[MPCH]

WHITE PAPER

The Key Decision: How GSIBs Should Approach Key Management on Canton

Explore how GSIBs can secure Canton operations through robust key management, enforced signing policies, and resilient infrastructure. Learn how MPCH Stronghold KMS protects institutional control while supporting flexible deployment models.

As GSIBs prepare to participate in institutional initiatives on Canton, including tokenized collateral, one infrastructure decision deserves attention early: how the institution will control and protect its cryptographic keys.

On Canton, those keys do more than secure access. They define the institution's identity on the network and determine its authority to act. Every transaction a node authorizes ultimately depends on them.

For a bank, that makes key management more than a technical implementation decision. It becomes a question of governance, operational control, auditability, and resilience.

And those decisions need to be made before the node goes live.

Start With the Questions Risk and Security Teams Will Ask

Any GSIB evaluating key infrastructure for Canton should be able to clearly answer three questions:

- Who can authorize a signature?
- How is that authority enforced?
- How can the institution prove it?

Simply storing keys securely is not enough.

The infrastructure surrounding those keys needs to enforce the bank's own approval policies, maintain separation of duties, and create an immutable record of signing activity.

That means looking beyond basic key storage and considering the full lifecycle surrounding every signing request.

At MPCH, that includes keys generated and maintained inside FIPS-validated HSMs, bank-configured approval mandates that act as hard gates before signing, independent validation of key ownership, and immutable audit records covering signing requests and key events.

Not Every Canton Key Should Be Treated the Same

One of the most important distinctions for institutions operating on Canton is between the node's root namespace key and the operational keys used for day-to-day activity.

The root namespace key anchors the node's identity and cannot simply be rotated if compromised. That makes its security requirements fundamentally different from keys that need to remain available for continuous protocol signing.

A strong institutional architecture should account for both.

The root key can be maintained cold and offline, while operational keys remain protected within HSMs and available for the activity the network requires.

The important question for a GSIB is not simply, "Where are our keys stored?"

> **What level of protection does each key require, and how do we maintain consistent governance across both hot and cold environments?**

Separate the Node From Signing Authority

There is another architectural decision institutions should consider carefully: whether compromising the node could also compromise the institution's ability to authorize transactions.

MPCH approaches this with Stronghold KMS by separating signing authority from the Canton node.

The bank's node prepares and submits transactions and maintains ledger state. MPCH performs the gated signing step. This means the node itself cannot independently bypass the bank's established approval policy.

That separation also allows MPCH to maintain a deliberately narrow role.

MPCH does not hold the bank's assets, operate its wallets, tokenize assets, broadcast transactions, settle transactions, or report balances. The bank retains control of those functions while MPCH focuses specifically on protecting keys and enforcing signing policy.

For institutions evaluating third-party infrastructure, that distinction matters.

Build for the Environment Canton Is Creating

Institutional digital asset infrastructure cannot assume traditional banking hours.

Tokenized collateral and repo markets can operate beyond them, which means the systems protecting signing authority need to be designed around availability and recovery as well as security.

MPCH Stronghold KMS operates active infrastructure with HSMs located in separate secure facilities, real-time replication of key metadata, and documented disaster recovery and recovery testing.

The goal is not simply to protect a key from compromise.

It is to make sure institutions retain controlled access to their infrastructure when they need it.

There Isn't One Deployment Model for Every Bank

GSIBs also differ in how much infrastructure they want to operate or physically control.

Some institutions may prefer a fully managed model. Others may require an independently held copy of their cold root key. Others may need hardware deployed inside their own facilities for physical control or data-residency requirements.

MPCH supports all three approaches:

- **Fully managed:** MPCH operates the hot HSM environment and cold root-key storage.
- **Bank-held cold-key copy:** the managed service remains in place while the institution maintains its own copy of the cold root key.
- **On-premises:** MPCH hardware is deployed within the bank's facility and operated by MPCH.

Across those models, the underlying controls, audit approach, and assurance remain consistent.

Evaluating the Available Approaches

There are several ways institutions can approach key management on Canton. The right model depends on the bank's existing infrastructure, internal control requirements, and operational resources.

Why MPCH Is the Right Choice

APPROACH	WHAT GSIBS SHOULD CONSIDER	HOW MPCH STRONGHOLD KMS COMPARES
Turnkey wallet provider	Determine whether the node, keys, and signing policy sit with the same third party, and whether that structure meets internal key-control requirements.	MPCH manages keys and signing only. The bank keeps its node, its assets, and its signing policy.
Cloud KMS	Evaluate how cold root-key storage, approval workflows, audit evidence, and recovery will be handled beyond the core KMS.	MPCH delivers cold root-key storage, enforced approvals, immutable audit, and tested recovery as one service.
Build in-house	Consider the integration timeline, HSM expertise, ongoing operations, resiliency, and support requirements.	MPCH is a running service with active-active resilience and full operational support, including an on-premises option.
Purpose-built key management	Evaluate whether hot and cold key management, policy enforcement, auditability, recovery, and deployment flexibility can be managed under one architecture.	MPCH meets every one of these requirements under a single architecture, backed by SOC 2 Type II and ISO/IEC 27001.
MPCH Stronghold KMS	Meets every consideration above in one service.	Hot and cold keys, enforced approval mandates, dual independent checks, immutable audit, active-active recovery, three deployment models, and no custody. The bank keeps control of its node and assets.

How MPCH approaches it: MPCH combines hot and cold key management, enforced approval mandates, immutable audit records, and multiple deployment models while keeping the bank's node and assets under the bank's control.

MPCH builds and operates its platform in-house and already manages Canton validator keys in production. It understands both the cryptography and the network.

The Decision Should Happen Before Go-Live

Key management is difficult to treat as an afterthought.

The architecture chosen during node setup determines how the institution protects its identity, governs signing authority, demonstrates control to auditors, and recovers when something goes wrong.

That is why institutions preparing for Canton initiatives should evaluate key hierarchy, approval mandates, hot and cold key requirements, audit evidence, recovery procedures, and deployment

architecture before going live.

MPCH already manages Canton validator keys in production and has built its platform and operations around these requirements.

The question that remains for institutions preparing to participate on Canton is not simply whether their node will be ready.

> **It's whether the infrastructure protecting the keys behind that node will be ready too.**

A Purpose-Built Approach to Infrastructure Keys: Securing the Network Beyond the Assets

MPCH Stronghold KMS is developed for the management of authority keys used by infrastructure such as blockchain validators, certificate authorities, and signing systems.

Critical keys shouldn't have to rely on public-cloud infrastructure alone. Hardware Security Models (HMS's), combined with offline protection for root keys stored cold within geographically diverse military grade facilities on two continents along with tightly controlled key operations can provide a stronger foundation for securing network-level trust.

The architecture is designed to scale from startups to the largest banks in the world requiring FIPS 3 Level 3 hardware, fully immutable audit logging and multiple site redundancy where operational continuity matters. Explore the platform: https://mpch.com/stronghold-kms.

About MPCH

MPCH is a trusted third-party cybersecurity infrastructure company providing high-assurance cryptographic key management, operational continuity, and disaster recovery for institutional tokenization, enterprise, and mission-critical environments. The MPCH platform unifies hot and cold key management, HSM integration, policy-based controls, and resilient offline-capable architectures, grounded in zero-trust cryptographic design. MPCH's defense subsidiary, Ti22, builds technologies that enable governments and institutions to adopt AI without surrendering execution controls or exposing their operations, re-establishing human control and privacy over money, agents, and data. Together, MPCH and Ti22 secure the cryptographic foundations of institutional and national security infrastructure worldwide. For more information, visit www.mpch.com.