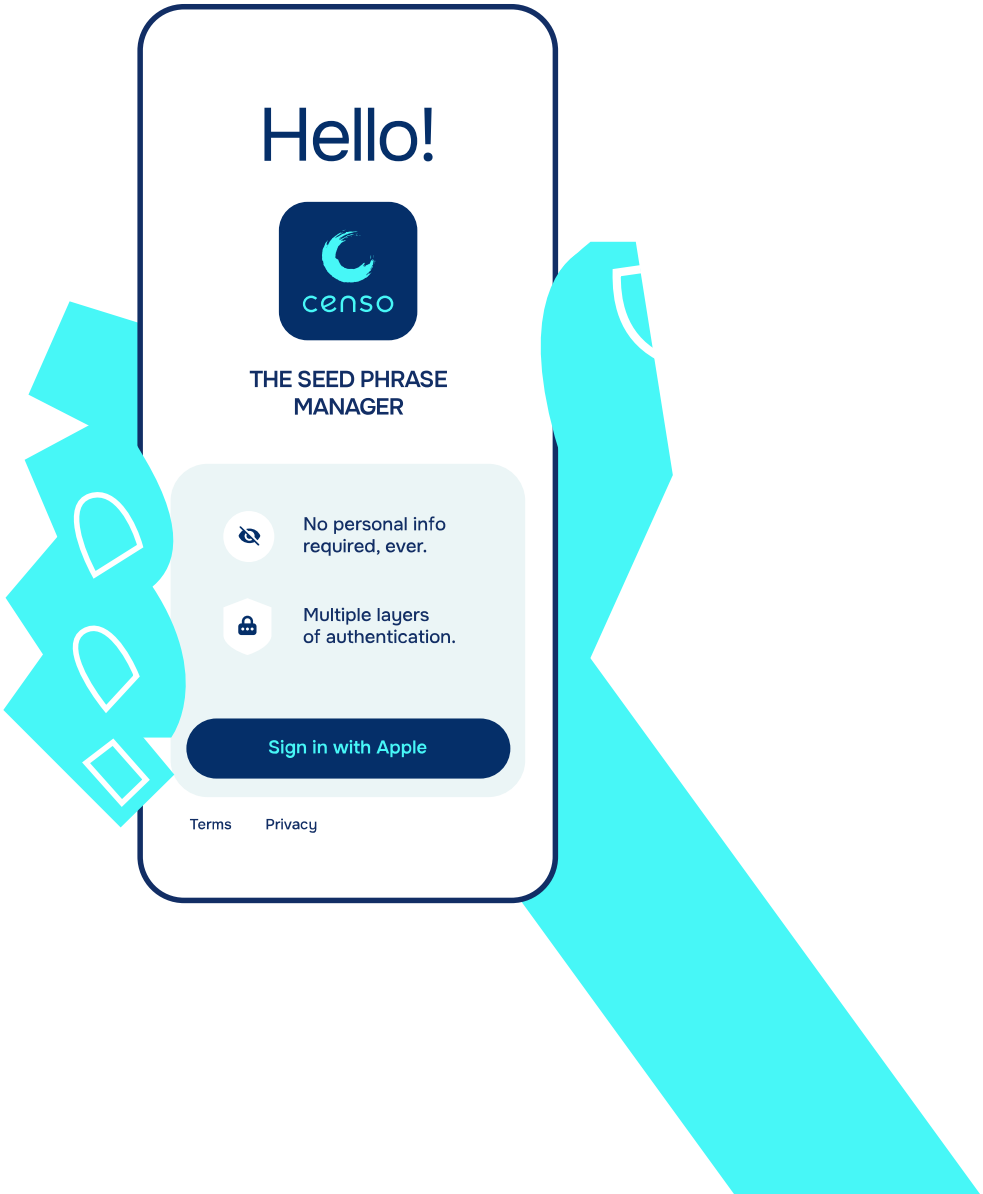
censo

# CENSO SECURITY DESIGN

December 2023



# TABLE OF CONTENTS

# PRINCIPLES

The Censo Seed Phrase Manager provides users for the first time ever the ability to store, manage, and access their seed phrases without anxiety, knowing that they'll never lose access to their crypto. To achieve these goals, Censo has been designed in compliance with the following guiding principles:

**Robust security**
Seed phrases are users' most precious digital records. Censo is designed so that no matter how large the value of those records, Censo's security exceeds the standards required to protect them and keep them safe.

**Total privacy**
Users never need, nor can, identify themselves with Personally Identifiable Information or by any other means that link back to their real-world identities to use Censo. Users do not need to rely upon Censo protecting their information; they are guaranteed that Censo has never collected any of their information to start, making it impossible to be compromised.

**Complete control**
No one other than the user managing their seed phrase can ever be able to access or read any part of that seed phrase whatsoever. Users have complete control and sole access to their seed phrases.

**Censorship resistance**
Users are guaranteed that they can access their seed phrases at any time without the permission, assistance, or operation of Censo, or for that matter, any other 3rd-party. Users cannot be subject to forfeiture risk owing to sovereign or corporate encroachment.

**Loss tolerant**
Users must be protected against a permanent loss of both their authentication credentials and/or encrypted shares of their seed phrases, and they must have the ability to restore either in those loss circumstances. Trusted Approvers assist Censo users' management of their seed phrases while providing a factor of authentication, and they provide resilience against a loss of either.

**Acceptance of human nature**
Virtually all of us are not good at things like remembering passwords or securely storing physical items for retrieval at a later date. We cannot be relied upon for extraordinary feats of memory, nor to ensure that our computers or mobile phones will not be lost or damaged in the future. Censo recognizes all these things and is designed to conform to human nature, rather than hoping that human beings will change and conform themselves to something unnatural.

# IMPLEMENTATION

The Censo feature set delivers to users Censo's promised guiding principles:

## KEYS & ENCRYPTION

### Encryption

All cryptographic keys are generated on users' mobile devices, and all encryption and decryption operations are controlled by users and executed securely on their mobile devices. Industry-standard and long-proven asymmetric and symmetric encryption techniques are exclusively employed. Users always remain in sole control of any keys used for decryption.

### Signed data in transit

All communication traffic between users and Censo or users and each other is encrypted and signed, ensuring against man-in-the middle attacks or the possibility of being read while in transit.

### Shamir secret sharing

Users' seed phrases are sharded into fragments using Shamir secret sharing, prior to being encrypted. This ensures that firstly no single piece of private material could be used to expose an underlying plain text version of a seed phrase, and secondly that access to a seed phrase does not rely upon any single point of failure.

## AUTHENTICATION & PRIVACY

### Authentication resiliency

Censo relies upon multiple factors of authentication for users, and this enables resilience of authentication should a user lose access to one of their authentication factors.

### Authentication accuracy

By utilizing 3D biometry with liveness check as one of several factors of authentication, users are authenticated with the highest degree of accuracy possible.

### Authentication anonymity

When users sign-in to Censo with Apple or Google, Censo collects a login ID (in the case of Apple, a Pairwise Pseudonymous Identifier, in the case of Google, an identifier unique to the user) that is persistent and is not associated with any PII. Censo collects no PII whatsoever and all users remain anonymous to Censo. Censo maintains only a SHA2 hashed version of user login IDs and has no other data such as PII to identify them. In addition, it is impossible for Censo to tie the 3D biometry data provided by users to any real-world credentials or identities.

## TRUST & OPENNESS

### Open-source code

All of the components of Censo that require trust are open-source and audited. In addition, Censo mobile apps use attestation to ensure that only the signed Censo version of the app can access a user's data.

### No trust in Censo backend

Censo acts as a relay server to allow communication between seed phrase owners and approvers, but no trust of the backend is required as all traffic is encrypted and signed, and out-of-band channels are used for important verification and establishment of trusted connections (typically via TOTP over phone call). The maximum damage an attacker could achieve on the backend would be a temporary denial of service.

### Users' Trusted Approvers

Users may select those individuals whom they trust to assist them in the management of their seed phrases, rather than being compelled to use agents of Censo's choice.

### Secure deletion

Users have complete control over all their data at every moment. This includes the right of deletion. Users may securely delete their data whenever they desire.

## COLLUSION, COERCION & CENSORSHIP RESISTANCE

### Offline mode

Censo may be optionally operated in offline mode, without a connection to Censo or the Internet. In offline mode it is impossible to censor user access to seed phrases, nor is it possible for a 3rd-party, such as a sovereign entity, to interfere with a user's actions.

### Owner control

Seed phrases can only be accessed at the direction and control of the seed phrase owner. Even a theoretically plausible mathematical quorum of Shamir share holders cannot access a seed phrase without the owner's action and agreement.

### Data persistence

Censo maintains fully encrypted versions of user seed phrases on its backend. Users may at any time delete the Censo app from their mobile devices, download it at a future date, and instantly reestablish a full connection and access. This ability to wipe the app from the phone may appeal to users crossing national borders or in other situations. As well, this data persistence means that Censo is not hardware reliant, and users are resilient to the loss or replacement of any hardware device.

### Timelock

Users may optionally employ a timelock that gates the speed at which a seed phrase can be accessed, after a valid approval of the access request. This timelock may be considered a useful security measure for some users.

## EASE OF USE

### Simple operation

Users can activate in Censo and achieve their seed phrase security in a matter of minutes. While ease of use may not often be considered a security feature in common thought, it is a critical element of security – allowing users to secure their seed phrases easily and rapidly, and with comprehension, despite the sophistication of the underlying cryptography and operations.

# WHO IS THIS DOCUMENT FOR?

This document is for anyone interested in a technical overview of how Censo is designed and implemented, or for anyone with an interest in seed phrase and cryptocurrency security. At Censo, we believe we have designed the optimal solution for seed phrase security that endows users with the longstanding goal of sovereignty, and now for the first time, in the absence of anxiety.

The following sections likely do require a basic grasp of a handful of related technical concepts including public/private key encryption, hashing algorithms, digital signatures, Shamir secret sharing, and mobile phone secure hardware components. However, one need not be expert in any of these subjects to understand the document.

Separately, for the more technically inclined, Censo's mobile code may be reviewed here:
**https://github.com/censo-inc**

Before proceeding further, you may consider downloading the Censo apps and trying them out in concert with your review of our implementation discussion. A picture is worth a thousand words, and the apps may be an illuminating companion to your review. Please find the links here:

**Censo, App Store** - https://apps.apple.com/us/app/censo/id6470887140

**Censo, Google Play** - https://play.google.com/store/apps/details?id=co.censo.censo&hl=en&gl=US

**Censo Approver, App Store** - https://apps.apple.com/us/app/censo-approver/id6470887275

**Censo Approver, Google Play** - https://play.google.com/store/apps/details?id=co.censo.approver&hl=en&gl=US

# FUNCTIONAL OVERVIEW

The Censo Seed Phrase Manager allows users to securely store, manage, and access seed phrases for the very first time. Before proceeding on to a detailed discussion of how it's implemented, this section reviews user roles, mobile applications, and principal app functions.

## USER ROLES

**Owner** – An Owner uses Censo to securely store, manage, and access their seed phrases. They may also be referred to as a 'seed phrase owner'.

**Approver** – An Approver is invited and activated by an Owner to help them manage their seed phrase(s). When requested, an Approver will need to approve of a request from the Owner to access their seed phrase. Owners rely upon Approvers, and therefore they should be chosen with care and may also be referred to as a 'Trusted Approvers'.

## MOBILE APPLICATIONS

**Censo app for App Store or Google Play** – Simply named 'Censo', this is the app with the main functionality of Censo, and it is used by seed phrase Owners to manage their seed phrases as well as their Approvers.

**Censo Approver app for App Store or Google Play** – The Censo Approver app is used by Trusted Approvers. Its main functionality is quite parsimonious and is comprised of firstly, accepting an invitation to activate as a Trusted Approver, and secondly, to approve an Owner's access to their seed phrase when requested.

Users may be both Owners and Approvers, although the present configuration does not permit for an Owner to be a Trusted Approver for themselves.

## PRINCIPAL APP FUNCTIONS

**Authentication** – Properly identifying users and gating access to Censo and all of its functions.

**Initial Policy Creation** – Creating a policy that governs the security, management and access to seed phrases that have been input to Censo.

**Approver Activation** – Activating Trusted Approvers utilizing the Censo Approver app that will help the owner secure and access seed phrases into the future.

**Update Initial Security Policy** – An initial security policy may be updated by adding one or two Approvers.

**Add Seed Phrase** – An Owner may add an unlimited number of seed phrases at any time without the need to interact with Approvers.

**Seed Phrase Access** – An Owner may access their seed phrase by obtaining approvals that meet the requirements of their security policy.

**Remove Approvers** – An Owner may wish to remove their current Approvers.

# DETAILED IMPLEMENTATION DISCUSSION

Immediately below here is a detailed implementation discussion for each principal action class. While Censo allows for a variety of Security Policy configurations including zero Trusted Approvers (Owner is sole approver), as well as one or two Trusted Approvers, the implementation discussion below assumes two Trusted Approvers. A final note, there is no need for Owners and their Approvers to be on the same platform: An Owner could be an iOS user and have Android users as Approvers.

## AUTHENTICATION

### Function

Authentication gates access to the Censo app & Censo Approver app and is required by all app functions.

### Implementation

Owners and Approvers are authenticated and restored with the following factors and in the following manner:

| FACTORS | OWNER (CENSO APP) | APPROVER (CENSO APPROVER APP) |
|---|---|---|
| 1 | Apple / Googe ID | Apple / Google ID |
| 2 | Facetec face scan / Liveness | Owner verification via TOTP |
| Restoration for a single factor | Owner verification with 2 approvers + 1 other existing factor | New policy creation (requires 1 approver plus owner) |

The ability to login via Apple or Google on a mobile device is a feature offered by Apple on iOS and Google on Android. This functionality has unique advantages for Censo and its users:

- Because it is available to 100% of all mobile phone users on those platforms, if a user can login using iOS or Google, they can authenticate for Censo.
- No Personally Identifying Information (“PII”) or any material linking a user to a real-world identity is disclosed to Censo.
- User can pay Censo for usage, again without disclosing their PII.
- User can store persistent data in cloud storage, again without disclosing PII.

In either of these cases, when a user signs into Censo using Apple or Google, those entities return an identifier (we will refer to this as the login ID) to the Censo mobile app on login and Censo handles it in the following way:

- the Login ID is used in the mobile code but never disclosed to the Censo backend.
- the Login ID is hashed using SHA2 and passed to the backend to allow Censo to identify the user. Taking this additional step of hashing the Login ID ensures that it will be impossible for Censo to identify the user.

Users require both security and resilience. Two factors of authentication ensure security. If an Owner has also activated two Trusted Approvers, then they will be able to recover any lost factor of authentication with the Owner and ensure resilience.

# INITIAL POLICY CREATION

## Function

An owner must initially configure the Censo app with an initial security policy for access control. This initial security policy may be subsequently updated by adding trusted approvers.

## Implementation

The Censo app will create an initial security policy on behalf of the Owner that makes the Owner a 1 of 1 approver on their data. When this process is complete the owner may enter seed phrases and a use any other features of the app.

During this process the following keypairs are created:

### Master Key

The public Master Key is used to encrypt all seed phrases.

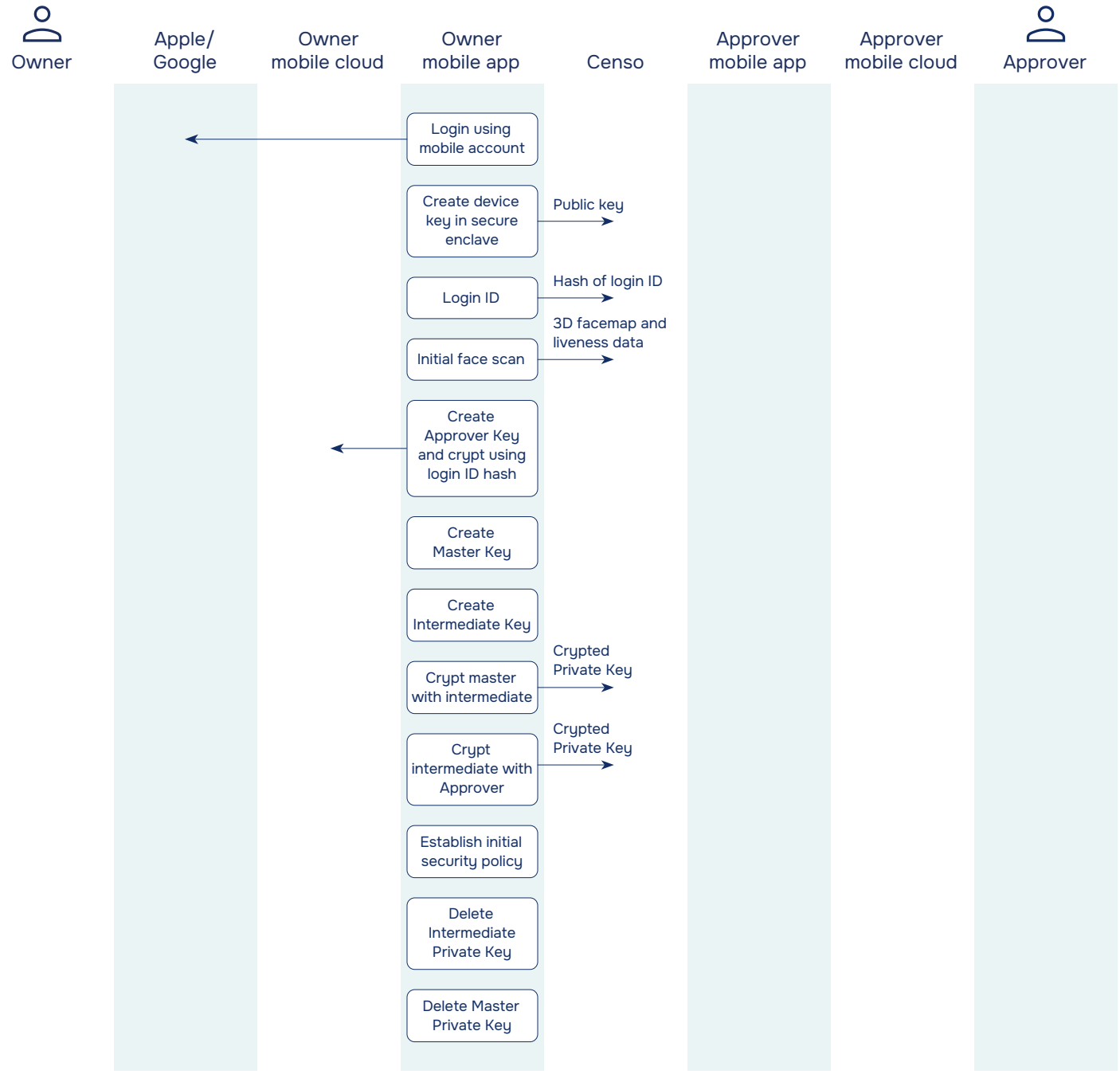
### Intermediate Key

The Intermediate Key is used to encrypt the Master Key. Once the Master Private Key has been encrypted using the Intermediate Public Key, the Master Key plaintext is securely deleted, so the encrypted copy of the Master Private Key is the sole copy. The Intermediate Private Key is then sharded into a single shard using Shamir secret sharing.

### Approver Key

The Approver Key is created, which is used to encrypt the intermediate key (in the form of a single shard from the initial security policy of only the owner).

# INITIAL POLICY CREATION



# APPROVER ACTIVATION

## Function

Subsequent to an Initial Policy Creation, an Owner may wish to activate one or more Trusted Approvers as part of their security policy, to assist them in the management and access of their seed phrases.

Censo's secure Approver Activation protocol ensures that:

- The Approver that the Owner selected to be activated is in fact verified as the one that is configured.
- The Approver is authenticated in the Censo Approver app.
- A secure cryptographic channel between the Approver's phone and the Owner's phone is established.

## Implementation

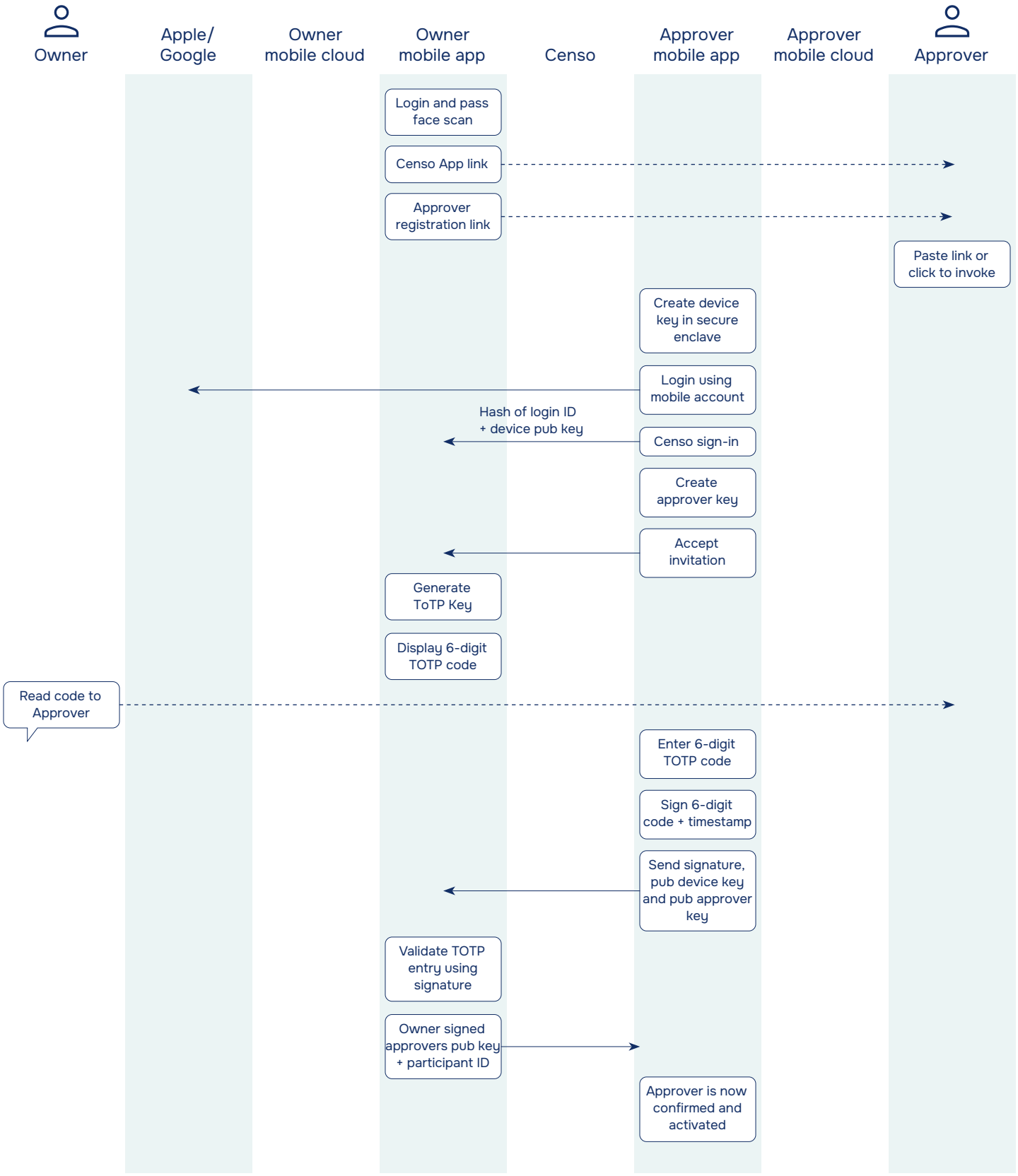
The Owner establishes a secure live conversation with their intended Trusted Approver and walks them through the process of configuring the Censo Approver app. The process between the Owner and the Approver entails the following steps, performed sequentially:

1. The Owner uses their app to convey via an out of band channel (Telegram, email, e.g.) a link to the Censo Approver app for the Approver to download.
2. After the Approver downloads the Approver app, the app generates an Approver Key.
3. The Owner uses their app to convey a link to the Approver via an out of band channel (SMS, Telegram, email...) which contains a registration identifier that will allow for encrypted traffic between the Owner's app and the Approvers app.
4. Once the Approver activates the link with the registration identifier, the Owner's app generates a rotating time-based six-digit TOTP code that they will verbally recite to the Approver. Using a digital signature sent from the Approver's app to the Owner's app via Censo, the Owner app can verify the Approver. Since only the signature is passed between the Approver and Owner apps there is no attack possible through the Censo channel.

After the activation steps above are successfully executed, the Owner's Censo app will have trusted public keys for the Approver device and their Approver Key. These public keys enable:

- A secure communication channel between the Approver's current device and the Owner's phone.
- The Approver's ability to sign an approval at the request of the owner.

# APPROVER ACTIVATION



# UPDATE INITIAL SECURITY POLICY

## Function

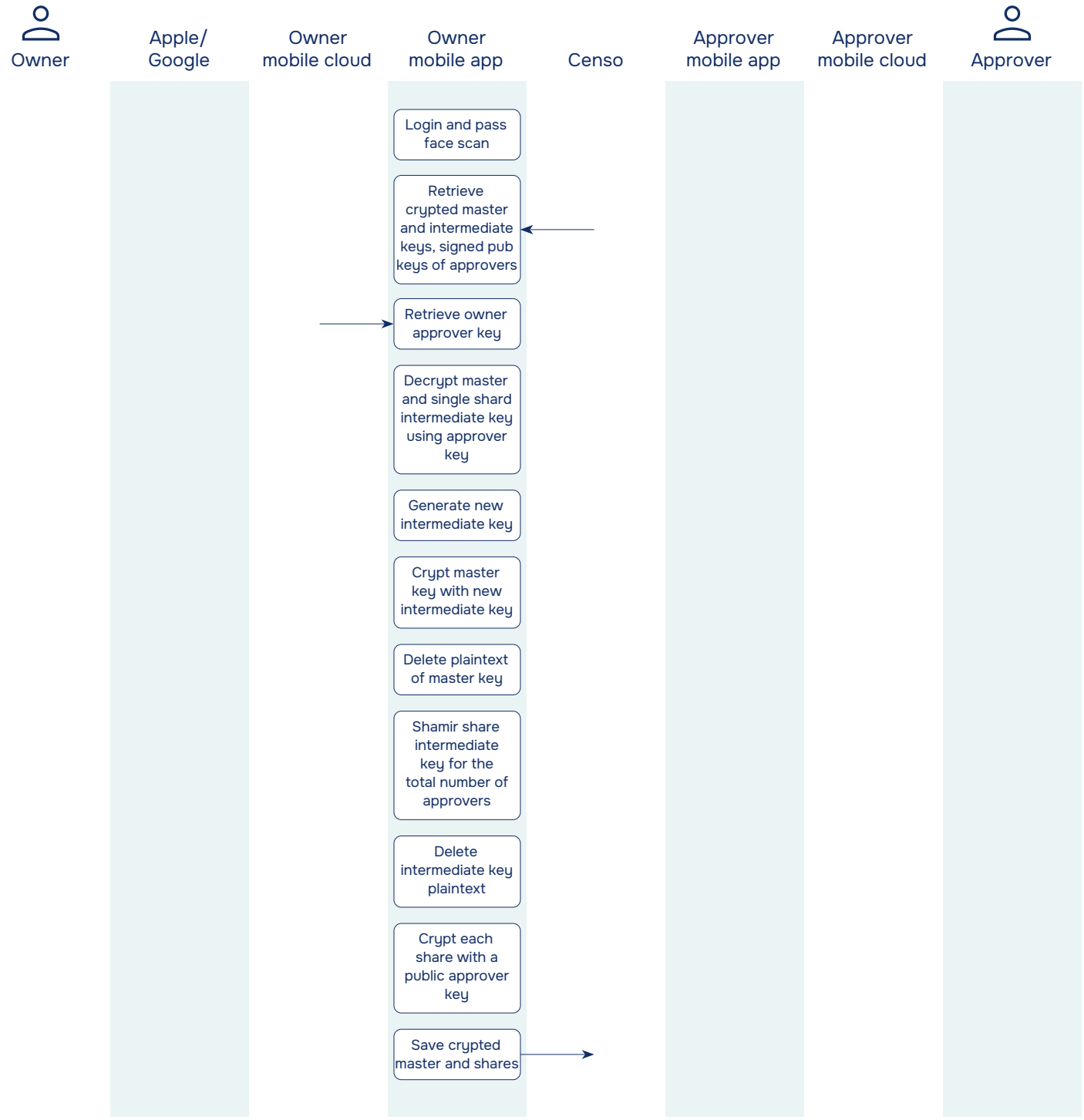
After an Owner approves the activation of one or more Trusted Approvers, the Initial Security Policy must be updated to reflect those changes.

## Implementation

This implementation does not require any actions on the part of the Owner or the Approvers.

The plaintext version of the Master Private Key must be made available via decryption utilizing the existing Intermediate Private Key in the Owner's phone. This Master Key decryption is precedent to a new Intermediate Key pair being created, reflecting the updated Security Policy. The existing Intermediate Key is securely deleted, the Master Private Key is encrypted with the new Intermediate Key, which is then Shamir shared and encrypted with the new Approvers' Public Keys. The API call to save the new Security Policy must be signed with the existing Intermediate Key to prove that the proper Intermediate Key had been recovered and therefore the updated Security Policy will be able to access the seed phrases properly into the future.

# UPDATE INITIAL SECURITY POLICY



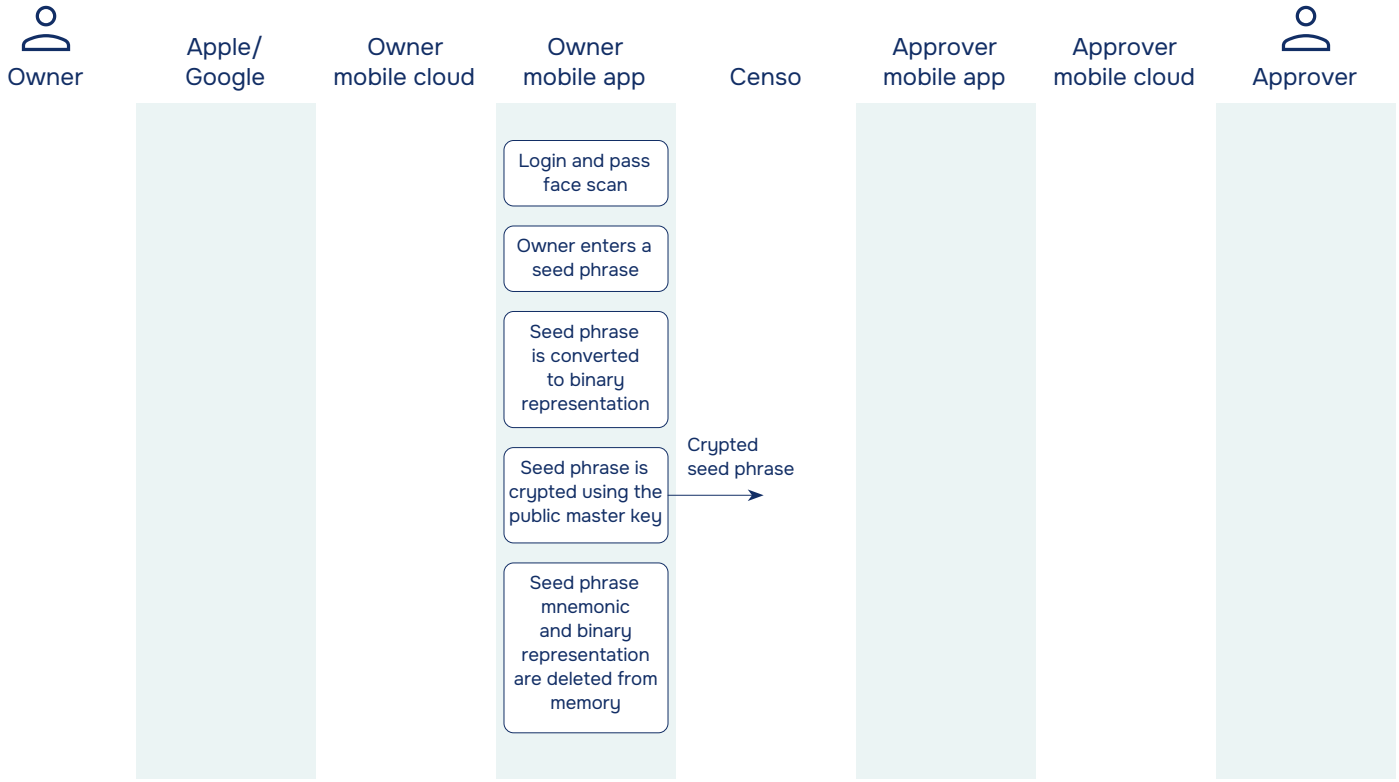
# ADD SEED PHRASE

## Function

An Owner may add a new seed phrase at any time without any interaction with their Approvers.

## Implementation

This process consists of Owner input of the seed phrase into the Censo app, which then obtains the binary representation of the seed phrase, encrypts that binary representation using the Master Public Key, and then securely deletes the binary and mnemonic versions of the seed phrase. Because the only way the plaintext Master Private Key can be obtained is to assemble and decrypt the shards of the Intermediate Private Key and subsequently decrypting the Master Private Key, the newly added seed phrase is now secured using the security policy without further action.



# SEED PHRASE ACCESS

## Function

An Owner may access their seed phrases by obtaining approvals that meet the requirements of their security policy.

## Implementation

The Seed Phrase Access process shares similarities with Approver Activation, however, with an important difference: During Approver Activation the Owner provides a TOTP code for the Approver to enter in order to verify the Approver's identity. For Seed Phrase Access however, the roles are reversed - the Approver provides a code for the Owner to enter in the Owner's Censo app so that the Approver effectively verifies the Owner's identity.

After initiating access via their app, the Owner establishes a secure live conversation with their Trusted Approver. The process between the Owner and the Approver entails the following steps, performed sequentially:

1. The owner uses their app to convey a link via an out of band channel (sms, telegram, email...) with a registration identifier that will allow for encrypted traffic between the the Owner's app and the Approver's app.
2. The Approver's app generates a rotating time-based six-digit TOTP code which they will verbally recite to the Owner. Using a digital signature sent from the Owner's app to the Approver's app via Censo, the approver app can verify the Owner. Since only the signature is passed between the Owner and Approver apps there is no attack possible through the Censo channel.

Once this secure connection has been established, the Owner's app will request that the Approver's app decrypt their Intermediate Key shard (with their Approver Key) and re-crypt it with the public device key (generated within the secure enclave or Strongbox of the Owner's phone) of the Owner's phone and send to the Owner.

After the above processes are complete, the Owner is now in possession of the following:

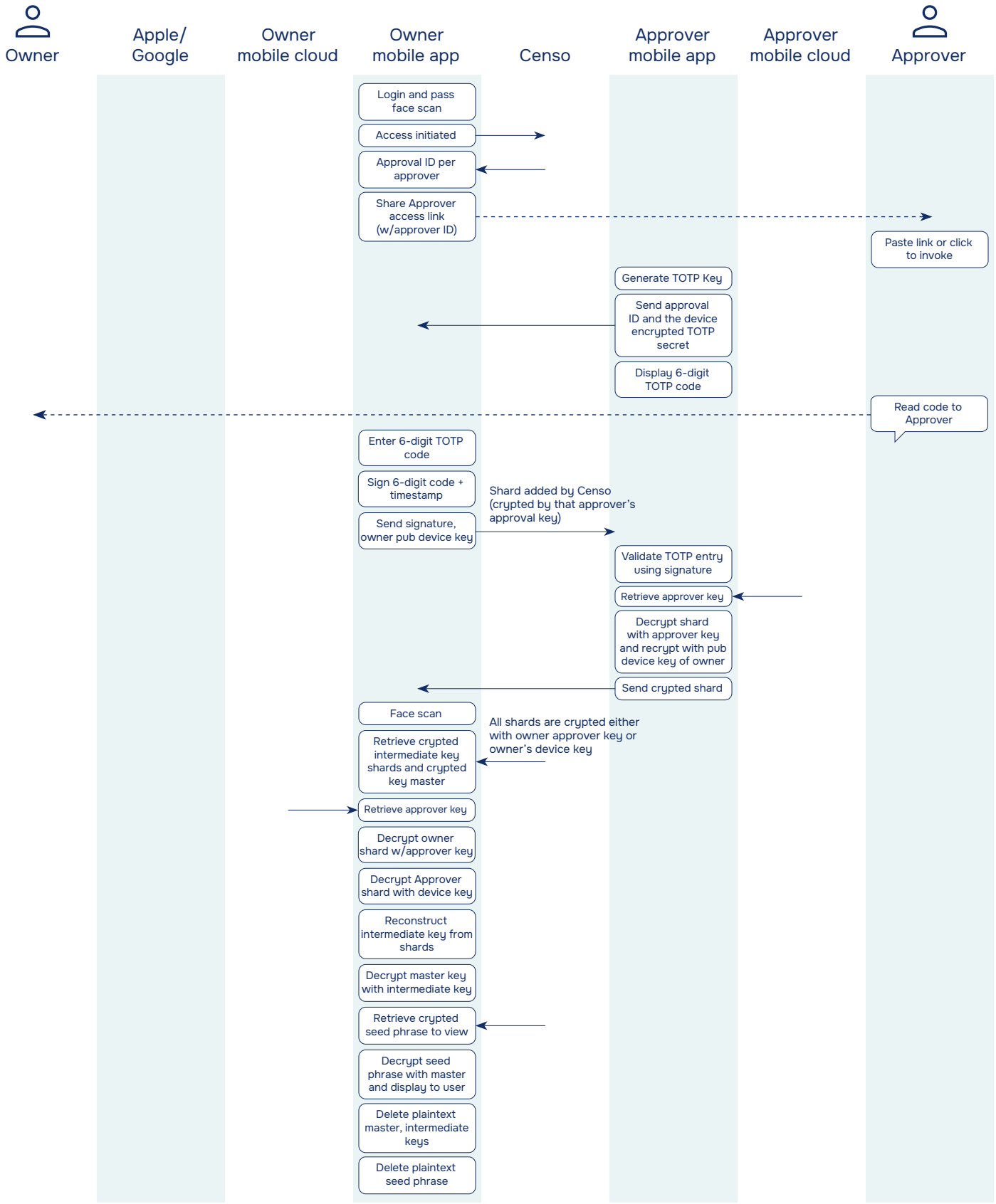
- Their own Intermediate Key shard which they can decrypt using their Approver Key in plaintext (from cloud storage, decrypted by their login ID)
- The Approver's Intermediate Key shard which they can decrypt using their device key

The Owner's app can now use these shards to reconstruct the Intermediate Private Key, decrypt the Master Private Key and decrypt any of the seed phrase binaries for the Owner. When Seed Phrase Access is complete, all plaintext copies of the Intermediate and Master Private Keys and shards are securely deleted from the Owner's phone.

## Drawing

For purposes of simplicity, this drawing reflects a security policy of an Owner plus 1 Trusted Approver. Other potential security policies behave similarly.

# SEED PHRASE ACCESS



# REMOVE APPROVERS

## Function

An Owner may elect to remove their existing Approvers and return to the Security Policy Configuration of Owner as a single Approver. This could be motivated by and enable any of the following use cases:

- The Owner wishes to be the only Approver and no long wants any 3rd-party Trusted Approvers.
- The Owner wishes to replace the current Approvers with new Approvers.
- The Owner wants to modify the number of Approvers, for example moving from a single Approver to two Approvers.

## Implementation

This process can be thought of as a combination of the Seed Phrase Access combined with the Initial Policy Creation.

Since the Owner must first make the Master Key available in plaintext from in their phone, they must execute the Seed Phrase Access. Once this is complete, they can setup a new security policy with just the owner in the same fashion as the Initial Policy Creation.

# RESOURCES

### BIP 0039
How a mnemonic code – or set of words – is used for the generation of a cryptocurrency wallet:
https://en.bitcoin.it/wiki/BIP_0039

### Shamir secret sharing
An efficient secret sharing algorithm for distributing private information:
https://en.wikipedia.org/wiki/Shamir%27s_secret_sharing

### FaceTec
Private, 3D liveness biometry for secure digital identity: https://www.facetec.com/

### PPIDs
Pairwise Pseudonymous Identifiers for privacy preservation: https://curity.io/resources/learn/ppid-intro/

### Security audits
All Censo code requiring trust is audited: https://github.com/censo-inc

### Open-source repos
All Censo code requiring trust is open-source: https://github.com/censo-inc

### App attestation documentation
https://developer.apple.com/documentation/devicecheck/validating_apps_that_connect_to_your_server
https://developer.android.com/google/play/integrity