storage service.


Keevo Hardware Wallet
Public Data
MCU
Keevo Carbon Key
Carbon key Data (encrypted by PK if user is using our service)

1. Device ID (Uniq per device)
2. PK (Public key of the user)

1. F1, stored as plaintext in MCU
2. en(F2, PIN), encrypted by user's PIN
3. en(F3, Fingerprint), encrypted by user's fingerprint

1. F4, plaintext
2. en(F2, PIN1), encrypted by user's PIN
3. en(F3, Fingerprint1), encrypted by user's fingerprint
2. en(F2, PIN2), encrypted by custodian's PIN
3. en(F3, Fingerprint2), encrypted by custodian's fingerprint

Comparison of Hardware only and Keevo HW Device + Service

	Hardware only	HW + Service
Restore from losing PIN	Yes	Yes
Restore from losing Fingerprint	Yes	Yes
Restore from losing device	Yes	Yes
Secure Carbon Key	Yes	Yes
Beneficiary Service	No	Yes

Signing Transactions

1. The user Connects their Keevo HW Wallet Device to their laptop or another power source

2. The user inputs their PIN (F_2) in the Keevo HW Wallet Device. For example, the user's F_2 is 123Abc, the Keevo HW Wallet will $decrypt(encrypt(F_2, PIN), 123Abc)$, if $123Abc$ is the same as the PIN, then the Keevo HW Wallet can decrypt and retrieve F_2
3. The user inputs their fingerprint (F_3) in the Keevo HW Wallet Device. For example, the user's F_3 is y, the Keevo HW Wallet will $decrypt(encrypt(F_2, PIN), y)$, if y is the same as the $Fingerprint$, then the Keevo HW Wallet can decrypt and retrieve
4. Since F_1 is securely stored in the Secure MCU of the Keevo HW Wallet Device which the user is using to enter their other keys, we will have the 3 of 4 Factors required to validate and authenticate a signed transaction. With F_1, F_2, and F_3 and using Shamir's algorithm and our MF/MSA rules, the Keevo HW Wallet Secure MCU can create the Master Key_0 and use it to sign transaction. All of this process and the last step of securely signing the transaction with the Master Key_0 will take place in the secure MCU.

Keevo Hardware Wallet Device Restoration

A user may need to restore and/or reset one of the keys which they initially set up with the Device. This could happen for one of many reasons. For example, ... :

- A user could lose their Keevo HW Wallet Device or fear that it was stolen
- A user could forget their PIN
- A user could unfortunately lose a limb and not have access to their thumb or finger which they used to create their biometric information.

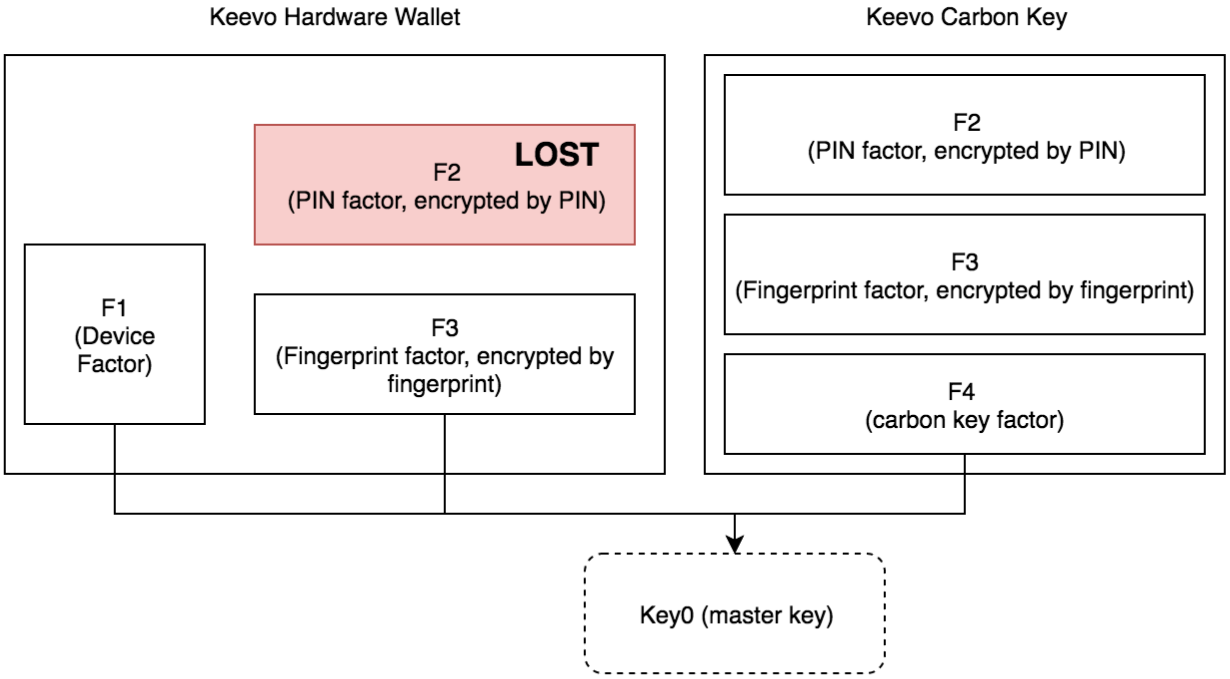
Even in any of these cases, a user can still decrypt and retrieve their Master Key_0 and restore a new device or reset any of these Factors

- If a user is missing any one of three of the required factors (F_1, F_2, or F_3), they can still use F_4, their encrypted Keevo Carbon Key with the other two Factors to restore the Master Key_0.
    - In this case where they are missing only 1 of the 3 factors (F_1, F_2, or F_3), they can use their Keevo Carbon Key whether they keep it themselves or use the Keevo Service to Store it in the Keevo Secure Vault Storage
    - Of course, if they do not opt in for the Keevo Service and they also lose their Keevo Carbon Key (i.e., F_4), then they will not be able to restore their Device and there is nothing which Keevo can do to help them.
    - On the other hand, if they register and pay for the Keevo Service, Keevo will be responsible for securely storing and providing user's access to their Keevo Carbon KeyF_4
- There are two scenarios for restoration in the case where a user loses two of their factors (for example ,they lose both their finger and forget their PIN or they lose their HW Wallet and forget their PIN).

- If a user has opted NOT to register and pay for the Keevo service or has registered for the service but did not Initialize a Beneficiary, there is no way to restore their Keevo HW Wallet Device. This is not a service we can provide securely.
- If a user has registered for the service and set up a Beneficiary, they can restore their Keevo HW Wallet Device. In this case, the Keevo service will go through a process to validate and send the user their Keevo Carbon Key and will enable the user to then use their Beneficiary's PIN and Biometric (e.g., F_2K_2 and/or F_3K_2 to re-store their Keevo HW Wallet Device.

Restoration with Hardware only Purchase (i.e., No Keevo Service)

If a user did not register for the Keevo service, they are essentially on their own. Specifically, the user will be responsible for securely and safely storing and retrieving their Keevo Carbon Key. But as per above and with their Keevo Carbon Key, they can still restore their Master Key_0 if they have misplaced or are missing one of their PIN, Fingerprint or HW Wallet Device. If a user loses two or more Factors, and even with their Keevo Carbon Key there is nothing that Keevo can do to help them restore their Master Key_0. Below are the mechanics for restoration given the various scenarios for missing/lost Factors for the Hardware only user. Forgotten PIN (F_2)


Keevo Hardware Wallet
Keevo Carbon Key
LOST
F2
(PIN factor, encrypted by PIN)
F1
(Device
Factor)
F3
(Fingerprint factor, encrypted by
fingerprint)
F2
(PIN factor, encrypted by PIN)
F3
(Fingerprint factor, encrypted by fingerprint)
F4
(carbon key factor)
Key0 (master key)

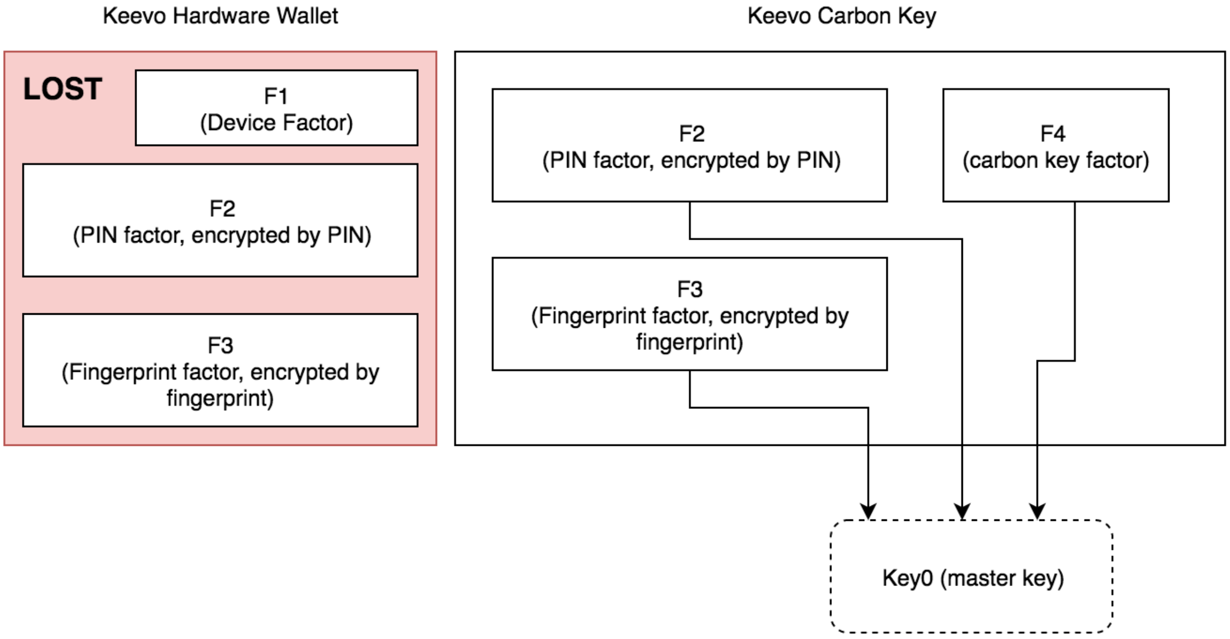
1. The user connects their Keevo HW Wallet Device to their laptop or another power source.
2. The user retrieves and connects their Keevo Carbon Key to the Keevo HW Wallet Device.
3. The user chooses the “Restore from Carbon Key” option in the Keevo HW Wallet Device UI and selects the “Forgot PIN” option in the UI.

4. The Keevo HW Wallet Device will then communicate with Keevo Carbon Key schema and know user didn't sign up with our service. The Keevo HW Wallet Device will then use the encrypted data stored in Keevo Carbon Key (F_4) directly.
5. The user will be prompted to input their Fingerprint
6. With 3 of 4 Factors -- F_1 (HW Wallet Device), F_3 (user Fingerprint) and F_4 (Carbon key), the HW Wallet can retrieve the Master Key_0
7. After the Master Key_0 is restored, the Device will wipe out all of the initial Keys for each Factor (i.e. F_1, F_2, F_3, and F_4)
8. The user will then be guided through another initialization flow again to re-set all of the keys for each Factor. They will also be reminded of the benefits of the Keevo Service prompted to upgrade and register for it.

Missing Fingerprint (F_3)

If for some reason, the user is no longer able to enter their fingerprint, the restoration process is very similar to the scenario where the user forgets their PIN. In this case, in step 3, the user selects "New Fingerprint" and in step 5, the user will be prompted to enter their PIN.

Lost Device (F_1)

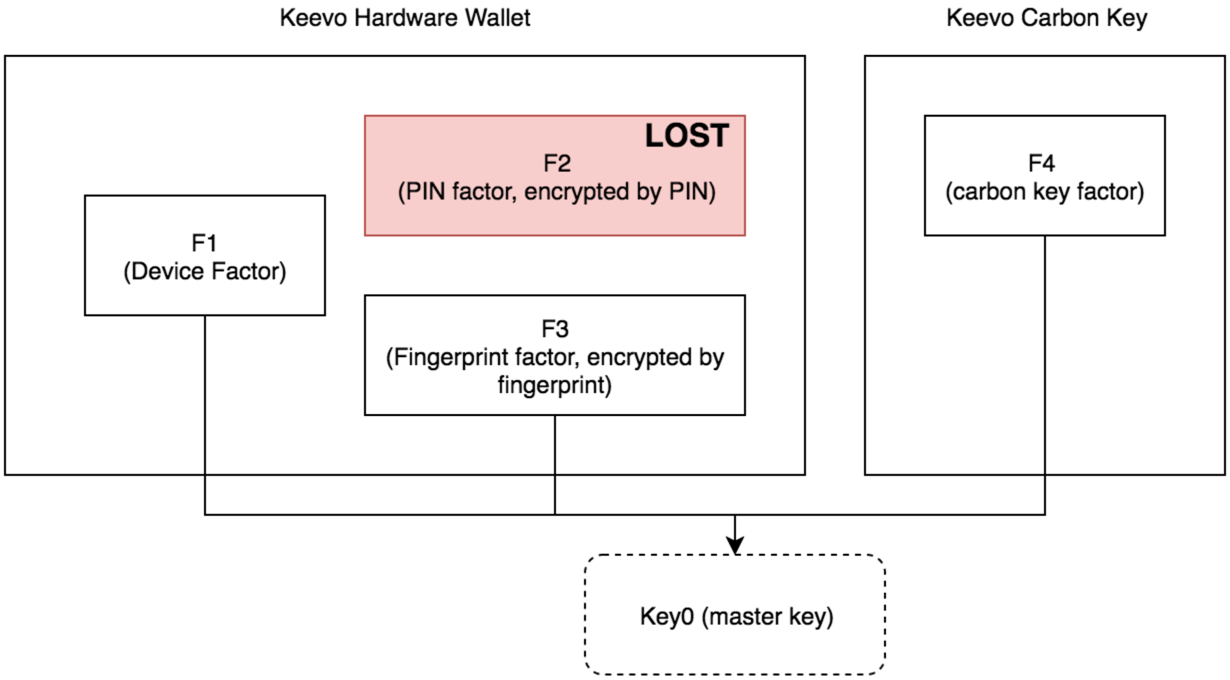

Keevo Hardware Wallet
Keevo Carbon Key
LOST
F1
(Device Factor)
F2
(PIN factor, encrypted by PIN)
F3
(Fingerprint factor, encrypted by fingerprint)
F2
(PIN factor, encrypted by PIN)
F4
(carbon key factor)
F3
(Fingerprint factor, encrypted by fingerprint)
Key0 (master key)

1. If a user loses their Keevo HW Wallet Device, they need to buy a new device.
2. After the user receives new Keevo HW Wallet Device, they will connect it to their laptop.
3. The user chooses the "Restore from Carbon Key" option in the Keevo HW Wallet Device UI and selects the "Restore new Keevo HW Wallet" option in the UI.
4. The Keevo HW Wallet Device will check if the Keevo Carbon Key is connected. If not, the user will be prompted to connect their Keevo Carbon Key.

5. The Keevo HW Wallet Device will then communicate with Keevo Carbon Key schema and know user didn't sign up with our service. The Keevo HW Wallet Device will then use the encrypted data stored in Keevo Carbon Key (F_4) directly.
6. The UI will prompt the user to input their PIN and Fingerprint into the new Keevo HW Wallet Device
7. With 3 of 4 Factors -- F_2 (user PIN), F_3 (user Fingerprint) and F_4 (Carbon key), the new HW Wallet can retrieve the Master Key_0
8. After the Master Key_0 is restored, the Device will wipe out all of the initial Keys for each Factor (i.e. F_1, F_2, F_3, and F_4)
9. The user will then be guided through another initialization flow again to reset all of the keys for each Factor. They will also be reminded of the benefits of the Keevo Service prompted to upgrade and register for it.

Restoration with Hardware Purchase and Service Registration

Forgotten PIN (F_2)



1. In this case and since the Keevo Service is storing the user's Keevo Carbon Key, the user would begin the restoration process online. They would go to their Keevo Web App and sign in their keevo account
    - User enters their email, password
    - User chooses restore HW Wallet -> forgot PIN

    - User will be prompted a 2nd factor authentication, they can choose either email or SMS
    - (Optional) If there’s more KYC items for the user, a customer representative will call the user and confirm their identity
    - Keevo will do risk analysis based on all the information keevo has to verify if that user is the actual person who registered for the service. Risk analysis includes: IP address, when is the account created, when the device was initialized, etc.
    - Keevo Desktop App will show the user information based on the risk analysis. E.g. show success in the page if risk is very low.

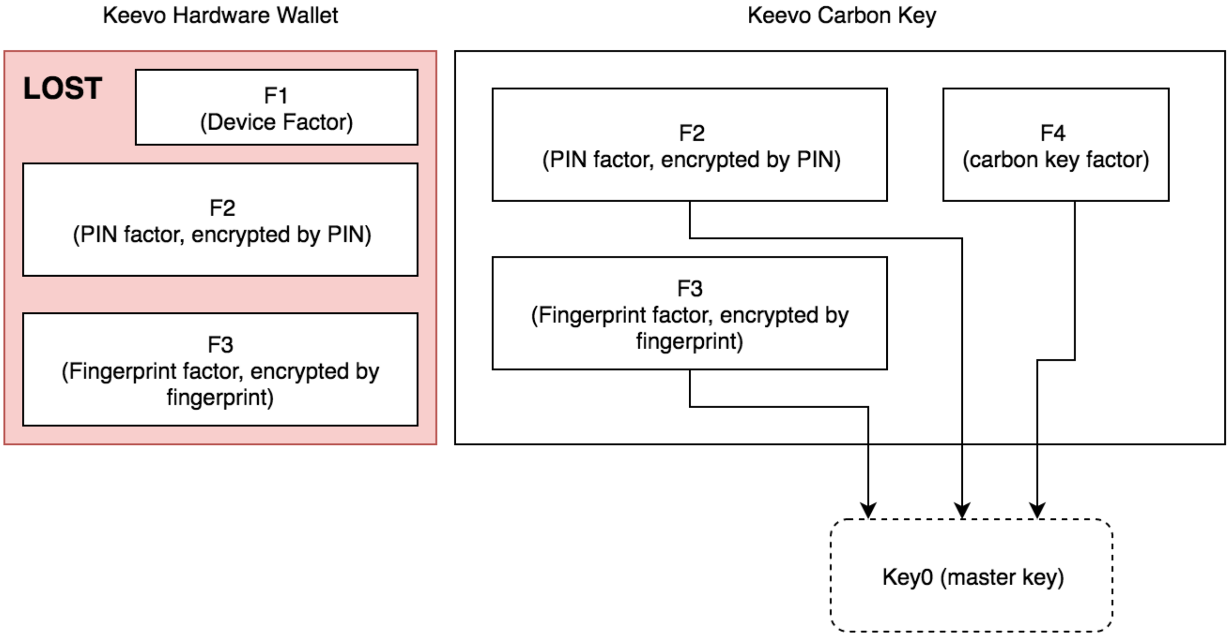
2. Once the user’s identity and account sign in are confirmed and before sending the User their Keevo Carbon Key, the Keevo Service will create a strong, one-time passcode (Key_{one}) and send it to the user’s recovery email or other contact info.
3. The Keevo Service will then locate the user’s Keevo HW Wallet Device ID (securely stored) and find the corresponding public and private key pairings ($PubKey$ and $PrivateKey$ pair). By using $PrivateKey$ to decrypt the carbon key, the Keevo Service can then retrieve the Carbon Key Factor (F_4)
4. Keevo would then encrypt the Carbon Key Factor (F_4) with the one-time strong passcode Key_{one} and send the Keevo Carbon Key to the user
5. Upon receiving their Keevo Carbon Key, the user will connect the Carbon key to their Keevo HW Wallet Device and begin the restoration process.
    - The user would choose the “Restore from Carbon Key” option in the Keevo HW Wallet Device UI and select the “Forgot PIN” option in the UI.
    - The HW Wallet Device would then check the Carbon Key schema and know that the user has signed up with the Keevo Service
    - The user will then be prompted to input the one time passcode Key_{one} that was sent to their recovery email
    - Upon validation of the one time passcode Key_{one}, the Keevo HW Device can decrypt the data on the Carbon Key and retrieve the Carbon Key factor (F_4).
    - After receiving the carbon key, the user can recover the Master Key_0 with these 3 factors -- F_1 (the Keevo HW Wallet Device), F_3 (User Fingerprint) and F_4 (The Keevo Carbon Key)
    - After the Master Key_0 is restored, the Keevo HW Wallet Device can sign the transaction to erase all of the Factors (F_1, F_2, F_3, F_4) and begin a reinitialization processes whereby the user will be prompted to enter their new PIN and re-enter their fingerprint information
    - *[Research item, not necessary in MVP, we could try if it’s possible to not do a full reinitialization and just recover the F_2 and ask user to input a new PIN, so everything in the back up is not voided. However it’s debatable if this is a secure behavior, but it does simplify the process especially user do not need to set up custodianship again]*

6. User will then be prompted to send back to the newly re-encrypted Keevo Carbon Key with their new Factor information to the Keevo Service.

Missing Fingerprint (F_3)

If for some reason, the user is no longer able to enter their fingerprint, the restoration process is very similar to the scenario where the user forgets their PIN. In this case, in step 8 above, the user can recover the Master Key_0 with these 3 factors -- F_1 (the Keevo HW Wallet Device), F_2 (User Passcode) and F_4 (The Keevo Carbon Key)

Lost Keevo HW Wallet Device (F_1)


Keevo Hardware Wallet
LOST
F1
(Device Factor)
F2
(PIN factor, encrypted by PIN)
F3
(Fingerprint factor, encrypted by fingerprint)
Keevo Carbon Key
F2
(PIN factor, encrypted by PIN)
F4
(carbon key factor)
F3
(Fingerprint factor, encrypted by fingerprint)
Key0 (master key)

1. In this case and since the Keevo Service is storing the user's Keevo Carbon Key, the user would begin the restoration process online. They would go to their Keevo Desktop App and sign in keevo account.
   - User enters their email, password
   - User chooses restore HW Wallet -> lost device
   - User will be prompted with a 2nd factor authentication, they can choose either email or SMS
   - User chooses payment, they can use the credit card which subscribes the service or use some other form of payment (e.g., paypal, BitPay, …).
   - User will verify their shipping address and confirm that they want to buy a replacement device.
   - (Optional) If there's more KYC items for the user, a customer representative will call the user and confirm their identity
   - Keevo will do risk analysis based on all the information Keevo has to verify that the user is the actual person who registered for the service. Risk analysis

    - includes: IP address, when is the account created, when the device was initialized, etc.
    - The Keevo Desktop App will show the user information based on the risk analysis. E.g. show success in the page if risk is very low.
2. Once the user's identity and account sign in are confirmed and before sending the User their Keevo Carbon Key, the Keevo Service will create a strong, one-time passcode (Key_{one}) and send it to the user's recovery email or other contact info.
3. The Keevo Service will then locate the user's Keevo HW Wallet Device ID (securely stored) and find the corresponding public and private key pairings ($PubKey$ and $PrivateKey$ pair). By using $PrivateKey$ to decrypt the Keevo Carbon Key, the Keevo Service can then retrieve the Carbon Key Factor (F_4)
4. Keevo would then encrypt the Carbon Key Factor (F_4) with the one-time strong passcode Key_{one} and send the Keevo Carbon Key along with a new Keevo HW Wallet Device to the user
5. Upon receiving their Keevo Carbon Key and new Keevo HW Wallet Device, the user will connect the Carbon key to their Keevo HW Wallet Device and begin the restoration process.
    - The user would choose the "Restore from Carbon Key" option in the Keevo HW Wallet Device UI and select the "New HW Wallet Device" option in the UI.
    - The HW Wallet Device would then check the Carbon Key schema and know that the user has signed up with the Keevo Service
    - The user will then be prompted to input the one time passcode Key_{one} that was sent to their recovery email
    - Upon validation of the one time passcode Key_{one}, the Keevo HW Device can decrypt the data on the Carbon Key and retrieve the Carbon Key factor (F_4).
    - The user will then be prompted to input their fingerprint (F_3) and their Pin (F_2). with these 3 factors -- F_2 (the user PIN), F_3 (User Fingerprint) and F_4 (The Keevo Carbon Key), they will have the 3 Factors required to retrieve the Master Key_0
    - After the Master Key_0 is restored, the Keevo HW Wallet Device can sign the transaction to erase all of the Factors (F_1 , F_2 , F_3 , F_4) and begin a reinitialization processes whereby the user will be prompted to enter their new PIN and re-enter their fingerprint information
6. The user will then be prompted to send back to the newly re-encrypted Keevo Carbon Key with their new Factor information to the Keevo Service.

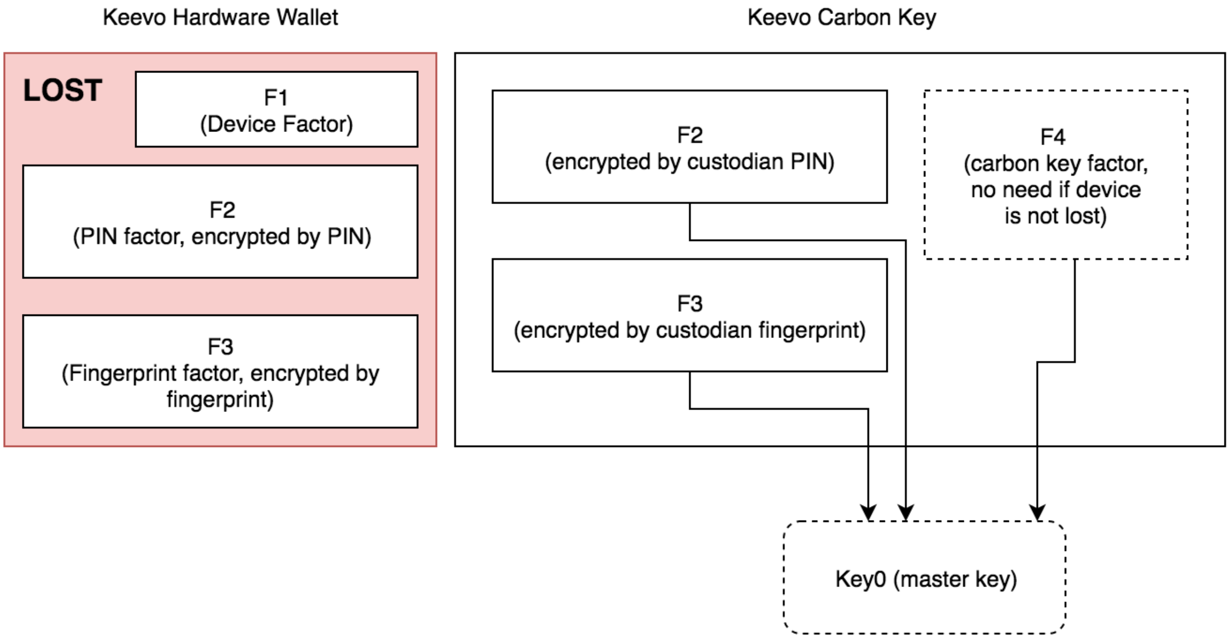
Comparison with Keevo Hardware Wallet Device Purchase Only

The Keevo Carbon Key is the most important element in the Keevo whole security system. When registering for and using the Keevo Service, the user does not need to worry about the security of their Keevo Carbon Key; it is secured (both in physical storage and with the Carbon Key Factor (F_4). When needed, the user will be provided their Carbon Key securely. We will also encrypt and only provide the selective information required on the Carbon Key (e.g., encrypted PIN or Fingerprint) so as to send only the minimum information required (and incomplete) in the Carbon Key when transporting it from the Keevo Service to the user. This will increase the security and make each "link in the chain" more safe from potential hacking and theft.

If the user does not opt in and register/pay for the Keevo Service, the information on the Carbon Key will not be encrypted or include minimal information. In addition, the user will be responsible for storing and keeping it safe and secure for retrieval at a future point.

Beneficiary Service

If the user opts in and registers for the Keevo Service, they will also be able to take advantage of the Beneficiary Services which come along with the membership. More specifically if the user dies, they will be able to set up a process and procedure managed by the Keevo Service to i) validate their death, ii) authenticate the beneficiary which they have designated, iii) send their Keevo Carbon Key to the designated beneficiary, and iv) enable their beneficiary to use their multi factor / multi sig authentication signatures to retrieve the Master Key_0 and restore/reset the Keevo HW Wallet Device and all of the Factors. In addition, the Beneficiary Service along with Keevo's MF/MSA system could also be leveraged by the registered user themselves in the case where they forget their passcode, lose their Keevo HW Wallet Device and are unable to use their fingerprint.


Keevo Hardware Wallet
LOST
F1 (Device Factor)
F2 (PIN factor, encrypted by PIN)
F3 (Fingerprint factor, encrypted by fingerprint)
Keevo Carbon Key
F2 (encrypted by custodian PIN)
F4 (carbon key factor, no need if device is not lost)
F3 (encrypted by custodian fingerprint)
Key0 (master key)

1. In the case of a user’s death and since the Keevo Service is storing the user’s Keevo Carbon Key, the user’s designated beneficiary would begin the custodian transfer and restoration process online.
2. The Beneficiary would go to their Keevo Desktop App and sign in with their Beneficiary credentials they registered when sign up.
   - Beneficiary enter their email, password
   - Beneficiary choose restore HW Wallet -> custodianship
   - Beneficiary will be prompted a 2nd factor authentication, they can choose either email or SMS
   - The beneficiary will also be asked if they need a new device and allow them to setup payment and shipping address for the new device
3. Before sending the beneficiary the user’s Keevo Carbon Key, The Keevo Service would also guide the beneficiary through a process to validate that the user had indeed died. This process will be a combination of online and offline information collection, review and verification including, but not limited to, receipt and verification of a valid, apostilled original copy of a user’s death certificate and other information to be defined by the Keevo Beneficiary Service process.
4. Once the user’s death has been verified, the Keevo Service will create a strong, one-time passcode (Key_{one}) and send it to the beneficiary’s recovery email or other contact information.
5. The Keevo Service will then locate the user’s Keevo HW Wallet Device ID (securely stored) and find the corresponding public and private key pairings ($PubKey$ and $PrivateKey$ pair). By using $PrivateKey$ to decrypt the Keevo Carbon Key, the Keevo Service can then retrieve the Carbon Key Factor (F_4)
6. Keevo would then encrypt the Carbon Key Factor (F_4) with the one-time strong passcode Key_{one} and send the Keevo Carbon Key to the Beneficiary.
7. Upon receiving the Keevo Carbon Key, the beneficiary will connect the Carbon key to the user’s Keevo HW Wallet Device and begin the transfer and restoration process.
   - The Beneficiary would choose the “Restore from Carbon Key” option in the Keevo HW Wallet Device UI and select the “Beneficiary Transfer” option in the UI.
   - The HW Wallet Device would then check the Carbon Key schema and know that the user has signed up with the Keevo Service
   - The Beneficiary will then be prompted to input the one time passcode Key_{one} that was sent to their email or other contact information
   - Upon validation of the one time passcode Key_{one}, the Keevo HW Device can will decrypt the carbon key and retrieve the Carbon Key Factor F_4, $encrypt(F_2, PIN)$ and $encrypt(F_3, Fingerprint)$
   - Upon receiving the HW wallet and the Keevo Carbon Key, the Beneficiary will then be prompted to input their their PIN (F_2K_2) and their fingerprint (F_3K_3). With these 3 factors - the beneficiary *PIN* (F_2K_2), the Beneficiary

    $fingerprint\ (F_{3}K_{3})$ and the Carbon Key factor (F_{4}), the Keevo HW Wallet Device and the Beneficiary will have the 3 Factors required to retrieve the Master Key_{0}

    - After the Master Key_{0} is restored, the Keevo HW Wallet Device can sign the transaction to erase all of the Factors (F_{1}, F_{2}, F_{3},F_{4}) and begin a reinitialization processes whereby the beneficiary will be prompted to enter a new PIN and fingerprint information. They will also be prompted to opt in to the Keevo Service and if they opt in and register for the service, they will be able to designate and initialize their own beneficiaries.

8. The new user will then be prompted to send back to the re-encrypted Keevo Carbon Key with their new Factor information to the Keevo Service.

Summary Use Cases and Factors Used for Restoration

Each row represents the use case for lost or unavailable factor information. For example, the first row is the scenario where the HW Device is lost or stolen. The required Factors which a user or beneficiary can use to retrieve the Master Key_{0} and restore the Factors is included in the relevant cells. In our initial model and Service, we will required 3 out of four factors (e.g., F_{1}, F_{2}, F_{3} or F_{4}) to be validated in order to retrieve the Master Key_{0}

The tables below provide a checklist for how users -- with and without having registered for the Keevo Service -- would be able to securely recover their Master Key_{0} and then re-set their factors (e.g., PIN, fingerprint, ...) using 3 out of the initial 4 factors in our first implementation of the MF/MSA system. It also provides a checklist for how Beneficiaries would be able to do the same upon the valid confirmation of certain events (e.g., the death of a user).

Hardware Purchase Only:

	User's Keevo Hardware Wallet	User's PIN	User's Fingerprint	Beneficiary's PIN	Beneficiary's Fingerprint	Keevo Carbon Key
Lost Keevo Hardware Wallet	NA	F2, K1	F3, K1	NA	NA	F4, K1
Forgotten User PIN	F1, K1	NA	F3, K1	NA	NA	F4, K1
Missing User Fingerprint	F1, K1	F2, K1	NA	NA	NA	F4, K1
Beneficiary transfer upon user death	NA	NA	NA	NA	NA	NA
Beneficiary	NA	NA	NA	NA	NA	NA

authentication upon catastrophic loss						

Hardware Purchase + Keevo Service:

	User's Keevo Hardware Wallet	User's PIN	User's Fingerprint	Beneficiary's PIN	Beneficiary's Fingerprint	Keevo Carbon Key
Lost Keevo Hardware Wallet	NA	F2, K1	F3, K1	NA	NA	F4, K1
Forgotten User PIN	F1, K1	NA	F3, K1	NA	NA	F4, K1
Missing User Fingerprint	F1, K1	F2, K1	NA	NA	NA	F4, K1
Beneficiary transfer upon user death	NA	NA	NA	F2, K2	F3, K2	F4, K1
Beneficiary authentication upon catastrophic loss	NA	NA	NA	F2, K2	F3, K2	F4, K1

FAQs

What if a Keevo Carbon Key is lost During Transportation to/from a User who Registered for the Keevo Service?

If the user has registered for the Keevo Service and the Keevo Carbon Key is lost or stolen during transfer to/from Keevo, as long as the user still has the Keevo HW Wallet Device, they can ask for a new Keevo Carbon Key to be created and encrypted with a new strong Passcode. Once they receive this new Keevo Carbon Key and the new strong Passcode, they can restore their Factors as per the above processes.

All of the data on the original (lost or stolen) Keevo Carbon Key will be invalidated and useless. Also, the Keevo Carbon Key is encrypted either by the Keevo HW Wallet Device's public key or by the one-time strong passcode.   Both of these will be a very strong encryption.   It should be computationally infeasible to crack this in a reasonable amount of time.   So, even if the Keevo

Carbon Key falls into the possession of a person with bad intentions, they cannot get the data from it.

Can Keevo Hack into a Registered User's Account by Virtue of Keevo storing the User's Carbon Key?

Keevo cannot hack into a user's account because the only Factor which Keevo can decrypt is the Carbon Key Factor (F_4). Even if Keevo were to brute force attack or try to social engineering drill into a users PIN to decrypt and retrieve F_2, they would still only have 2 factors. It would not be possible for Keevo to decrypt any of the other factors including the HW Wallet Device or the User Fingerprint. This is also true for the Beneciary Factors. In any situation, Keevo could not recreate and decrypt 3 out of 4 factors required to retrieve a user's Master Key_0.

Can a Beneficiary Restore a Keevo HW Wallet Device before a User Dies?

This is not possible. Even if the Registered User asks Keevo to send them their Carbon Key and the Beneficiary somehow gains access to both the user's Keevo HW Wallet Device and their Carbon Key, they cannot use their secondary Factors to restore the Master Key_0. The information on the Carbon Key is encrypted by the strong passcode (long random number D14) and Keevo's public key. So without Keevo having validated the user's death and setup and encrypted the user's Carbon Key with the Beneficiary's secondary Factors, the Beneficiary cannot decrypt the Carbon Key.

Can a Keevo HW Wallet or Carbon Key be Intercepted during Transport such that a User Receives a Hacked Device?

The Keevo Service will use a secure transportation service which will be require a user's signatures and other means of security to maintain the integrity of the chain of custody while transporting devices. However, there is no way to ensure complete integrity of a device from being hacked once it is in the possession of a user.

That said and in the case where a Keevo Device may become tampered with, the Keevo solution has designed in other alerts, tripwires and mitigation and remediation approaches. For instance, Keevo will plan to enable the Keevo Desktop app to detect any compromises to the Firmware and alert Keevo and the User. We may also be able to have the Firmware and/or other user Factors such as the Fingerprint check for and detect tampering with the Desktop App.

When/how do I renew and what happens if I decide not to renew for the Keevo Service?

The Keevo Service plan is set up as an “evergreen” service which will auto-renew on the anniversary each year. In the case where a registered member of the Keevo Service decides to cancel their service, they may do so with at least 30 days advance notice of their renewal date. [terms and conditions to be checked with local and national regulatory requirements for annual subscription services and potential break-up fees]. In the case of cancellation, Keevo will send back the user’s Carbon Key which we have in our vault storage and any other air-gapped data backup of the user’s encrypted information.

Below are the mechanics for return of the Keevo Carbon Key and the user’s reset of their account as a Hardware only account upon cancellation of the Keevo Service Plan.

1. Before returning the User’s Keevo Carbon Key to them, the Keevo Service will create a strong, one-time passcode (Key_{one}) and send it to the user’s primary email or other contact info held on file
2. The Keevo Service will then locate the user’s Keevo HW Wallet Device ID (securely stored) and find the corresponding public and private key pairings ($PubKey$ and $PrivateKey$ pair). By using $PrivateKey$ to decrypt the carbon key, the Keevo Service can then retrieve the Carbon Key Factor (F_4)
3. Keevo would then encrypt the Carbon Key Factor (F_4) with the one-time strong passcode Key_{one} and send the Keevo Carbon Key to the user
4. Upon receiving their Keevo Carbon Key, the user will follow the instructions to connect the Carbon key to their Keevo HW Wallet Device and begin the re-set process.
    - The user would choose the “Unregister Keevo Service” option in the Keevo HW Wallet Device UI and select the “Full Factory Reset” option in the UI.
    - The HW Wallet would then check the Carbon Key schema and know that the user has cancelled their Keevo Service and opted to re-set their Keys.
    - The user will then be prompted to input the one time strong passcode Key_{one} that was sent to their primary email
    - Upon validation of the one time passcode Key_{one}, the Keevo HW Device can decrypt the data on the Carbon Key and retrieve the Carbon Key factor (F_4).
    - The user will then be prompted to input their fingerprint (F_3) and PIN and with these 4 factors -- F_1 (the Keevo HW Wallet Device), F_2 (User PIN), F_3 (User Fingerprint) and F_4 (The Keevo Carbon Key), they will have the Factors required to retrieve the Master Key_0

- After the Master Key_0 is restored, the Keevo HW Wallet Device can sign the transaction to erase all of the Factors (F_1, F_2, F_3, F_4) and begin a reinitialization processes whereby the user will be prompted to enter their new PIN and re-enter their fingerprint information
- The Keevo UI will then present the user the benefits and cost of the Keevo service and will offer the user the opportunity to re-register for the Keevo service.
- If the user opts NOT to register for the Keevo Service, the UI will continue to guide the user through the process to set up, encrypt and save their information on the Keevo Carbon Key. The first step in this UX will be to connect the Keevo Carbon Key to their Keevo HW Wallet Device. The UX will then inform the user of the key steps and inform the user when the process is complete and they can disconnect the Keevo Carbon Key from the Keevo HW Wallet Device.
- All of this encrypted user information along with the Keevo Carbon Key Factor (F_4) will be stored securely on the Keevo Carbon Key.