RM-S-STABLE-001 Stablecoin Trust Verification Standard

Standard ID: RM-S-STABLE-001 **Version:** v1.0-F **Status:** Frozen **Publication Date:** 2026-07-22 **Effective Date:** 2026-07-22 **Standard Family:** RM-S — Canonical Standards Namespace **Normative Status:** Normative **Publisher:** RuleMark **Document Language:** English **Machine ID:** `rulemark:standard:rm-s-stable-001:v1.0-F`

Document Control

Field	Content
Standard ID	RM-S-STABLE-001
Standard Name	Stablecoin Trust Verification Standard
Version	v1.0-F
Status	Frozen
Publication Date	2026-07-22
Effective Date	2026-07-22
Standard Family	RM-S
Domain	Stablecoin, digital asset, reserve verification, redemption, disclosure
Normative Status	Normative
Target Subject	Fiat-referenced, reserve-backed stablecoins that promise redemption
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 trust basis of a stablecoin.

This standard requires verification of the stablecoin's issuer identity, token canonical identity, circulating supply, outstanding liabilities, reserve asset coverage, reserve asset quality, asset segregation, custody arrangements, redemption rights, disclosure, independent attestation, smart-contract permissions, material events, machine-readable data, evidence integrity, and the final verification result.

This standard does not determine whether a stablecoin is worth investing in, and does not guarantee that a stablecoin will not de-peg, will not become insolvent, will not incur losses, or will be able to complete redemption under all circumstances.

This standard answers only:

> At a specified time, under a specified standard version, for a specified stablecoin arrangement and a specified evidence set, does the stablecoin satisfy the applicable requirements of RM-S-STABLE-001?

1. Applicability

1.1 Conditions of Applicability

This standard applies to a digital token that meets all of the following conditions:

1 issued through a blockchain, distributed ledger, or other verifiable digital system;

2 claims to maintain a stable value referenced to a fiat currency;

3 claims to be backed by reserve assets;

4 has an issuance, minting, burning, or redemption mechanism;

5 has an identifiable issuer or responsible party;

6 circulates to the public, institutions, exchanges, payment systems, wallets, or machine systems.

1.2 Out of Scope

This standard does not apply to:

- algorithmic stablecoins;
- stablecoins without an identifiable responsible party;
- stablecoins collateralized solely by over-collateralized crypto assets;
- commodity-referenced tokens;
- multi-asset or basket-referenced tokens;
- central bank digital currencies;
- tokenized bank deposits;
- security tokens;
- points for use in closed systems only;
- digital assets that do not promise redemption;
- test tokens not yet in public circulation.

The above subjects should be governed by separate standards or dedicated profiles.

1.3 Non-Goals

This standard:

- does not provide investment advice;
- does not predict market price;
- does not guarantee that a stablecoin will not de-peg;
- does not guarantee that the issuer will not become insolvent;
- does not guarantee that reserve assets will not incur losses;
- does not certify legal compliance in any specific jurisdiction;
- does not replace a regulator, auditor, court, or legal counsel;
- does not constitute a credit rating;
- does not decide whether a stablecoin should be listed by an exchange;
- does not constitute a RuleMark guarantee, recommendation, or endorsement of any stablecoin.

1.4 Conforming Subject

A conformance claim MUST correspond to one clear, unique, and reproducibly identifiable stablecoin arrangement, including at least:

- issuing legal entity;
- stablecoin name and symbol;

- reference currency;
- blockchain or ledger;
- smart-contract address;
- contract version;
- reserve arrangement;
- custody arrangement;
- redemption arrangement;
- verification point;
- evidence set.

Where multiple issuing entities, multiple contracts, or multiple chains exist under one brand, a conformance claim MUST NOT be made for the brand in the aggregate only.

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:

- **Issuer**: the legal entity responsible for the stablecoin's issuance, liabilities, reserves, or redemption; it is the subject of the conformance claim.
- **Verifier**: the party or machine system that performs verification under this standard and signs the verification result.
- **Machine Validator**: the system that performs deterministic schema and rule validation on machine records.
- **Evidence Provider**: a party that produces or provides an item of evidence in the evidence set, such as a custodian, attestation firm, or on-chain data source.

Where a commercial, fee, ownership, or control relationship exists between the Verifier and the Issuer, it MUST be disclosed under §19.3. An undisclosed material conflict of interest 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
Stablecoin	A digital token that claims to maintain a stable value relative to a specified reference currency. This standard covers only fiat-referenced, reserve-backed stablecoins that promise redemption.
Reference Currency	The fiat currency against which the stablecoin claims to maintain a value correspondence.

Term	Definition
Issuer	The legal entity bearing express responsibility for the stablecoin's issuance, liabilities, reserves, or redemption.
Responsible Party	A party bearing identifiable responsibility for a key function within the stablecoin arrangement.
Stablecoin Arrangement	The combination of issuer, token, ledger, reserves, custody, redemption, and governance mechanisms.
Canonical Identity	The set of identifiers that uniquely identifies the issuer, token, chain, contract, and version.
Circulating Supply	The quantity of stablecoins issued and not yet redeemed or effectively burned as of the verification point.
Outstanding Liabilities	The total redemption obligations borne by the issuer for issued stablecoins.
Reserve Assets	Assets designated and held to support the stablecoin's redemption obligations.
Eligible Reserve Assets	Reserve assets that satisfy the identity, ownership, valuation, segregation, custody, and evidence requirements of this standard.
Reserve Coverage Ratio	The verified value of eligible reserve assets divided by the verified value of outstanding liabilities.
Reserve Segregation	The legal, accounting, and operational separation of reserve assets from the issuer's own assets and other unrelated assets.
Custodian	The designated party that holds, controls, or records reserve assets.
Redemption	The return of a stablecoin by a holder in exchange for the reference currency or an expressly specified settlement asset.
Direct Redemption	The holder may submit a redemption request directly to the issuer or an authorized redemption party.
Attestation Report	A report issued by an independent professional firm on specified information, period, and procedures.
Evidence Set	All documents, records, data, signatures, digests, and source information used in one verification.
Verification Point	The specific UTC time used to uniformly compute supply, liabilities, reserves, and other data.
Material Event	An event that may alter reserve coverage, redemption capacity, custody arrangements, responsible parties, contract permissions, or the conformance result.
Verifier	The party or machine system that performs verification under this standard and signs the verification result.
Conformance Claim	A signed conclusion as to whether a specified stablecoin arrangement satisfies this standard at a specified verification point.

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.

Where such a word is used, the clause MUST also define:

- a measurable value;
- a time range;
- test conditions;
- the responsible party;
- the determination method.

4. Core Principles

4.1 Evidence First

Any trust conclusion MUST be supported by identifiable, verifiable, and time-bounded evidence. An issuer statement by itself MUST NOT be automatically treated as independent evidence.

4.2 Identifiable Responsibility

It MUST be possible to identify the parties responsible for issuance, reserve management, reserve custody, redemption, contract management, and disclosure.

4.3 Same-Point Reconciliation

Supply, outstanding liabilities, and reserve data MUST use the same verification point. Where the exact same point cannot be used, a clear and re-computable adjustment method MUST be provided.

4.4 Two-Sided Asset and Liability Verification

Verification MUST simultaneously confirm eligible reserve assets, outstanding liabilities, and the computed relationship between the two.

4.5 Legal and Technical Dual Verification

On-chain data MUST NOT replace verification of reserve ownership, reserve segregation, custody, redemption rights, and legal responsibility; legal documents MUST NOT replace verification of on-chain supply and contract permissions.

4.6 Non-Discretionary Determination

The same standard version, the same inputs, and the same evidence set MUST produce the same result.

4.7 Machine Readability

Core identity, data, evidence, and verification results MUST be provided in a structured machine representation.

4.8 Minimum Necessary Claim

A verification result MUST NOT exceed the actual scope of verification.

4.9 Freshness

Expired evidence MUST NOT serve as valid proof of current state.

4.10 Traceability

Every mandatory requirement MUST be traceable to evidence, verification procedure, individual result, and final determination.

5. Canonical Identity and Responsible Parties

5.1 Stablecoin Canonical Identity

Every stablecoin arrangement submitted for verification MUST have a unique canonical identity, containing at least:

```
{
  "issuer_legal_name": "",
  "issuer_identifier": "",
  "token_name": "",
  "token_symbol": "",
  "reference_currency": "",
  "network": "",
  "chain_id": "",
  "contract_address": "",
  "contract_version": "",
  "deployment_transaction": ""
}
```

5.2 Multi-Chain Issuance

Where a stablecoin is issued on multiple chains, each chain MUST separately record the chain name, chain ID, contract address, contract version, issued amount, frozen amount, burn-pending-settlement amount, and cross-chain locked amount. Brand-level totals MUST NOT replace per-chain data.

5.3 Responsible Party Registration

The issuer MUST disclose its legal name, registration number, jurisdiction of registration, registered address, official website, official machine interface, and the parties responsible for reserves, custody, redemption, contract management, and disclosure.

5.4 Change of Responsibility

Where a responsible party changes, the issuer MUST:

1. record the party before and after the change;
2. record the effective time;
3. publish a material event notice;
4. update machine records;
5. trigger re-verification.

6. Supply and Liability Verification

6.1 Verification Point

Each verification MUST specify one UTC verification point in the format `YYYY-MM-DDTHH:MM:SSZ`.

6.2 Total Issued Amount

The verifier MUST independently compute the total issued amount from on-chain data or an authoritative issuance ledger. Aggregate figures provided by the issuer MUST NOT be the sole computation source.

6.3 Effective Circulating Supply

Effective circulating supply is computed as:

```
effective circulating supply = total issued amount − completed burn amount − completed redemption-settled amount − exclusi
```

Any exclusion MUST record the reason for exclusion, the legal or accounting basis, the amount, the address or record identifier, the timestamp, and the evidence.

6.4 Frozen Stablecoins

Stablecoins frozen by the issuer but still constituting a redemption obligation MUST continue to be included in outstanding liabilities.

6.5 Burned-Pending-Settlement Stablecoins

Stablecoins submitted for burning but for which the corresponding fiat or settlement-asset payment has not been completed MUST be disclosed separately. Unless the redemption obligation has terminated, they MUST NOT be deducted from outstanding liabilities.

6.6 Cross-Chain Assets

Cross-chain bridges, wrapped tokens, or lock-and-mint mechanisms MUST NOT cause the same economic unit to be double-counted. The verifier MUST reconcile native-chain supply, locked amount, destination-chain minted amount, burn and unlock records, bridge failures, and pending transactions.

6.7 Outstanding Liabilities

Outstanding liabilities MUST include at least:

- directly redeemable stablecoins;
- stablecoins redeemable through an authorized intermediary;
- frozen stablecoins that still carry a redemption obligation;
- burned stablecoins for which settlement is not yet complete;
- other unterminated stablecoin payment obligations.

6.8 Liability Computation Consistency

The currency, valuation time, and exchange-rate source of outstanding liabilities MUST be consistent with the reserve coverage ratio computation.

7. Reserve Asset Requirements

7.1 Minimum Coverage Requirement

At the verification point:

```
verified value of eligible reserve assets ≥ verified value of outstanding liabilities
reserve coverage ratio = verified value of eligible reserve assets ÷ verified value of outstanding liabilities
```

The minimum reserve coverage ratio required for PASS is `100%`.

7.2 Reserve Asset Detail

Each reserve asset MUST disclose asset type, issuer, currency, nominal value, book value, verified value, maturity date, liquidity class, custodian, account identifier, valuation source, haircut or impairment, lien, pledge, and related-party attribute.

7.3 Eligible Reserve Asset Conditions

An asset may be counted as an eligible reserve asset only when it simultaneously satisfies all of the following:

1. ownership or beneficial interest is verifiable;
2. held in a designated account;
3. not double-counted;
4. not used to support other undisclosed liabilities;
5. free of undisclosed liens or pledges;
6. valuation method is re-computable;
7. custody status is verifiable;
8. currency and exchange rate are explicit;
9. valid at the verification point;
10. able to provide liquidity within the disclosed redemption period, or an explicit liquidity adjustment has been made.

7.4 Ineligible Assets

The following assets MUST NOT be counted as eligible reserve assets:

- assets whose ownership or custody status cannot be confirmed;
- assets already double-counted;
- assets supporting other undisclosed liabilities;
- assets with undisclosed pledges or liens;
- assets for which no reliable valuation can be obtained;
- assets frozen and unavailable to fulfill redemption;
- undisclosed debt instruments of the issuer or related parties;
- assets for which no verifiable record exists.

7.5 Reserve Asset Concentration

The issuer MUST disclose the proportions attributable to a single asset, single issuer, single custodian, single bank, single jurisdiction, and single maturity band.

7.6 Liquidity Structure

The issuer MUST classify reserve assets into at least: available same-day, realizable within 7 days, realizable within 30 days, over 30 days, and restricted or not immediately realizable. The liquidity classification MUST match the published redemption times.

7.7 Liquidity Stress Disclosure

The issuer SHOULD disclose the realizable capacity of reserves under the following redemption stress scenarios, and quantify the proportion of redemptions that can be satisfied in each scenario:

1. large single-day redemption (single-day redemption requests reaching a specified percentage of effective circulating supply);
2. seven consecutive days of redemption;
3. a single major custodian being unavailable;
4. bank settlement disruption;
5. widening market-price haircuts on reserve assets.

Failure to provide liquidity stress disclosure does not cause FAIL, but where this SHOULD is not satisfied it may affect a CONDITIONAL determination under §16.2.

8. Reserve Segregation and Custody

8.1 Legal Segregation

Reserve assets MUST be legally separated from the issuer's own assets, related-party assets, other product assets, other client assets, and assets corresponding to undisclosed liabilities.

8.2 Accounting Segregation

Reserve assets MUST have independent ledgers, accounts, or sub-account records. Internal labels alone MUST NOT be relied upon to prove segregation.

8.3 Operational Segregation

Transfer authority over reserve assets MUST be restricted to disclosed authorized parties and purposes.

8.4 Custodian Disclosure

The issuer MUST disclose the custodian's legal name, regulatory or licensing status, custody jurisdiction, account structure, account control, transfer authorization, rehypothecation rules, and commingling rules.

8.5 Rehypothecation

Reserve assets MUST NOT be rehypothecated, unless expressly permitted by a dedicated profile, fully disclosed by the issuer, with coverage adjusted and the related risk separately verified. In RM-S-STABLE-001 v1.0-F, undisclosed rehypothecation directly results in FAIL, using failure code `RMFSTABLE-CUS-002`.

8.6 Insolvency Rights

The issuer MUST disclose the holders' legal rights over reserve assets upon insolvency of the issuer or custodian, the priority of those rights, whether the assets form part of the bankruptcy estate, other priority creditors, and the redemption or distribution procedure.

8.7 Legal Proof of Bankruptcy Remoteness

Where the issuer claims that reserve assets have a bankruptcy-remoteness attribute, it MUST provide an independent legal opinion or equivalent legal proof, and that legal opinion MUST cover:

1. the legal ownership of the reserve assets;
2. the scope of the bankruptcy estate (whether the reserve assets would be included in the bankruptcy estate of the issuer or custodian);
3. the priority of holders' rights;
4. the applicable law.

Where the above legal proof is not provided, the issuer MUST NOT claim that the reserves have a bankruptcy-remoteness attribute; it may disclose only accounting or operational segregation arrangements. The corresponding legal opinion MUST enter the §14 evidence set as EVD-015.

> Note: the legal wording of this clause MUST be confirmed by a bankruptcy and trust law expert before formal freezing.

9. Reserve Valuation

9.1 Valuation Policy

The issuer MUST publish a reserve valuation policy specifying at least the price source, exchange-rate source, valuation time, haircut method, impairment method, handling where no market price exists, and handling of price conflicts.

9.2 Independent Re-computation

The verifier MUST be able to independently re-compute each asset's verified value, total reserve value, outstanding liabilities, and the reserve coverage ratio.

9.3 Foreign-Currency Assets

Where a reserve asset differs from the reference currency, the issuer MUST disclose the exchange rate used, the rate source, the rate time, the FX-risk adjustment, and any hedging arrangement.

9.4 Valuation Haircut

Where price volatility, credit risk, insufficient liquidity, maturity mismatch, FX risk, legal restriction, or custody restriction exists, the verified value MUST apply an explicit haircut. Book value MUST NOT be automatically treated as verified value.

9.5 Deterministic Computation Rules

To ensure that different verifiers produce the same result for the same evidence, computation MUST comply with the following rules:

1. **Numeric precision**: all monetary amounts MUST be represented as strings per §18.3, using the decimals declared for that asset's currency; intermediate computations MUST retain at least 8 decimal places.
2. **Rounding rule**: where rounding is required, round half up to the declared number of decimals MUST be used.
3. **Exchange-rate precision**: exchange rates MUST retain at least 8 decimal places, and the rate source and rate time MUST be recorded.
4. **Coverage-ratio precision**: the reserve coverage ratio MUST be computed to at least 6 decimal places before the boundary determination is made.
5. **Boundary tolerance**: `100%` coverage is a hard boundary. No rounding or tolerance may cause a situation where the verified reserve value is below the verified outstanding-liability value to be determined as PASS; that is, rounding and tolerance MUST NOT produce a PASS in such a situation. Where the verified value of eligible reserves < the verified value of outstanding liabilities, regardless of how small the difference, the result MUST be FAIL using `RMFSTABLE-RES-001`.

10. Redemption Requirements

10.1 Redemption Rights Disclosure

The issuer MUST disclose who is entitled to redeem, whether direct redemption is permitted, whether an authorized intermediary is required, the minimum amount, fees, settlement asset, processing time, identity-verification requirements, and refusal or suspension conditions.

The issuer MUST further disclose information on the legal enforceability of the redemption claim, including at least:

1. the source of the redemption claim (contractual basis or statutory basis);
2. whether the claim is judicially enforceable;

3 the applicable law;

4 the governing court or dispute-resolution mechanism;

5 the distinction between legal right and commercial policy, i.e. which redemption arrangements are commercial policy that the issuer may unilaterally change and which are legal rights that holders may assert at law.

> Note: the legal wording of this clause MUST be confirmed by a stablecoin legal expert before formal freezing.

10.2 Direct Redemption Restriction

Where holders do not have a direct redemption right, the issuer MUST disclose this expressly. Expressions such as "redeemable" MUST NOT be used in a way that leads ordinary users to mistakenly believe they have a direct redemption right.

10.3 Redemption Value

The issuer MUST clearly state the reference value corresponding to each stablecoin unit, fee deductions, exchange-rate adjustments, and how the final settlement amount is computed.

10.4 Redemption Time

The maximum processing time for normal redemption MUST be quantified in hours or business days.

10.5 Redemption Suspension

The issuer MUST disclose all conditions that may lead to suspension, refusal, delay, partial redemption, or substitution of the settlement asset.

10.6 Redemption Anomalies

Where the actual redemption time exceeds the disclosed maximum, the issuer MUST record the request time, the due completion time, the actual completion time, the reason for delay, the affected amount, and the current status.

10.7 AML/CFT Boundary

This standard does not constitute a complete anti-money-laundering or counter-terrorist-financing (AML/CFT) standard. To prevent compliance restrictions from being misused, the following boundaries apply:

1 identity-verification requirements MAY affect the redemption eligibility of individual holders;

2 lawful compliance restrictions MUST NOT be treated as proof of reserve adequacy or issuer solvency;

3 the issuer MUST NOT refuse or freeze individual redemptions on AML/CFT grounds in order to conceal widespread redemption failure or reserve shortfall. Where redemption failure is widespread, it MUST be handled as a material event under §13, not classified as a case-by-case compliance refusal.

11. Attestation and Audit

11.1 Attestation Frequency

A stablecoin arrangement MUST undergo an independent reserve and liability attestation at least once per month.

11.2 Attestation Scope

The attestation scope MUST include reserve assets, outstanding liabilities, the verification point, the reserve coverage ratio, material limitations, and exceptions. A report that states only the total reserves does not satisfy this clause.

11.3 Attestation Firm Information

The attestation report MUST disclose the firm's legal name, professional qualification, signatory, report date, verification point, methods applied, scope of work, limitations, and exceptions.

11.4 Distinction of Evidence Types

The issuer MUST distinguish among self-declaration, reserve report, independent attestation report, financial-statement audit, on-chain proof, custody confirmation, and legal opinion.

11.5 Annual Audit

The issuer SHOULD undergo at least one complete financial-statement audit each year. The annual audit MUST NOT replace continuous reserve and liability verification.

11.7 Attestation Firm Independence

The attestation firm MUST disclose any ownership, control, common-control, employment, fee-dependency, or other interest relationship with the issuer or a related party of the issuer that may affect its independence.

An attestation report MUST NOT be counted as independent evidence under §4.1 where the attestation firm is owned or controlled by the issuer, is under common control with the issuer, or has not disclosed its interest relationships. In such a case the report is treated as an issuer self-declaration under §11.4.

Where the required independence disclosure is absent, or the attestation firm is not independent of the issuer, the result MUST be FAIL using `RMFSTABLE-ATT-003`.

11.6 Attestation Materiality and Limitation Disclosure

The attestation report SHOULD expressly disclose:

- the materiality level used;
- the sampling scope and method;
- exceptions;
- subsequent events;
- the scope of use of management representations.

Management representations MUST NOT replace external independent evidence. For any reserve or liability item that relies on management representations without independent verification, the verifier MUST note that limitation in the verification record.

12. Contract and Permission Control

12.1 Permission Disclosure

The issuer MUST disclose all roles able to perform mint, burn, freeze, unfreeze, pause, upgrade, change implementation, migrate, change fee, change admin, and change oracle.

12.2 Single-Key Restriction

Critical operations MUST NOT be independently controlled by a single undisclosed key. Critical permissions MUST use one or more of: multi-signature, threshold signature, timelock, governance approval, hardware security module, or functionally equivalent control.

12.3 Permission Verification

The verifier MUST independently inspect the actual on-chain permissions. Where documentation conflicts with on-chain state, the on-chain state is taken as the technical fact and an inconsistency record is produced.

12.4 Contract Upgrade

A contract upgrade MUST be treated as a material event. After an upgrade, the prior verification result MUST be marked STALE until the new version has completed re-verification.

12.5 Proxy Upgrade Pattern Disclosure

Where the contract uses an upgradeable proxy pattern, the issuer SHOULD disclose:

- Proxy type;
- Implementation address;
- Admin address;
- Timelock;
- Emergency upgrade mechanism;
- Upgrade event history.

This disclosure is a SHOULD-level enhancement; failure to provide it does not cause FAIL, but it affects the completeness assessment of the §12.3 permission verification.

13. Material Events

13.1 Types of Material Event

At least: reserve coverage ratio falling below 100%, reserve loss, creation of a pledge, lien, or other encumbrance over reserve assets, loss of attestation firm independence, custodian change, issuing-entity change, redemption suspension, large-scale redemption delay, contract upgrade, minting-permission change, compromise of a critical key, security incident, attestation withdrawal, change of legal structure, freezing of a major bank account, and conflict between machine data and human disclosure.

13.2 Notice Deadline

The issuer MUST publish a machine-readable notice within 24 hours after confirming a material event.

13.3 Notice Content

```
{
  "event_id": "",
  "event_type": "",
  "detected_at": "",
  "published_at": "",
  "affected_subject": "",
  "affected_requirements": [],
  "description": "",
  "current_status": "",
  "evidence": [],
```

```
  "requires_reverification": true
}
```

13.4 Verification Status Handling

Where a material event may affect conformance, the current verification result MUST be marked `STALE`, `SUSPENDED`, or `REVERIFICATION_REQUIRED`.

14. Evidence Requirements

14.1 Required Evidence

Evidence ID	Evidence Type	Provided By	Required
EVD-001	Issuer identity record	Issuer; company registry or trusted identity system	Mandatory
EVD-002	Stablecoin canonical identity record	Issuer	Mandatory
EVD-003	On-chain supply snapshot	Blockchain node; indexer; authoritative issuance ledger	Mandatory
EVD-004	Outstanding liabilities record	Issuer	Mandatory
EVD-005	Reserve asset detail	Issuer	Mandatory
EVD-006	Custody confirmation	Custodian	Mandatory
EVD-007	Reserve segregation evidence	Issuer; custodian	Mandatory
EVD-008	Valuation record	Issuer; valuation source	Mandatory
EVD-009	Redemption policy	Issuer	Mandatory
EVD-010	Contract permission record	Blockchain node; issuer	Mandatory
EVD-011	Independent attestation report	Attestation firm	Mandatory
EVD-012	Material event record	Issuer	Mandatory where a material event has occurred
EVD-013	Machine-readable disclosure	Issuer	Mandatory
EVD-014	Signature and digest record	Issuer; verifier	Mandatory
EVD-015	Legal opinion or equivalent legal proof	Issuer; legal counsel	Mandatory where bankruptcy remoteness is claimed under §8.7

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

```
{
  "evidence_id": "",
  "evidence_type": "",
  "issuer": "",
  "source": "",
  "issued_at": "",
  "effective_at": "",
  "expires_at": "",
  "sha256": "",
  "signature": "",
  "signer_id": "",
  "status": ""
}
```

14.3 Evidence Integrity

Evidence MUST satisfy: source identifiable, content digest verifiable, version identifiable, timestamp present, signer identifiable, status confirmable, and not silently overwritten.

14.4 Evidence Freshness

Unless otherwise specified in this standard:

- supply evidence must be no earlier than 24 hours before the verification point;
- reserve and liability attestation must be no older than 35 days, measured from the

attestation's own verification point (not its report date) to the verification point of this verification;

- responsible-party information must have no unprocessed changes;
- contract permissions must be based on current on-chain state;
- material-event records must cover the valid period prior to the verification point.

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

14.5 Missing Evidence

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

14.6 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.

15. Verification Procedure

15.1 Verification Sequence

The verifier MUST execute in the following order:

1. confirm the standard version;
2. confirm the stablecoin canonical identity;
3. confirm the issuer and responsible parties;
4. confirm the verification point;
5. compute per-chain supply;
6. compute effective circulating supply;
7. compute outstanding liabilities;
8. verify reserve asset ownership;
9. verify reserve segregation;
10. verify custody status;
11. re-compute reserve asset value;
12. re-compute the reserve coverage ratio;
13. verify redemption terms;
14. verify the attestation report;

15 verify contract permissions;

16 check material events;

17 verify consistency between machine data and human disclosure;

18 verify evidence digests and signatures;

19 compute individual results;

20 compute the overall result;

21 sign the verification record.

15.2 Determinism Requirement

The verification procedure MUST use fixed rules. Requirements MUST NOT be lowered based on the issuer's size, brand, market share, or reputation.

15.3 Individual Result

Each requirement MUST produce one of `PASS`, `FAIL`, `NOT_APPLICABLE`, or `NOT_ASSESSED`.

15.4 NOT_APPLICABLE

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

15.5 Reproducibility of Verification

A third party using the same standard version and the same evidence set MUST be able to re-compute the verification result.

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 all required evidence is present and valid;

4 human disclosure is consistent with machine data;

5 there are no unresolved evidence conflicts;

6 the reserve coverage ratio is not below 100%;

7 the verification record is signed.

16.2 CONDITIONAL

The overall result may be CONDITIONAL only where all MUST and MUST NOT are satisfied, all required evidence is valid, and only SHOULD items that do not affect mandatory conformance are unsatisfied.

16.3 FAIL

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

- any applicable MUST fails;
- any MUST NOT is violated;
- required evidence is missing;
- required evidence exceeds the maximum age stated in §14.4;
- the declared result validity period exceeds 35 days, or exceeds the earliest expiry

of the mandatory evidence on which the result depends;

- the attestation firm is not independent of the issuer, or its independence is not disclosed;
- a signature cannot be verified;
- the reserve coverage ratio is below 100%;
- reserves or liabilities cannot be independently re-computed;
- human disclosure conflicts with machine data;
- an evidence source cannot be confirmed;
- a material event is undisclosed;
- the conforming subject cannot be uniquely identified.

16.4 NOT ASSESSED

`NOT ASSESSED` may be used only where verification has not been formally completed; it does not constitute a conformance conclusion.

16.5 Result Validity Period

Each verification result MUST have an expiry time, with a default validity period not exceeding 35 days. Upon a material event, the result may expire early.

Where a verification record declares a validity period exceeding 35 days, the result MUST be FAIL using `RMFSTABLE-VER-002`.

The expiry time MUST NOT be later than the earliest expiry of any item of mandatory evidence on which the result depends, computed under the freshness limits of §14.4. A result MUST NOT remain valid on the strength of evidence that has itself expired. Where the declared expiry time exceeds that limit, the result MUST be FAIL using `RMFSTABLE-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;

1. no MUST NOT is violated and no evidence conflict under §14.6 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
RMFSTABLE-ID-001	Stablecoin canonical identity incomplete
RMFSTABLE-ID-002	Issuer or responsible party cannot be confirmed
RMFSTABLE-SUP-001	Supply cannot be re-computed
RMFSTABLE-SUP-002	Multi-chain supply double-counted
RMFSTABLE-LIA-001	Outstanding liabilities cannot be confirmed
RMFSTABLE-RES-001	Reserve coverage ratio below 100%
RMFSTABLE-RES-002	Reserve asset ownership cannot be confirmed
RMFSTABLE-RES-003	Reserve assets double-counted
RMFSTABLE-RES-004	Undisclosed pledge or lien present
RMFSTABLE-CUS-001	Custody status cannot be confirmed
RMFSTABLE-CUS-002	Undisclosed rehypothecation present
RMFSTABLE-SEG-001	Reserve segregation cannot be proven
RMFSTABLE-VAL-001	Reserve valuation cannot be re-computed
RMFSTABLE-RED-001	Redemption rights undisclosed
RMFSTABLE-RED-002	Redemption time not quantified
RMFSTABLE-ATT-001	Attestation report missing or expired
RMFSTABLE-ATT-002	Attestation scope does not include liabilities
RMFSTABLE-ATT-003	Attestation firm not independent of the issuer, or independence not disclosed
RMFSTABLE-SEC-001	Critical permission controlled by an undisclosed single key
RMFSTABLE-EVT-001	Material event not disclosed on time
RMFSTABLE-DAT-001	Human and machine data inconsistent
RMFSTABLE-EVD-001	Required evidence missing
RMFSTABLE-EVD-002	Evidence digest mismatch
RMFSTABLE-EVD-003	Evidence exceeds the maximum age stated in §14.4
RMFSTABLE-SIG-001	Digital signature invalid
RMFSTABLE-VER-001	Verification result cannot be re-computed
RMFSTABLE-VER-002	Result validity period exceeds the maximum stated in §16.5

18. Machine Interface

18.1 Common Record

```
{
  "canonical_id": "",
  "standard_id": "RM-S-STABLE-001",
  "standard_version": "v1.0-F",
  "record_type": "stablecoin_trust_verification",
  "status": "",
```

```
  "subject_id": "",
  "issued_at": "",
  "updated_at": "",
  "expires_at": "",
  "sha256": "",
  "signature": "",
  "signer_id": "",
  "evidence": [],
  "verification_result": "",
  "verification_timestamp": "",
  "verifier_id": ""
}
```

18.2 Stablecoin Fields

```
{
  "issuer": {},
  "token": {},
  "networks": [],
  "reference_currency": "",
  "verification_point": "",
  "total_supply": "",
  "circulating_supply": "",
  "outstanding_liabilities": "",
  "eligible_reserve_value": "",
  "reserve_coverage_ratio": "",
  "reserve_assets": [],
  "custodians": [],
  "redemption": {},
  "attestations": [],
  "contract_permissions": [],
  "material_events": [],
  "requirements": [],
  "failure_codes": []
}
```

18.3 Numeric Format

All monetary values MUST use string representation, specify currency and decimals, prohibit floating-point, and specify the valuation time and exchange-rate source.

```
{
  "amount": "1000000.00",
  "currency": "USD",
  "decimals": 2
}
```

18.4 Time Format

All times MUST use ISO 8601 UTC format.

18.5 Human–Machine Consistency

Where a machine record conflicts with the human-readable document of the same version, the result MUST be FAIL, using failure code `RMFSTABLE-DAT-001`.

18.6 Canonicalization and Digest

Before signing, a machine record MUST use a deterministic canonicalization procedure and generate a SHA-256 digest or the result of a digest algorithm subsequently approved by RuleMark.

18.7 Digest Algorithm Identifier

A machine record MUST include a digest-algorithm identifier field indicating the digest algorithm used. The default value is `sha-256`.

When RuleMark approves a new digest algorithm, it MUST register the algorithm identifier, approval version, effective date, and status in an algorithm registry. A verifier MUST NOT use a digest algorithm not registered in the registry to produce a formal verification record. During algorithm migration, a record MUST clearly identify the algorithm actually used, to avoid ambiguity.

19. Security Considerations

19.1 Principal Threats

This standard considers at least: forged reserve evidence, double-counted reserves, hidden liabilities, manipulation of the verification point, use of expired evidence, forged signatures, cross-chain double issuance, rehypothecation, related-party asset disguise, account commingling, compromise of an admin key, data inconsistency, verifier conflict of interest, attestation by a firm controlled by the issuer, a result outliving the evidence it rests on, and selective deletion of contrary evidence.

19.2 Security Controls

The issuer and the verifier MUST verify evidence digests and signatures, retain historical versions, record provenance, prevent silent overwriting, verify actual permissions, record material events, retain failure results, and sign critical machine records.

19.3 Verifier Independence

The verifier MUST disclose commercial, fee, ownership, control, and other interest relationships with the issuer 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, a court reaching a different interpretation, insolvency of a custodian or bank, changes in market value, a redemption run, smart-contract vulnerabilities, key compromise, regulatory change, or an evidence provider concealing facts.

19.5 Threat Mapping Matrix

The table below maps principal threats to the corresponding control requirements, evidence, and failure codes, for use in automated verification and consistency checking.

Threat	Control Requirement	Evidence	Failure Code
Forged reserve evidence	§7.3, §14.3	EVD-005, EVD-014	RMFSTABLE-RES-002, RMFSTABLE-EVD-002
Double-counted reserves	§7.3, §6.6	EVD-003, EVD-005	RMFSTABLE-RES-003, RMFSTABLE-SUP-002
Hidden liabilities	§6.7, §4.4	EVD-004	RMFSTABLE-LIA-001
Manipulated verification point	§4.3, §6.1	EVD-003, EVD-004	RMFSTABLE-SUP-001
Use of expired evidence	§14.4, §4.9	EVD-003, EVD-011	RMFSTABLE-EVD-003
Forged signature	§14.3, §18.6	EVD-014	RMFSTABLE-SIG-001
Cross-chain double issuance	§6.6, §5.2	EVD-003	RMFSTABLE-SUP-002
Undisclosed rehypothecation	§8.5	EVD-006, EVD-007	RMFSTABLE-CUS-002
Related-party asset disguise	§7.2, §7.4	EVD-005	RMFSTABLE-RES-002
Account commingling	§8.1, §8.2	EVD-007	RMFSTABLE-SEG-001
Admin key compromise	§12.2	EVD-010	RMFSTABLE-SEC-001
Data inconsistency	§18.5	EVD-013	RMFSTABLE-DAT-001

Threat	Control Requirement	Evidence	Failure Code
Attestation firm controlled by issuer	§11.7, §4.1	EVD-011	RMFSTABLE-ATT-003
Result outliving its evidence	§16.5, §14.4	EVD-011, EVD-013	RMFSTABLE-VER-002
Pledge created after verification	§13.1, §7.4	EVD-005, EVD-012	RMFSTABLE-EVT-001
Verifier conflict of interest	§1.5, §19.3	—	verification result invalid
Selective deletion of contrary evidence	§14.3, §19.2	EVD-014	RMFSTABLE-EVD-002

20. Conformance Claim

20.1 Minimum Fields

A conformance claim MUST include at least the standard ID, standard version, stablecoin canonical identity, issuing entity, verification point, result, reserve coverage ratio, evidence-set digest, verifier identity, verification time, expiry time, signature, failure codes, and limitations.

20.2 Example

```
{
  "standard_id": "RM-S-STABLE-001",
  "standard_version": "v1.0-F",
  "subject_id": "stablecoin:example:usd:chain:contract",
  "verification_point": "2026-01-01T00:00:00Z",
  "result": "PASS",
  "reserve_coverage_ratio": "1.0125",
  "evidence_set_sha256": "",
  "verifier_id": "",
  "verified_at": "",
  "expires_at": "",
  "signature": ""
}
```

20.3 Prohibited Statements

A conformance claim MUST NOT use expressions such as "completely safe", "zero risk", "government approved", "RuleMark guaranteed", "permanently valid", "guaranteed not to de-peg", "guaranteed redeemable at any time", or "guaranteed that the issuer will not become insolvent".

21. Test Cases

21.1 PASS Case

The issuing entity is clear; all on-chain supply and outstanding liabilities are re-computable; the eligible reserve coverage ratio is 102%; reserve ownership, segregation, and custody are verifiable; attestation is valid; redemption and permission disclosures are complete; human and machine data are consistent; all required evidence is signed and valid.

Expected result: PASS

21.2 Reserve Shortfall Case

- outstanding liabilities: 100,000,000 USD;
- verified value of eligible reserves: 98,500,000 USD.

Expected result: `FAIL`, `RMFSTABLE-RES-001`

21.3 Missing Evidence Case

Total reserves are sufficient, but the custodian account confirmation is missing.

Expected result: `DEFICIENT`, `RMFSTABLE-CUS-001`, `RMFSTABLE-EVD-001`

The custody evidence is absent rather than contradicted, so §16.6 applies.

21.4 Data Conflict Case

The PDF discloses circulating supply of 500,000,000; the JSON interface records 510,000,000.

Expected result: `FAIL`, `RMFSTABLE-DAT-001`

21.5 SHOULD Not Satisfied Case

All MUST requirements are satisfied; reserves, liabilities, custody, redemption, attestation, contract permissions, evidence, and signature are all valid; the issuer does not publish the liquidity stress disclosure recommended by §7.7, which is a SHOULD-level requirement and does not affect mandatory conformance.

Expected result: `CONDITIONAL`

22. Requirement Traceability Matrix

Requirement Area	Core Evidence	Core Verification
Canonical identity	EVD-001, EVD-002	Identity and contract reconciliation
Supply	EVD-003	On-chain re-computation
Outstanding liabilities	EVD-004	Liability re-computation
Reserve assets	EVD-005	Ownership, valuation, and double-counting checks
Custody	EVD-006	Custodian and account confirmation
Reserve segregation	EVD-007	Legal, accounting, and account-structure checks
Valuation	EVD-008	Independent re-computation
Redemption	EVD-009	Terms and process verification
Contract permissions	EVD-010	On-chain role verification
Attestation	EVD-011	Report scope and freshness verification
Attestation independence	EVD-011	Interest-relationship disclosure check
Material events	EVD-012	Event completeness and deadline verification
Machine interface	EVD-013	Schema and consistency verification
Evidence integrity	EVD-014	Digest and signature verification
Evidence freshness	EVD-003, EVD-011	Age check against §14.4 limits
Result validity period	EVD-013	Expiry check against §16.5

23. Lifecycle

23.1 Draft

In Draft status, the standard must not serve as a basis for formal RuleMark conformance; it may be used for public consultation and test verification; verification results must be marked experimental.

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 a standard is withdrawn, it 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

- RFC 2119;
- RFC 8174;
- RFC 8785;
- JSON Schema Draft 2020-12;
- ISO 8601;
- SHA-256.

24.2 RuleMark Dependencies

This standard is self-contained. The rules for canonical identity, digital evidence, verification and determination, digital signature, and lifecycle are all defined directly within this standard, respectively at:

- canonical identity: §5;
- digital evidence: §14;
- verification and determination: §15, §16;
- digital signature and digest: §18.6;
- lifecycle: §23.

The freezing of this standard does not depend on any external RuleMark standard.

After RuleMark publishes the corresponding core-layer standards in future, subsequent versions of this standard MAY align or replace the above internal clauses with normative references to those core-layer standards. Until then, this standard MUST NOT use a fictitious identifier as a formal normative reference.

24.3 Informative References

Current international regimes and industry materials in the areas of stablecoin governance, reserves, custody, redemption, and disclosure may be consulted. Informative references shall not be automatically converted into normative requirements of this standard.

25. Implementation Requirements

An implementation conforming to this standard MUST be able to:

1. uniquely identify the stablecoin arrangement;
2. re-compute on-chain supply;
3. re-compute outstanding liabilities;
4. verify reserve asset ownership;
5. verify reserve segregation and custody;
6. re-compute the verified reserve value;
7. compute the reserve coverage ratio;
8. check redemption terms;
9. check the attestation report;
10. check smart-contract permissions;
11. check material events;
12. verify machine records;
13. verify evidence digests and signatures;
14. produce a deterministic conformance result;
15. sign and retain the verification record.

26. Final Non-Claim

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

> At the specified verification point, under the specified standard version, for the specified stablecoin arrangement and the specified evidence set, all applicable mandatory requirements of RM-S-STABLE-001 are satisfied.

PASS does not indicate future continued conformance, absence of financial risk, absence of technical risk, absence of legal risk, absence of credit risk, absence of market risk, absence of liquidity risk, regulatory approval, an investment recommendation, or a RuleMark guarantee.

Document Status Declaration

```
Standard ID: RM-S-STABLE-001
Version: v1.0-F
Status: FROZEN
Publication Date: 2026-07-22
Effective Date: 2026-07-22
Normative Status: NORMATIVE
Conformance Use: AUTHORIZED
Machine ID: rulemark:standard:rm-s-stable-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.