SplitSecure

# Digital Asset Custody Operations & Control

## Context

As banks and regulated financial institutions expand into digital asset custody, regulators increasingly focus on **demonstrable control over cryptographic keys** governing client assets. Regulations like DORA, MiCA, or FINMA, or industry standards like DASCP, require enterprises working with digital assets to maintain stricter security controls. Unlike traditional securities custody, loss or misuse of private keys is irreversible and exposes institutions to direct fiduciary, financial, and reputational risk.

## Problem

Current generation custody architectures rely on:

- Single-party key control (even if operationally distributed)
- Vendor-managed key infrastructure
- Procedural controls without cryptographic enforcement

These models make it difficult for institutions to prove that no individual or system can unilaterally move client assets, including internal administrators or the custodian itself.

## Key Requirements

- Enforced multi-party or multi-entity authorization for asset movement
- Elimination of persistent, unilateral signing keys
- Cryptographic proof that custody policies were followed
- Compatibility with existing custody platforms and workflows

## How SplitSecure Addresses the Use Case

SplitSecure introduces a cryptographic control-integrity layer above or alongside custody signing systems. Asset-movement authorization requires coordinated approval from multiple independent entities or devices, with no single actor ever possessing a complete signing secret.

That means that even if a device is fully compromised, it is not possible for the attacker to extract the protected information. It also means that if an employee falls for a social engineering attack (or clicks on a link in an email) there is no way for them to expose the protected data.

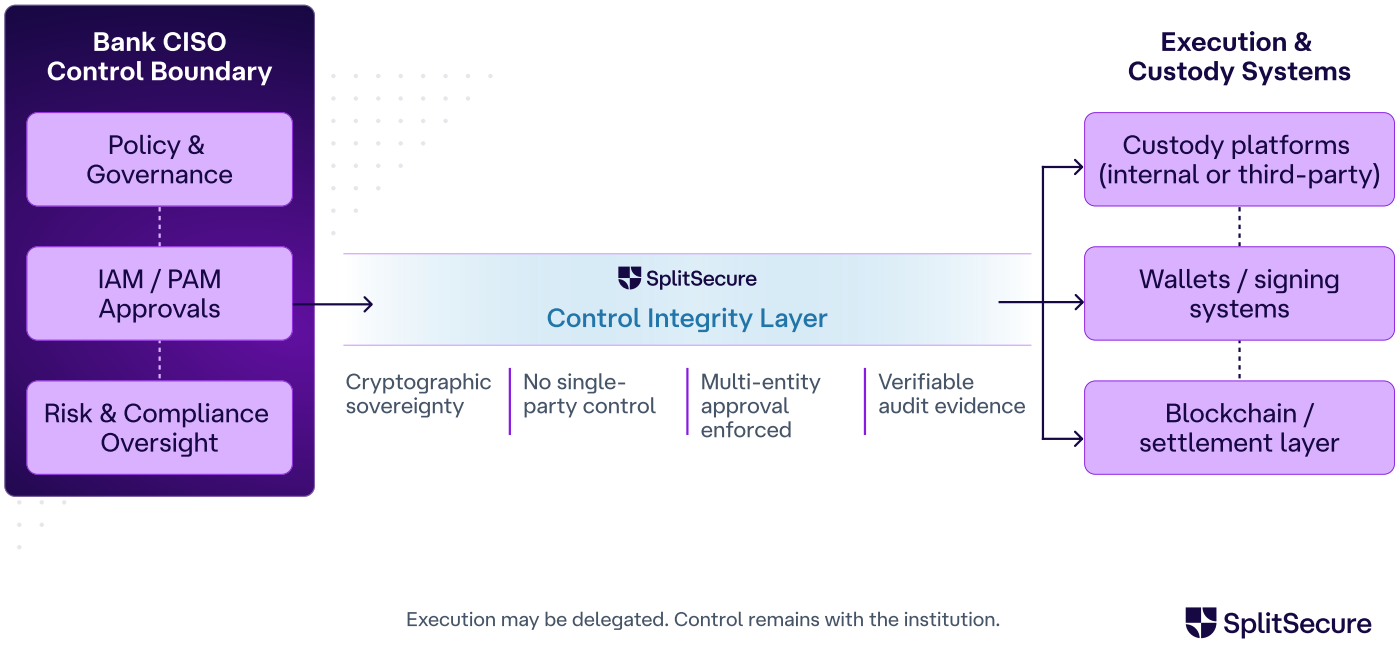
Our solution is quantum-resistant, and offers protection from zero-day vulnerabilities (as the multiple approving entities can be heterogeneous). This is the security standard digital assets demand, and it allows enterprises to future-proof.

## Differentiation

- No persistent private keys held by any individual or system
- Control policies enforced cryptographically, not procedurally
- Verifiable evidence suitable for regulator and auditor review
- Custodian-agnostic and infrastructure-neutral

## Buyer Impact

Enables institutions to offer digital asset custody with provable fiduciary control, reduced insider risk, and regulator-grade assurance without redesigning their custody stack.




## Digital Asset Custody: Regulatory Control Requirements Addressed by SplitSecure

Across the EU, UK, Switzerland, U.S., and Singapore, regulators converge on a single expectation for digital asset custody: institutions must be able to prove that no individual, system, or vendor can unilaterally move client assets. The cited frameworks explicitly support this interpretation, and SplitSecure aligns by replacing procedural trust with cryptographic enforcement and verifiable evidence.

| Jurisdiction | Regulation / Framework | Regulatory Emphasis | How SplitSecure Aligns |
|---|---|---|---|
| **European Union** | DORA – Digital Operational Resilience Act Source: ESMA / EIOPA | ICT risk management, elimination of single points of failure, demonstrable operational controls, auditability of critical functions | Removes unilateral control through cryptographic multi-entity authorization; no persistent keys; produces tamper-evident, regulator-grade evidence of enforced controls |
| **European Union** | MiCA – Markets in Crypto-Assets Regulation Source: ESMA | Safekeeping of client crypto-assets, governance over private keys, prevention of misuse or loss, operational resilience for CASPs | Enforces cryptographic custody policies; prevents custodian, admin, or vendor unilateral asset movement; aligns with MiCA expectations for effective control |
| **Switzerland** | FINMA Guidance on Crypto-Based Asset Custody (FINMA Guidance 01/2026) Source: FINMA (PDF) | Clear allocation of control, segregation of duties, prevention of key misuse, demonstrable internal safeguards | Cryptographic separation of authority across independent entities; no single signer exists; control integrity is provable rather than procedural |
| **United Kingdom** | FCA Cryptoasset Custody & Safeguarding Regime (FSMA), Related consultation (custody) | Asset safeguarding, governance and oversight, third-party and outsourcing risk, supervisory evidence of control | Custodian-agnostic cryptographic control layer; removes trust in vendors or individuals; produces independent evidence supervisors can assess |
| **United States** | SEC Custody Rule (as applied to crypto) & supervisory guidance. Explainer on SEC no-action position and custody expectations | Protection against misappropriation, insider abuse, and loss of client assets; auditable custody controls | Eliminates administrator key risk; enforces multi-entity authorization cryptographically; supports defensible custody attestations |
| **Singapore** | MAS Digital Asset Custody Expectations / Project Guardian principles Source: MAS – Project Guardian | Institutional-grade safeguards, prevention of unilateral asset movement, control integrity for tokenised assets | Aligns with "trust anchor" and control-integrity concepts via distributed cryptographic authorization independent of any single system |
| **Global / Industry** | DASCP – Digital Asset Security Control Principles, industry standard custody & control | Defense-in-depth key management, elimination of single points of compromise, continuous assurance | Native fit: no persistent private keys; heterogeneous approval entities; continuous cryptographic enforcement rather than policy claims |

## Built by leaders in security engineering.

Tristan Morris is a security engineering prodigy who started attending college at age 12. After graduating from Cornell, he went on to lead Federal Security at KNOX, Samsung's military and defense cybersecurity group.

**Tristan Morris**
Cofounder & CEO

Marc Tremblay has been a security engineer on some of the most capable and prestigious security teams in the world, including the core security teams of Netflix and Stripe. He has six patents for security technology.

**Marc Trembley**
Cofounder & CTO