Wallet Security

Suggest Edits

Security setup and best practices

Programmable Wallets leverage Shamir's secret sharing and secure multi-party computation (MPC) technology to ensure your wallet has the highest level of security. Shamir's secret sharing lets you, the developer, your end users, and Circle each have a key shard that can reconstruct a golden key, which can be used to access the MPC access tokens and sign through three separate MPC nodes. Circle's security model manages the complexity of hosting MPC nodes and enables developers to go to market quickly. The following diagram shows the architecture for user-controlled wallets and how signing works:

We also offer the option for self-hosting MPC nodes for enterprises with higher security needs and the requirement and ability to host and maintain their own MPC nodes.

Security settings for Web3

To further enhance your security settings, we recommend establishing an API call IP allowlist as it:

- Restricts accepted API calls to those originating from designated IPs, blocking potential unauthorized usage.
- Reduces the potential for loss due to API key exposure.
- Block bad IP addresses.

Note: Neglecting to establish an IP allowlist can expose APIs to exploit from unauthorized IP addresses. Updated5 months ago *