Managing Your Keys

This guide informs chain operators on important key management considerations. There are certainprivileged roles that need careful consideration. The privileged roles are categorized as hot wallets or cold wallets.

Hot Wallets

The addresses for theBatcher and theProposer need to have their private keys online somewhere for a component of the system to work. If these addresses are compromised, the system can be exploited.

It is up to the chain operator to make the decision on how they want to manage these keys. One suggestion is to use a Hardware Security Module (HSM) to provide a safer environment for key management. Cloud providers often times provide Key Management Systems (KMS) that can work with your developer operations configurations. This can be used in conjunction with theeth_signTransaction RPC method.

You can take a look at the signer clientsource code(opens in a new tab) if you're interested in whats happening under the hood.

Cold Wallets

The addresses for the cold wallets cannot be used without human intervention. These can be setup as multisig contracts, so they can be controlled by groups of community members and avoid a single point of failure.

Refer to theprivileged roles documentation for more information about these different addresses and their security concerns.

Node Operations Troubleshooting