lokblok

toughbox

Toughbox – phantom secrets recovery and hierarchical signatures

WHAT IS IT?

Toughbox is a revolutionary solution designed for the secure recovery of sensitive digital secrets, including BIP39 seed phrases, cryptocurrency private keys, passwords, and more. Unlike traditional methods, Toughbox ensures that your secrets are never permanently stored on any system. Instead, through the concept of Phantom Secrets, your secret only exists for the exact moment it is needed and then disappears, offering unparalleled security.

HOW DOES IT WORK?

Toughbox employs a unique, mathematically advanced method to transform your secret into Public Data. This Public Data is harmless and can exist anywhere without needing to be kept secure. The original secret, now referred to as a Phantom Secret, is destroyed and only reconstituted inside your Toughkey (a hardware security module) when you initiate the recovery process.

To recover your secret, you and your designated Recovery Agents (which can be individuals, devices, or institutions) enter your Toughkeys into your computers. Through a secure authentication process, you approve the recovery, and the secret is reconstituted. Once the secret is used, it disappears again, becoming a Phantom Secret - ensuring it doesn't persist in any form that could be compromised.

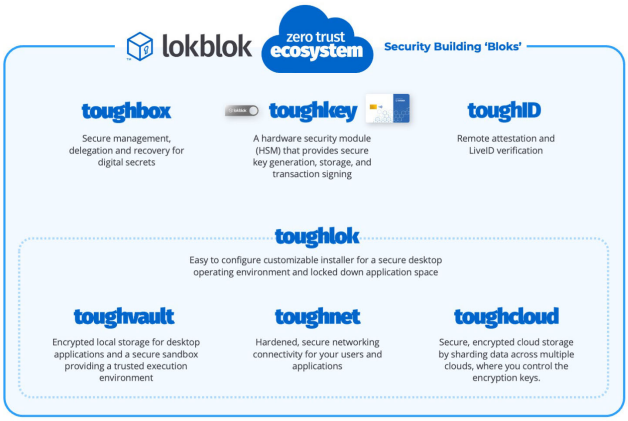
Every Toughbox user and their Recovery Agents have their own Toughkey, used for both enrollment and recovery. The number of Recovery Agents needed to access a secret is entirely up to the user, ensuring flexibility and control over the process.

HIERARCHICAL SIGNATURES

Toughbox introduces the concept of Hierarchical Signatures, which allows policy-driven signing of private keys, aligning with how approval processes work in the real world. Users can be defined in a hierarchy of roles, and various individuals at different levels of authority can be required for sign-off before a transaction is completed.

For example, an organization may require approvals from multiple departments or roles before a sensitive transaction or decision is finalized. With Hierarchical Signatures, this can be replicated digitally, ensuring that the private key used for signing a transaction is only reconstituted within secure hardware for the exact moment of signing. Once the transaction is complete, the key becomes a Phantom Secret, securely "burned" and no longer existing, maintaining the highest level of security.

This feature is particularly valuable for enterprises, where compliance and internal approval processes are critical to secure operations.



Lokblok Zero Trust Ecosystem

WHY USE TOUGHBOX?

In a world where digital assets and sensitive

information are increasingly valuable, the need for a robust, secure recovery solution is more critical than ever. Toughbox addresses the key challenges faced by users, such as device loss, password forgetting, and security threats like hacking or malware, by eliminating the risk of secrets being permanently stored or exposed through the use of Phantom Secrets.

BENEFITS OF TOUGHBOX:

- Uncompromising Security: Your secrets are never stored, minimizing the risk of exposure or theft. Toughbox's Phantom Secrets approach ensures that secrets only exist when needed and disappear immediately after use.
- Flexible Recovery Options: Toughbox allows you to designate trusted Recovery Agents to assist in the recovery of your secrets without giving them direct access.
- Hierarchical Signatures: Ensure that multiple roles can be integrated into the approval process, allowing for policy-driven signing of private keys. This feature mimics real-world decision-making and ensures that sensitive actions require approval from the correct authorities.
- Cross-Platform Compatibility: Toughbox works across various operating systems and platforms, including Windows, MacOS, Linux, Android, and iOS, making it easy to implement in diverse environments.
- Seamless Integration: With the provided SDK, Toughbox can be effortlessly integrated into applications, allowing developers to streamline both the enrollment and recovery processes.

TECHNICAL FEATURES

Toughbox is equipped with patent applied for secret-sharing technology and supports a variety of key management options, including hardware, software, and hybrid keys. The REST API enables developers to incorporate Toughbox into their systems for easy, secure recovery of digital secrets.

Rest API
Patented Secret Sharing
Hardware, Software & Hybrid Keys
Library that supports multiple languages

SUMMARY

Toughbox is an essential solution for anyone managing sensitive digital assets, providing peace of mind through its secure, trustless, and flexible recovery mechanisms. Whether you're managing cryptocurrency private keys, passwords, or other confidential information, Toughbox ensures that your secrets are safe, recoverable, and never stored in a way that could be compromised.

With the added Hierarchical Signatures, organizations can mirror real-world approval processes, ensuring that only authorized personnel can sign off on critical transactions. The use of Phantom Secrets ensures that secrets only exist when needed and are securely erased afterward, making Toughbox the most secure and versatile tool for digital secret management.