TARGET AUDIENCE: EXECUTIVE AND SENIOR MANAGEMENT

Stablecoin and Crypto Asset Wallet Types

Custody and Security Requirements

Governance Under PCI DSS, ISO/IEC 27001, ISO/IEC 42001, NIST CSF, and the EU AI Act

---

By Kim | CISO
Chief Information Security Officer | CyAN Member
linkedin.com/in/kimabdalian
06 August 2026

Executive Summary

Stablecoins and tokenized cash equivalents have moved from experimental instruments to core payment rails, with market capitalization exceeding 300 billion US dollars and regulators across the EU, the United States, and the GCC now treating issuer and custodian security as a supervisory priority rather than an afterthought. For a CISO, the practical question is no longer whether the organization will touch digital assets, but whether the wallet architecture, key management lifecycle, and reserve custody model can withstand regulatory examination and adversarial pressure at the same time.

This paper sets out the five recognized wallet classes and four custody models in use today, maps the controls a CISO must operationalize across PCI DSS, ISO/IEC 27001, ISO/IEC 42001, NIST CSF, and the EU AI Act, and closes with board-level recommendations for organizations issuing, custodying, or settling in stablecoins and other crypto assets.

Introduction

Digital asset custody differs from traditional financial custody in one decisive respect: control of a private key is equivalent to control of the asset itself, with no reversal mechanism once a transaction is signed and broadcast. This makes wallet architecture and key management the single highest-priority control domain in the stack, ahead of network security, application security, or fraud analytics, because a failure at the key layer is typically irrecoverable.

At the same time, AI-enabled monitoring, anomaly detection, and transaction risk scoring are becoming standard components of custody platforms. That shift pulls a second governance layer into scope for CISO: ISO/IEC 42001 and the EU AI Act now apply wherever an AI system materially influences a custody, minting, or sanctions-screening decision. This paper treats digital asset security and AI governance as a single overlapping control problem, because in practice they increasingly are.

Wallet Architecture and Custody Models

Five wallet classes now cover essentially all production digital asset deployments, each with a distinct exposure profile. The relative exposure ranking below (Figure 1) reflects attack surface and reversibility of loss, not asset value.

Wallet Class	Connectivity	Typical Use	Primary Control
Hot wallet	Always online	Exchange liquidity, daily settlement	Withdrawal limits, velocity checks, 90-day key rotation
Warm / MPC wallet	Limited, policy-gated	Treasury operations, liquidity buffer	Threshold signatures (m-of-n), time locks
Cold wallet	Air-gapped, offline	Long-term reserves	Hardware wallet, geographic vault separation
MPC operational wallet	Online, no single key exists	Day-to-day operational signing	Distributed key shares, secure enclave signing
HSM-backed wallet	Online, hardware-enforced	Regulated institutional custody	FIPS 140-3 Level 3+, tamper-evident hardware

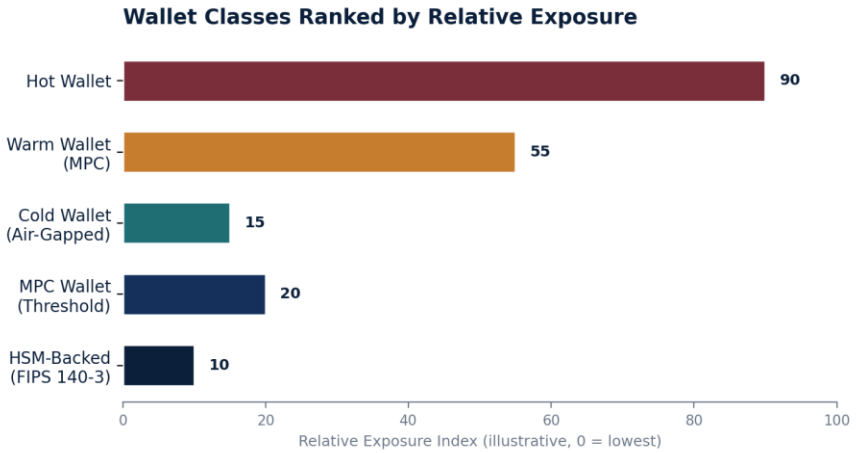

Figure 1: Wallet classes ranked by relative exposure (illustrative index).

Custody Model Selection

Self-custody: User or firm holds keys directly. *Not acceptable for institutional balance sheets; no regulatory recognition in most GCC and EU frameworks.*

Qualified custodian: Regulated third party holds keys under statute. *Required for institutional clients under most Central Bank virtual asset regimes.*

Hybrid custody: MPC plus HSM plus multi-signature. *Current industry standard for exchanges, issuers, and institutional custodians.*

Smart contract custody: On-chain multi-signature or DAO treasury logic. *Transparent but exposed to governance and oracle manipulation attacks; use with caution.*

Regulatory posture increasingly dictates the choice: Central Bank virtual asset frameworks across the GCC, alongside the EU Markets in Crypto-Assets Regulation, now require qualified or hybrid custody for any institution holding client assets, effectively closing the door on unsupervised self-custody at scale.

Key Management Lifecycle

Because possession of a private key is equivalent to ownership, the key management lifecycle carries more residual risk than any other control domain in a digital asset program. Five stages require documented, auditable controls.

Generation: Formal, witnessed key ceremonies with hardware-verified randomness and multi-stakeholder sign-off.

Storage: Private key material never exposed in plaintext; FIPS 140-3 Level 3+ hardware security modules for production operations.

Rotation: Mandatory rotation cadence for hot and warm wallets, with immediate rotation on any suspected compromise or personnel change.

Segmentation: The large majority of reserves held in air-gapped cold storage; only a small operational float held in warm or hot wallets.

Recovery: Documented, tested break-glass procedures using threshold secret sharing across geographically distributed shard holders.

Stablecoin Reserve Security and Attestation

A stablecoin is only as trustworthy as the custody and disclosure regime protecting the assets that back it. Boards should expect three controls as a baseline: reserve assets held with approved, segregated custodians with daily reconciliation; independent, periodic attestation of reserve adequacy; and mint and burn authorization that requires multi-party approval, so that no single actor can create or destroy tokens unilaterally.

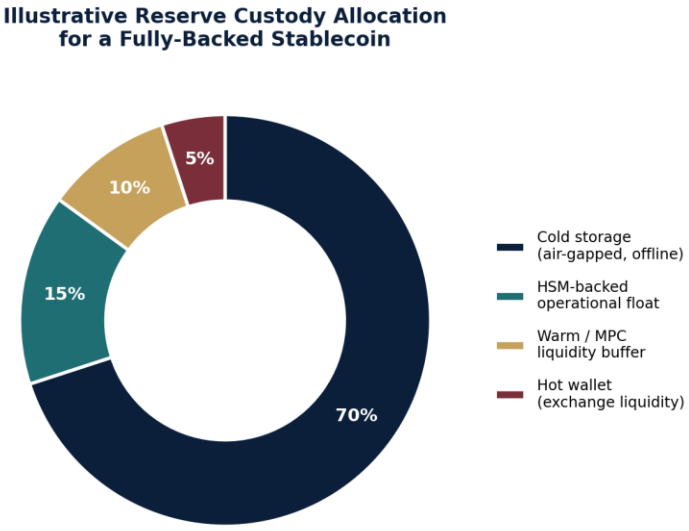

Figure 2: Illustrative reserve custody allocation for a fully backed stablecoin.

Regulatory Governance Overlay

Digital asset custody now sits at the intersection of five frameworks that most institutions already hold or are pursuing. PCI DSS v4.0, ISO/IEC 27001:2022, and NIST CSF 2.0 govern the technical security baseline; ISO/IEC 42001:2023 and the EU AI Act govern the AI systems increasingly embedded in transaction monitoring, sanctions screening, and anomaly detection within custody platforms. The table below traces each wallet custody control introduced earlier in this paper to the clause, requirement, or subcategory that governs it, so examiners and auditors can move directly from control to evidence.

Wallet Custody Control	PCI DSS v4.0	ISO 27001:2022	ISO 42001:2023	NIST CSF 2.0	EU AI Act 2024/1689
HSM key generation and storage	Req. 3.5–3.7	A.8.24	N/A	PR.DS	N/A
MPC threshold signing (m-of-n)	Req. 3.6	A.8.24, A.5.17	N/A	PR.AC	N/A
Cold storage segregation	Req. 3.6	A.8.24, A.5.9	N/A	PR.DS	N/A
Key rotation and break-glass recovery	Req. 3.7, 12.10	A.5.17, A.5.26	N/A	PR.DS, RC.RP	N/A
Reserve custody and daily reconciliation	Req. 9.4	A.8.12, A.8.13	N/A	DE.CM	N/A
Mint / burn multi-party authorization	Req. 7.2, 8.3	A.5.15, A.8.2	N/A	PR.AC	N/A
AI-enabled withdrawal anomaly detection	N/A	A.5.9 (asset scope)	Clause 6.1, 8.2	DE.AE	Art. 9, 13
AI-enabled sanctions / KYC screening	Req. 12.8	A.5.19 (suppliers)	Clause 8.3	ID.RA	Art. 14
Custody incident response	Req. 12.10	A.5.24–A.5.28	Clause 10.1	RS.RP, RC.RP	Art. 26

Figure 3: Wallet custody controls mapped to PCI DSS v4.0, ISO/IEC 27001:2022, ISO/IEC 42001:2023, NIST CSF 2.0, and the EU AI Act (2024/1689). N/A indicates the control sits outside that framework's scope.

Why AI Governance Now Belongs on This Map

Custody and treasury platforms increasingly rely on AI-enabled monitoring to flag anomalous withdrawal patterns, score counterparties, and support sanctions screening. Once such a system materially influences a custody or transaction decision, it falls within scope of ISO/IEC 42001's AI management system requirements and, in the European Union, the AI Act's obligations for high-risk AI systems.

The regulatory timeline has moved recently and CISOs should track it directly rather than rely on the original 2024 schedule. *Following the Digital Omnibus on AI approved by the European Parliament in June 2026, compliance obligations for standalone high-risk AI systems under Annex III (the category most custody-monitoring tools would fall under) were deferred from 2 August 2026 to 2 December 2027, with Annex I product-related obligations deferred to August 2028.* The deferral is a scheduling relief, not a scope reduction; institutions with EU exposure should continue building AI governance capability, including model documentation, human oversight, and post-market monitoring, ahead of the revised deadlines.

Recommendations for Boards and Senior Management

- Mandate hybrid custody (MPC plus HSM plus multi-signature) as the default model for any institutional balance sheet; treat self-custody and unsupervised smart contract custody as exceptions requiring board-level risk acceptance.
- Place key management lifecycle controls (generation, storage, rotation, recovery) under second-line CISO oversight with independent audit rights, not solely under the technology function that operates the wallets.
- Require independent, periodic reserve attestation for any stablecoin the organization issues or accepts at scale, with Merkle-proof or equivalent real-time verification where feasible.
- Bring AI-enabled monitoring and screening tools into the same governance register as the wallets they protect, mapped explicitly to ISO/IEC 42001 and EU AI Act obligations rather than treated as a technology procurement decision.
- Rehearse break-glass key recovery at least annually, with geographically distributed shard holders, and treat the exercise as a board-reportable resilience control under ISO 22301 business continuity requirements.
- Map every custody and key management control explicitly to PCI DSS v4.0, ISO/IEC 27001:2022, and NIST CSF 2.0 subcategory references so that examiners and auditors can trace evidence directly, rather than relying on narrative assurance.

Closing Note

Digital asset custody rewards institutions that treat key management as a governance discipline rather than a purely technical function. The organizations best positioned for the next wave of stablecoin adoption and regulatory scrutiny are those that have already aligned wallet architecture, custody model, and AI governance under a single, board-visible control framework.

About the Author

Kim | Chief Information Security Officer
CISM, CCSP, CDPO, CBCMP | linkedin.com/in/kimabdalian

Kim is a Chief Information Security Officer with more than 28 years of experience in information security leadership, including over 20 years within GCC Central Bank-regulated financial institutions. His scope spans information security strategy, risk assessment, IT governance, and crypto and virtual asset security, with a sustained track record of continuous PCI DSS certification with zero critical findings.

He has led AI governance and EU AI Act implementation programs, maintains working alignment across NIST CSF, ISO/IEC 27001, ISO/IEC 42001, and ISO 22301, and holds specializations in AI Governance and ISO 42001 Readiness (BSI) and Blockchain Security. Kim is an ISACA Platinum Member, a Member of the Pakistan Engineering Council (MPEC), a Member of the Cyber Security Advisors Network (CyAN), and a Cyberr® member.

Disclaimer

This white paper reflects the professional views and independent analysis of the author and does not constitute legal, regulatory, financial, or investment advice. Frameworks, thresholds, and regulatory timelines referenced herein, including the EU AI Act, are subject to ongoing amendment; readers should confirm current requirements with qualified legal counsel and the relevant regulator before acting. The views expressed are the author's own and do not represent the official position of any employer, client, or organization with which the author is affiliated.

References

[1] PCI Security Standards Council, Payment Card Industry Data Security Standard, Version 4.0.1, Jun. 2024.

[2] International Organization for Standardization, ISO/IEC 27001:2022, Information Security, Cybersecurity and Privacy Protection, Information Security Management Systems, Requirements. Geneva, Switzerland: ISO, 2022.

[3] International Organization for Standardization, ISO/IEC 42001:2023, Information Technology, Artificial Intelligence, Management System. Geneva, Switzerland: ISO, 2023.

[4] National Institute of Standards and Technology, The NIST Cybersecurity Framework (CSF) 2.0, NIST Cybersecurity White Paper NIST CSWP 29, Feb. 2024.

[5] European Parliament and Council of the European Union, Regulation (EU) 2024/1689 Laying Down Harmonized Rules on Artificial Intelligence (Artificial Intelligence Act), Jun. 2024.

[6] European Parliament, Approval of the Digital Omnibus on Artificial Intelligence, Jun. 16, 2026.

[7] European Parliament and Council of the European Union, Regulation (EU) 2023/1114 on Markets in Crypto-Assets (MiCA), May 2023.

[8] Financial Action Task Force, Updated Guidance for a Risk-Based Approach to Virtual Assets and Virtual Asset Service Providers, 2026 update.

[9] Central Bank of Bahrain, Crypto-Asset Module (CRA), Rulebook Volume 6, current edition.

[10] OWASP Foundation, Smart Contract Top 10, 2026 edition.

[11] National Institute of Standards and Technology, Recommendation for Key Management, NIST SP 800-57 Part 1 Rev. 5.