lokblok

toughkey

Toughkey is a hardware security module (HSM) that is EAL 6+ and FIPS 140-2 Level 3 certified to provide secure key generation, storage, and transaction signing.

WHAT IS IT?

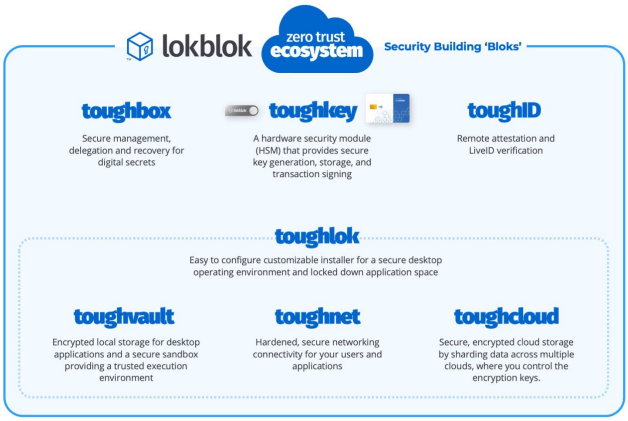
Toughkey is a physical USB device that is core to the Lokblok Zero Trust Ecosystem and serves as the ignition key to unlock other Lokblok secure services.

WHAT DOES IT DO?

Toughkey is a military grade hardware device that provides 4 key functions:

1. Secure key generation
2. Secure key storage
3. A secure cryptographic execution environment
4. Split Knowledge security services

This makes it essential for developers who value security when building applications that utilize public / private key pairs.



Lokblok Zero Trust Ecosystem

1. GENERATING SECURE KEYS

The importance of strong entropy in private key generation cannot be overstated. Entropy refers to the randomness or unpredictability of the values used to generate a private key. It doesn't matter how secure your key storage is if an attacker can guess or deduce your private key due to poor entropy. A private key with weak entropy can be easily compromised, leaving the digital assets it is meant to secure vulnerable to theft or manipulation. Therefore, it is critical that the private key is generated with a high level of entropy to ensure that it is truly random and unpredictable.

Toughkey is a Common Criteria EAL6+ and FIPS 140-2 Level 3 certified device that means it is certified to the highest standards of entropy for key generation.

2. SECURELY STORING KEYS

At its core, Toughkey is a hardware device that provides a secure way to store private keys. A private key is an essential component of public key cryptography, which is used to secure online transactions. In the context of cryptocurrency, a private key is used to access funds in a particular wallet. By storing the private key on Toughkey, users can protect it from being compromised by hackers or malware.

3. SECURE KEY SIGNING

In addition to key storage, Toughkey also provides the ability to sign transactions with secure cryptographic functions. When a user wants to send cryptocurrency, they need to sign the transaction with their private key. Toughkey provides a secure environment for signing transactions, ensuring that the private key is not exposed to malicious actors. Secure key signing can also be used as an authentication method to authorize specific computer and web services. No more forgotten passwords.

4. OTHER FEATURES

Toughkey's support both traditional whole keys as well as key-splits. Toughkey's key split capability delivers a significant advantage in terms of security and disaster recovery. With a traditional key, if it is lost or compromised then the whole key and everything it protects is lost. But if a Toughkey key split is lost or stolen, not only will the attacker not have access to the whole key but the part they stole does not provide any details about the whole key. If the split is simply lost, then the remaining split holders can come together to reconstitute the lost key-split to replace the missing one, reconstitute the whole key or re-split the whole key into a new set of key splits.

Toughkey allows a subset rather than all of the key split holders to recover a whole key or a key split when a threshold number of split holders come together. Toughkey's support backing up its whole keys using key splits making Toughkey both secure and resilient for all types of keys. Toughkey's split key capability makes it an ideal tool for online businesses and individuals who want to ensure the security of their online transactions.

In addition to key generation, storage, splitting and signing, Toughkeys can be used to derive other keys for temporary or long-term use.

WHY USE TOUGHKEY?

While software solutions for key generation and storage may be available, they are far less secure than hardware solutions. This is where Toughkey comes in. With Toughkey, developers can generate private keys securely, store them securely, and execute algorithms that use the keys in a secure environment. This is essential for protecting the application and its data from cyber-attacks. Additionally, Toughkey offers a split key architecture that further enhances security by storing key fragments in multiple locations, so that if one location is compromised, the entire system is not compromised.

While Toughkey is a hardware solution, at Lokblok we're also developing improved security for software solutions using multiparty computation, which allows for cryptographic operations to be completed using calculations done on multiple devices, both hardware and software. This could offer a more flexible and scalable solution for developers, while still maintaining a high level of security. Overall, Toughkey offers developers a reliable and secure solution for key generation and storage, with the added benefit of a split key architecture for enhanced security.

TECHNICAL SPECIFICATION

USB Interface: CCID
NFC Interface
Crypto Algorithms RSA 2048, RSA 4096, ECC P256, ECC P384, SHA2, AES
Optional Support for Remote Attestation
Optional Support for FIDO2
Support for Windows, Linux, MacOS, Android, and iOS
Support for PKCS#11
Hardware protection to protect cryptographic keys

SUMMARY

Public key cryptography is becoming increasingly prevalent as more and more cryptocurrency and blockchain-based applications are built. Toughkey is an essential building blok for developers who want to build secure applications that use public key cryptography. While it may seem like a simple USB device, it is a critical component of the larger Lokblok Zero Trust Ecosystem that enables secure transactions and digital asset protection in the digital age.