Updated May 2020

Operational Security Guide

unchained capital

General Security Principles

Unchained Recommendations for 2-of-3 multisig

- Client holds two keys; Unchained holds one key
- Unchained recommends that clients hold two hardware wallets and back-up recovery seeds for each hardware wallets (four total secrets to protect).

Multisignature security background

- With single key wallets, both hardware devices (e.g. Trezors, Ledgers, etc.) and back-up recovery seeds represent single points of failure; hardware devices and recovery seeds back each other up but if either is compromised, an attacker has a clear path to stealing funds.
- With multisig, the risk associated with any single hardware device or recovery seed is materially reduced; if a single secret is compromised, funds are not only not at risk, but an attacker would not be in possession of any information related to a multisig address which a single secret helps protect. For example, if a single Trezor is stolen and accessed, the attacker would have no way of knowing addresses or balances associated with a multisig address. This is a principal benefit of multisig security over single sig.
- Separately, in a 2-of-3 multisig setup, the combination of i) two hardware devices or ii) one hardware device and the recovery seed of the other hardware device would remain insufficient to compromise funds without additional information related to a multisig address. In order to compromise funds, the attacker would either need the third key or the redeem script associated with the multisig address. Essentially, possession of either one key or a combination of two keys, without access to other information, would not put funds immediately at risk because an attacker would not have the information required to know which address those keys protect; in this scenario, it is important to understand that security would be materially reduced as an attacker would be one secret away from being able to spend funds but additional information would be required.

Why two hardware devices AND two recovery seeds

- A single hardware device and a recovery seed associated with the hardware device back up each other. If either is lost due to non-malicious reasons, the other can be used to recover funds. Non-malicous attacks would include a client traveling with a Trezor and unintentionally losing the device; or it would include storing a Trezor in a safe deposit box with a bank and a client losing access to the safe deposit box (assuming that the bank is simply preventing access rather than maliciously attempting to compromise the device). In either scenario, the non-compromised secret can still be used to provide 1-of-3 signatures. Both would have to be compromised or be inaccessible contemporaneously in order for 1-of-3 keys to be rendered completely incapable of recovering funds, in which case the 2-of-3 multisig setup would effectively revert to a 2-of-2 with one key lost entirely.

- Separately, if either a hardware device or its recovery seed is singularly compromised for malicious reasons, the attacker is not in possession of sufficient information to compromise funds. In fact, the attacker would still need access to multiple independent secrets in order to steal funds.

- It is important to note that the risks associated with a hardware device and a backup recovery seed are not the same; if a hardware device is compromised, it should be protected by a PIN and if so, the seed would still need to be extracted from the device. While a PIN provides additional security and hardware devices are designed specifically to prevent extraction of a seed, it should be assumed that if a hardware device is stolen, a well motivated attacker will eventually gain access to the device or ultimately be able to extract the seed even if protected by a PIN. However, if a full recovery seed is stored unencrypted and it is compromised, a malicious actor could restore the seed to any hardware device very easily without the need for any additional information. Separately, an unencrypted recovery seed could be compromised without the owner ever knowing it; an attacker could compromise a security location, copy the unencrypted recovery seed and leave the original recovery seed without the owner ever knowing that the location and seed had been compromised. In this regard, a malicious compromise of a hardware device presents less risk than a malicious compromise of an unencrypted recovery seed.

- However, technology cuts both ways. An unencrypted recovery seed is significantly less susceptible to non-malicious attack vectors. Technology fails all the time. A hardware device could fail due to bitrot (think a hard-drive failing to load or a smart phone dying permanently). Separately, if exposed to water, a hardware device may be rendered entirely inoperable or an unsuspecting user could unintentionally download corrupted software. In any of these cases, a hardware device could fail where an analog storage mechanism would not.

- Relying on both, hardware and analog storage mechanisms, creates redundancy and diversification against various attack vectors. Security is about balancing risks. Multisig provides

redundancy in keys, specifically securing against risk created by a loss of any individual secret, whether malicious or non-malicious and having backups to each key reinforce the security of the quorum as a whole.

- With two hardware devices and a backup recovery seed for each hardware device, three secrets could be compromised or rendered inaccessible with funds remaining both recoverable and secure. In such a case when working with Unchained, a client could use its single uncompromised and accessible device (or recovery seed) and collaborate with Unchained to transfer funds to a secure address within a new quorum of secure keys.

- Practically, once any single secret is believed to be compromised, it is best practice to rotate and replace the key (and create a new backup recovery seed), but redundancy combined with multisig security ensures that multiple secrets could be contemporaneously compromised while ultimately being able to securely recover funds.

- This is Unchained's ultimate goal: ensuring that a client's funds are secure and recoverable even when multiple standard paths fail unexpectedly and contemporaneously.

Key Storage: Individual User

Client Controlled

Quorum Structure

2-of-3

Client Keys

2

Requirements

2 Client Hardware Wallets

2 Client Recovery Seeds

4 Client Secure Locations

Secure Locations

Primary home safe

Secondary home safe
e.g. mountain house, lake house, beach house, etc

Safe deposit box - bank A

Safe deposit box - bank B

Safe or safe deposit box
held by trusted family member or friend (F&F)

Security Principles

- Hold backup recovery seeds for each key/hardware wallet pair
- Avoid co-locating any combination of hardware wallets or backup recovery seed while in storage (2 HW + 2 recovery seeds = 4 unique locations).
- Multiple safe deposit boxes within the same bank may be used, however this is not ideal; if holding a combination of hardware wallets and recovery seeds with the same bank, avoid holding two recovery seeds with the same bank and make sure to use different safe deposit boxes and secure hardware wallet with a strong pin (e.g. 6 characters).
- Trusted family members or friends: if relying on a trusted family member or friend, the person should be aware of the nature of what he or she is asked to secure to prevent unintentional security breaches; this family member or friend should be someone that would also be trusted to hold a partial share of a recovery seed in a single key wallet backup recovery plan.
- Ideally one recovery seed would be held in a different geographic location (different city or state), whether it be held by a trusted family/friend or in a bank safe deposit box.

	Key 1 (Primary)	Key 2 (Secondary)
Secure Location 1	Hardware Wallet 1	
Secure Location 2		Hardware Wallet 2
Secure Location 3	Recovery Seed 1	
Secure Location 4		Recovery Seed 2

Individual - Example Scenario A

Individual that owns or runs a business and has a close friend or family that is highly trusted.

- Individual would store two hardware wallets (signing devices) in separate locations, one in a home safe and one at a second secure location, such as an office (if the business is owned by the individual and has a dedicated safe) or a safe deposit box.
- A backup recovery seed for one hardware wallet would be stored in a safe deposit box
- A backup recovery seed for a second hardware wallet would be stored in a safe held by a close and trusted family member (such as parent or sibling).

	Key 1 (Primary)	Key 2 (Secondary)
Home Safe	Hardware Wallet 1	
Office Safe		Hardware Wallet 2
Safe Deposit Box - Bank A	Recovery Seed 1	
Trusted F&F Safe		Recovery Seed 2

Individual - Example Scenario B

Individual that does not own or run a business but has a close friend or family that is highly trusted.

- Individual would store two hardware wallets (signing devices) in separate locations, one in a home safe and one at a second secure location, such as a safe deposit or a safe in a second home.
- A backup recovery seed for one hardware wallet would be stored in a safe deposit box.
- A backup recovery seed for a second hardware wallet would be stored in a safe held by a close and trusted family member (such as parent or sibling).

	Key 1 (Primary)	Key 2 (Secondary)
Home Safe	Hardware Wallet 1	
Safe Deposit Box - Bank A		Hardware Wallet 2
Safe Deposit Box - Bank B	Recovery Seed 1	
Trusted F&F Safe		Recovery Seed 2

Individual - Example Scenario C

Individual that does not own or run a business and does not have a close friend or family that is highly trusted

- Individual would store two hardware wallets (signing devices) in separate locations, one in a home safe and one at a second secure location, such as a safe deposit or a safe in a second home.
- A backup recovery seed for one hardware wallet would be stored in a safe deposit box.
- A backup recovery seed for a second hardware wallet would be stored in a separate safe deposit box, ideally in a separate bank.

	Key 1 (Primary)	Key 2 (Secondary)
Home Safe	Hardware Wallet 1	
Safe Deposit Box - Bank A		Hardware Wallet 2
Safe Deposit Box - Bank B	Recovery Seed 1	
Safe Deposit Box - Bank A or C		Recovery Seed 2

Key Storage: Business User

Client Controlled (Multi-Person Organization)

Quorum Structure
2-of-3

Client Keys
2

Requirements
2 Client Hardware Wallets
2 Client Recovery Seeds
4 Client Secure Locations

Secure Locations
Office Safe A
Office Safe B
Safe Deposit Box - Bank A
Safe Deposit Box - Bank B
Home Safe - Principal Owner

Security Principles

- Hold backup recovery seeds for each key/hardware wallet pair
- Avoid co-locating any combination of hardware wallets or backup recovery seeds while in storage (2 HW + 2 recovery seeds = 4 unique locations).
- Multiple safe deposit boxes within the same bank may be used, however this is not ideal; if holding a combination of hardware wallets and recovery seeds with the same bank, avoid holding two recovery seeds with the same bank and make sure to use different safe deposit boxes and secure hardware wallets with a strong pin (e.g. 6 characters).
- Ideally one recovery seed would be held in a different geographic location (different city or state), preferably in a bank safe deposit box.

Key Holders

Principal owner, Partner, CEO, COO, CIO, CFO, Controller, Assistant controller, General counsel

	Key 1 (Primary)	Key 2 (Secondary)
Secure Location 1	Hardware Wallet 1	
Secure Location 2		Hardware Wallet 2
Secure Location 3	Recovery Seed 1	
Secure Location 4		Recovery Seed 2

Business (Client-Controlled) - Example Scenario A

Family office or investment fund run by a principal with multiple employees that help manage assets; assumes office is physically secure (key access) with secure locations within office.

- One hardware wallet (signing device) held in a safe at the corporate location with a second hardware wallet (signing device) held in the same office but in a separate safe with a unique combination.
- A backup recovery seed for one hardware wallet would be stored in a safe deposit box.
- A backup recovery seed for a second hardware wallet would be stored in a separate safe deposit box, preferably in a separate bank.
- *Internal threat:* different individuals should have access to unique safes and access rights should have redundancy; multiple employees would have to collude and account protections would provide an additional layer of security to prevent theft or loss. Ideally, non-principal owners should not have dual access to both keys / signing capability and the ability to author transactions.
- *External threat:* even if multiple secure locations are compromised, an external attacker would not have access to account level controls necessary to transfer funds; in a 2-of-3 multisig, possession of a single key or a combination of two keys would remain insufficient to spend without also having a redeem script.

	Key 1 (Primary)	**Key 2 (Secondary)**
Office Safe A	Hardware Wallet 1 Access: Individual A & B	
Office Safe B		Hardware Wallet 2 Access: Individual B & C
Safe Deposit Box - Bank A	Recovery Seed 1 Access: Individual A & B	
Safe Deposit Box - Bank B		Recovery Seed 2 Access: Individual B & C

Individual A	**Individual B**
Family principal or CIO	CFO
Individual C	**Individual D**
Investment team member	Controller

Business (Client-Controlled) - Example Scenario B

Operating business with multiple employees that help manage assets/treasury, assumes office(s) is physically secure (key access) with secure locations within office. Also assumes business has outside investors, limited partners or shareholders.

- One hardware wallet (signing device) held in a safe at the corporate location with a second hardware wallet (signing device) held in either the same office (but in a separate safe with a unique combination) or a separate office location.
- A backup recovery seed for one hardware wallet would be stored in a safe deposit box.
- A backup recovery seed for a second hardware wallet would be stored in a separate safe deposit box, preferably in a separate bank.
- *Internal threat:* different individuals should have access to unique safes and access rights should have redundancy; multiple employees would have to collude and account protections would provide an additional layer of security to prevent theft or loss. Ideally, non-principal owners should not have dual access to both keys / signing capability and the ability to author transactions.
- *External threat:* even if multiple secure locations are compromised, an external attacker would not have access to account level controls necessary to transfer funds; in a 2-of-3 multisig, possession of a single key or a combination of two keys would remain insufficient to spend without also having a redeem script.

	Key 1 (Primary)	Key 2 (Secondary)
Office Safe A	Hardware Wallet 1 Access: Individual A & B	
Office Safe B		Hardware Wallet 2 Access: Individual B & C
Safe Deposit Box - Bank A	Recovery Seed 1 Access: Individual A & B	
Safe Deposit Box - Bank B		Recovery Seed 2 Access: Individual B & C

Individual A	**Individual B**
CFO	Controller
Individual C	**Individual D**
COO or CEO	Assistant controller or senior treasury management/accounting professional

Key Storage: Business User

Multi-Institution (Multi-Person Organization)

Quorum Structure
2-of-3

Client Keys
1

Requirements
1 Client Hardware Wallets
1 Client Recovery Seeds
2 Client Secure Locations

Secure Locations
Office Safe A
Office Safe B
Safe Deposit Box - Bank A
Safe Deposit Box - Bank B
Home Safe - Principal Owner

Security Principles

- Hold backup recovery seed for key/hardware wallet pair
- Avoid co-locating hardware wallets and backup recovery seed while in storage (1 HW + 1 recovery seeds = 2 unique locations).
- Multiple safe deposit boxes within the same bank may be used, however this is not ideal; if holding a combination of hardware wallets and recovery seeds with the same bank, make sure to use different safe deposit boxes and secure hardware wallet with a strong pin (e.g. 6 characters).

Key Holders

Principal owner, Partner, CEO, COO, CIO, CFO, Controller, Assistant controller, General counsel

	Key 1 (Primary)	Key 2 (Secondary)
Secure Location 1	Hardware Wallet 1	n/a
Secure Location 2	Recovery Seed 1	n/a
Secure Location 3	n/a	n/a
Secure Location 4	n/a	n/a

Business (Multi-Institution) - Example Scenario A

Family office or investment fund run by a principal with multiple employees that help manage assets, assumes office is physically secure (key access) with secure locations within office.

- One hardware wallet (signing device) held in a safe at the corporate location.
- A backup recovery seed for one hardware wallet would be stored in a safe deposit box.
- *Internal threat:* different individuals should have access to hardware wallet and recovery seed and access rights should have redundancy; an employee would have to collude with Unchained or Unchained's key agent and account protections would provide an additional layer of security to prevent theft or loss. Ideally, non-principal owners should not have dual access to both keys / signing capability and the ability to author/approve transactions.
- *External threat:* even if client secure locations were compromised, an external attacker would only have possession of 1-of-3 keys and would not have access to account level controls necessary to transfer funds; in a 2-of-3 multisig, possession of a single key or a combination of two keys would remain insufficient to spend without also having a redeem script.

	Key 1 (Primary)	**Key 2 (Secondary)**
Office Safe A	Hardware Wallet 1 Access: Individual A & B	n/a
Office Safe B	n/a	n/a
Safe Deposit Box - Bank A	Recovery Seed 1 Access: Individual C & D	
Safe Deposit Box - Bank B	n/a	n/a

Individual A	**Individual B**
Family principal or CIO	CFO
Individual C	**Individual D**
Family principal or CIO	Controller

Business (Multi-Institution) - Example Scenario B

Operating business with multiple employees that help manage assets/treasury, assumes office(s) is physically secure (key access) with secure locations within office. Also assumes business has outside investors, limited partners or shareholders.

- One hardware wallet (signing device) held in a safe at the corporate location.
- A backup recovery seed for one hardware wallet would be stored in a safe deposit box.
- *Internal threat:* different individuals should have access to hardware wallet and recovery seed and access rights should have redundancy; an employee would have to collude with Unchained or Unchained key agent and account protections would provide an additional layer of security to prevent theft or loss. Ideally, non-principal owners should not have dual access to both keys / signing capability and the ability to author or approve transactions.
- *External threat:* even if client secure locations were compromised, an external attacker would only have possession of 1-of-3 keys and would not have access to account level controls necessary to transfer funds; in a 2-of-3 multisig, possession of a single key or a combination of two keys would remain insufficient to spend without also having a redeem script.

	Key 1 (Primary)	Key 2 (Secondary)
Office Safe A	Hardware Wallet 1 Access: Individual A & B	n/a
Office Safe B	n/a	n/a
Safe Deposit Box - Bank A	Recovery Seed 1 Access: Individual C & D	
Safe Deposit Box - Bank B	n/a	n/a

Individual A	**Individual B**
CFO	Controller
Individual C	**Individual D**
CFO or COO	Assistant controller or senior treasury management/accounting professional