RM-S-EXCH-001 Exchange Transparency Verification Standard

Standard ID: RM-S-EXCH-001 **Version:** v1.0-F **Status:** Frozen **Publication Date:** 2026-07-23 **Effective Date:** 2026-07-23 **Standard Family:** RM-S — Canonical Standards Namespace **Normative Status:** Normative **Publisher:** RuleMark **Document Language:** English **Machine ID:** `rulemark:standard:rm-s-exch-001:v1.0-F`

Document Control

Field	Content
Standard ID	RM-S-EXCH-001
Standard Name	Exchange Transparency Verification Standard
Version	v1.0-F
Status	Frozen
Publication Date	2026-07-23
Effective Date	2026-07-23
Standard Family	RM-S
Domain	Custodial digital asset trading platforms: reserve and liability reconciliation, customer asset segregation, withdrawal processing, operating entity and control disclosure, event disclosure
Normative Status	Normative
Target Subject	A specific trading platform operated by a specific legal entity, at a specific verification point
Default Determination	PASS / CONDITIONAL / DEFICIENT / FAIL / NOT ASSESSED
Conformance Use	Authorized

Abstract

This standard establishes a unified, deterministic, and machine-executable set of rules for verifying the transparency of a custodial digital asset trading platform at a specified verification point.

This standard requires verification of the operating entity and every affiliated entity that holds customer assets, the reserve addresses and cryptographic proof of control over them, the total customer liabilities and the proof that each customer can verify their own inclusion, the per-asset reserve coverage, the segregation of customer assets from platform assets, withdrawal processing and suspension disclosure, control over privileged operations, material events, evidence integrity, and the signed verification result.

This standard does not guarantee future solvency, going concern, or asset safety. It does not assess the quality or legality of listed assets, does not evaluate cyber-security defence strength, does not determine whether market manipulation or wash trading has occurred, does not certify the validity of any licence or registration, and does not determine the allocation of legal rights under the platform's user agreement.

This standard answers only:

> At a specified verification point, under a specified standard version, for a specified platform and a specified evidence set, does the platform satisfy the applicable requirements of RM-S-EXCH-001?

1. Applicability

1.1 Conditions of Applicability

This standard applies to an entity that meets all of the following conditions:

1. it operates a matching platform that matches purchases, exchanges, or trades of digital assets for unaffiliated third-party users;
2. it holds customer assets in the course of matching and settlement: customer assets are held in on-chain addresses, accounts, or third-party depository arrangements controlled by the platform;
3. the operator is a uniquely identifiable legal entity;
4. the platform is open to the public or to registered third-party users, and is not limited to affiliated internal use;
5. at the verification point the platform is operating: it accepts deposits and processes withdrawal requests;
6. the platform makes publicly accessible price or order-book data available for at least one asset.

1.2 Out of Scope

This standard does not apply to:

- fully on-chain decentralised trading protocols with no custody and no identifiable operating entity;
- non-custodial matching aggregators and DEX front ends;
- over-the-counter brokerage that only introduces counterparties who settle directly, without custody;
- pure fiat banks, payment institutions, and currency exchanges;
- digital asset custodians that provide custody without matching;
- wallet service providers, including hardware and software wallets;
- lending, staking, and yield platforms, other than any spot matching function they operate;
- central counterparties and settlement institutions themselves;
- internal trading or market-making systems used only by affiliated parties;
- testnet, sandbox, and simulated trading environments;
- platforms that have suspended withdrawals or entered bankruptcy, restructuring, or liquidation proceedings. Such platforms MUST be recorded as `NOT ASSESSED` under this standard.

1.3 Non-Goals

This standard:

- does not provide investment advice;
- does not certify legal compliance in any jurisdiction;
- does not replace a regulator, auditor, court, or legal counsel;
- does not constitute a credit rating;
- does not constitute a RuleMark guarantee, recommendation, or endorsement;
- does not guarantee the platform's future solvency, going concern, or asset safety. A conclusion describes only the verifiable state at the verification point;
- does not assess the quality, legality, or investment value of listed assets;
- does not evaluate cyber-security defence strength and does not replace penetration testing or security certification;
- does not determine whether market manipulation, wash trading, or insider dealing has occurred;
- does not certify whether a licence, registration, or authorisation is valid or in good standing;
- does not determine the allocation of legal rights under the platform's user agreement.

1.4 Conforming Subject

A conformance claim MUST correspond to a snapshot of the transparency state of one specific trading platform, operated by one specific legal entity, at one specific verification point. **The result is bound to that verification point and expires under §16.5.**

Unique identification MUST include at least:

- operating legal entity name, jurisdiction of registration, registration number;
- platform brand name and canonical domain;
- **the list of in-scope affiliated entities**: every group member that holds customer assets, named individually (see §6);
- licence or registration number and issuing authority, or an explicit `null` where none exists. This field MUST NOT be left empty;
- verification point, ISO 8601 UTC, precision to the second;
- the list of in-scope assets and their network identifiers;
- SHA-256 digest of the set of addresses holding customer assets.

A conformance claim MUST NOT be made for a corporate group in the aggregate without naming its in-scope entities, and MUST NOT be made for a platform whose in-scope entity list is incomplete.

1.5 Participant Roles

This standard distinguishes the following participant roles. A single legal entity MAY assume multiple roles, but the responsibilities of each role MUST be separately identifiable.

- **Obligated Party**: the legal entity operating the trading platform. It submits the conformance claim, the machine record, and all mandatory evidence; discloses every in-scope affiliated entity; provides cryptographic proof of control over reserve addresses; and discloses material events within the stated deadlines. It is the subject of the conformance claim.
- **Verifier**: the party that executes the verification procedure of §15.1, confirms that reserves and liabilities are taken at the same verification point, confirms human–machine consistency, determines the result, and signs the verification record.
- **Machine Validator**: the system that executes the schema and determination logic of this standard, recomputes coverage, validates the liability Merkle root, checks evidence freshness, and outputs deterministic failure codes.
- **Evidence Provider**: an independent attestation firm, on-chain data (control signatures and balance snapshots), a third-party depository or bank confirmation, an external auditor, and the platform itself for declaration-type evidence only.

A platform statement alone MUST NOT constitute independent evidence.

Where a commercial, fee, ownership, or control relationship exists between the Verifier and the Obligated Party, it MUST be disclosed under §19.3. An undisclosed material interest relationship renders the verification result invalid.

2. Normative Terminology

The normative keywords in this standard are used with the following meanings:

- **MUST / SHALL**: mandatory requirement;
- **MUST NOT / SHALL NOT**: express prohibition;
- **SHOULD**: recommended requirement; a documented reason MUST be recorded where not satisfied;
- **SHOULD NOT**: not recommended; a documented reason MUST be recorded where adopted;
- **MAY**: optional capability.

Only the above English keywords appearing in uppercase have normative effect. Informative explanations, examples, and clarifications shall not override normative requirements.

3. Definitions

Term	Definition
Platform	A custodial digital asset trading service meeting all conditions of §1.1.
Operating Entity	The legal entity that operates the platform and bears responsibility for the conformance claim.
In-Scope Entity	The operating entity and every affiliated entity that holds, controls, or can direct the transfer of customer assets of the platform.
Affiliation	Ownership, common control, common ultimate beneficial ownership, or a contractual arrangement conferring the ability to direct the transfer of customer assets.
Customer Asset	A digital asset held by an in-scope entity on behalf of an identified customer, whether or not segregated at address level.
Customer Liability	The obligation of the in-scope entities to deliver a stated quantity of a stated asset to an identified customer on demand.
In-Scope Asset	An asset for which customer liabilities exist at the verification point and which is included in the conformance claim.
Reserve Address	An on-chain address, account, or depository position held by an in-scope entity and asserted to back customer liabilities.
Proof of Control	A cryptographic demonstration that an in-scope entity controls a reserve address, by message signature or by a verifiable spend originating from that address.
Reserve Balance	The quantity of an in-scope asset held across all reserve addresses at the verification point.
Per-Asset Coverage Ratio	Reserve balance of one in-scope asset divided by customer liabilities denominated in that same asset.
Liability Commitment	A cryptographic commitment to the complete set of customer liabilities, from which each customer can verify the inclusion of their own balance.
Inclusion Proof	The data allowing one customer to verify that their balance is included in the liability commitment.
Verification Point	The single UTC time at which reserve balances and customer liabilities are both taken.
Segregation	The separation of customer assets from the proprietary assets of the in-scope entities, in law, in accounting, and in operation.
Withdrawal	The transfer of a customer asset out of the platform to an address or account designated by the customer.
Withdrawal Suspension	Any state in which withdrawal requests for an in-scope asset are not processed within the disclosed maximum processing time.
Privileged Operation	An operation capable of moving customer assets, altering balances, or halting withdrawals.
Material Event	An event that changes the conformance conclusion, see §13.1.
Evidence	A verifiable record, report, log, on-chain datum, signature, or third-party confirmation supporting or refuting a requirement.
PASS	All applicable MUST requirements are satisfied, no MUST NOT is violated, all mandatory evidence is valid, and the verification record is signed.
CONDITIONAL	All MUST and MUST NOT requirements are satisfied and one or more SHOULD requirements are unsatisfied.
DEFICIENT	Nothing is violated on the available evidence, but one or more mandatory items cannot be verified because evidence is missing, incomplete, or expired, and the gap is curable.
FAIL	At least one applicable MUST is unsatisfied, a MUST NOT is violated, mandatory evidence is missing or invalid, or the result is not re-computable.
NOT_ASSESSED	Verification is not complete and no conformance conclusion is constituted.

3.1 Restriction on Ambiguous Terms

The following words MUST NOT be used alone in normative clauses: reasonable, appropriate, sufficient, adequate, timely, regular, high-quality, secure, transparent, real-time, independent, material, low-risk.

This standard additionally prohibits the standalone use of: fully backed, 1:1 backed, fully reserved, always available, instant withdrawal, bank-grade, audited (where the evidence is an attestation rather than an audit), and proof of reserves (where liabilities are not proven).

Where any such word is used, the clause MUST also define: a measurable value; a time range; test conditions; the responsible party; and the determination method. The terms defined in §3 satisfy this requirement for the meanings given there.

4. Core Principles

4.1 Evidence First

Any conformance conclusion MUST be supported by verifiable evidence. A platform statement alone MUST NOT constitute independent evidence.

4.2 Identifiable Responsibility

Every function, claim, and item of evidence MUST be traceable to a responsible party.

4.3 Same-Point Reconciliation

Reserve balances and customer liabilities MUST be taken at the same verification point. Where the exact same point cannot be used, a clear and re-computable adjustment method MUST be provided.

4.4 Complete Scope

Reserves and liabilities MUST be measured across **all** in-scope entities. A reserve figure that omits an entity holding customer assets MUST NOT be treated as a reserve figure of the platform.

4.5 Per-Asset Sufficiency

Coverage MUST be determined for each in-scope asset separately. **Aggregate coverage across assets MUST NOT be used to demonstrate sufficiency**, because a surplus in one asset does not discharge an obligation denominated in another.

4.6 Two-Sided Proof

A reserve figure without a corresponding liability figure MUST NOT be treated as evidence of sufficiency.

4.7 Customer-Verifiable Liabilities

Each customer MUST be able to verify that their own balance is included in the liability figure, without relying on the platform's assertion.

4.8 Control, Not Sight

An address balance MUST NOT be counted as a reserve unless control over that address by an in-scope entity is cryptographically proven.

4.9 Non-Discretionary Determination

The same inputs, the same standard version, and the same verification point MUST produce the same result.

4.10 Machine Readability

Core platform data and verification results MUST have a structured representation.

4.11 Minimum Necessary Claim

A conformance conclusion MUST NOT exceed the verified entities, assets, and verification point.

4.12 Freshness

Evidence exceeding the maximum age of §14.4 MUST NOT be used to prove current state.

4.13 Traceability

Every mandatory requirement MUST be traceable to evidence, a verification step, and a failure code.

4.14 Failure Closure

Where mandatory evidence is missing, evidence conflicts, or the result is not re-computable, the result MUST be FAIL or, where §16.6 applies, DEFICIENT. A default pass MUST NOT be applied.

5. Canonical Identity and Responsible Parties

5.1 Conforming Subject Canonical Identity

Every conforming subject submitted for verification MUST have a canonical identity containing at least:

```
{
  "operating_entity_legal_name": "",
  "operating_entity_jurisdiction": "",
  "operating_entity_registration_number": "",
  "platform_name": "",
  "canonical_domain": "",
  "in_scope_entities": [],
  "licence_number": null,
  "licence_authority": null,
  "verification_point": "",
  "in_scope_assets": [],
  "reserve_address_set_sha256": "",
  "standard_version": ""
}
```

`licence_number` and `licence_authority` MUST be explicitly `null` where none exists. They MUST NOT be omitted or left as empty strings.

5.2 Operating Entity Registration

The operating entity MUST disclose its legal name, jurisdiction of registration, registration number, canonical domain, and the official channel at which it publishes transparency reports and incident notices.

5.3 Change of Responsibility

Where the operating entity, an in-scope entity, or the control of a reserve address changes, the record MUST capture the position before and after the change, the effective time, and the supporting evidence, and the affected verification result MUST be recomputed.

6. Scope of Consolidation

6.1 Identification of In-Scope Entities

The obligated party MUST identify every entity that, at the verification point, holds, controls, or can direct the transfer of customer assets of the platform, and MUST name each of them individually in the conformance claim.

An entity is in scope where any of the following holds:

1. it holds customer assets in an address, account, or depository position;
2. it controls a key, signer, or authorisation that can move customer assets;
3. it is under common ownership or common control with the operating entity and holds customer assets;
4. a contractual arrangement confers on it the ability to direct the transfer of customer assets.

Where any entity satisfying the above is omitted from the in-scope list, the result MUST be FAIL using `RMSEXCH-SCOPE-001`.

6.2 Completeness Declaration

The obligated party MUST provide a signed declaration that the in-scope entity list is complete, and MUST provide independent evidence of the group structure sufficient for the verifier to test that completeness. Where the declaration or the independent group-structure evidence is absent, the result MUST be FAIL using `RMSEXCH-SCOPE-002`.

6.3 Assets Held by Third Parties

Where customer assets are held by a third-party depository, custodian, or bank that is not an in-scope entity, the obligated party MUST disclose that party, the assets and quantities held, and MUST provide a confirmation issued directly by that party to the verifier. Where the confirmation is absent or is relayed only by the platform, the result MUST be FAIL using `RMSEXCH-SCOPE-003`.

6.4 Assets Deployed Outside Custody

Where customer assets are lent, staked, pledged, used as collateral, or otherwise deployed such that they are not immediately available for withdrawal, the obligated party MUST disclose the arrangement, the asset, the quantity, the counterparty, and the recall period. Such assets MUST NOT be counted as reserve balance under §7 unless the recall period is shorter than the disclosed maximum withdrawal processing time. Where an undisclosed deployment is found, the result MUST be FAIL using `RMSEXCH-SCOPE-004`.

7. Reserves and Proof of Control

7.1 Reserve Address Disclosure

The obligated party MUST disclose the complete set of reserve addresses for each in-scope asset, including the network identifier, the address, the holding in-scope entity, and the balance at the verification point. Where the set is incomplete or an address cannot be attributed to an in-scope entity, the result MUST be FAIL using `RMSEXCH-RES-001`.

7.2 Proof of Control

For each reserve address, control MUST be proven by one of:

1. a message signature produced by the address key over a challenge string that includes the platform identifier and the verification point; or
2. a verifiable spend originating from that address within **24 hours** of the verification point, referenced by transaction hash.

An address balance MUST NOT be counted as reserve without such proof. Where proof is absent, invalid, or does not bind to the verification point, the result MUST be FAIL using `RMSEXCH-RES-002`.

7.3 Address Exclusivity

The same address MUST NOT be counted as reserve for more than one platform, and MUST NOT be counted more than once within one platform. The obligated party MUST disclose whether any reserve address is shared with a party outside the in-scope entity list. Where double counting or an undisclosed shared address is found, the result MUST be FAIL using `RMSEXCH-RES-003`.

7.4 Borrowed Assets

Assets borrowed, temporarily transferred in, or otherwise obtained for the purpose of presenting a reserve balance MUST be disclosed with the counterparty, the quantity, the receipt time, and the repayment obligation. Assets received within **72 hours** before the verification point and repayable within **72 hours** after it MUST be disclosed separately and MUST NOT be counted as reserve. Where an undisclosed borrowing is found, the result MUST be FAIL using `RMSEXCH-RES-004`.

7.5 Reserve Balance Determination

The reserve balance of an in-scope asset is the sum of proven balances across all reserve addresses of that asset, less assets excluded under §6.4 and §7.4. The verifier MUST recompute this sum independently from on-chain or depository data. Where the recomputed sum differs from the declared balance, the result MUST be FAIL using `RMSEXCH-RES-005`.

8. Customer Liabilities

8.1 Liability Determination

The obligated party MUST determine, for each in-scope asset, the total quantity owed to customers at the verification point, including balances available for trading, balances locked in open orders, balances in pending withdrawal, and any other obligation to deliver that asset to a customer. Where any category is omitted, the result MUST be FAIL using `RMSEXCH-LIA-001`.

8.2 Liability Commitment

The obligated party MUST publish a cryptographic commitment to the complete set of customer liabilities at the verification point, constructed such that:

1. each customer record contributes to the commitment;
2. the total of all customer records is derivable from the commitment structure;
3. no customer record can be removed or reduced without changing the commitment.

Where no commitment is published, or the commitment does not permit derivation of the total, the result MUST be FAIL using `RMSEXCH-LIA-002`.

8.3 Customer Inclusion Proof

Each customer MUST be able to obtain an inclusion proof allowing them to verify that their own balance is included in the published commitment, without relying on any further assertion by the platform. The verification method MUST be published.

Where inclusion proofs are unavailable or the verification method is not published, the result MUST be FAIL using `RMSEXCH-LIA-003`.

8.4 Negative and Excluded Balances

The commitment construction MUST NOT permit a customer record to reduce the derived total. Where negative balances exist, they MUST be disclosed separately and MUST NOT be netted against positive customer balances. Where netting or a total-reducing record is found, the result MUST be FAIL using `RMSEXCH-LIA-004`.

8.5 Independent Liability Attestation

The obligated party SHOULD obtain an opinion from an independent attestation firm on the completeness of the customer liability set, stating the procedures applied and any limitations.

9. Reserve Coverage

9.1 Per-Asset Coverage

For each in-scope asset, coverage is computed as:

```
per_asset_coverage_ratio = reserve_balance(asset) / customer_liability(asset)
```

The minimum required for PASS is `100%` for every in-scope asset, computed separately. Aggregate or cross-asset coverage MUST NOT be substituted. Where any in-scope asset has coverage below 100%, the result MUST be FAIL using `RMSEXCH-COV-001`.

9.2 Deterministic Computation

Coverage MUST be computed at the smallest indivisible unit of each asset. Intermediate computation MUST retain the full precision of that unit. Rounding MUST NOT be applied in a manner that raises a ratio below 100% to 100% or above. `100%` is a hard boundary: where reserve balance is less than customer liability by any quantity, however small, the result MUST be FAIL using `RMSEXCH-COV-001`.

Boundary test. The 100% test MUST be performed by comparing the two integer quantities directly, at the smallest indivisible unit. It MUST NOT be performed on a rounded ratio.

Declared ratio. The `coverage_ratio` recorded under §18.2 MUST be stated to exactly six decimal places, truncated toward zero. The verifier MUST recompute it and MUST require exact equality with the declared value; any difference is an inconsistency and the result MUST be FAIL using `RMSEXCH-RES-005`.

9.3 Assets With Liabilities But No Reserve

Where customer liabilities exist for an asset and no reserve address is disclosed for that asset, coverage is `0` and the result MUST be FAIL using `RMSEXCH-COV-002`.

9.4 Cross-Asset Substitution

Where the obligated party asserts that a shortfall in one asset is covered by a surplus in another, it MUST disclose the substitution, the conversion basis, and the mechanism by which a customer would receive the asset actually owed. **Such an assertion MUST NOT be used to satisfy §9.1.** Where substitution is used to claim sufficiency, the result MUST be FAIL using `RMSEXCH-COV-003`.

10. Segregation of Customer Assets

10.1 Legal Segregation

The obligated party MUST disclose whether customer assets are legally separated from the proprietary assets of the in-scope entities, and MUST state the basis of that separation. Where the disclosure is absent, the result MUST be FAIL using `RMSEXCH-SEG-001`.

10.2 Operational Segregation

The obligated party MUST disclose whether customer assets and proprietary assets are held in separate addresses or accounts, and where they are commingled, MUST disclose the accounting method by which customer entitlements are distinguished. Where the disclosure is absent, the result MUST be FAIL using `RMSEXCH-SEG-002`.

10.3 Proprietary Trading Against Customer Assets

The obligated party MUST disclose whether any in-scope entity or affiliated party uses customer assets for proprietary trading, market making, lending, or collateral.

Where such use occurs and is not disclosed, the result MUST be FAIL using `RMSEXCH-SEG-003`.

Where no disclosure on this question is provided at all, the item cannot be verified: the result is `DEFICIENT` under §16.6, recorded with the same code.

10.4 Insolvency Position

The obligated party MUST disclose the position of customers in an insolvency of any in-scope entity: whether customer assets would form part of the estate, the priority of customer claims, and the applicable law. Where the disclosure is absent, the result MUST be FAIL using `RMSEXCH-SEG-004`.

> Note: the legal wording of this clause MUST be confirmed by an insolvency law expert before formal freezing.

11. Withdrawal Processing

11.1 Maximum Processing Time

The obligated party MUST publish, for each in-scope asset, the maximum normal withdrawal processing time, expressed in hours or business days. Where no quantified maximum is published, the result MUST be FAIL using `RMSEXCH-WDR-001`.

11.2 Withdrawal Performance

The obligated party MUST record, for the **30 days** preceding the verification point and for each in-scope asset: the number of withdrawal requests, the number completed within the published maximum, the number exceeding it, and the number refused. Where the record is absent, the result MUST be FAIL using `RMSEXCH-WDR-002`.

This clause requires the record, not any particular level of performance. A high proportion of withdrawals exceeding the published maximum does not by itself produce FAIL under this clause; it is disclosed so that a reader can assess it. Where withdrawals for an in-scope asset were not processed within the published maximum for a continuous period, §11.3 applies and the period MUST be disclosed as a suspension.

11.3 Suspension Disclosure

Any suspension of withdrawals for an in-scope asset MUST be disclosed with the asset, the start time, the end time or current status, and the reason. A suspension in effect at the verification point MUST be disclosed in the conformance claim. Where an undisclosed suspension is found, the result MUST be FAIL using `RMSEXCH-WDR-003`.

11.4 Selective Processing

The obligated party MUST NOT prioritise withdrawal requests by customer identity, size, or public visibility in a manner not disclosed in its published withdrawal policy. Where undisclosed selective processing is found, the result MUST be FAIL using `RMSEXCH-WDR-004`.

11.5 Test Withdrawal

The verifier SHOULD execute or obtain evidence of a test withdrawal for each in-scope asset within the 30 days preceding the verification point.

12. Operating Entity and Control

12.1 Privileged Operation Disclosure

The obligated party MUST disclose every role capable of moving customer assets, altering customer balances, or halting withdrawals, and the control mechanism applied to each. Where the disclosure is absent or incomplete, the result MUST be FAIL using `RMSEXCH-OPS-001`.

12.2 Single-Key Restriction

Movement of customer assets MUST NOT be capable of being executed by a single undisclosed key. Privileged operations MUST use one or more of: multi-signature, threshold signature, hardware security module, dual authorisation, or a functionally equivalent control. Where a single undisclosed key can move customer assets, the result MUST be FAIL using `RMSEXCH-OPS-002`.

12.3 Ultimate Beneficial Ownership

The obligated party MUST disclose the ultimate beneficial ownership of the operating entity to the extent required to identify who controls the platform, or MUST state the legal basis on which that disclosure is withheld. Where neither is provided, the result MUST be FAIL using `RMSEXCH-OPS-003`.

12.4 Related-Party Exposure

The obligated party MUST disclose any exposure of customer assets to a related party, including loans, collateral arrangements, and holdings of a token issued or controlled by an in-scope entity or its affiliates. Where such exposure exists and is not disclosed, the result MUST be FAIL using `RMSEXCH-OPS-004`.

13. Material Events

13.1 Types of Material Event

A material event includes at least: per-asset coverage falling below 100%; suspension of withdrawals for any in-scope asset; loss, theft, or unauthorised movement of customer assets; insolvency, restructuring, or liquidation of any in-scope entity; loss of control over a reserve address; the addition or removal of an in-scope entity; withdrawal or invalidation of an attestation; compromise of a key controlling customer assets; and any other event that changes the conformance conclusion.

13.2 Notice Deadline

The obligated party MUST record a material event within **24 hours** of confirming it, and MUST publish it through its disclosed official channel within **24 hours** of confirming it. Where either deadline is not met, the result MUST be FAIL using `RMSEXCH-EVT-001`.

13.3 Notice Content

```
{
  "event_id": "",
  "event_type": "",
  "affected_entities": [],
  "affected_assets": [],
  "detected_at": "",
  "published_at": "",
  "description": "",
  "current_status": "",
  "evidence_id": "",
  "requires_reverification": true
}
```

13.4 Verification Status Handling

Where a material event may affect conformance, the existing verification result MUST be treated as expired from the time of the event, and re-verification MUST be performed before the result is relied upon again.

14. Evidence Requirements

14.1 Required Evidence

Evidence ID	Evidence Type	Provided By	Required
EVD-001	Operating entity identity record	Operating entity; company registry	Mandatory
EVD-002	Group structure and in-scope entity list, with completeness declaration	Operating entity; independent corporate records	Mandatory
EVD-003	Reserve address set with network identifiers and holding entity	Operating entity	Mandatory
EVD-004	Proof of control for each reserve address	Operating entity; on-chain data	Mandatory
EVD-005	Reserve balance snapshot at the verification point	On-chain data; block explorer or node	Mandatory
EVD-006	Customer liability totals per in-scope asset	Operating entity	Mandatory
EVD-007	Liability commitment and published verification method	Operating entity	Mandatory
EVD-008	Segregation disclosure and supporting records	Operating entity	Mandatory
EVD-009	Withdrawal policy, maximum processing times, and 30-day performance record	Operating entity	Mandatory
EVD-010	Privileged operation and control mechanism disclosure	Operating entity	Mandatory
EVD-011	Third-party depository or bank confirmation	Depository; bank	Mandatory where §6.3 applies
EVD-012	Deployment disclosure for lent, staked, or pledged customer assets	Operating entity; counterparty	Mandatory where §6.4 applies
EVD-013	Independent attestation on liability completeness	Attestation firm	Optional (SHOULD, §8.5)

Evidence ID	Evidence Type	Provided By	Required
EVD-014	Material event record and public notice	Operating entity	Mandatory where a material event has occurred
EVD-015	Machine-readable conformance record	Operating entity	Mandatory
EVD-016	Human disclosure version	Operating entity	Mandatory
EVD-017	Verifier digital signature and key information	Verifier	Mandatory

Evidence marked `Mandatory` MUST be present for every verification. Evidence marked `Mandatory where …` MUST be present only when the stated condition holds; where the condition does not hold, the verifier MUST record it as `NOT_APPLICABLE` with the reason.

14.2 Evidence Metadata

All mandatory evidence MUST contain the source, the generation time, the acquisition time, the content digest, and access location information. Where any of these is absent, the result MUST be FAIL using `RMSEXCH-EVD-001`.

```
{
  "evidence_id": "",
  "evidence_type": "",
  "provider_id": "",
  "provider_independence_disclosed": false,
  "generated_at": "",
  "acquired_at": "",
  "uri": "",
  "sha256": ""
}
```

14.3 Evidence Digests

All evidence files and machine records MUST use SHA-256 digests, expressed as 64-character lowercase hexadecimal strings. Where a digest does not match or the format is incorrect, the result MUST be FAIL using `RMSEXCH-EVD-002`.

14.4 Evidence Freshness

- reserve balance snapshots and proofs of control (EVD-004, EVD-005) MUST be no older than **24 hours** before the verification point;
- customer liability totals and the liability commitment (EVD-006, EVD-007) MUST be taken at the verification point, and expire **24 hours** after it;
- the withdrawal performance record (EVD-009) MUST cover the 30 days preceding the verification point;
- third-party confirmations (EVD-011) MUST be no older than **35 days** before the verification point;
- an independent attestation, where provided (EVD-013), MUST be no older than **35 days** before the verification point.

Age is computed in days, as the verification time minus the evidence generation time, rounded down to whole days. Age MUST NOT be computed in calendar months.

Where an evidence item exceeds the stated maximum age, the result MUST be FAIL using `RMSEXCH-EVD-003`. Expired evidence MUST NOT be reported as missing evidence.

14.5 Evidence Provider Independence

An attestation firm, auditor, or depository providing EVD-011 or EVD-013 MUST disclose any ownership, control, common-control, employment, or fee-dependency relationship with any in-scope entity. Evidence provided by a party owned or controlled by an in-scope entity MUST NOT be counted as independent evidence and is treated as a platform statement under §4.1. Where the disclosure is absent or the provider is not independent, the result MUST be FAIL using `RMSEXCH-EVD-004`.

14.6 Missing Evidence

Where any mandatory evidence is missing, the overall result MUST be `FAIL` or, where §16.6 applies, `DEFICIENT`. `CONDITIONAL` MUST NOT be used in its place.

14.7 Conflicting Evidence

Where evidence conflicts, the verifier MUST record both sides of the conflict, their source and time, stop the PASS determination for the affected requirements, and determine the overall result as FAIL until the conflict is resolved.

14.8 Evidence Authority Ordering

Evidence sources are ordered by authority as follows, from highest to lowest:

1. on-chain data independently retrieved by the verifier;
2. a confirmation issued directly to the verifier by a third-party depository, bank, or attestation firm;
3. a signed record produced by an in-scope entity;
4. an unsigned statement or interface display of an in-scope entity.

This ordering MUST be recorded for each item of conflicting evidence and MUST be used when reporting a conflict. It MUST NOT be used to resolve a conflict automatically: §14.7 continues to apply.

An unsigned statement or interface display of an in-scope entity MUST NOT be the sole evidence for reserve balance, customer liabilities, or proof of control.

15. Verification Procedure

15.1 Verification Sequence

The verifier MUST execute in the following order:

1. confirm the standard identifier, version, and machine identifier;
2. confirm the operating entity and the platform canonical domain;
3. confirm the in-scope entity list and test its completeness against independent group-structure evidence;
4. confirm the verification point in UTC and freeze the evidence set;
5. confirm the in-scope asset list;
6. retrieve the reserve address set and attribute every address to an in-scope entity;
7. verify proof of control for every reserve address, and its binding to the verification point;
8. test for address double counting and undisclosed shared addresses;
9. verify disclosure of borrowed or temporarily received assets and exclude them where §7.4 applies;
10. verify disclosure of lent, staked, or pledged customer assets and exclude them where §6.4 applies;
11. retrieve third-party depository confirmations directly from the issuing party;
12. recompute the reserve balance for each in-scope asset independently from on-chain or depository data;
13. verify the customer liability determination for each in-scope asset, including locked and pending-withdrawal balances;
14. verify the liability commitment structure and derive the total from it;
15. verify that a customer inclusion proof can be obtained and independently checked;
16. verify that no record can reduce the derived liability total, and that negative balances are not netted;

17 compute per-asset coverage and apply the 100% hard boundary to each asset separately;

18 verify that no cross-asset substitution is used to claim sufficiency;

19 verify segregation disclosures, including proprietary use of customer assets;

20 verify the insolvency position disclosure;

21 verify published maximum withdrawal processing times and the 30-day performance record;

22 verify withdrawal suspension disclosure, including any suspension in effect at the verification point;

23 verify privileged operation disclosure and control mechanisms;

24 verify ultimate beneficial ownership disclosure and related-party exposure;

25 verify material event records and notice deadlines;

26 verify the source, generation time, acquisition time, age, digest, and provider independence of all mandatory evidence;

27 verify consistency between the machine record and the human disclosure;

28 recompute all SHA-256 digests;

29 compute each requirement result and record the evidence used, the verification step, and any failure code;

30 compute the overall result under §16;

31 sign the verification record and record the signing time.

15.2 Determinism Requirement

The verification procedure MUST use fixed rules. Requirements MUST NOT be lowered based on the platform's size, brand, trading volume, or reputation.

15.3 Individual Result

Each requirement MUST record an applicability of `APPLICABLE` or `NOT_APPLICABLE`, and each applicable requirement MUST produce one of `PASS`, `FAIL`, or `NOT_ASSESSED`. Where the result is `FAIL`, a failure code from §17 MUST be recorded.

15.4 NOT_APPLICABLE

A requirement may be marked `NOT_APPLICABLE` only where this standard expressly permits and the verifier records the reason. It MUST NOT be used to bypass a generally applicable MUST requirement.

15.5 Re-computability

The verification record MUST contain, for every applicable requirement, the result, the evidence used, the verification step, and any failure code, such that the overall result can be re-computed by a second conforming implementation. Where the result cannot be re-computed, the result MUST be FAIL using `RMSEXCH-VER-001`.

15.6 Verification Signature

The verification record MUST be signed by the verifier using a verifiable digital signature, and MUST include the signing time, the signature algorithm, the key identifier, and the certificate or public key location. Where the signature is missing, invalid, or cannot be verified, the result MUST be FAIL using `RMSEXCH-SIG-001`.

16. Conformance Determination

16.1 PASS

The overall result may be PASS only when all of the following are simultaneously satisfied:

1. all applicable MUST requirements are PASS;
2. no MUST NOT is violated;
3. the in-scope entity list is complete and supported by independent group-structure evidence;
4. control is cryptographically proven for every reserve address counted;
5. per-asset coverage is at least 100% for **every** in-scope asset;
6. the liability commitment is published and customer inclusion proofs can be independently checked;
7. no withdrawal suspension is in effect at the verification point for any in-scope asset;
8. all mandatory evidence is present, valid, and within its stated freshness limits;
9. the human disclosure is consistent with the machine record;
10. there are no unresolved evidence conflicts;
11. the result can be re-computed by a second conforming implementation;
12. the verification record is signed by the verifier with a valid digital signature.

16.2 CONDITIONAL

The overall result may be CONDITIONAL only where all MUST and MUST NOT requirements are satisfied, all mandatory evidence is valid, and one or more SHOULD requirements are unsatisfied.

16.3 FAIL

Except where §16.6 applies, the overall result MUST be FAIL where any of the following occurs:

- any applicable MUST is unsatisfied;
- any MUST NOT is violated;
- an entity holding customer assets is omitted from the in-scope list;
- an address balance is counted as reserve without proof of control;
- the same address is counted more than once, or across more than one platform;
- borrowed or deployed assets are counted as reserve contrary to §6.4 or §7.4;
- per-asset coverage is below 100% for any in-scope asset;
- cross-asset substitution is used to claim sufficiency;
- no liability commitment is published, or customer inclusion proofs cannot be checked;
- a withdrawal suspension in effect at the verification point is undisclosed;
- a single undisclosed key can move customer assets;
- mandatory evidence is missing, expired, digest-mismatched, or provided by a party controlled by an in-scope entity;
- the human disclosure conflicts with the machine record;
- a second verification implementation cannot re-compute the same result;
- the verification record is unsigned or the signature is invalid.

16.4 NOT ASSESSED

`NOT ASSESSED` is used where verification is not formally complete, the evidence set has not been frozen, the verifier has not signed, or the platform falls within §1.2 by reason of suspended withdrawals or insolvency proceedings. It does not constitute a conformance conclusion.

16.5 Result Validity Period

Each verification result MUST have an expiry time. The expiry time MUST NOT be later than the earlier of:

1. **35 days** after the verification point;
2. the earliest expiry of any mandatory evidence under §14.4.

Because reserve and liability evidence under §14.4 is bound to a 24-hour window and to the verification point respectively, a result under this standard describes a point in time and MUST NOT be presented as a continuing state.

Upon a material event under §13, the result expires immediately regardless of the stated expiry time. Where the declared expiry exceeds the limits above, the result MUST be FAIL using `RMSEXCH-VER-002`.

16.6 DEFICIENT

`DEFICIENT` is used where **no requirement is affirmatively violated on the evidence available, but one or more mandatory items cannot be verified** because the required evidence is missing, incomplete, or expired, and the gap is curable by supplying that evidence.

`DEFICIENT` MUST be used, in preference to `FAIL`, where all of the following hold:

1. every requirement that could be evaluated on the available evidence is satisfied;
2. one or more mandatory items could not be evaluated because evidence was absent, incomplete, or beyond the freshness limits of §14.4;
3. no MUST NOT is violated and no evidence conflict under §14.7 is present.

Where any requirement is affirmatively violated on the available evidence, the result MUST be `FAIL`, not `DEFICIENT`. Where both a violation and a gap are present, `FAIL` takes precedence.

A `DEFICIENT` result MUST list every item that could not be verified and state, for each, the evidence that would resolve it.

Assessment from public information only. Where an assessment is not based on an evidence set submitted by the obligated party, but on publicly available information alone, the result MUST NOT be reported as `FAIL` on the ground that evidence is absent. Items that cannot be verified from the available information MUST be reported as `DEFICIENT` and identified individually. Such an assessment MUST state that the obligated party did not participate.

`DEFICIENT` states only that specified items could not be verified within the scope assessed. It is not a statement about the quality, soundness, or good faith of the obligated party.

17. Failure Codes

Code	Meaning
RMSEXCH-ID-001	Conforming subject identifier incomplete or not unique
RMSEXCH-ID-002	Operating entity cannot be confirmed
RMSEXCH-SCOPE-001	An entity holding customer assets is omitted from the in-scope list
RMSEXCH-SCOPE-002	Completeness declaration or independent group-structure evidence absent
RMSEXCH-SCOPE-003	Third-party depository confirmation absent or not issued directly to the verifier
RMSEXCH-SCOPE-004	Undisclosed deployment of customer assets
RMSEXCH-RES-001	Reserve address set incomplete or address not attributable to an in-scope entity
RMSEXCH-RES-002	Proof of control absent, invalid, or not bound to the verification point
RMSEXCH-RES-003	Address double counted or undisclosed shared address

Code	Meaning
RMSEXCH-RES-004	Undisclosed borrowed or temporarily received assets counted as reserve
RMSEXCH-RES-005	Reserve balance cannot be re-computed
RMSEXCH-LIA-001	Customer liability determination omits a required category
RMSEXCH-LIA-002	Liability commitment absent, or total not derivable from it
RMSEXCH-LIA-003	Customer inclusion proof unavailable or verification method unpublished
RMSEXCH-LIA-004	Liability total reducible by a record, or negative balances netted
RMSEXCH-COV-001	Per-asset coverage below 100%
RMSEXCH-COV-002	Customer liabilities exist for an asset with no disclosed reserve
RMSEXCH-COV-003	Cross-asset substitution used to claim sufficiency
RMSEXCH-SEG-001	Legal segregation disclosure absent
RMSEXCH-SEG-002	Operational segregation or commingling accounting disclosure absent
RMSEXCH-SEG-003	Undisclosed proprietary use of customer assets
RMSEXCH-SEG-004	Insolvency position disclosure absent
RMSEXCH-WDR-001	Maximum withdrawal processing time not quantified
RMSEXCH-WDR-002	30-day withdrawal performance record absent
RMSEXCH-WDR-003	Undisclosed withdrawal suspension
RMSEXCH-WDR-004	Undisclosed selective processing of withdrawals
RMSEXCH-OPS-001	Privileged operation disclosure absent or incomplete
RMSEXCH-OPS-002	Customer assets movable by a single undisclosed key
RMSEXCH-OPS-003	Ultimate beneficial ownership neither disclosed nor lawfully withheld
RMSEXCH-OPS-004	Undisclosed related-party exposure of customer assets
RMSEXCH-EVT-001	Material event not recorded or published within 24 hours
RMSEXCH-DAT-001	Human disclosure inconsistent with machine record
RMSEXCH-EVD-001	Mandatory evidence missing
RMSEXCH-EVD-002	Evidence digest mismatch or incorrect format
RMSEXCH-EVD-003	Evidence exceeds the maximum age stated in §14.4
RMSEXCH-EVD-004	Evidence provider independence undisclosed, or provider controlled by an in-scope entity
RMSEXCH-SIG-001	Digital signature missing, invalid, or unverifiable
RMSEXCH-VER-001	Verification result cannot be re-computed
RMSEXCH-VER-002	Result validity period exceeds the limits of §16.5

18. Machine Interface

18.1 Conformance Record

```
{
  "record_id": "",
  "schema_version": "1.0",
  "verification_point": "",
  "result_expires_at": "",
  "digest_algorithm": "sha-256",
  "standard": {},
  "conformity_subject": {},
  "operating_entity": {},
  "in_scope_entities": [],
  "assets": [],
  "reserve_addresses": [],
  "liability_commitment": {},
  "segregation": {},
  "withdrawals": {},
  "privileged_operations": [],
```

```
  "related_party_exposure": [],
  "material_events": [],
  "evidence": [],
  "requirement_results": [],
  "human_disclosure": {},
  "overall_result": {},
  "verifier": {},
  "signature": {}
}
```

`assets` MUST contain one entry per in-scope asset, each carrying its reserve balance, customer liability, and per-asset coverage ratio. A single aggregate figure across assets MUST NOT be recorded in place of per-asset entries.

18.2 Quantity Format

All asset quantities MUST be expressed as decimal strings in the smallest indivisible unit of the asset, together with the unit name and the number of decimals. Binary floating-point values MUST NOT be used.

```
{
  "asset": "BTC",
  "network": "bitcoin",
  "reserve_balance": "1234500000000",
  "customer_liability": "1230000000000",
  "unit": "satoshi",
  "decimals": 8,
  "coverage_ratio": "1.003658"
}
```

18.3 Time Format

All times MUST use ISO 8601 UTC format with a precision of at least one second. The `verification_point` MUST be a single value used for every asset in the record.

18.4 Address Records

Each reserve address record MUST contain the network identifier, the address, the holding in-scope entity, the balance at the verification point, the proof-of-control method, and a reference to the proof.

```
{
  "network": "",
  "address": "",
  "holding_entity_id": "",
  "balance": "",
  "control_proof_method": "SIGNATURE | SPEND",
  "control_proof_reference": "",
  "control_proof_time": ""
}
```

18.5 Human–Machine Consistency

The in-scope entity list, the per-asset reserve balance, the per-asset customer liability, the per-asset coverage ratio, any withdrawal suspension in effect, and the overall result MUST be consistent between the human disclosure and the machine record. Where they conflict, the result MUST be FAIL using `RMSEXCH-DAT-001`.

18.6 Canonicalisation and Digest

Before signing, a machine record MUST use a deterministic canonicalisation procedure and generate a SHA-256 digest.

18.7 Digest Algorithm Identifier

The machine record MUST record the digest algorithm identifier. The default value is `sha-256`. A verifier MUST NOT use an unregistered digest algorithm to produce a formal verification record.

19. Security Considerations

19.1 Principal Threats

This standard considers at least: assets held by an undisclosed affiliated entity; assets borrowed shortly before the verification point and returned shortly after; the same reserve address presented by more than one platform; an address balance presented without control; customer records omitted or reduced in the liability commitment; negative balances netted against positive ones; a shortfall in one asset concealed by a surplus in another; customer assets lent, staked, or pledged without disclosure; proprietary trading against customer assets; withdrawals processed selectively for visible customers; an undisclosed withdrawal suspension; a single key able to move customer assets; an attestation firm controlled by an in-scope entity; and verifier conflict of interest.

19.2 Security Controls

The obligated party and the verifier MUST verify evidence digests and signatures, retrieve on-chain data independently, obtain third-party confirmations directly from the issuing party, bind proofs of control to the verification point, compute coverage per asset, retain failure results, and sign the verification record.

19.3 Verifier Independence

The verifier MUST disclose commercial, fee, ownership, control, and other interest relationships with any in-scope entity that may affect independence. An undisclosed material interest relationship renders the verification result invalid.

19.4 Residual Risk

Even where the result is PASS, there may still be losses after the verification point, undetected fraud, loss of keys, insolvency of a counterparty or depository, an asset held by an entity that the group structure evidence did not reveal, a change in the reserve position immediately after the verification point, regulatory action, or concealment by an evidence provider.

A PASS under this standard describes a point in time. It does not establish that the position held before that point or continues after it.

19.5 Threat Mapping Matrix

Threat	Control Requirement	Evidence	Failure Code
Assets held by an undisclosed affiliate	§6.1, §6.2	EVD-002	RMSEXCH-SCOPE-001, RMSEXCH-SCOPE-002
Borrowed assets shown as reserve	§7.4	EVD-003, EVD-005	RMSEXCH-RES-004
Address shared across platforms	§7.3	EVD-003, EVD-004	RMSEXCH-RES-003
Balance shown without control	§7.2, §4.8	EVD-004	RMSEXCH-RES-002
Customer records omitted from liabilities	§8.2, §8.3	EVD-006, EVD-007	RMSEXCH-LIA-002, RMSEXCH-LIA-003
Negative balances netted	§8.4	EVD-007	RMSEXCH-LIA-004
Shortfall concealed by cross-asset surplus	§4.5, §9.1, §9.4	EVD-005, EVD-006	RMSEXCH-COV-001, RMSEXCH-COV-003
Customer assets lent or pledged undisclosed	§6.4	EVD-012	RMSEXCH-SCOPE-004
Proprietary trading against customer assets	§10.3	EVD-008	RMSEXCH-SEG-003
Selective withdrawal processing	§11.4	EVD-009	RMSEXCH-WDR-004
Undisclosed withdrawal suspension	§11.3	EVD-009, EVD-014	RMSEXCH-WDR-003
Single key moves customer assets	§12.2	EVD-010	RMSEXCH-OPS-002

Threat	Control Requirement	Evidence	Failure Code
Related-party exposure undisclosed	§12.4	EVD-008, EVD-010	RMSEXCH-OPS-004
Attestation firm controlled by the group	§14.5, §4.1	EVD-011, EVD-013	RMSEXCH-EVD-004
Stale reserve or liability evidence	§14.4	EVD-004 to EVD-007	RMSEXCH-EVD-003
Result presented as a continuing state	§16.5, §19.4	EVD-015	RMSEXCH-VER-002
Verifier conflict of interest	§1.5, §19.3	—	verification result invalid

20. Conformance Claim

20.1 Minimum Fields

A conformance claim MUST include at least the standard identifier and version, the operating entity, the platform canonical domain, the in-scope entity list, the in-scope asset list with per-asset coverage, the verification point, the result, the result expiry, the evidence set digest, the verifier identity, the signature, and any failure codes.

20.2 Example

```
{
  "standard_id": "RM-S-EXCH-001",
  "standard_version": "v1.0-F",
  "operating_entity_legal_name": "Example Exchange Ltd",
  "canonical_domain": "example-exchange.com",
  "in_scope_entities": ["Example Exchange Ltd", "Example Custody SA"],
  "verification_point": "2026-01-01T00:00:00Z",
  "result_expires_at": "2026-01-02T00:00:00Z",
  "assets": [
    {"asset": "BTC", "coverage_ratio": "1.003658"},
    {"asset": "USDT", "coverage_ratio": "1.011200"}
  ],
  "verification_result": "PASS",
  "evidence_set_sha256": "",
  "verifier_id": "",
  "signature": ""
}
```

20.3 Prohibited Statements

A conformance claim MUST NOT use expressions such as "fully backed", "1:1 backed", "fully reserved", "completely safe", "zero risk", "government approved", "RuleMark guaranteed", "permanently valid", "always available", or "audited" where the evidence is an attestation rather than an audit.

A conformance claim MUST NOT be described as "proof of reserves" unless customer liabilities have been proven under §8. A claim MUST NOT be presented as describing a continuing state.

21. Test Cases

21.1 PASS Case

All in-scope entities are named and supported by independent group-structure evidence; every reserve address carries a valid proof of control bound to the verification point; no address is double counted; no borrowed or deployed assets are counted; per-asset coverage is 100.37% for BTC and 101.12% for USDT; the liability commitment is published and a customer inclusion proof is independently checked; no withdrawal suspension is in effect; segregation, privileged operations, and related-party exposure are disclosed; all mandatory evidence is present, fresh, and independently provided; the verification record is signed.

Expected result: `PASS`

21.2 Undisclosed Affiliate

Independent corporate records show a group member holding customer assets that is absent from the in-scope entity list.

Expected result: `FAIL`, `RMSEXCH-SCOPE-001`

21.3 Balance Without Control

An address contributing 12% of the BTC reserve has no signature and no verifiable spend within 24 hours of the verification point.

Expected result: `FAIL`, `RMSEXCH-RES-002`

21.4 Cross-Asset Concealment

BTC coverage is 152%; USDT coverage is 61%. The platform asserts that aggregate coverage across both assets exceeds 100%.

Expected result: `FAIL`, `RMSEXCH-COV-001`, `RMSEXCH-COV-003`

21.5 No Liability Commitment

Reserve addresses and proofs of control are complete and valid; no liability commitment is published and no inclusion proof is available.

Expected result: `FAIL`, `RMSEXCH-LIA-002`, `RMSEXCH-LIA-003`

21.6 Stale Reserve Snapshot

All requirements are otherwise satisfied; the reserve balance snapshot was generated 96 hours before the verification point.

Expected result: `FAIL`, `RMSEXCH-EVD-003`

21.7 SHOULD Not Satisfied

All MUST and MUST NOT requirements are satisfied and all mandatory evidence is valid; the platform has not obtained an independent attestation on liability completeness, which is a SHOULD under §8.5.

Expected result: `CONDITIONAL`

21.8 Public Information Only

The assessment is based on the platform's published transparency page alone: reserve addresses and balances are published and independently checkable on chain; proofs of control, the liability commitment, segregation disclosure, withdrawal performance, and privileged operation disclosure are not published; the platform did not participate.

Expected result: `DEFICIENT`, with each unverifiable item listed individually

22. Requirement Traceability Matrix

Requirement Area	Clause	Core Evidence	Verification Step	Failure Code
Subject identity	§1.4, §5.1	EVD-001	2	RMSEXCH-ID-001
Operating entity	§5.2	EVD-001	2	RMSEXCH-ID-002
In-scope entity completeness	§6.1, §6.2	EVD-002	3	RMSEXCH-SCOPE-001, RMSEXCH-SCOPE-002
Third-party depository	§6.3	EVD-011	11	RMSEXCH-SCOPE-003
Deployed customer assets	§6.4	EVD-012	10	RMSEXCH-SCOPE-004
Reserve address disclosure	§7.1	EVD-003	6	RMSEXCH-RES-001
Proof of control	§7.2	EVD-004	7	RMSEXCH-RES-002
Address exclusivity	§7.3	EVD-003, EVD-004	8	RMSEXCH-RES-003
Borrowed assets	§7.4	EVD-003, EVD-005	9	RMSEXCH-RES-004
Reserve balance re-computation	§7.5	EVD-005	12	RMSEXCH-RES-005
Liability determination	§8.1	EVD-006	13	RMSEXCH-LIA-001
Liability commitment	§8.2	EVD-007	14	RMSEXCH-LIA-002
Inclusion proof	§8.3	EVD-007	15	RMSEXCH-LIA-003
Netting prohibition	§8.4	EVD-007	16	RMSEXCH-LIA-004
Per-asset coverage	§9.1, §9.2	EVD-005, EVD-006	17	RMSEXCH-COV-001
Declared ratio consistency	§9.2, §18.2	EVD-005, EVD-006, EVD-015	12, 17	RMSEXCH-RES-005
Liability without reserve	§9.3	EVD-003, EVD-006	17	RMSEXCH-COV-002
Cross-asset substitution	§9.4	EVD-005, EVD-006	18	RMSEXCH-COV-003
Legal segregation	§10.1	EVD-008	19	RMSEXCH-SEG-001
Operational segregation	§10.2	EVD-008	19	RMSEXCH-SEG-002
Proprietary use	§10.3	EVD-008	19	RMSEXCH-SEG-003
Insolvency position	§10.4	EVD-008	20	RMSEXCH-SEG-004
Withdrawal processing time	§11.1	EVD-009	21	RMSEXCH-WDR-001
Withdrawal performance	§11.2	EVD-009	21	RMSEXCH-WDR-002
Suspension disclosure	§11.3	EVD-009, EVD-014	22	RMSEXCH-WDR-003
Selective processing	§11.4	EVD-009	22	RMSEXCH-WDR-004
Privileged operations	§12.1	EVD-010	23	RMSEXCH-OPS-001
Single-key restriction	§12.2	EVD-010	23	RMSEXCH-OPS-002
Beneficial ownership	§12.3	EVD-001, EVD-002	24	RMSEXCH-OPS-003
Related-party exposure	§12.4	EVD-008, EVD-010	24	RMSEXCH-OPS-004
Material events	§13.2	EVD-014	25	RMSEXCH-EVT-001
Evidence metadata	§14.2	EVD-001 to EVD-017	26	RMSEXCH-EVD-001
Evidence digests	§14.3	EVD-015, EVD-017	28	RMSEXCH-EVD-002
Evidence freshness	§14.4	EVD-004 to EVD-007, EVD-011	26	RMSEXCH-EVD-003
Provider independence	§14.5	EVD-011, EVD-013	26	RMSEXCH-EVD-004
Human–machine consistency	§18.5	EVD-016	27	RMSEXCH-DAT-001
Re-computability	§15.5	EVD-015	29, 30	RMSEXCH-VER-001
Result validity	§16.5	EVD-015	30	RMSEXCH-VER-002
Verification signature	§15.6	EVD-017	31	RMSEXCH-SIG-001
Independent liability attestation (SHOULD)	§8.5	EVD-013	26	—
Test withdrawal (SHOULD)	§11.5	EVD-009	21	—

23. Lifecycle

23.1 Draft

In Draft status, this standard MUST NOT serve as a basis for formal RuleMark conformance.

23.2 Frozen

Once formally published, this standard may be referenced and implemented.

23.3 Frozen

A version may be frozen only after all of the following are satisfied:

- the automated consistency check reports zero errors;
- each MUST is mapped to evidence, a verification step, and a failure code;
- the machine schema accepts a conforming record and rejects non-conforming records;
- failure codes are stable;
- test cases pass;
- the human and machine versions are consistent;
- all normative references are confirmed to exist. This standard is self-contained; normative references are limited to the public technical specifications listed in §24.1;
- a SHA-256 digest has been generated for the normative files and the digest manifest has been signed by RuleMark;
- RuleMark sovereign approval has been recorded, stating the approver, the date, the approved version, and the approved digest.

Independent review by an external expert is recommended and, where performed, MUST be recorded with the reviewer's identity, the reviewed version, and the reviewed digest. It is not a condition of freezing.

23.4 Superseded

Where a new version replaces this version, it MUST record the new version number, effective date, compatibility changes, migration rules, and the last valid date of the old version.

23.5 Withdrawn

After withdrawal, this standard MUST NOT be used for new conformance claims. Historical verification records MUST continue to be retained.

24. References and Dependencies

24.1 Normative Technical References

- FIPS 180-4 (SHA-256);
- RFC 8785 JSON Canonicalization Scheme;
- ISO 8601 date and time representation;
- ISO 4217 currency codes;

- BIP-137 and EIP-191 signed message formats, for proof of control;
- JSON Schema Draft 2020-12.

24.2 RuleMark Dependencies

This standard is self-contained and does not depend on any external RuleMark standard. Canonical identity, evidence, verification and determination, digital signature, and lifecycle rules are defined internally at §5, §14, §15, §16, §15.6, and §23 respectively.

Where RuleMark later issues corresponding core-layer standards, a subsequent version of this standard MAY align these internal clauses with normative references to those standards. Until then, this standard MUST NOT cite an identifier that has not been issued.

24.3 Informative References

ISAE 3000 (Revised) and AT-C 105 may be referenced within evidence as the framework under which an attestation was prepared. This standard does not repeat or replace the assessment performed under those frameworks.

25. Implementation Requirements

An implementation conforming to this standard MUST be able to:

1. enumerate in-scope entities and test the list against independent group-structure evidence;
2. retrieve reserve addresses and balances independently from on-chain or depository sources;
3. verify a proof of control bound to the verification point for each address;
4. detect double counting of addresses within and across platforms;
5. exclude borrowed and deployed assets from reserve balance;
6. determine customer liabilities per asset including locked and pending-withdrawal balances;
7. validate a liability commitment and derive the total from it;
8. check a customer inclusion proof;
9. compute coverage per asset at the smallest indivisible unit, applying a 100% hard boundary;
10. reject cross-asset substitution as a demonstration of sufficiency;
11. evaluate segregation, withdrawal, privileged operation, and related-party disclosures;
12. verify evidence metadata, age, digests, and provider independence;
13. verify consistency between the machine record and the human disclosure;
14. produce a deterministic conformance result with per-requirement traceability;
15. bound the result expiry to the earliest evidence expiry;
16. sign and retain the verification record;
17. allow a second conforming implementation to re-compute the same overall result.

26. Final Non-Claim

A PASS result under RM-S-EXCH-001 indicates only:

> At the specified verification point, under the specified standard version, for the specified platform, the specified in-scope entities, the specified in-scope assets, and the specified evidence set, all applicable mandatory requirements of RM-S-EXCH-001 are satisfied.

PASS does not indicate future continued conformance, solvency, going concern, or the safety of customer assets. It does not indicate that customer assets will remain available for withdrawal, that no fraud exists, that listed assets are of any particular quality or legality, that market conduct is fair, that any licence is valid, that cyber-security defences are effective, that the position held before the verification point or continues after it, regulatory approval, an investment recommendation, or a RuleMark guarantee.

Document Status Declaration

```
Standard ID: RM-S-EXCH-001
Version: v1.0-F
Status: FROZEN
Publication Date: 2026-07-23
Effective Date: 2026-07-23
Normative Status: NORMATIVE
Conformance Use: AUTHORIZED
Machine ID: rulemark:standard:rm-s-exch-001:v1.0-F
```

This standard MUST NOT be marked `FROZEN` before the automated consistency check reports zero errors, the machine schema has been tested against conforming and non-conforming records, the digest manifest has been signed by RuleMark, and RuleMark sovereign approval has been recorded.