Half Epsilon

Digital Asset Management & Transfers

Data Sheet

Half Epsilon One Time Spend Machine (OTSM)

Next Generation HSM for Digital Assets

Digital Asset Custodians are tasked with the secure storage and transfer of digital assets on behalf of their clients. Present day Hardware Security Modules (HSMs) provide secure key storage and transaction signing, but do not support peer-to-peer transfer of digital assets between custody solutions. Consequently, digital asset transfers require submitting transactions to blockchains which add variable transaction fees and delays. Also, confidentiality is often lost.

With Half Epsilon One Time Spend Machine (OTSM), you can not only store and transfer digital assets in normal fashion, but also convert them to digital asset titles. These titles can be transferred with high security, confidentiality, and regulatory compliance. OTSM achieves these properties by enabling purely peer-to-peer transfers that do not require blockchains for transaction processing. This is achieved by a novel technique called *Localized Double-spend Prevention*. OTSM also allows regulated custodians to issue their own digital IOUs while maintaining custody of digital or physical assets.

Key Features and Benefits

- **LIGHTNING NETWORK:** Custodians operating OTSMs become part of the Half Epsilon Lightning Network. Digital asset title transfers among network members happen with high security, confidentiality, and regulatory compliance.

- **SWITCH BETWEEN DIGITAL ASSETS AND DIGITAL ASSET TITLES:** Custody solution users can easily convert digital assets to digital asset titles and vice-versa.

- **ISSUE DIGITAL IOUs:** Regulated custodians can issue their own digital IOUs while maintaining custody of digital or physical assets. For instance, a custodian may issue a stable-coin or a tokenized bond.

- **ONE TIME SPEND:** Our localized double-spend prevention technique prevents a digital asset title from being spent multiple times.

- **INTEGRATED KEY MANAGEMENT SERVICE (KMS):** OTSM has an integrated Key Management Service which enables secure generation, storage and use of millions of cryptographic keys.

- **COMPLETE PRIVACY:** End-to-end security for keys and protocol data (at-rest, in-transit, and in-use) protected with layers of defense and FIPS-validated hardware.

- **CENTRALIZED VISIBILITY AND CONTROL:** Centralized intuitive web-based user interface for management. Role-based access control (RBAC) for users, applications and groups with segregation of duties. Comprehensive tamper-proof audit logs to track all activity; including administration, authentication, access, and key operations.

- **ADVANCED ADMINISTRATION:** Single Sign-on support (SAML, OAuth, and Active Directory/LDAP). Auditing integration with SIEM tools (Syslog, Splunk, and CSP logging). Quorum approval policy (M of N) for enhanced protection.

- **CLOUD-SCALE PROTECTION:** Distributed scale-out architecture provides scalable performance on demand. Simplified operations with built-in synchronization, high availability and disaster recovery.

Use Cases

- **DIGITAL ASSET MANAGEMENT:** OTSM delivers unmatched security and availability for digital assets and titles including support for powerful yet easy to use policies for multi-sig with quorum approval, and strong access control.

- **SUPPORT FOR OTC TRADES:** Digital assets can be transferred over-the-counter in a peer-to-peer manner without intermediaries. Transfers are confidential. This opens an unprecedented opportunity for OTC markets where various tokenized financial instruments could be traded OTC.

- **CONFIDENTIAL DE-FI:** It is possible to develop confidential versions of various DeFi protocols. In addition to confidential payments, the Half Epsilon Network can support the flow of various other DeFi instruments, e.g., AMM pool shares.

- **GLOBAL STABLECOIN PAYMENTS:** VASPs on the Half Epsilon Lightning Network can facilitate the transfer of stable-priced Digital Assets (rather their titles) at low or no cost. The transfers will be instant and regulation compliant. Transferring small values across borders has always been a challenge and the Half Epsilon Lightning Network can facilitate this use case.

- **INTER-BANK SETTLEMENT COINS AND WHOLESALE CBDC:** Settlement coins and Central Bank Digital Currencies (CBDC) can be transferred in a peer-to-peer manner without intermediaries. Transfers are secure, regulation compliant, and confidential.

OTSM vs. Traditional HSM Solutions

Feature/Attribute	OTSM	Traditional HSM
1. Total cost of ownership	Predictable all-inclusive model, no additional costs for connectors	Needs specialized expertise required to maintain complicated pricing based on multiple variables.
2. Security	FIPS 140-2, security extends to KMS, authentication, authorization	FIPS 140-2, security limited to keys and key operations
3. Horizontal Scalability	Infinitely Scalable	Not Scalable
4. Performance	Single node 25% faster than fastest HSM, and then increases linearly with size of cluster	Limited based on hardware configuration
5. High Availability	Built-in redundancy and fault tolerance in cluster	Generally achieved by replicating HSMs, done using client's help.
6. Seamless disaster recovery and backup	Built-in	Not available
7. Multi-user support	Integrates with single-sign on, authorization using RBAC, advanced quorum control	Not available
8. Localized double-spend prevention	Built-in	Not available
9. Audit Logs	Secure, comprehensive, tamper proof	No audit logs for key operations, some support for getting appliance health information