

# We built it so you don't have to.

Managing digital assets used to require a degree in cryptography. Our flexible, extensible, and easy-to-implement solution means it doesn't have to.



## Introducing Lock-Keeper

Lock-Keeper from Bolt Labs is a next-generation digital asset management system built on advanced cryptographic techniques and a robust cloud architecture. Our platform takes the complexity out of cryptographic key management for both service providers and end users.

At a high level, Lock-Keeper performs the following actions:

- Generates signing keys within a highly isolated Secure Enclave
- Splits those keys into three “shards” using Shamir’s Secret Sharing
- Stores each shard on separate key servers managed by Bolt or a third party

## Digital Asset Security for Everyone

To an asset holder, there’s no such thing as a “low value asset”. With the right balance of speed, security, and scalability, Lock-Keeper bridges the gap between complex cryptography and everyday transactions. End users get leading edge security for all the assets they care about, while developers get a flexible, scalable, and hosted platform to build off of – no crypto PhD required.

### Advanced Cryptography

Advanced Cryptography techniques like Shamir’s Secret Sharing and Multi-Party Computation ensure private keys stay private.

### Robust Architecture

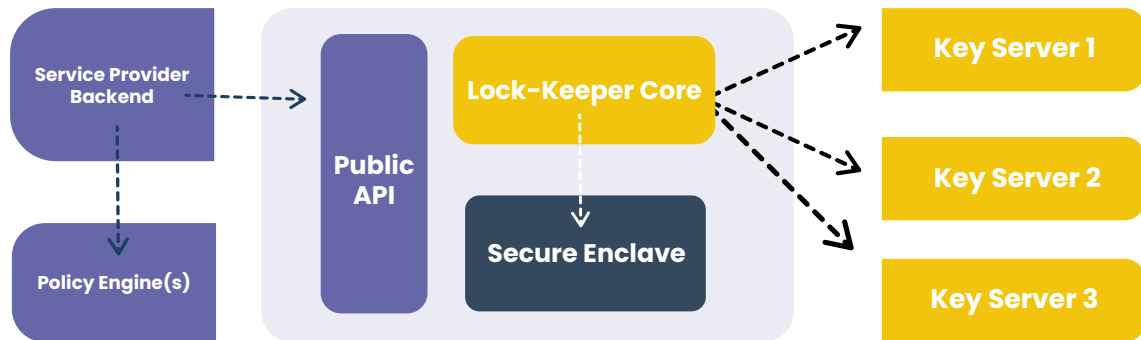
Crucial key operations take place in a highly isolated Secure Enclave built on AWS Nitro. Distributed and geographically redundant storage guarantees key availability.

### Flexible Policies and Access Control

End users get fine-grained control over usage of their keys. Service providers can implement biometric or PIN-based authentication.

### Extensible and Easy to Customize

A modular architecture makes Lock-Keeper adaptable to your specific needs.



## Policy Engine

Lock-Keeper ensures the proper use of cryptographic keys through a flexible policy system. Policies define one or more Authorizing Entities (AEs), which are responsible for approving or denying a transaction. Service providers can also layer their own policy engines on top of Lock-Keeper, (if desired).

## Secure Enclave

A highly isolated and secure environment for performing crucial key operations. Keys are generated, sharded, and reassembled here, and plaintext key material never leaves the enclave. Each enclave is verified using cryptographic attestation to mitigate against hardware and software level attacks.

## Key Servers

Encrypted key shards are stored on separate, geographically redundant key servers. Lock-Keeper's flexible architecture supports Bolt hosted, customer hosted, and hybrid key server deployment models.

## Lock-Keeper Protects Your Keys:

### Confidential

Encryption and Shamir's Secret Sharing provide confidentiality both in use and at rest.

### Available

Keys are persistent and available for permitted uses (e.g., signing compliant transactions).

### Tamper-free

Lock-Keeper guarantees that customers' signing keys cannot be tampered with.

## ABOUT BOLT LABS

At Bolt Labs, our mission is to build a usable, secure, and scalable infrastructure that enables everyone to securely store and use their keys/assets. Our signature product, Lock-Keeper, provides the infrastructure to help developers bridge the gap between complex cryptography and everyday transactions.