Key Management Best Practices for Solo Stakers

Individuals managing a limited number of validator keys typically do not require intricate distributed infrastructure for running nodes or employing remote signers. For these individuals, extensive staking services may be excessive and unnecessary. This means they will often store the keys with the decryption keys locally with the validator client or Node (which they maintain), which increases the vulnerability of the secrets, but, while stakers must safeguard validator keys against attacks, most key losses typically result from mundane reasons, such as losing the hardware containing the key. Users necessitate a backup strategy, mindful that if an attacker accesses the backed-up keys, they can sign any message deemed valid against the validator's public key. Appropriate precautions should be implemented to guarantee that backed-up validator keys are as inaccessible as feasible, ideally being completely offline and physically secure. Some of these precautions can be listed:

- Use hardware wallets: Store backed-up keys on secure hardware wallets such as Ledger or Trezor devices. These wallets provide an additional layer of protection by isolating the keys from internet-connected devices.
- Create multiple backups: Generate multiple copies of your backed-up keys and store them in separate, secure locations, such as safety deposit boxes, fireproof safes, or encrypted USB drives.
- Encrypt backups: Ensure your backed-up keys are encrypted using robust encryption algorithms. This protects the keys from unauthorized access in case the storage medium falls into the wrong hands.
- Implement physical security: Ensure the stored locations for backed-up keys are secure, with controlled access and protection against theft or damage.
- Regularly test recovery: Periodically test the recovery of your backed-up keys to ensure that they remain accessible and functional in case of an emergency.
- Employ secure communication channels: When transferring backed-up keys, use secure communication methods such as end-to-end encrypted messaging or other secure channels to prevent interception by malicious actors.
- Limit access: Restrict access to backed-up keys to a select few trusted individuals, and consider implementing a multi-signature scheme to require multiple parties for key recovery.
- Maintain secrecy: Avoid discussing the location or existence of your backed-up keys with others, and do not store any written records that could lead an attacker to their location.
- Continuously update security measures: Regularly assess and update the security measures in place to protect your backed-up keys, staying informed about the latest threats and best practices.
- Use an air-gaped device: Consider using an air-gapped device, such as a computer not connected to the internet, to store backed-up keys. This provides an additional layer of security against remote attacks. Use USB devices or QR codes for sharing the keys with the air-gaped device.

Securing Mnemonic or Seed Phrases for Key Generation

The mnemonic (if applicable) or seed phrase utilized for generating keys should not be stored on any device, and the aforementioned precautions should be taken into account for safekeeping. Avoid key generation tools that write the mnemonic to the Terminal, an insecure buffer, or a file. Aim to generate keys on an air-gapped device, ensuring the mnemonic and passphrase are securely stored or loaded into memory. Previous Key Management Best Practices for Node Operators Next Restaking User Guide