Key Management Best Practices for Node Operators

- Secure keys, including secrets such as passphrases or mnemonics, using services like AWS Secrets Manager or Hashicorp Vault. These services can be seamlessly integrated with automated mechanisms that safely retrieve secrets or keys (e.g., remote signers). If resources permit, consider running your own Hashicorp Vault instance, which grants full custody of keys and secrets while sacrificing the service provider's availability and security guarantees.
- Avoid generating all keys with the same mnemonic. Minimize the attack surface by employing a new mnemonic for every 200 or 1000 validator keys, depending on your preference. This approach also reduces the risk of losing key generation capabilities if a single mnemonic is lost, and limits the impact if an attacker gains access to a few mnemonics.
- Use a remote signer likeWeb3signer
- or, better yet, distributed signers to eliminate single points of failure.
- Develop a custom solution involving tailor-made tools. For instance, use Web3signer for remote signing and store keys on AWS Secrets Manager. A custom tool can manage automatic key storage in Secrets Manager and facilitate interactions with Web3signer. Previous Introduction Next Key Management Best Practices for Solo Stakers