



Architecture

Copied from the core repository

This page is [docs/ARCHITECTURE.md](#) in Garkuwa-Studio/assay, copied from a local copy with changes not yet pushed. To change it, edit it there.

Open proof of reserves and circuit breakers for RWAs and stablecoins on Stellar.

Garkuwa Labs · Version 0.1 (draft for SCF submission) · 2026-10-14 Repository:

<https://github.com/Garkuwa-Studio/assay> · Licence: Apache-2.0

Status legend. Every component is tagged so readers can tell what exists from what is planned. Switch a tag to Built only when there is a linked contract ID, tx hash or live URL. **[Built]** live and verifiable · **[Demo sprint]** built before submission · **[T1/T2/T3]** funded by that tranche.

Where things stand: registry v0 and guard v0 run on testnet, with contract IDs and transactions in [TESTNET.md](#) and [DEMO-RUN.md](#). The SEP draft is [SEP-DRAFT-reserve-report.md](#).

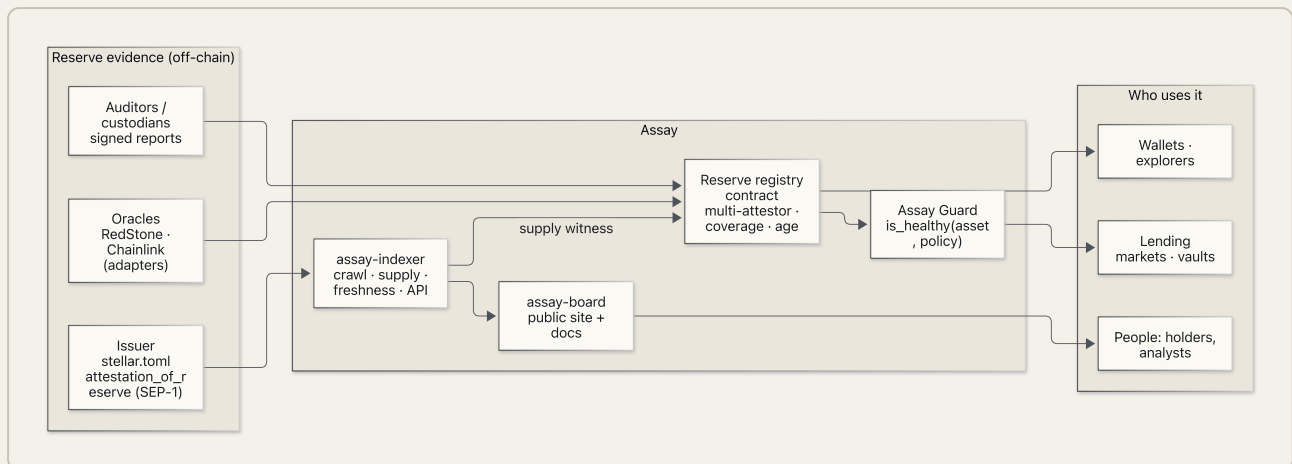
1. Summary

Every token on Stellar that claims off-chain backing — a stablecoin, a tokenized treasury fund, a bond, a loan pool — makes a promise: “there is enough real money or assets behind this token.” Assay checks that promise in three ways:

1. **Board** — a public website that checks every anchored asset on Stellar: is there a reserve report, how old is it, what does it say, and does it cover the supply on the ledger? [Demo sprint → T1]
2. **Registry** — a Soroban contract where independent attestors post signed reserve reports, so contracts can read the latest status. [Demo sprint → T2]

3. **Guard** — circuit breakers that let lending markets and vaults stop new exposure to an asset when its backing is missing, stale or short. [Demo sprint → T2]

Plus a **standard (SEP)** for machine-readable reserve reports, so every issuer publishes in the same format. [Demo sprint draft → T2]



› Diagram source (Mermaid)

2. The problem in technical terms

- **SEP-1 offers a reserve link but nothing checks it.** For each currency, SEP-1 (v2.7.0) has an optional `attestation_of_reserve` field: “URL to attestation or other proof, evidence, or verification of reserves, such as third-party audits.” It points at a PDF or web page. No standard format, no signature, no date field, no consumer.
- **Contracts can’t see backing.** A lending market listing an RWA as collateral has no on-chain signal for “the issuer stopped reporting” or “reserves fell below supply.” Oracles provide price or NAV, which can stay flat while backing disappears.
- **The result:** about \$4B of RWAs on Stellar, about \$2M usable as collateral. Risk teams can’t approve what they can’t monitor.

3. Design principles

1. **Facts, not ratings.** Show what is reported, when, by whom, with links.
 2. **Many attestors, disagreements visible.** No single source of truth.
 3. **Provider-agnostic.** Auditors, custodians, issuers, RedStone, Chainlink all plug in through the same report format.
 4. **Fail safe.** Missing or stale data is treated as unhealthy by default; each consumer chooses its own thresholds.
 5. **Read-only by default.** The guard never moves funds. Protocols decide what “pause” means for them.
 6. **Fully open.** Apache-2.0, self-hostable indexer, public API, no tracking.
-

4. Components

4.1 assay-indexer (off-chain) [Demo sprint → T1]

- **Asset census:** list every asset on Stellar mainnet with an issuer home domain; fetch each issuer’s `stellar.toml`; read `is_asset_anchored`, `anchor_asset_type`, `anchor_asset`, `attestation_of_reserve`, `redemption_instructions`, `collateral_addresses`.
- **Report checks:** does the link resolve; content type; report date (from the SEP format if present, else document metadata, else manual entry clearly labeled “manually transcribed” with source); reserves and liabilities as stated.
- **Supply:** classic assets via Horizon (`/assets`), SEP-41/SAC balances via Stellar RPC; recorded per ledger.
- **Collateral addresses:** verify the signatures in `collateral_address_signatures` and read on-chain balances.
- **Risk context [T1]:** the checks a lender asked for before accepting RWA collateral: issuer account flags (`auth_required`, `auth_revocable`, `auth_clawback_enabled`, `auth_immutable`) and signer thresholds; the redemption path (the anchor’s transfer server lists the asset for withdrawal); exit liquidity (amount sellable within 2% and 5% of mid on the Stellar DEX and AMM pools); and `collateral_address_signatures` validity windows. Each read at a recorded ledger.

- **Outputs:** versioned JSON API (/v1/assets, /v1/assets/{code-issuer}, /v1/summary, /v1/history) refreshed at least daily [T1], board data under CC BY 4.0, a public correction log, and supply snapshots posted on-chain as a “supply witness” (see 4.2; on mainnet in T3).

4.2 Reserve registry contract (Soroban) [Demo sprint → T2]

Roles

Role	Who	Can do
Asset admin	The issuer (proved via a key listed in its stellar.toml) or Assay’s admin until the issuer claims it	Register the asset, add/remove attestors (timelocked)
Attestor	Auditor, custodian, issuer, oracle adapter; recorded as independent or issuer [T2]	Post signed reserve reports for assets they’re registered on
Supply witness	assay-indexer or any independent party	Post on-chain supply snapshots
Anyone	—	Read status

Report (stored per asset, per attestor): reserves (amount, unit, breakdown optional), liabilities as stated, as-of timestamp, ledger, report URI, report hash (SHA-256 of the full document), attestor address.

Status (computed on read):

```

status(asset) -> {
  coverage_bps,          // min over attestors of reserves /
max(liabilities, witnessed supply)
  newest_age_secs,        // age of the most recent report
  attestor_count,         // attestors with a report inside the max age
  disagreement_bps,       // spread between attestors' coverage figures
  supply_mismatch,        // stated liabilities below witnessed supply
(beyond tolerance)
  independent_count,      // [T2] fresh attestors recorded as independent
}

```

Using the minimum across attestors and the larger of stated liabilities or witnessed supply makes the status conservative by design.

Why a supply witness: a contract cannot read the total supply of a classic Stellar asset through the Stellar Asset Contract, and SEP-41 does not require `total_supply`. So supply is posted as a signed snapshot by an independent witness and cross-checked against the attestor's stated liabilities. D0 verifies this assumption.

Storage: reports in persistent storage with TTL extension on write; bounded history (last N reports per attestor) to keep rent predictable.

4.3 Assay Guard [Demo sprint → T2]

A small library and contract that protocols call before accepting more exposure to an asset:

```

is_healthy(asset, policy) -> (bool, reason)
policy = { min_coverage_bps: 10000, max_age_secs: 35 days,
           min_attestors: 1, max_disagreement_bps: 500,
           max_supply_mismatch_bps: 50 }
// Missing or stale data is always unhealthy; there is no setting for
it.

```

Integration patterns:

1. **Inline check** — a lending pool calls `is_healthy` in `borrow` / `supply` for RWA collateral and rejects with a readable reason.

2. **Scoped keeper** (after launch) — for protocols that can't change code, a keeper watches the registry and calls the protocol's own admin action (e.g. set reserve status) using an OpenZeppelin smart-account policy that allows *only* that function on *only* that pool.
3. **Off-chain alerts** — webhooks and a public RSS/JSON feed for risk teams.

Reason codes [T2]: UNKNOWN_ASSET, NO_REPORT, STALE, UNDERCOVERED, TOO_FEW_ATTESTORS, NO_INDEPENDENT_ATTESTOR, DISAGREEMENT, SUPPLY_MISMATCH. It fails closed: an unknown asset, no report, a stale report, coverage below policy, issuer-only attestation when the policy needs an independent one, or a failed registry call all return false with a reason. Strict and lenient policy profiles come from the same contract, with an integration guide and test kit. (v0 on testnet has six reasons, from NoReport to SupplyMismatch; an unknown asset reads as NoReport.)

The guard never moves funds and never unpauses automatically without the protocol's own rule allowing it.

4.4 Reserve report standard (SEP draft) [Demo sprint draft → T2]

Extends SEP-1: attestation_of_reserve may point to a JSON document:

```
{
  "sep": "reserve-report-v0",
  "asset": "CETES:GC...ISSUER",
  "as_of": "2026-10-31T23:59:59Z",
  "ledger": 61234567,
  "reserves":
  [{ "type": "government_bond", "amount": "12500000.00", "unit": "MXN" } ],
  "liabilities": { "supply": "12480000.00", "unit": "CETES" },
  "attestor": { "name": "Example Audit
LLP", "stellar_key": "GA...", "role": "auditor" },
  "evidence": [ { "uri": "https://.../report.pdf", "sha256": "..." } ],
  "signature": "..." // Ed25519 over the canonical JSON, key listed in
stellar.toml
}
```

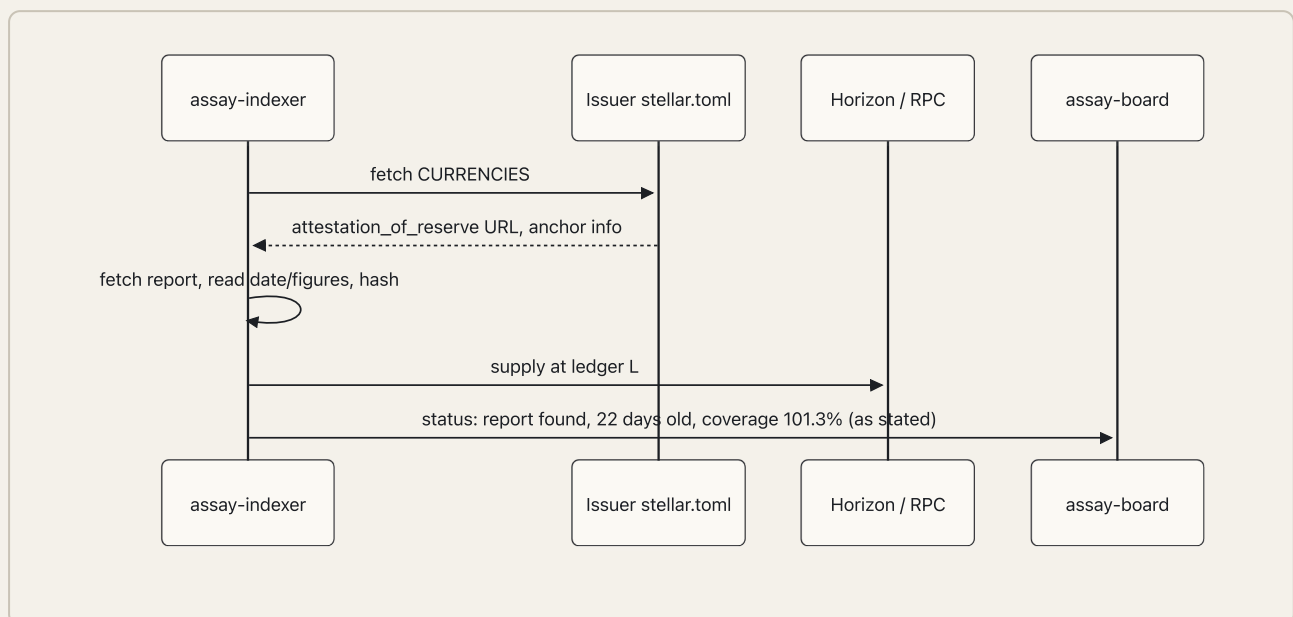
Backwards compatible: a plain PDF link still works; the board labels it “unstructured report”.

4.5 SDK and CLI [T2]

- assay-stellar CLI (binary assay): `assay check <asset>`, `assay report sign <file>`, `assay report post <file>`, `assay watch <asset>`.
- @garkuwa/assay-sdk (TypeScript): status lookups and a “reserve status” badge for wallets and explorers.

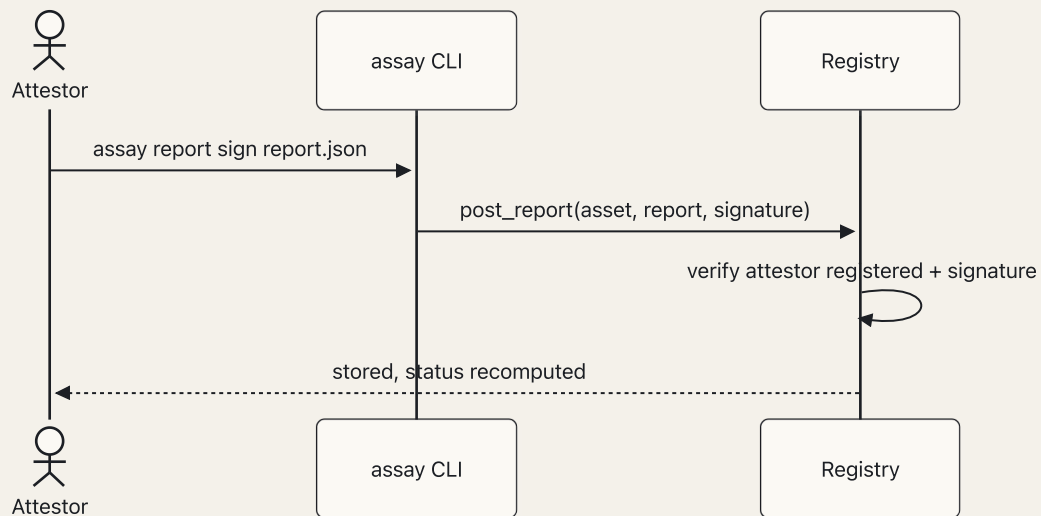
5. Key flows

5.1 Board check (no permission needed)



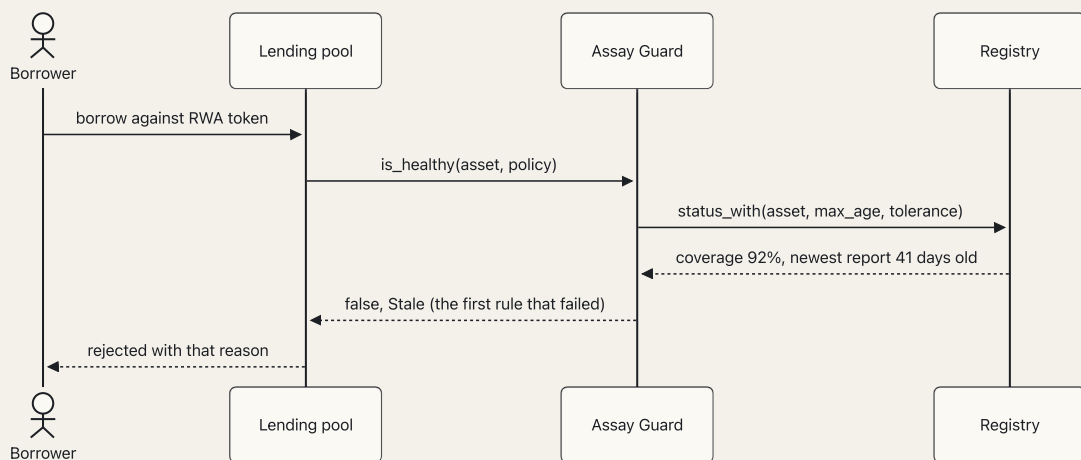
› Diagram source (Mermaid)

5.2 Attestor posts a signed report



› Diagram source (Mermaid)

5.3 Circuit breaker trips



› Diagram source (Mermaid)

6. Security model

Trust assumptions: attestors tell the truth (Assay makes them accountable, not honest); the issuer's stellar.toml and keys are not compromised; the supply witness is

honest (anyone can run one; disagreement is visible).

Threat summary (full STRIDE in T2):

Threat	Example	Mitigation
Spoofing	Fake attesor posts a glowing report	Attestors registered per asset by the asset admin; keys listed in stellar.toml; timelock on attesor changes
Tampering	Report edited after posting	Report hash on-chain; board shows hash mismatch
Repudiation	Attestor denies a report	Signed, on-chain, attributable
Information disclosure	—	All data is public by design
Denial of service	Spam reports to bloat storage	Only registered attestors post; bounded history
Elevation of privilege	Keeper abuses admin rights on a protocol	Keeper's smart-account policy allows one function on one contract only
Stale-data blindness	Attestor stops posting	Age is part of status; missing = unhealthy by default

Known limitations: Assay cannot detect a lying attesor whose numbers are internally consistent; it can only show disagreement with other attestors and mismatch with on-chain supply. Report figures in non-token units (e.g. MXN) need an FX assumption, stated explicitly.

7. Legal and editorial safeguards

- The board shows facts with source links and timestamps; it does not rate, rank or recommend.

- Every asset page has an issuer right-of-reply link and a correction log.
- Disclaimer: not investment advice, not an audit, not a guarantee.
- Wording reviewed by a lawyer before mainnet (budget line).

8. Infrastructure

- **On-chain:** registry and guard contracts (testnet → mainnet).
- **Off-chain:** indexer (container on a small VM, public RPC or own RPC), Postgres for history, static board site, read-only public API. Self-hostable by anyone.
- **No tracking:** no analytics, cookies or accounts on the board.

9. Roadmap

Stage	Scope	Estimate
Demo sprint (before submission)	Board v0 on mainnet data; registry v0 on testnet; guard demo; SEP draft	5 weeks
T1 — MVP	Board, indexer and API v1 on mainnet data	5 weeks
T2 — Testnet	Registry, standard, guard, pilots, threat model	6 weeks
T3 — Mainnet	Audit, mainnet launch, go-live, transparency report	6 weeks

After launch (coverage expansion): oracle adapters (RedStone, Chainlink), a scoped keeper for protocols that can't change their code, more attestors per asset, and quarterly “State of reserves on Stellar” reports.

10. Glossary

- **Reserves** — the real assets (cash, bonds, loans) backing a token.
- **Liabilities / supply** — how many tokens exist and are owed back.

- **Coverage** — reserves divided by liabilities; 100% means fully backed.
- **Attestor** — a party that signs a statement about reserves.
- **Attestation of reserve** — SEP-1 field linking to an issuer's proof.
- **Supply witness** — a party that records on-chain token supply.
- **Circuit breaker** — an automatic stop when a safety condition fails.
- **SEP** — Stellar Ecosystem Proposal, a standard for apps on Stellar.
- **RWA** — real-world asset; a token representing something off-chain.

[Board](#) · [Core repo](#) · [Docs repo](#) · [GitHub organisation](#)

Assay, by Garkuwa Labs. The board reads Stellar mainnet; Assay's contracts run on Stellar testnet and have not been audited. Figures are as stated by issuers or attestors. Assay is not an audit and not investment advice. Open source under Apache-2.0.