BALDIVICIO & CO.

CCSS: CryptoCurrency Security Standard

Document Title
Baldivicio CCSS CryptoCurrency Security Standard Compliance Paper

Document Type
Standards-oriented cryptocurrency security and control-governance narrative

Subject
Custodial digital-asset security, key-control governance, transaction safeguards, operational resilience, and service-integrity alignment

Effective Date
April 13, 2026

1. Introduction

This paper explains Baldivicio's cryptocurrency security posture through the lens of the CryptoCurrency Security Standard (CCSS). It is intended to provide a comprehensive and structured account of how Baldivicio's service model, custodial architecture, transaction controls, onboarding framework, access protections, privacy practices, outage response, and account-lifecycle safeguards support a disciplined approach to cryptocurrency security governance.

Baldivicio is a digital financial services platform made available primarily through its mobile application. Across its service, operational, privacy, and legal materials, Baldivicio states that it currently supports USDC-only activity on Ethereum Mainnet through a custodial model, that Baldivicio holds and manages the private keys associated with supported wallet functionality on behalf of users, and that users do not receive, possess, or export private keys. These characteristics are central to a CCSS-oriented reading of Baldivicio because CCSS is concerned with secure governance of digital-asset operations, secure control of sensitive cryptographic material, secure handling of transactions, and resilient operation of cryptocurrency-bearing services.

This paper is written as a governance and compliance document. It is not a product brochure, not a marketing statement, and not a substitute for internal engineering specifications, operational runbooks, or implementation diagrams. Its purpose is to explain, in standards-oriented language, how Baldivicio's service framework aligns with the major security concerns addressed by CCSS while remaining faithful to the control boundaries, service claims, and operating practices reflected across Baldivicio's published materials.

2. Purpose and Objectives

The purpose of this paper is to document how Baldivicio's cryptocurrency custody and operational framework can be understood in relation to CCSS principles.

CCSS is concerned with the secure operation of cryptocurrency systems, including governance of sensitive cryptographic material, management of wallets and transaction capability, access control, authorization, auditability, resilience, incident handling, and the prevention of unauthorized or unsafe movement of digital assets. Within Baldivicio, those themes are directly relevant because the platform is a custodial, transaction-bearing, blockchain-connected financial service in which users can hold and move supported USDC while Baldivicio retains responsibility for private-key control and service-level transaction execution.

The objectives of this paper are fivefold.

First, it explains the cryptocurrency security context in which Baldivicio operates.

Second, it establishes the foundational control principles visible across Baldivicio's service and policy framework that are relevant to custodial digital-asset security.

Third, it explains how those controls apply to wallet governance, access security, transaction handling, monitoring, operational response, and service continuity.

Fourth, it organizes those controls into a structure suitable for standards, governance, legal, operational, security, and risk review.

Fifth, it defines the boundaries of the documented control narrative without making technical claims beyond what Baldivicio's service materials support.

3. Scope

This paper applies to Baldivicio's cryptocurrency-related security posture to the extent that posture is reflected in the service environment supporting the mobile application, custodial wallet functionality, supported USDC activity on Ethereum Mainnet, account onboarding, identity verification, access

protection, transaction review, incident handling, outage response, privacy-related operational records, and account restriction or closure processes.

This includes cryptocurrency security governance as reflected in:

- the custodial service model and private-key responsibility structure;
- account creation, verification, and lifecycle controls that govern access to cryptocurrency functionality;
- supported transfer initiation, validation, review, restriction, refusal, and execution;
- access protection, credential handling, device and session awareness, and suspicious-access intervention;
- fraud prevention, legal-compliance controls, sanctions-related review, and misuse prevention;
- monitoring, traceability, record retention, and evidentiary preservation;
- service continuity, degraded-service handling, emergency maintenance, and recovery-related actions; and
- third-party dependencies affecting connected services, communications, or operational outcomes.

This paper should be read consistently with Baldivicio's Terms of Service, Privacy Policy, 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, and Account Suspension, Freezing, and Closure Policy.

4. Cryptocurrency Security Context of the Baldivicio Service

Baldivicio's cryptocurrency security posture must be understood in light of the type of service it provides. Baldivicio is not presented as a self-custody wallet or as a neutral blockchain interface that merely exposes direct signing control to end users. Instead, it is presented as a custodial digital financial-services platform in which supported balances and supported transaction functionality are delivered through Baldivicio's account controls, custodial systems, and related operational processes.

This means cryptocurrency security within Baldivicio extends across several connected domains at once. It includes secure governance of private-key responsibility, protection of user access to the service boundary, integrity of transaction review and execution, lawful and risk-aware control of supported wallet functionality, prevention of misuse and financial-crime exposure, resilience of service operations during outages or degraded conditions, and preservation of records necessary to reconstruct and review digital-asset activity.

Because Baldivicio supports USDC on Ethereum Mainnet, the service also operates in a public-blockchain environment where certain transaction-related information may be visible outside Baldivicio's direct systems and where completed transfers may become functionally irreversible after execution. This heightens the importance of strong pre-execution controls, accurate transaction handling, and reliable operational traceability.

5. Foundational Cryptocurrency Security Position

Baldivicio's foundational cryptocurrency security position is that supported digital-asset functionality is delivered through a centralized custodial control environment in which Baldivicio retains responsibility for private keys, wallet-related operations, transaction governance, and security intervention.

This position is expressed clearly throughout the service framework. Baldivicio states that it currently supports USDC-only activity on Ethereum Mainnet through a custodial model. It states that Baldivicio holds and manages the private keys associated with supported wallet functionality and that users do not receive or export those keys. It further states that supported transaction functionality is governed through account controls, custodial systems, and related operational processes and that transactions may be

delayed, reviewed, restricted, refused, or executed depending on account status, fraud review, compliance review, operational conditions, and service-integrity considerations.

Taken together, these elements establish a cryptocurrency security model based on controlled custody rather than user-side key possession, controlled transaction invocation rather than direct raw signing, and layered governance rather than unrestricted blockchain interaction.

6. Foundational CCSS-Relevant Control Principles

Several recurring principles in Baldivicio's service framework are directly relevant to CCSS.

The first principle is centralized custody. Private-key responsibility is assigned to Baldivicio rather than to the end user.

The second principle is restricted key exposure. Users do not receive, possess, or export private keys, which materially narrows user-side exposure and confirms that wallet-control authority remains within Baldivicio's service boundary.

The third principle is controlled invocation of cryptocurrency functionality. Supported wallet activity is mediated through account controls, custodial systems, and operational review rather than through unmanaged user-side key operations.

The fourth principle is pre-execution review. Before a transaction is executed or completed, Baldivicio may apply fraud checks, compliance review, operational checks, destination restrictions, account-state rules, and other protective measures.

The fifth principle is service-state awareness. Availability of digital-asset functionality depends on account status, onboarding completion, identity verification, service availability, security review, legal eligibility, and operational conditions.

The sixth principle is traceability. Authentication events, account activity, transaction metadata, support interactions, compliance review materials, incident logs, audit trails, and preservation records form part of the operating environment.

The seventh principle is intervention authority. Baldivicio may delay or refuse transactions, restrict functionality, suspend or freeze accounts, conduct emergency maintenance, and preserve evidence where necessary to protect users or service integrity.

The eighth principle is continuity-aware cryptocurrency operation. Outages, degraded conditions, external infrastructure issues, and third-party disruptions are expressly recognized as circumstances that may affect digital-asset operations and may require controlled recovery measures.

7. Custodial Governance and Control Allocation

CCSS places great importance on governance of cryptocurrency control. Baldivicio's service framework supports a clear and deliberate allocation of responsibility.

Baldivicio is responsible for holding and managing the private keys associated with supported wallet functionality. That responsibility necessarily includes the secure governance of the service environment through which supported balances are represented, supported transactions are reviewed and processed, account-state controls are enforced, communications are delivered, incidents are handled, and restrictions are applied where necessary.

Users are responsible for lawful 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 private-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 service framework does not treat those providers as the holders of user-exported private keys within the Baldivicio custodial model. Their role is described in relation to connected operational workflows and service dependencies rather than core wallet-custody ownership.

This responsibility structure is central to a CCSS-oriented reading because it clarifies who exercises control, who is authorized to initiate service actions, and how the service boundary is defined.

8. Wallet Governance and Supported Asset Boundaries

A cryptocurrency security standard requires clarity about what assets and networks are supported and how wallet functionality is bounded. Baldivicio's service framework is very clear on this point.

Baldivicio currently supports USDC on Ethereum Mainnet only. Users are responsible for ensuring that activity involving the service is compatible with the supported asset and network. Unsupported assets, unsupported networks, incorrect transaction details, incompatible transfer methods, or unsupported routing may result in delays, failed transactions, or permanent loss where recovery is not possible.

This supported-asset boundary is significant from a CCSS perspective because it reduces ambiguity in wallet operations and establishes a defined operational perimeter. By limiting support to a specific asset and network context, Baldivicio reduces the complexity of uncontrolled asset interaction and clarifies the conditions under which cryptocurrency functionality is intended to operate.

9. Sensitive Cryptographic Material Governance

CCSS is strongly concerned with the handling of sensitive cryptographic material. Baldivicio's service framework establishes the governance position around such material, even though it does not publish implementation-specific technical details.

The most important documented fact is that Baldivicio holds and manages the private keys associated with supported wallet functionality and that those keys are not exported to users. This means sensitive cryptographic control remains within Baldivicio's custodial environment.

The service framework also supports this position indirectly through references to protected sign-in flows, secure credential handling, access controls, device-level trust signals, monitoring, incident-response measures, and operational restrictions. While these controls are broader than key custody alone, they contribute to the protection of the environment in which sensitive cryptographic authority is exercised.

At the same time, Baldivicio does not present public technical detail about how sensitive key material is generated, stored, archived, rotated, retired, or destroyed. Accordingly, the security narrative here is a governance narrative based on the control environment, not a public specification of cryptographic implementation detail.

10. Controlled Use of Wallet Functionality

A central CCSS concern is that cryptocurrency controls should be used only within authorized, valid, and reviewable operating conditions. Baldivicio's service framework strongly supports that principle.

Supported transaction functionality is described as being handled through controlled workflows designed to prioritize accuracy, authorization, and traceability. Requests may be reviewed, delayed, restricted, refused, or executed. Account state, fraud checks, compliance review, operational checks, security considerations, and destination restrictions may all affect whether a transaction proceeds.

This means wallet functionality is not presented as an always-on, user-triggered signing mechanism. It is part of a governed financial-service process in which authorization, legality, safety, and operational integrity are evaluated before execution where appropriate. That is highly consistent with a CCSS-style expectation that cryptocurrency control should be mediated through well-defined procedures rather than exposed as unmanaged authority.

11. Transaction Authorization and Execution Governance

Transaction authorization is one of the clearest areas of CCSS relevance within Baldivicio.

Users do not directly perform self-custodial signing. They submit instructions through Baldivicio. Baldivicio may act on those instructions subject to account controls, review procedures, fraud checks, compliance checks, operational conditions, and service protections. A transaction may be pending, queued, under review, delayed, limited, or refused before execution. After execution or completion, the transaction may become irreversible.

This structure is important because it places cryptocurrency transfer execution inside a governed authorization environment. The authorization environment includes account validity, destination review, accuracy of transaction details, supported asset and network limits, account restrictions, and broader legal and operational considerations.

In CCSS terms, this shows that Baldivicio treats transfer capability as a controlled service function subject to security and governance measures rather than as an unrestricted raw blockchain action.

12. User Access, Authentication, and Wallet-Access Conditions

The security of cryptocurrency functionality depends not only on custody but also on the integrity of user access. Baldivicio's service framework addresses this area in a meaningful way.

Baldivicio refers to protected sign-in flows, secure credential handling, device-level trust signals, authentication events, session records, login timestamps, account access history, and suspicious-sign-in review. It may also process technical and behavioral signals to help detect suspicious access, account takeover risk, fraud, or attempts to evade compliance or security controls.

Users are required to maintain confidentiality of credentials, safeguard device access, and notify Baldivicio promptly of suspected unauthorized activity or compromise. Where suspicious access or security issues are detected, Baldivicio may apply restrictions, suspend functionality, request additional information, or take further protective action.

This access-control posture is important in a CCSS context because secure cryptocurrency custody depends on ensuring that only valid, authorized, and reviewed account conditions can lead to transaction execution.

13. Onboarding, Identity Verification, and Cryptocurrency Access Control

The Customer Identification Program Notice and related service descriptions show that access to cryptocurrency-related functionality is tied to onboarding and identity controls rather than granted automatically.

Baldivicio may require personal identification information, government-issued identification, compliance-related information, and additional supporting information where necessary. It may use automated systems, manual review, and third-party support to verify identity, assess risk, and determine whether an account may be approved, restricted, reviewed, suspended, or closed.

This is directly relevant to cryptocurrency security because it means access to custodial wallet functionality is not detached from identity assurance and account legitimacy. Instead, wallet access is integrated into a framework of onboarding integrity, compliance screening, and ongoing account review.

14. Fraud, Misuse, and Financial-Crime Controls

A strong CCSS posture requires meaningful safeguards against misuse of cryptocurrency functionality. Baldivicio's policy framework addresses this directly.

The Acceptable Use Policy prohibits money laundering, concealment of proceeds of crime, terrorist financing, darknet activity, structuring, fraud, phishing, impersonation, spoofing, social engineering, cybercrime-related misuse, and attempts to probe or compromise Baldivicio's systems or controls. The Customer Identification Program Notice and Privacy Policy reinforce these controls by explaining that Baldivicio may collect and process information to detect and respond to suspicious activity, fraud, sanctions concerns, destination risk, and broader misuse of the platform.

These measures are important to CCSS alignment because they show that cryptocurrency transfer capability is not treated as neutral infrastructure indifferent to misuse. It is bounded by a financial-crime-aware control environment designed to reduce abuse and preserve service legitimacy.

15. Restrictions, Suspension, Freezing, and Closure as Cryptocurrency Security Controls

Baldivicio's account-control framework is a major part of its cryptocurrency security posture.

Under the Account Suspension, Freezing, and Closure Policy, Baldivicio may restrict, suspend, freeze, review, or close accounts for reasons including incomplete verification, fraud concerns, unauthorized access, suspicious activity, sanctions-related concerns, operational anomalies, legal process, security incidents, misuse of the platform, or other circumstances where protective intervention is appropriate.

These powers are directly relevant to CCSS because they provide a mechanism for interrupting or preventing further digital-asset movement when the integrity of the account, the legitimacy of the transaction, or the safety of the service is in doubt. The policy also clarifies that balances may remain visible while movement is restricted and that closure may depend on draining the remaining balance through supported transfer or off-ramp processes where applicable.

This demonstrates that Baldivicio's cryptocurrency controls include not only execution capability, but also strong containment and restriction capability.

16. Monitoring, Logging, and Traceability

CCSS places importance on traceability of cryptocurrency operations. Baldivicio's service framework supports this principle through a broad record and monitoring environment.

Baldivicio may collect and process authentication events, session records, account access history, transaction instructions, source and destination addresses, transaction hashes, timestamps, blockchain confirmations, on-chain status, routing data, state changes, review status, support interactions, escalation records, incident logs, audit trails, compliance materials, and legal or investigative records. The outage and account-control policies further describe reconciliation, validation, preservation of records, and post-incident review.

This means cryptocurrency-related activity within Baldivicio is surrounded by a meaningful evidentiary framework. In a custodial environment, this traceability is important because it supports accountability for how transaction authority was exercised, what reviews were applied, and what decisions or state transitions occurred around supported wallet activity.

17. Incident Response and Compromise Handling

A cryptocurrency security standard must account for abnormal conditions, suspected compromise, and incident response. Baldivicio's service framework contains a substantial operational response posture in this area.

The Acceptable Use Policy prohibits attempts to disrupt or compromise the service. The Privacy Policy refers to monitoring, audit logging, security-related processing, and incident-response measures. The System Outage and Degradation Policy describes emergency maintenance, temporary disabling or limiting of features, delayed or suspended execution, revalidation of transaction state, enhanced verification, manual review, incident communication, and post-incident reconciliation. The Account Suspension, Freezing, and Closure Policy adds the authority to restrict, suspend, freeze, or close accounts where security or integrity concerns arise.

Taken together, these measures establish that Baldivicio can contain risk, preserve evidence, delay further activity, investigate abnormal conditions, and restore operational integrity after incidents. While the service framework does not publish an implementation-specific cryptocurrency compromise runbook, it clearly establishes the governance and operational capabilities required to respond to cryptocurrency-related security events in a custodial environment.

18. Service Continuity and Availability

CCSS is not limited to secrecy and authorization; it also has implications for the availability and resilience of cryptocurrency operations. Baldivicio's service framework addresses this area meaningfully.

Access to supported balances and transactions depends on Baldivicio's custodial systems, operational controls, and service continuity. Baldivicio recognizes the possibility of outages, degraded performance, maintenance events, software defects, infrastructure failures, blockchain disruptions, third-party provider failures, legal or compliance interventions, and other abnormal conditions. In such cases, the service may delay transaction execution, restrict account actions, revalidate transaction state, apply additional review measures, and perform reconciliation after restoration.

This demonstrates that cryptocurrency security in Baldivicio includes a continuity dimension. The service is not portrayed as unconditionally available, but as a controlled operational environment in which continuity is preserved through protective intervention, validation, and recovery actions.

19. Public Blockchain and Irreversibility Considerations

Because Baldivicio supports USDC activity on Ethereum Mainnet, public-blockchain conditions are part of the cryptocurrency security environment.

Baldivicio explains that public-ledger data may include address activity, transaction amounts, timestamps, hashes, transfers between addresses, and historical address relationships. It also explains that completed transfers may be functionally irreversible once executed or confirmed. These public-ledger characteristics heighten the security importance of transaction accuracy, destination verification, pre-execution review, and protected user access.

This is highly relevant to CCSS because it underscores that prevention and control before execution are particularly important in a public-blockchain environment where post-execution reversal may be unavailable.

20. Reserve Representation and Custodial Operating Context

Baldivicio's Reserve and Transparency Attestation explains that customer balances are represented through internal records and custodial systems and that access, transferability, or withdrawal may depend on transaction timing, blockchain confirmation requirements, account status, fraud and compliance review, operational controls, and third-party dependencies.

This matters to cryptocurrency security because it clarifies that balance visibility and balance mobility are not identical concepts. Even where value is represented within the service, access to that value may still be conditioned by custodial controls, operational state, service restrictions, and legal or security review. In a CCSS-oriented reading, this reflects a controlled operating model in which cryptocurrency capability is governed through service logic rather than through uncontrolled access.

21. Privacy, Recordkeeping, and Cryptocurrency Security

Cryptocurrency security within Baldivicio is closely tied to privacy and recordkeeping. The Privacy Policy explains that Baldivicio may process identity information, device and access signals, transaction metadata, public blockchain information, support communications, compliance materials, and other operational records. These records support account administration, authentication, fraud prevention, sanctions screening, suspicious activity review, investigations, service improvement, and protection of the platform and broader financial system.

This means privacy-governed records are also part of the cryptocurrency security environment. They provide the evidentiary context needed to authenticate access, review transactions, investigate misuse, preserve service integrity, and respond to disputes or legal requests.

22. Third-Party Dependencies and Cryptocurrency Security Boundaries

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

Within a CCSS-oriented reading, these relationships serve as important boundary markers. They show that some service outcomes may depend on external systems and decisions. At the same time, Baldivicio's custodial model remains separately defined: Baldivicio holds and manages private keys associated with supported wallet functionality, and users do not export those keys.

Accordingly, third-party-connected services may influence operational timing, review steps, payout outcomes, and related workflows, but they do not alter the core fact that cryptocurrency custody and service-level wallet control remain centered within Baldivicio's own custodial framework.

23. Conformance-Oriented Reading of CCSS Themes

Read against the major themes associated with CCSS, Baldivicio's service framework supports a coherent cryptocurrency security narrative.

It supports clear custody allocation by assigning private-key control to Baldivicio rather than to the user.

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

It supports controlled transaction use by routing supported wallet functionality through account controls, custodial systems, and operational review.

It supports authorization discipline by requiring valid account status, identity assurance, supported asset and network compatibility, and pre-execution review where necessary.

It supports containment and intervention through restrictions, suspensions, freezes, refusal rights, security measures, compliance controls, and incident-response actions.

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

It supports resilience through outage handling, degraded-service response, validation, reconciliation, and controlled restoration.

It supports public-blockchain-aware security by acknowledging irreversibility, destination accuracy risk, public-ledger visibility, and the operational significance of pre-execution control.

Taken together, these themes support a standards-oriented view of Baldivicio as a custodial cryptocurrency service whose security posture is governed through layered control, review, traceability, and operational resilience.

24. Boundaries of This Paper

This paper is intentionally limited to matters established by Baldivicio's published service descriptions, policies, disclosures, and operating framework.

It does not describe implementation details that are not stated in those materials. It does not specify wallet-creation ceremonies, backup-secret design, hardware modules, quorum schemes, secure-generation procedures, secret-sharing arrangements, internal role matrices, recovery-seed management, secure-room controls, or other technical methods that are not expressly described in Baldivicio's service framework.

It also does not convert service disclosures into technical guarantees beyond what they support. Where Baldivicio's materials describe a control objective, service principle, or intervention authority at a high level, this paper states that matter at the same level and does not transform it into an unsupported implementation-specific claim.

25. Conclusion

Baldivicio's service framework establishes a clear and disciplined cryptocurrency security posture for a custodial USDC-on-Ethereum-Mainnet environment. The platform is built around centralized custody, protected service access, transaction review, fraud and compliance controls, privacy-aware recordkeeping, intervention authority, service continuity, and public-blockchain-aware risk handling.

The resulting control environment is not limited to private-key custody in isolation. It is reinforced by onboarding and identity verification, secure sign-in and access review, transaction validation, monitoring and traceability, incident handling, account restriction and closure controls, third-party dependency awareness, and recovery-oriented service operations. Together, these elements create a coherent standards-oriented narrative in which cryptocurrency security is governed through layered operational, security, compliance, and resilience measures rather than through end-user possession of critical cryptographic material.

Accordingly, Baldivicio's CCSS posture is best characterized as a custodial, control-driven, service-integrated cryptocurrency security framework in which wallet functionality, transaction authority, and digital-asset protection are exercised through centralized governance, pre-execution safeguards, traceable operations, and protective intervention capability.

26. Final Statement

This paper should be read as Baldivicio's CCSS compliance narrative in the context of its custodial digital financial-services model. It reflects the service architecture, control positions, operational safeguards, privacy practices, and governance principles expressed across Baldivicio's published policies, disclosures, and service descriptions, and it should be interpreted consistently with those materials.