

# Acceptance Criteria

# Acceptance Criteria (MVP Refactor)

Generated: 2026-02-24

## ## M1 — Stability & Security Patch

- [ ] All HTTP responses follow a consistent envelope (success/error) and include `requestId`.
- [ ] Central error middleware exists; unhandled exceptions do not crash the process for malformed requests.
- [ ] `/my-costs` (or equivalent billing/admin endpoints) require explicit admin permission.
- [ ] WebSocket endpoint requires auth handshake and rejects unauthenticated messages.
- [ ] Package/version is read once at startup (no per-request filesystem reads).
- [ ] Basic rate limits exist for auth and command endpoints.

## ## M2 — Modular Boundaries + Validation

- [ ] `routes/account/index.mjs` is split into thin routes + services + repositories.
- [ ] Zod (or equivalent) validation is applied to all command inputs.
- [ ] At least 10 contract tests cover the highest-traffic endpoints.
- [ ] OpenAPI spec exists and is kept in sync with the routes.

## ## M3 — Receipts + Signing (Concord-style)

- [ ] Canonical receipts are written append-only to Spaces; no overwrites of historical receipts.
- [ ] Each receipt includes `prevHash`, `hash`, and an ECDSA P-256 signature.
- [ ] Server verifies `prevHash` continuity before accepting a new receipt (per stream).
- [ ] Signatures are produced by Vault Transit and keys are non-exportable by default.
- [ ] A verifier can replay receipts and validate hash chain + signatures from public keys.
- [ ] Idempotency-Key prevents duplicate receipts on retried commands.

## ## M4 — Projection & Replay

- [ ] Postgres projection can be rebuilt from receipts via a CLI/job with no manual edits.
- [ ] Rebuild produces identical projections when rerun on the same receipt set.
- [ ] Snapshots (optional) speed replay and are rebuildable from receipts.

## ## Operational

- [ ] Health endpoints cover Postgres connectivity, Spaces access, and Vault Transit access.
- [ ] Metrics include request counts, latencies, error rates, and signing failures.
- [ ] K8s manifests exist for API, Vault, and projector job (dev/staging).