Legacy Transfer White Paper

zengo

Version 1.0
August 2023

Legacy Transfer White Paper

Abstract

Zengo is preparing to launch Legacy Transfer: A self-custodial, inheritance-style feature that supports a user-initiated and chain-agnostic transfer of assets and tokens after a prolonged period of account inactivity. While completely game-changing, its capabilities are deeply rooted within Zengo's longstanding Secure Recovery feature, which has been working flawlessly since the Zengo wallet was first introduced (reaching 1 million wallets in 2023). Legacy Transfer, therefore, represents a natural evolution of this secure technology.

Legacy Transfer V1 will launch in Q3 2023 and we plan to refine and upgrade its capabilities over time by drawing on user insights, cryptographic developments, and developer input.

This paper is organized as follows:

Section 1: Legacy Transfer Background and Motivation

Private keys are the technology trusted to secure most cryptoassets like Ether (ETH), Bitcoin (BTC) and more. The widespread narrative with private key technology is "Not Your Keys, Not Your Coins," referring to the common belief that the only way to truly protect your cryptoassets is by managing your private keys yourself.

However, as millions of dollars in cryptoassets are lost to private key theft or loss[1] every day, it is becoming increasingly clear that the other side of this narrative is "Your Keys, Your Problems" and realizes that self-custody with private keys does not necessarily mean sustainable security.

Unfortunately, the traditional alternative has been a reliance on un- or under-regulated centralized custodians: To date, billions of dollars have been lost to irresponsible or fraudulent centralized custodians, those who have promised they'd handle the private key headache on behalf of their users.

To solve this dilemma and offer a reliable alternative, Zengo was established in 2018 and launched its consumer-focused Zengo wallet mobile app in 2019. By leveraging state of the art secure MPC (Multi-Party Computation) technology, Zengo is able to distribute the traditional private key generation and signing, traditionally performed by a single party, between the user device and Zengo servers. Since the key parts (secret shares) are never in the same place, the confidentiality aspect of their security (i.e., their resilience against theft) is vastly superior to classic single-point-of-failure private key wallets.

But private key wallets and their users are vulnerable not just because of their reliance on private keys as their only signing solution, but also and even more so, due to their reliance on seed phrases, a phrase that consists of 12 to 24 words, as their only recovery solution.

[1] https://www.nytimes.com/2021/01/13/business/tens-of-billions-worth-of-bitcoin-have-been-locked-by-people-who-forgot-their-key.html

If users lose their private keys, their hardware wallets, or their mobile devices, this seed phrase is the only way to restore their accounts. Just like private keys, this seed phrase must also be securely stored.

While wallets usually focus on making the private key as protected as possible, they largely leave the task of securing the seed phrase to the discretion of users. Once again, users must balance between the confidentiality of the seed phrase to protect against possible theft and its availability to protect against loss.

As a result, users are tormented with questions and doubts:

- Will a pen-and-paper solution survive the test of time?
- Where should I physically store it?
- Should I make multiple copies to avoid loss scenarios?
- How do I ensure others can access it in an emergency, but not beforehand?
- What will happen if I die? How would this seed phrase get to my heirs?

Delegating the important security question of recovery to users inevitably yields sub-optimal solutions. Many times users do not take the recovery question as seriously as they should until it is too late, and even when they do they are not equipped with the relevant tools to solve it correctly. This is especially true with respect to handling the consequences of our own mortality, which we would rather repress than handle despite its certainty.

Additionally, users handling their recovery data directly can be abused by attackers via common seed phrase phishing attack vectors, where scammers trick their victims into entering their seed phrase, giving them total access to the wallet. Therefore, we consider the seed phrase to be one of crypto's biggest vulnerabilities.

At Zengo we have taken a different approach. Instead of leaving it to our users, we offer a managed yet non-custodial Secure Recovery solution that allows users to recover their lost wallet, but without being bothered with making security decisions and manual actions.

We are now extending this recovery solution to support an even broader range of situations, including cases in which the original owner of a Zengo wallet becomes unavailable for a predefined amount of time. The solution allows users to set up (in-advance) a solution that grants their intended Legacy Recipient access to their account, making sure that funds are protected not only against device loss but also the loss of the owner: **Essentially, the industry's first secure, multi-chain, self-custodial inheritance-style solution for cryptoassets.**

Section 2: Zengo's MPC Architecture

Zengo was launched on the premise of creating a secure non-custodial crypto wallet that has no single-point-of-failure (SPOF). By leveraging Threshold Signature Scheme (TSS) cryptography, Zengo launched the first consumer MPC crypto wallet in 2019. To date, this distributed system has secured over 1 million Zengo wallets, with zero instances of hacks or account takeovers.

The SPOF of the private key is solved by distributing the private key between multiple parties as discussed in this section. The SPOF of seed phrase recovery is solved by Zengo's Secure Recovery feature, which will be described in proceeding sections.

While the exact technical details of Zengo MPC are outside of the scope of this paper (see our White Paper[2] on the matter, our open source implementation of it[3] and a general overview here), some high-level description of it is required to understand Zengo's Secure Recovery solution.

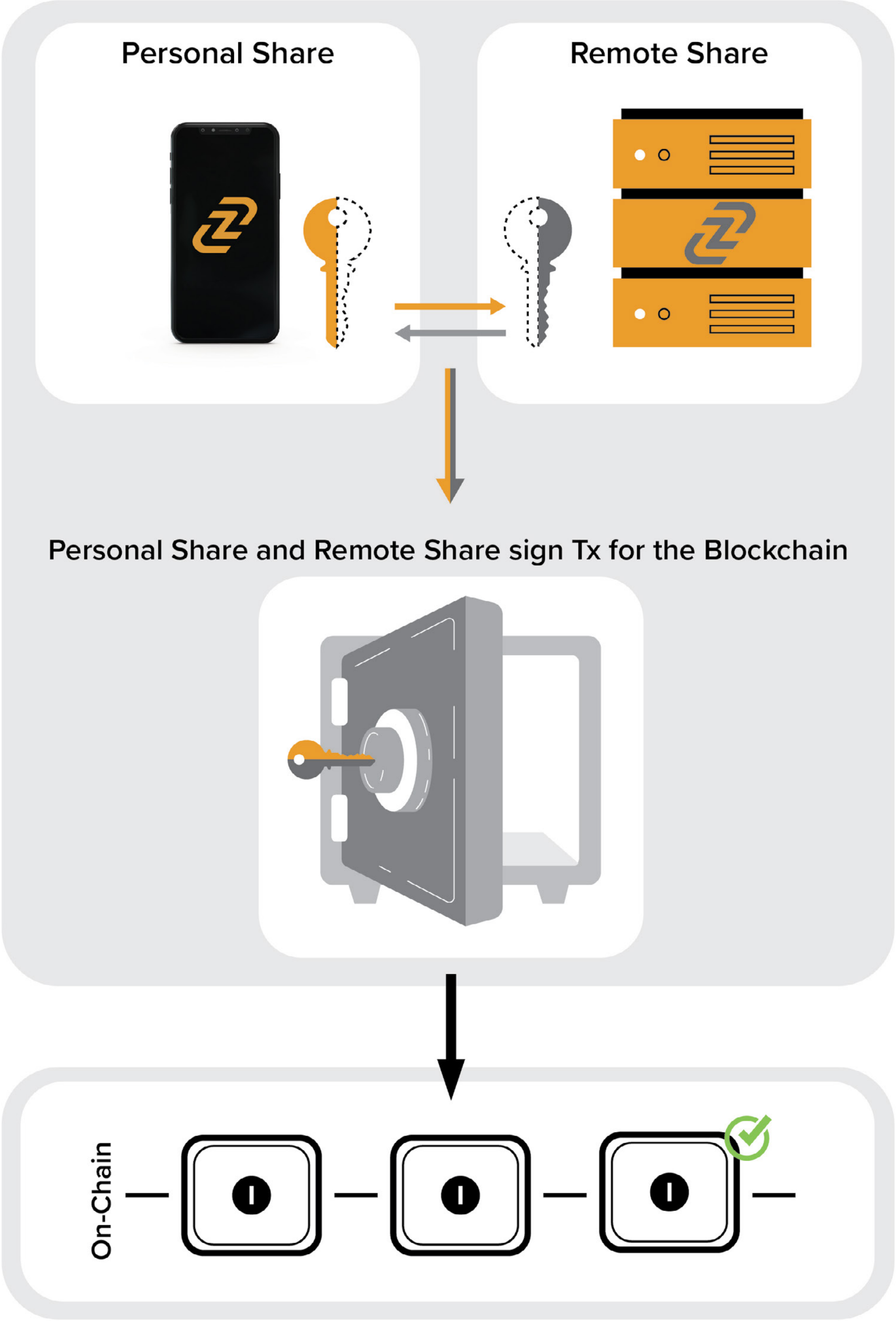
Using a 2-of-2 Multi-Party Computation (MPC) framework, each of the two Zengo parties (Zengo Server and Zengo app on the user device) independently generate their own "Secret Share" during the wallet creation process. The share generated on the user's device is called the Personal Share and is tied to the user's device hardware. The share generated on Zengo's server is called the Remote Share. Only the Personal share can initialize and sign transactions, all of which are verified by the device's hardware (Secure Enclave or Trusted Execution Environment).

Using MPC, these two "Secret Shares" are able to compute their corresponding public key and make sure the process was done in a secure manner.

[2] https://github.com/ZenGo-X/gotham-city/blob/master/white-paper/white-paper.pdf

[3] https://github.com/ZenGo-X/gotham-city/

MPC



To sign transactions and effectively spend the cryptoassets, the parties engage in a multi-staged protocol to mutually sign the transaction without revealing their shares to one another.

Section 3: Zengo's Secure Recovery

Secure Recovery: High-level description

A user's mobile device might get lost, stolen, or broken, taking the share stored on their device (the Personal Share) with them. As a result, without a proper solution users could potentially lose access to their funds. Such an outcome is obviously unacceptable and therefore the Personal Share must not exist solely on the user's device.

But where can the Personal Share be stored?

While storing a copy of the user's Personal Share on Zengo's server would keep it safe, it would break MPC's aforementioned promise of avoiding a single point of failure, as both the Remote Share and Personal Share would reside on the server.

Another option is to store the Personal Share on the user's personal cloud solution (Google Drive for Android, iCloud for iOS). The personal cloud option keeps the Personal Share out of the reach of the remote server, keeping the system properly distributed. However, personal cloud accounts are known to be successfully targeted by hackers.

To get the best of both worlds, at Zengo we combined these two alternatives into one solution that highlights their advantages and mitigates their weaknesses. This reflects Zengo's secure approach to user account recovery, as differentiated by the way a seed phrase is used to recover cryptoassets in a traditional wallet.

Here's a high-level overview of Zengo's Secure Recovery Model:

1. During Zengo wallet setup, the Zengo app encrypts a copy of the Personal Share on the user device with a key.
2. The Zengo app sends this encrypted copy of the Personal Share to the Zengo server.
3. The Zengo app Stores the decryption key on the user's personal cloud.

This process ensures the Personal Share is both secured and out of reach of the server (or any malicious actor).

When Secure Recovery is activated, the user:

1. Authenticates their identity on their device with the Zengo server.
2. App receives the encrypted Personal Share from the Zengo server.
3. App retrieves their decryption key from their personal cloud.
4. App decrypts their Personal Share on their device and their Zengo wallet returns to normal use.

We'll explain this process in more detail below.

Secure Recovery: Technical description

Secure Recovery setup

Secure Recovery relies on three elements for account setup and activation which can be considered as 3-factor authentication (3FA). This system is based on orthogonal factors for user access, control, and personhood (unique user biometrics) that is both simple (no need for any passwords) and yet more secure (extremely difficult for a user to make a mistake or hack).

Zengo's 3FA relies on: 1) an email address with magic link; 2) a Recovery File, which is the encryption/decryption key for an encrypted copy of the user's Personal Share; and 3) 3D FaceLock, a biometric liveness verification scan.

1. Email address: When a new Zengo user first installs a Zengo wallet on their device, registration begins through a "magic link" sent to their email inbox. They are free to quickly access their Zengo wallet with no need to set up Secure Recovery, after confirming their device lock is activated and integrated into their Zengo wallet (otherwise, a user is prompted to activate their device lock for the first time).

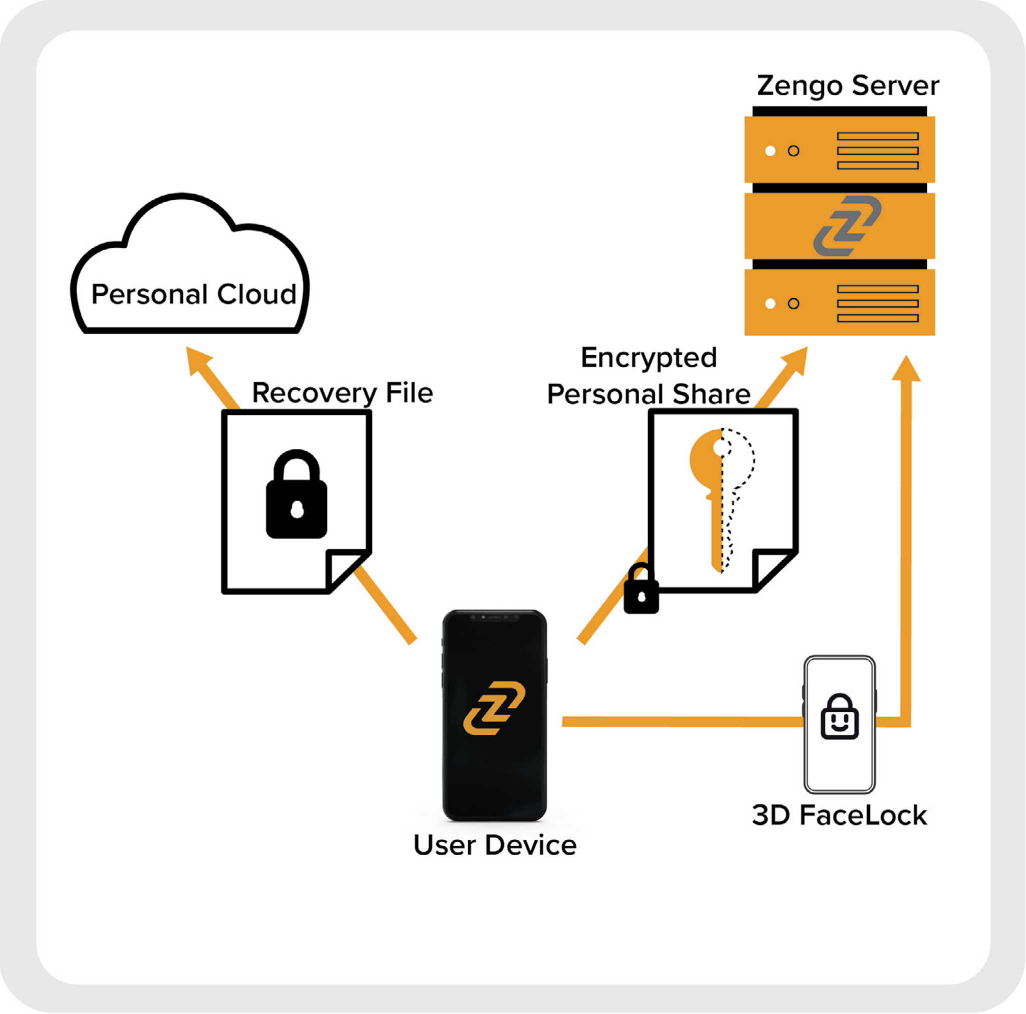
2. Recovery File: Once a user wants to purchase crypto or receive funds into their wallet, Zengo requires Secure Recovery setup before the user is able to access their crypto wallet addresses.

   The user's Zengo app creates a Recovery File on-device:

   a. Securely generates an encryption/decryption key (Recovery File) by leveraging the device cryptographic capabilities
   b. Encrypts a copy of the user's Personal Share with this key
   c. Sends this encrypted Personal Share to Zengo's server
   d. Stores the encryption/decryption key (Recovery File) on the user's personal cloud

3. 3D FaceLock: A secure liveness verification technology developed by FaceTec[4] to enable a user's verification biometrics. This server-side biometric authentication is not KYC; verification is done on Zengo's server.

Secure Recovery Setup



Secure Recovery activation

If the user's Personal Share is lost, either due to loss of the mobile device or deletion of the app, Secure Recovery can be activated:

1. To recover their account, users need to re-install the Zengo app on their device.
2. The user then authenticates by supplying their email address and clicking a "magic link" sent to

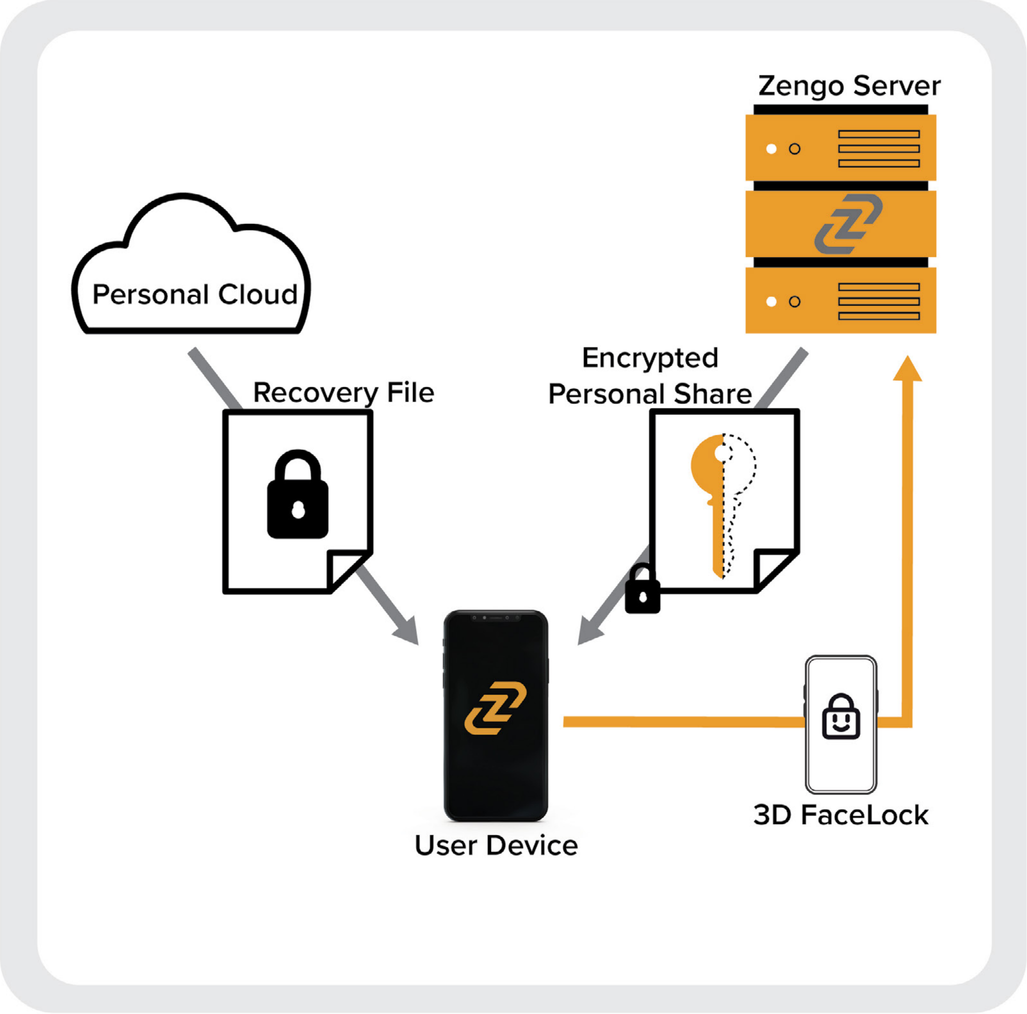
[4] Magic links are a one-time use link sent to the customer during the authentication process

their inbox, as they did when setting up the account (see above).

3. Zengo's server recognizes that the user account already exists and initiates the Secure Recovery process.
4. The user is requested to pass 3D FaceLock: The server-side biometric verification that was created during wallet setup.
5. Once verified, Zengo's server sends the encrypted Personal Share to the user's device.
6. The Zengo app on the user device retrieves the Recovery File from the user's personal cloud and uses it to decrypt the Personal share on-device.

By following this process, the Personal Share is fully recovered and the user can resume any wallet interaction.

Secure Recovery Activation



Zengo's Guaranteed Access solution

Similar to the Secure Recovery solution that protects against the loss of the user's Personal Share, Zengo also developed a reciprocal Guaranteed Access solution for the potential loss of the Remote Share stored on Zengo's servers.

When a new Zengo user first creates their account or performs Secure Recovery, they also receive an encrypted copy of their Remote Share.

A public and transparent escrow and trustee solution was established to automatically release the decryption key in the unlikely event that Zengo goes out of business. Once the Remote Share is decrypted on the user device, the user regains full control over their now-reconstituted private key and can export it to another wallet.

This is an abbreviated description of the Guaranteed Access solution and is included here for exhaustiveness purposes. For a more detailed description and a deeper analysis of the Guaranteed Access solution, please review the links above.

Security Analysis

Zengo's Secure Recovery, based on 3FA, has helped tens of thousands of Zengo users successfully and securely recover their accounts since the first version of Zengo was launched in 2019. Below we explain how this system aims for the right balance between simplicity and security.

Resilience against account takeover

Account takeover (ATO) is a form of online identity theft in which a cybercriminal illegally gains unauthorized access to an account belonging to someone else.

For attackers to take over a Zengo's user account using Secure Recovery, they'd need to obtain three separate authentication factors:

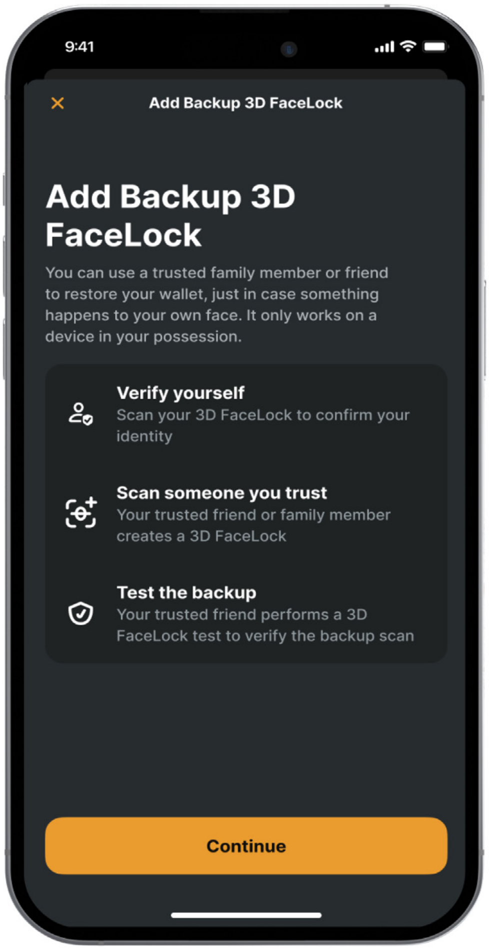
1. Email inbox access: Verified via magic link.
2. Cloud access: The Recovery File (Personal Share encryption/decryption key) key, which resides on the user's cloud.
3. 3D FaceLock: Zengo's server-side biometric liveness verification.

It should be noted that users can amplify their security even further by extending the security of their email or cloud access, through the addition of extra authentication factors. For example, users can add a hardware security key to access[5] their email account, effectively adding a hardware element to Zengo's authentication.

[5] https://support.google.com/accounts/answer/6103523?hl=en&co=GENIE.Platform%3DAndroid

Resilience against loss of access

Each of the aforementioned authentication factors can have an additional equivalent factor, to protect against possible loss of an authentication factor. Therefore, users can and are in fact actively encouraged to define a backup email address, a backup cloud provider and a backup 3D FaceLock with the liveness verification of a trusted person.



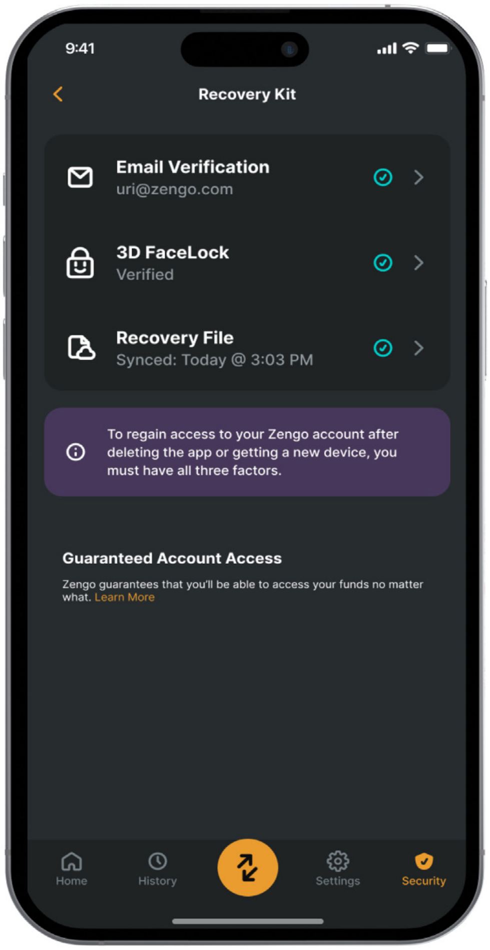
Add Backup 3D FaceLock

You can use a trusted family member or friend to restore your wallet, just in case something happens to your own face. It only works on a device in your possession.

Verify yourself
Scan your 3D FaceLock to confirm your identity

Scan someone you trust
Your trusted friend or family member creates a 3D FaceLock

Test the backup
Your trusted friend performs a 3D FaceLock test to verify the backup scan



Email Verification
uri@zengo.com

3D FaceLock
Verified

Recovery File
Synced: Today @ 3:03 PM

To regain access to your Zengo account after deleting the app or getting a new device, you must have all three factors.

Guaranteed Account Access
Zengo guarantees that you'll be able to access your funds no matter what. Learn More

Resilience against malicious servers

Even a malicious server cannot access the user's Personal Share stored and encrypted on Zengo's Server. To do so, it would need to obtain the Recovery File that is generated by the user and stored by the user on their personal cloud.

Therefore, Zengo's recovery still maintains the MPC promise of distribution of power without any SPOF.

Resilience against the loss of Zengo's Remote Share

When users perform Secure Recovery, they simultaneously receive their encrypted Remote Share, which re-enables them to be eligible for Zengo's Guaranteed Access solution, if needed.

Section 4: Zengo’s Legacy Transfer

General Introduction

Because ensuring secure (and simple) self-custody remains a centerpiece of the crypto industry, we developed Legacy Transfer to offer a multi-chain inheritance-style solution for cryptoassets.

Today, the industry has no simple and secure solution for self-custodial inheritance: When a user stops engaging with their cryptoassets, whether due to absence, injury, or death (physical or digital), their cryptoassets become inaccessible unless some complex arrangements with a seed phrase were made ahead of time.

Fortunately, Zengo’s aforementioned Secure Recovery solution can be extended to accommodate such cases.

To support such a process, Zengo’s Legacy Transfer feature enables the original wallet owner (Legacy Sender) to designate a Legacy Recipient: A close friend, family member, or estate manager. The Legacy Recipient will be able to gain access to the original wallet owner’s assets after a certain period of inactivity (as determined by the wallet owner) in a non-custodial process. No KYC is required, and the original wallet owner can adjust or disable Legacy Transfer at any time.

How it works:

Legacy Transfer enables the intended receiver (Legacy Recipient) to recover the Personal Share of the Legacy Transfer sender (Legacy Sender) in case the sender’s predefined inactivity period within the Zengo app has elapsed.

To achieve this, the following settings must be initialized in advance:

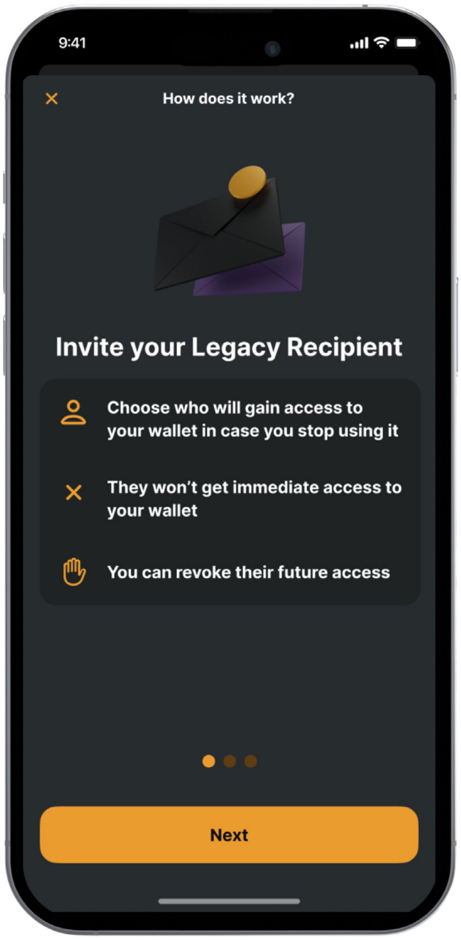
- The Legacy Recipient’s authentication details (email and 3D FaceLock) must be set up within Zengo’s system.
- The sender’s Legacy File (a variation of the above mentioned Recovery File) must be accessible

to the Legacy Recipient, in order to decrypt the sender's encrypted Personal Share.
- A mechanism must be put in place that detects when the sender has become inactive, and after a set time initializes the Legacy Transfer process to be triggered.

Legacy Transfer setup

To initiate Legacy Transfer, the Legacy Sender begins by performing an extended authentication process that includes local and 3D FaceLock verification. They then specify the Legacy Recipient's email address and the desired inactivity period. The Legacy Recipient can be an existing user of Zengo, or not yet.

The Legacy Sender defines the desired inactivity period after which the Legacy Transfer process can be activated. The inactivity mechanism requires a minimum of 90 days. Any app interaction by the Legacy Sender resets the inactivity period. Additionally, multiple in-app and email based notifications are sent to the Legacy Sender as the inactivity period threshold approaches.

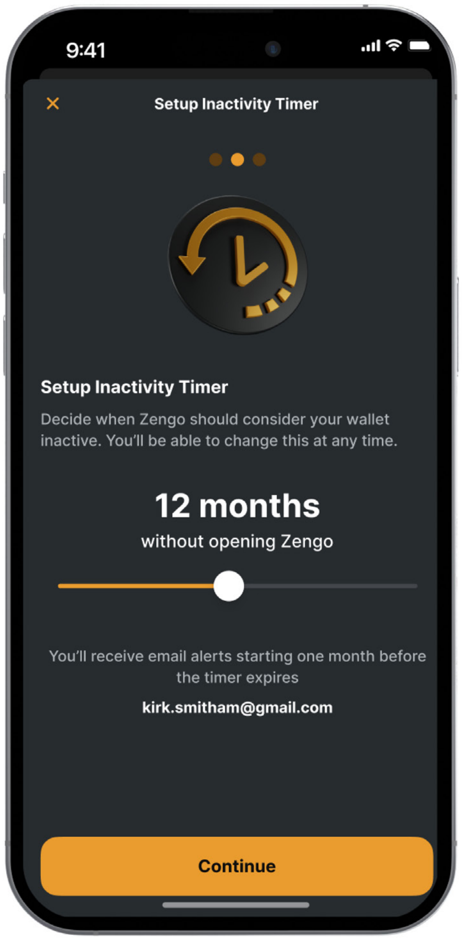


Invite your Legacy Recipient

Choose who will gain access to your wallet in case you stop using it

They won't get immediate access to your wallet

You can revoke their future access



Setup Inactivity Timer

Decide when Zengo should consider your wallet inactive. You'll be able to change this at any time.

12 months
without opening Zengo

You'll receive email alerts starting one month before the timer expires

kirk.smitham@gmail.com

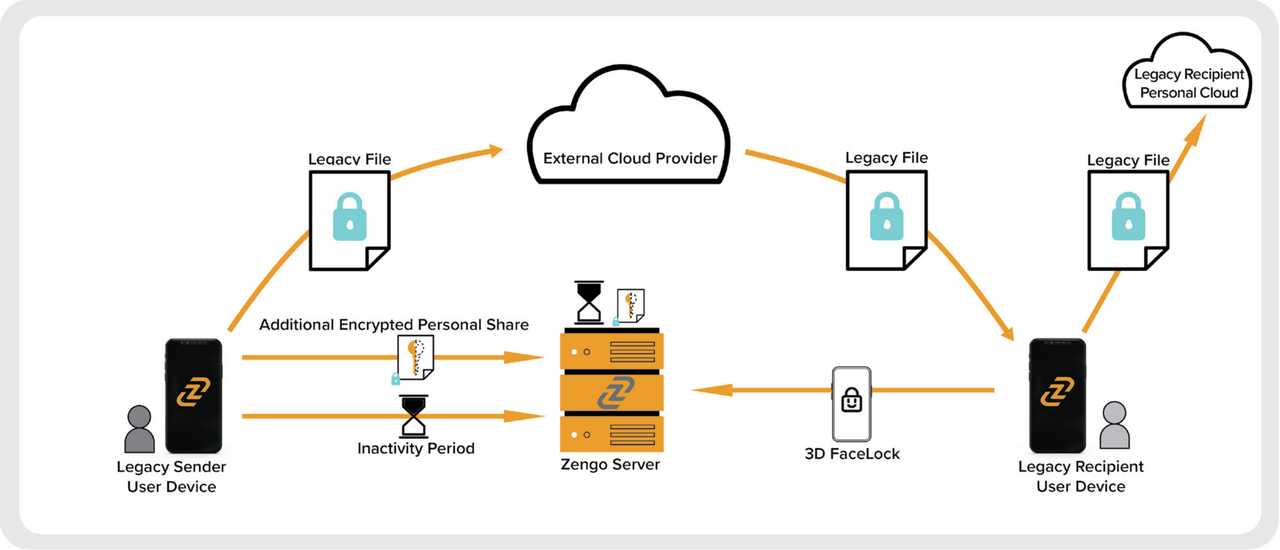
The Legacy Sender's app generates an additional encrypted Personal Share, in a variant of the process used for Secure Recovery, as described in the Secure Recovery Activation section, above.

The Legacy Sender's Zengo app creates a Legacy File on-device:

1. Securely generates an encryption/decryption key (Legacy File) by leveraging the device cryptographic capabilities
2. Encrypts this additional Legacy Sender's Personal Share with this key
3. Send this encrypted Personal Share to Zengo's server, which now associates this encrypted Personal Share with the Legacy Recipient's email address
4. Stores the encryption/decryption key (Legacy File) on the Legacy Sender's personal cloud
5. Shares this Legacy File with the Legacy Recipient using the Legacy Sender's personal cloud service's sharing feature[6] and specifying the Legacy Recipient's email address
6. The Legacy Recipient makes a copy of the Legacy Sender's Legacy file, storing it on the same cloud service used for the Legacy Recipient's personal Recovery File

When this process ends, the Legacy Sender has an encrypted Personal Share stored on Zengo's server associated with their Legacy Recipient's email address, and the Legacy Recipient has its corresponding Legacy File stored on their personal cloud.

Legacy Transfer Setup


Legacy Recipient Personal Cloud
Legacy File
External Cloud Provider
Legacy File
Legacy File
Additional Encrypted Personal Share
Inactivity Period
Zengo Server
3D FaceLock
Legacy Sender User Device
Legacy Recipient User Device

If the Legacy Sender wants to change, update, or even remove their Legacy Recipient, they can do so with a simple confirmation inside of their Zengo app (see below under Legacy Transfer Revocation).

It is important to note that during the entire Legacy Transfer setup process, the Legacy Recipient does not know the contents, amounts, or types of assets inside of the Legacy Sender's wallet, thereby ensuring a high-level of privacy for the Legacy Sender.

[6] Legacy Transfer V1 supports Dropbox for Legacy File sharing; future versions will include all supported personal cloud services

When the Legacy Recipient approves and opts-into this process, they only know they may gain access to the Legacy Sender's wallet at some point of time in the future, assuming all conditions are met. They do not know what they are getting access to until the inactivity period elapses and Legacy Transfer activates.

Legacy Recipient setup

To be an eligible destination for Legacy Transfer the Legacy Recipient must:

- Be a Zengo user: If the Legacy Recipient is not yet a user, they are informed by the server via email of their designation as a requested Legacy Recipient and that they should install the Zengo wallet on their mobile device.
- Have their Secure Recovery solution in place: The Legacy Recipient already extended their authentication information with their 3D FaceLock and Recovery File as described in sections above. If this is not the case, the user is prompted by the server within the app to do so and cannot proceed until they do.

Legacy Transfer activation

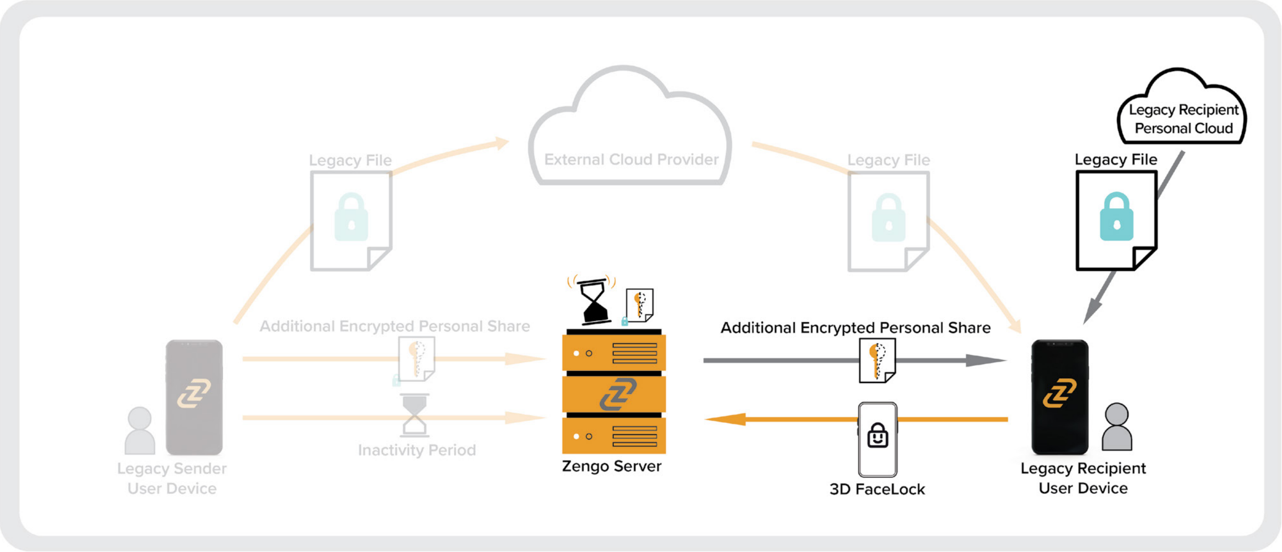
Once the inactivity threshold is crossed, the Legacy Recipient can begin the process to gain access to the Legacy Sender's wallet, as pre-designated by the Legacy Sender.

The activation process is a variant of the process used for Secure Recovery, as described in sections above.

1. Zengo notifies the Legacy Recipient that the inactivity period has elapsed and invites them to begin the Legacy Transfer activation process.
2. The Legacy Recipient re-authenticates their email address by clicking a magic link sent to their inbox.
3. The Legacy Recipient is requested to pass 3D FaceLock, the server-side biometric authentication that was created during Legacy Transfer setup.
4. Once verified, the Zengo server sends the Legacy Sender's encrypted Personal Share to the Legacy Recipient's Zengo wallet.
5. The Legacy Recipient's Zengo wallet retrieves the Legacy File from their personal cloud and uses it to decrypt the sender's Personal Share on-device.

Upon successful completion of the activation process, Zengo's server now associates the Legacy Sender's original account with the Legacy Recipient's account. The Legacy Recipient now holds the MPC key material for both their original account and the Legacy Sender's account as two wallets and can manage both.

Legacy Transfer Activation


Legacy File
External Cloud Provider
Legacy File
Legacy Recipient Personal Cloud
Legacy File
Additional Encrypted Personal Share
Additional Encrypted Personal Share
Inactivity Period
Legacy Sender User Device
Zengo Server
3D FaceLock
Legacy Recipient User Device

Legacy Transfer revocation

It is impossible to “take back” a seed phrase once it’s been shared with another person.

This is not the case with Legacy Transfer, which allows the Legacy Sender to change or completely cancel their Legacy Recipient in a few simple taps inside their Zengo app.

If the Legacy Sender wants to revoke Legacy Transfer for their defined Legacy Recipient, they can instruct the server to purge their encrypted share, rendering Legacy Transfer impossible for the originally-designated Legacy Recipient. They can then simply designate a new Legacy Recipient if so desired, following the process described above.

Security Analysis

Receiver resilience against account takeover

This is the same as for Zengo’s original Secure Recovery process, as the authentication factors remain the same.

Sender resilience against account takeover

In theory, the ability to define Legacy Transfer in itself may constitute a way for attackers to take over a sender’s account.

However, to define such:

- Legacy Sender must be logged into the app and perform local authentication and 3D FaceLock. If attackers can bypass that, then they are also able to send funds from the wallet and steal assets in a more direct manner.
- The definition of Legacy Transfer and its activation is highly visible within the Legacy Sender's app and email inbox, and the minimal inactivity period is long enough for the sender to detect and revoke a rogue Legacy Transfer setup.

Resilience against loss of access

This is the same as it is for Zengo's Secure Recovery, as the authentication factors and their additional redundancy remains the same. The Legacy Sender's Legacy File remains on the Legacy Recipient's cloud, even if the app or the device is lost.

Resilience against a malicious server

Similarly to Zengo's Secure Recovery, a malicious server cannot access the Legacy Sender's Personal Share stored in an encrypted manner on the server. To do so, it would need to obtain the Legacy File (encryption/decryption key) that is generated by the Legacy Sender, transferred via Cloud sharing and stored by the Legacy Recipient on their personal cloud.

Therefore, Zengo's Legacy Transfer still maintains the MPC promise of distribution of powers and no single point of failure.

In theory, a rogue server could collude with a rogue Legacy Recipient to release the encrypted share before its due time. However, this is highly unlikely:

- The Remote Server cannot trigger the setup of Legacy Transfer as it's fully controlled and initiated by the sender.
- The Remote Server is not involved in choosing the identity of the receiver as it is fully controlled by the sender.
- This is not a systemic risk to the system that can fully compromise the system, or at least the users that set up Legacy Transfer, as it would require each of the receivers to collude with a rogue server.
- The server is incentivized to remain honest, since if it were to collude in the aforementioned way to defraud a single user, it would be known publicly and undermine Zengo's entire business model.

Resilience against loss of the server's Remote Share

Prior to the actual activation of Legacy Transfer, the Legacy Sender is protected as in before with Zengo's Guaranteed access solution.

Post activation of Legacy Transfer, the Legacy Recipient is protected as before with Zengo's Guaranteed access solution, since it receives the relevant encrypted Remote Share on activation.

Authors and Acknowledgements

This report was assembled by the Zengo research team led by Zengo Co-founder and Chief Technical Officer, Tal Be'ery and contains contributions from many members across the company.

Questions or comments? Email us at security@zengo.com