Wallet Verification

How the Celo wallet uses phone number verification to map phone number hashses to addresses.

How does Wallet Verification work?

The Celo Wallet leverages the Lightweight Identity protocol to construct mappings of phone number hashes to addresses.

Phone Number Verification in the Wallet

During the final step of new user onboarding in the Celo Wallet, a user completes phone number verification. Given that the Celo Protocol supports a variable, the Celo Wallet implements this as a binary notion ofverified (>= 3 attestations) orunverified (< 3 attestations). During the verification process, three attestations are attempted, and the user receives three text messages, upon receipt of which the user is considered verified. Future implementations of the wallet may explore using requested/received verification ratios or variable numbers of attestations to provide a notion of non-binary verification so as to account for variable probabilities of ownership of a phone number.

Verifications

When verification is in progress, the celo wallet sends a request for three SMS attestations. The process of selecting the senders of each of these three messages is detailed in the Lightweight Identity documentation.

The following diagrams depict the user flows for the celo wallet:

- General Verification Flow
- Detailed Phone Number Hash Flow
- Detailed Flow for Receiving SMS Input and Compeleting Verification Edit this page Previous Celo Wallet Functionality Next Wallet Invitations