BALDIVICIO & CO.

ISO 11568 Key Management Compliance

Document Title
Baldivicio ISO 11568 Key Management Compliance Paper

Document Type
Standards-oriented compliance and control narrative

Subject
Key-management governance, custodial control, operational safeguards, and lifecycle treatment

Effective Date
April 13, 2026

1. Introduction

This paper explains Baldivicio's key-management posture through the lens of ISO 11568 key-management principles as they relate to retail financial services and custodial digital-asset operations. It is intended to provide a structured and comprehensive account of how Baldivicio's service model, custody design, operating controls, transaction controls, security measures, compliance processes, and continuity practices support disciplined management of cryptographic key responsibility within the Baldivicio environment.

Baldivicio is a digital financial services platform made available primarily through its mobile application. Across its service and legal materials, Baldivicio states that it currently supports USDC-only activity on Ethereum Mainnet through a custodial model and that Baldivicio holds and manages the private keys associated with supported wallet functionality on behalf of users. Users do not receive, possess, or export private keys. These statements are foundational to Baldivicio's key-management position and are central to this paper.

This paper is written as a control and governance document. It is not a customer marketing piece, not a product feature announcement, and not a substitute for detailed engineering specifications. Its purpose is to articulate, in standards-oriented language, what Baldivicio's service model establishes about key responsibility, key use, control boundaries, transaction authorization, incident response, recordkeeping, continuity, and related governance matters.

2. Purpose and Objectives

The purpose of this paper is to document how Baldivicio's custody and operational framework aligns with the core concerns addressed by ISO 11568 in relation to key management. Those concerns include responsibility for cryptographic key control, protection of key confidentiality, control over key use, traceability of financial operations, operational integrity, incident handling, and the relationship between key management and broader service governance.

The objectives of this paper are fourfold.

First, it establishes that key responsibility within Baldivicio is centrally assigned to Baldivicio as custodian rather than to the end user.

Second, it explains how Baldivicio's broader control framework supports controlled use of custodial wallet functionality through onboarding, identity verification, session and access controls, transaction review, restrictions, incident response, and account-lifecycle governance.

Third, it organizes those control themes in a way that is intelligible for standards, compliance, risk, and governance review.

Fourth, it sets out the functional boundaries of the documented key-management model without making technical claims beyond what Baldivicio's policies, disclosures, and service descriptions support.

3. Scope

This paper applies to Baldivicio's documented custodial wallet environment, mobile application context, supported USDC activity on Ethereum Mainnet, transaction-handling framework, account lifecycle, compliance review processes, outage and degradation response, account restriction and closure processes, and privacy and recordkeeping practices to the extent those matters bear on key management.

It therefore covers key-management governance as reflected in:

- the custodial service model;
- account creation and identity verification controls;
- protected access and transaction authorization controls;
- supported transfer processing and pre-execution review;

- service restrictions, suspensions, freezes, and closures;
- outage, degradation, and emergency response measures;
- privacy, logging, monitoring, and record-retention practices relevant to evidentiary support and operational traceability; and
- third-party dependencies where they affect connected service operations.

This paper does not redefine Baldivicio's public legal terms. It should be read consistently with Baldivicio's Terms of Service, Acceptable Use Policy, Deposit Insurance Disclosure, Reserve and Transparency Attestation, Customer Identification Program Notice, E-Sign Consent and Electronic Communications Agreement, Fee Schedule and Schedule of Charges, Irreversible Transactions Disclosure, System Outage and Degradation Policy, Account Suspension, Freezing, and Closure Policy, and Privacy Policy.

4. Service Context Relevant to ISO 11568

ISO 11568 is concerned with secure and disciplined management of cryptographic keys in financial-service environments. Within Baldivicio, the relevance of that framework arises from the fact that the service is custodial, transaction-bearing, and security-sensitive.

Baldivicio's published service model establishes that supported balances and supported transaction functionality are delivered through Baldivicio's custodial systems rather than through user-controlled key possession. The service also establishes that access to financial functionality depends on account status, identity verification, fraud review, security checks, transaction review, and service continuity. This means key management in Baldivicio is not merely a narrow cryptographic function. It is part of a larger operational structure that binds key responsibility to security, compliance, transaction integrity, service resilience, and user protection.

For ISO 11568 purposes, Baldivicio's model is best understood as a centralized custodial key-management environment supporting retail-facing digital financial services. The user interacts with an account and a service. Baldivicio, as custodian, retains responsibility for the keying material that underpins supported wallet operations.

5. Foundational Key-Management Position

Baldivicio's foundational key-management position is straightforward: Baldivicio holds and manages the private keys associated with supported wallet functionality, and those keys are not exported to users.

This statement has several important consequences.

It means that key custody is centralized inside Baldivicio's service environment. It means the user experience is intentionally separated from direct private-key possession. It means transaction capability is mediated through Baldivicio's systems, controls, and workflows rather than through raw end-user signing authority. It also means Baldivicio bears the responsibility for ensuring that key-related financial operations are governed by appropriate operational safeguards, account controls, review mechanisms, and service-protection processes.

This control model is consistent with Baldivicio's broader description of itself as a digital financial services platform that combines security, compliance, and usability. In a standards-oriented reading, the key-management function is inseparable from the account-control and transaction-control framework through which the service is delivered.

6. Key-Management Governance Principles Applied by Baldivicio

Within Baldivicio's custodial model, key management is governed by a set of principles that are clearly supported by the service framework.

The first principle is custodial responsibility. Baldivicio, not the user, is the controlling party for the private keys associated with supported wallet functionality.

The second principle is restricted key exposure. Users do not receive, possess, or export private keys. This materially narrows user-side key-exposure pathways and confirms that cryptographic control remains within the service boundary.

The third principle is controlled invocation. Supported transaction functionality is processed through Baldivicio's account controls, custodial systems, and related operational processes. This means key use is linked to service controls rather than being directly exposed as a user-managed cryptographic act.

The fourth principle is conditional execution. Transactions may be delayed, reviewed, limited, refused, or otherwise conditioned before execution based on fraud checks, compliance review, account state, operational checks, blockchain conditions, destination restrictions, and service integrity considerations.

The fifth principle is operational traceability. Baldivicio's policies establish that transaction handling, account state, review status, communications, access records, and service events are subject to monitoring, recordkeeping, and evidentiary preservation measures.

The sixth principle is security intervention authority. Baldivicio may restrict, suspend, freeze, review, or close accounts; delay or refuse transactions; conduct incident-response actions; and apply additional verification, reconciliation, or protective controls where necessary.

The seventh principle is continuity-aware custody. Because the custodial model depends on Baldivicio's systems and operational continuity, outage response, degradation response, emergency intervention, and post-incident reconciliation are integral to the overall key-management control environment.

7. Roles and Responsibility Allocation

Within Baldivicio's documented service model, responsibility for key-related control is allocated in a clear and deliberate way.

Baldivicio is responsible for holding and managing the private keys associated with supported wallet functionality. Baldivicio is also responsible for the operation of the custodial environment through which supported balances, supported transfers, transaction review, and account-state enforcement occur. That responsibility necessarily extends to the secure governance of key use, the maintenance of operational controls, the enforcement of account restrictions, and the preservation of service integrity.

Users are responsible for lawful and accurate use of the service, safeguarding their credentials and devices, reviewing transaction details before submission, complying with onboarding and verification requirements, and promptly reporting suspected unauthorized access, compromise, fraud, or suspicious activity. Users are not assigned direct cryptographic key responsibility within the custodial model.

Third-party providers such as Banxa may participate in connected service functions involving funding, payout, conversion, or settlement, but Baldivicio's documentation does not characterize those providers as holders of user-exported private keys within the Baldivicio custodial model. Their role is instead described in relation to connected workflows, approvals, processing, and settlement dependencies.

8. Key Lifecycle Treatment

ISO 11568 addresses key management across the full key lifecycle. Within Baldivicio, that lifecycle is best understood through the custody and service model described across the platform documentation.

Key establishment and provisioning occur within Baldivicio's custodial environment rather than at the user level. The service does not expose private-key creation, import, or export to users. Supported wallet functionality is therefore established under Baldivicio's control as part of the service model.

Key custody is maintained as part of Baldivicio's custodial wallet framework. The documentation makes clear that access to balances and supported transactions depends on Baldivicio's custodial systems, operational controls, and service continuity. This means key retention and control are inseparable from the service's controlled operating environment.

Key use occurs through governed transaction workflows rather than through direct end-user cryptographic possession. Users submit transaction instructions through the service. Baldivicio may validate, review, delay, restrict, or refuse those instructions before execution. Once permitted and executed, transaction finality may follow the conditions described in the Irreversible Transactions Disclosure.

Key replacement, withdrawal from service, or other lifecycle changes are not described in technical detail in the public-facing service framework. Instead, the governance position is that Baldivicio maintains responsibility for key-related operational integrity throughout account lifecycle events, security events, restriction scenarios, service incidents, and closure processes.

Key destruction, archival, or retirement procedures are not described in implementation-specific terms in the service framework. What is described is the broader governance environment for records, retention, account closure, restriction, preservation, and service continuity. This paper therefore treats those lifecycle elements at the level of governance principle rather than technical mechanism.

9. Key Confidentiality

Key confidentiality is a central requirement of Baldivicio's custodial model. Although the platform documentation does not present a hardware-by-hardware or algorithm-by-algorithm description of how private keys are protected, the documented service posture strongly supports the conclusion that private keys are intended to remain confidential within Baldivicio-controlled systems.

The most important expression of this is the non-exportability of private keys. Users do not receive, possess, or export those keys. This design sharply limits the possibility of direct user-side dissemination of keying material and confirms that private-key confidentiality is retained within the service boundary.

Additional support for the confidentiality objective appears in the platform's broader security framework. Baldivicio describes protected sign-in flows, secure credential handling, device-level trust signals, continuous checks supporting verification of account activity, authentication measures, access controls, monitoring, and incident-response measures. While these controls are broader than key confidentiality alone, they contribute to the environment in which confidential key use can be preserved.

The privacy framework also supports confidentiality through references to access controls, environment segregation, monitoring, encryption or protected transmission where appropriate, audit logging, vendor controls, and data minimization where reasonably practicable. In a key-management context, these are important environmental safeguards, even where the precise technical implementation of key storage is not described in public-facing materials.

10. Key Integrity and Controlled Use

In a custodial service, secure key management requires not only that keys remain confidential, but also that key use occur only within valid, authorized, and reviewable operational contexts.

Baldivicio's service materials strongly support this controlled-use principle. Transaction handling is described as prioritizing accuracy, authorization, and traceability. Requests are processed through controlled workflows. Account access depends on properly verified and authorized user states. Transactions may be delayed, reviewed, restricted, or refused before execution. Account restrictions, temporary holds, destination restrictions, enhanced review, and security measures may be applied where appropriate.

These controls establish that key use is not treated as an unmediated action. Instead, key-related transaction execution is conditioned on account validity, transaction review, operational state, security

checks, fraud review, and compliance considerations. That structure is directly relevant to ISO 11568 because it supports integrity of key use within a retail financial-service environment.

11. Transaction Authorization as a Key-Management Control

Baldivicio's model of transaction authorization is central to its key-management narrative.

The user does not directly sign blockchain transactions in a self-custodial sense. Rather, the user submits instructions through Baldivicio. Baldivicio may act on those instructions subject to account controls, review procedures, operational checks, security protections, and compliance measures. Before execution, a transaction may be pending, queued, under review, delayed, limited, or refused. After execution or completion, a transaction may become irreversible.

This distinction matters greatly for key management. It means that key invocation is embedded in a service-level authorization model. The authorization model incorporates account identity, transaction detail review, supported asset and network limits, destination accuracy, account restrictions, legal controls, and service integrity checks.

In effect, transaction authorization within Baldivicio acts as a gatekeeper around the custodial use of private keys. That arrangement is consistent with sound key-management governance in a custodial financial-service environment.

12. Account Lifecycle Controls and Their Relevance to Key Management

Baldivicio's account lifecycle framework is a meaningful part of its key-management posture.

The service is described as using structured account states from registration to activation and ongoing account use. The Customer Identification Program Notice, Privacy Policy, and system overview explain that onboarding includes identity verification, eligibility review, fraud controls, security controls, and, where necessary, additional documentation or escalation for review.

This is relevant to key management because the authority to access custodial functionality is not granted solely on the basis of app access or attempted login. It is bound to account state. Properly verified and authorized accounts may receive broader functional access; incomplete, unresolved, or suspicious accounts may be delayed, limited, reviewed, suspended, frozen, or closed.

That lifecycle-driven approach reduces the risk that custodial key-backed functionality is made available inappropriately. It also provides a clear governance bridge between identity assurance and controlled financial operation.

13. Access Security and Credential Safeguards

Although user credentials are distinct from custodial private keys, the security of account access materially affects the safe use of custodial functionality. For that reason, Baldivicio's access-security controls are part of the overall key-management environment.

Baldivicio's service framework refers to protected sign-in flows, secure credential handling, device-level trust signals, authentication events, session records, account access history, suspicious sign-in review, and risk signals derived from device, access, and technical information. Users are also expressly required to maintain credential confidentiality, use accurate information, notify Baldivicio of suspected unauthorized access, and cooperate with recovery or review requests.

These measures help ensure that the custodial use of keys occurs only after valid user-access conditions are met. They also provide a basis for intervention when suspicious access, account takeover risk, or unauthorized use is suspected.

14. Fraud, Financial Crime, and Sanctions Controls

A key-management framework in a custodial financial service must ensure that cryptographic control cannot be casually used to facilitate unlawful or high-risk conduct. Baldivicio's policy framework addresses this concern directly.

The Acceptable Use Policy prohibits money laundering, terrorist financing, sanctions evasion, structuring, fraud, scams, cybercrime, darknet activity, and other unlawful or abusive uses. The Customer Identification Program Notice describes onboarding and ongoing review measures, including identity verification, source-of-funds or source-of-wealth information where appropriate, expected activity review, sanctions and PEP-related declarations, automated systems, manual review, and additional documentation requests. The Privacy Policy further confirms that Baldivicio may use personal information to detect and respond to fraud, sanctions evasion, money laundering, terrorist financing, suspicious transfers, destination risk, and abuse of the platform.

These controls are highly relevant to key management because they govern the circumstances under which custodial wallet functionality may be activated, restricted, delayed, or refused. In practical terms, they help ensure that key-backed financial operations are subject to legal and risk controls rather than being treated as purely mechanical transaction execution.

15. Restrictions, Suspension, Freezing, and Closure as Protective Key-Use Controls

Baldivicio's Account Suspension, Freezing, and Closure Policy provides an important layer of protective governance around custodial functionality.

Under that policy, Baldivicio may restrict, suspend, freeze, review, or close accounts for reasons including incomplete verification, fraud concerns, unauthorized access, suspicious activity, sanctions concerns, operational or reconciliation concerns, legal process, security incidents, misuse of the service, or other circumstances where protective intervention is warranted.

These powers are relevant to key management because they allow Baldivicio to constrain or prevent further custodial key-backed activity when account integrity, transaction legitimacy, or service safety is in doubt. The policy also makes clear that balances may remain visible while movement is restricted, that pending transactions may remain under review, and that completed transactions remain subject to the principles of irreversibility.

From an ISO 11568 perspective, this demonstrates that key use is embedded in a broader authority structure capable of interruption, containment, and protective enforcement.

16. Logging, Monitoring, and Operational Traceability

A reliable key-management environment requires traceability. Baldivicio's service framework provides substantial support for that principle.

The Privacy Policy states that Baldivicio may collect and process authentication events, session records, account access history, device and access signals, transaction instructions, source and destination addresses, transaction hashes, timestamps, blockchain confirmations, state changes, review status, execution timing, routing data, support interactions, escalation records, incident logs, audit trails, and legal or investigative

materials. The outage policy and account-control policies further describe monitoring, diagnosing, reconciliation, validation, post-incident review, preservation of records, and follow-up review.

These statements support the conclusion that Baldivicio's environment is designed to preserve operational traceability around account access, transaction handling, review status, and service events. In a custodial key-management context, that traceability is critical because it supports review of how and when custodial transaction authority was exercised, what controls were applied, and what state transitions occurred around financial operations.

17. Incident Response and Compromise Handling

Key-management governance must account for compromise scenarios, security incidents, and abnormal operating conditions. Baldivicio's service framework contains meaningful control language in this area.

The Acceptable Use Policy prohibits attempts to disrupt, bypass, or compromise Baldivicio's systems or security controls. The Privacy Policy refers to monitoring, audit logging, incident-response measures, and security-related processing. The System Outage and Degradation Policy describes emergency maintenance, temporary disabling or limiting of features, suspension of transaction execution, revalidation of transaction state, enhanced verification requests, manual review, incident communication, and post-incident reconciliation. The Account Suspension, Freezing, and Closure Policy adds the ability to restrict, suspend, freeze, or close accounts in response to fraud, unauthorized access, security events, operational concerns, or legal requirements.

Together, these measures establish that Baldivicio maintains a documented authority to contain risk, investigate abnormal conditions, preserve records, delay further financial activity, and restore service integrity after incidents. While the service framework does not publish a technical key-compromise procedure, it does clearly establish the governance and operational controls needed to respond to compromise-related risk in a custodial environment.

18. Service Continuity and Availability Considerations

In a custodial model, continuity of service is directly relevant to key management because access to balances and transaction functionality depends on Baldivicio's systems and operational control environment.

Baldivicio expressly states that access to supported balances and transactions depends on its custodial systems, operational controls, and service continuity. It also states that the service may be affected by maintenance events, emergency maintenance, software defects, infrastructure failures, blockchain disruptions, third-party provider failures, compliance interventions, and other operational incidents. During such events, Baldivicio may delay transaction execution, restrict account actions, revalidate transaction state, apply additional review measures, and perform reconciliation after restoration.

This demonstrates that key-management governance in Baldivicio includes an availability dimension. It is not framed as unconditional availability, but as controlled continuity in which protective intervention may take precedence over uninterrupted feature access. That is consistent with a prudential custodial model in which safe operation and service integrity are prioritized during abnormal conditions.

19. Public Blockchain Considerations

Because Baldivicio supports USDC activity on Ethereum Mainnet, public blockchain considerations form part of the key-management and custody environment.

The Privacy Policy explains that public-ledger data may include address activity, transaction amounts, timestamps, hashes, transfers between addresses, and historical relationships over time. The Irreversible

Transactions Disclosure states that completed blockchain-related transactions may be functionally irreversible once executed. The Reserve and Transparency Attestation and Deposit Insurance Disclosure also recognize the role of blockchain confirmations, network conditions, operational timing differences, and external risk.

These public-ledger characteristics do not shift private-key custody away from Baldivicio, but they do shape the environment in which key-backed operations occur. They reinforce the importance of pre-execution review, transaction accuracy, controlled authorization, and strong operational traceability, because post-execution reversal may not be possible.

20. Relationship Between Key Management and Privacy

Key management within Baldivicio is closely linked to privacy governance because custodial operation depends on identity assurance, access monitoring, transaction review, investigation support, and legal compliance.

Baldivicio's Privacy Policy explains that the platform may process identity records, device and access signals, transaction metadata, blockchain data, support communications, compliance review materials, and other operational records. These data uses support account administration, authentication, fraud prevention, sanctions screening, suspicious activity review, investigations, service improvement, and protection of the platform and broader financial system.

In a standards-oriented reading, privacy governance and key-management governance are not separate silos. Privacy-controlled records provide the evidentiary and operational context through which custodial key-backed activity can be verified, investigated, restricted, and documented.

21. Record Retention and Evidentiary Preservation

Baldivicio's policies establish that records may be retained for legal, regulatory, security, operational, dispute-resolution, and investigative purposes. These records may include onboarding records, identity-verification records, compliance records, transaction records, communications, incident logs, audit trails, device and access records, and legal or investigative materials.

This retention model is important to key-management governance because it supports post-event review, service accountability, dispute resolution, and lawful cooperation with competent authorities. It also supports continuity of evidence where transaction handling, access events, incident response, or account restrictions must later be examined.

The public-ledger environment further reinforces this evidentiary model by creating persistent transaction records outside Baldivicio's direct control. Taken together, off-chain record retention and on-chain visibility help support the traceability expected of a custodial financial-service environment.

22. Third-Party Dependencies and Key-Management Boundaries

Baldivicio's documentation acknowledges that certain connected services may involve third-party providers such as Banxa. Those dependencies may affect funding, payout, conversion, settlement, verification-related workflows, communications, and operational timing.

Within the key-management context, these third-party relationships are important boundary markers. They show that some connected service outcomes may depend on external systems and decisions. At the same time, Baldivicio's custodial model remains separately defined: Baldivicio holds and manages the private keys associated with supported wallet functionality, and users do not export those keys.

This means third-party operational dependencies may influence the timing, review, completion, or availability of connected workflows, but they do not change the core governance allocation of custodial private-key responsibility within Baldivicio's service model.

23. Reserve Representation and Key-Control Context

Baldivicio's Reserve and Transparency Attestation states that customer balances are represented through Baldivicio's internal records and custodial systems and that operational timing, account status, blockchain confirmations, fraud review, and third-party dependencies may affect access, transferability, withdrawal, or related service outcomes.

This is relevant to ISO 11568 key management because it clarifies that balance display and balance accessibility are not solely matters of ledger existence. They are also shaped by custodial control, operational state, service restrictions, and lawful governance processes. In other words, the existence of custodial key control is embedded in a broader structure of records, account controls, and service-governance mechanisms.

24. Conformance-Oriented Reading of ISO 11568 Themes

Read against the major themes that ISO 11568 is designed to address, Baldivicio's service framework supports a coherent control narrative.

It supports clear assignment of key responsibility by placing private-key control with Baldivicio rather than with the user.

It supports restriction of key exposure by making private keys non-exportable to users.

It supports controlled key use by linking transaction execution to account controls, review measures, and operational workflows.

It supports authorization discipline by requiring properly verified and authorized account states and by allowing pre-execution review, delay, or refusal.

It supports integrity and containment through restrictions, suspensions, freezes, security controls, fraud controls, and legal or compliance intervention.

It supports traceability through transaction records, access records, review status, state changes, incident logs, audit trails, and record retention.

It supports compromise-response governance through incident handling, emergency maintenance, post-incident reconciliation, account restrictions, and preservation of records.

It supports continuity-aware custody by integrating key-backed service operation with outage handling and operational restoration procedures.

This paper therefore presents Baldivicio's key-management posture as one of centralized custodial responsibility governed by layered operational, security, compliance, and continuity controls.

25. Boundaries of This Paper

This paper is intentionally limited to matters established by Baldivicio's service and policy framework.

It does not describe implementation details that are not stated in that framework. It does not specify hardware architecture, proprietary cryptographic mechanisms, generation ceremonies, quorum procedures, key-component handling, privileged-access workflows, secure-module configurations, or other technical methods that are not set out in Baldivicio's service documentation.

It also does not reinterpret customer-facing legal disclosures as engineering specifications. Where Baldivicio's policies describe a control objective or governance authority at a high level, this paper states that objective at the same level and does not convert it into a technical claim beyond what is supported.

26. Conclusion

Baldivicio's documented service model establishes a clear custodial key-management position. Baldivicio holds and manages the private keys associated with supported wallet functionality. Users do not receive or export those keys. Supported USDC activity on Ethereum Mainnet is provided through Baldivicio's account controls, custodial systems, and related operational processes.

The resulting control environment is not limited to cryptographic custody in isolation. It is reinforced by onboarding and identity verification, transaction validation, fraud and sanctions review, session and access monitoring, service restrictions, incident response, outage management, record retention, privacy governance, and account-lifecycle controls. Together, these elements create a coherent standards-oriented narrative in which custodial key responsibility is centralized, key use is controlled, and operational integrity is preserved through layered governance measures.

Accordingly, Baldivicio's ISO 11568 key-management posture is best characterized as a custodial, control-driven, service-integrated framework in which cryptographic responsibility is exercised through security, compliance, operational oversight, and traceable transaction governance rather than through direct end-user possession or export of private keys.

27. Final Statement

This paper should be read as Baldivicio's key-management compliance narrative for ISO 11568-oriented review in the context of its custodial USDC-on-Ethereum-Mainnet service model. It reflects the service architecture, control positions, and governance principles expressed across Baldivicio's published policies, disclosures, and service descriptions, and it should be interpreted consistently with those materials.