

ZORA CONSTELLATION

Gap Closure & Continuation

Reviewed customer outcomes, portable memory, deletion recovery and owner-controlled fleet updates.

Meet Zora.
Build the relationship. Build the company.

Human construction document | Edition 2.7.0

Design, implementation and production verification are distinct. This volume states target decisions and retains the evidence boundary.

Contents

1. Customer outcomes now complete the local loop
 2. Portable memory and durable deletion
 3. Owners control fleet updates and management
 4. Verification and reproducibility
 5. Genuine gates versus remaining engineering
 6. Acceptance of this revision
 7. Department-scoped company work
 8. Overdue work and authority inbox
 9. Configurable AI assessment without execution authority
 10. Worker route restrictions
 11. Assessment cost reservations and reconciliation
- Edition 2.6.1: sovereign operations
- Edition 2.7.0: governed execution and development separation

This addendum supersedes earlier implementation-status statements for the changes below. The wider vision remains Meet Zora, sovereign personal relationships, ZoraTrade and the governed organic company. No change in first-product direction is introduced.

1. Customer outcomes now complete the local loop

A resolved company case can now receive a customer-safe summary through POST `/v1/company/outcomes/publish`. The company authority supplies `case_id`, exact current version and a 10-1500 character summary. Unresolved or stale cases fail. The last task producer cannot publish the outcome under a different role bearing the same actor identity. The published text is immutable; repeated identical publication is idempotent and changed text conflicts.

GET `/v1/company/outcomes` returns only the authenticated owner's linked cases, with the reviewed summary and publication timestamp. Internal assessment text is not copied into this response. This is in-account delivery, not permission to email or message a customer externally. A separately authorized notification adapter remains future integration work.

The HTTP acceptance journey now demonstrates consent, company intake, worker proposal, independent resolution, reviewed publication and owner-only retrieval. Stale version, self-review, changed text and other-owner paths are tested.

2. Portable memory and durable deletion

GET `/v1/privacy/export` produces a versioned JSON export of the authenticated owner's active local memories. POST `/v1/privacy/memory/delete` requires an owned `memory_id`, deletes the record and creates a durable deletion receipt. Repeating the owned deletion is safe. Another tenant cannot delete or export the record.

GET `/v1/privacy/tombstones` returns the owner's deletion records. During recovery, an authenticated recovery authority can call `Privacy.restore_tombstones` with independently retained, owner-scoped records before the restored service opens. The test restores a backup made before deletion, confirms the old memory exists in isolation, reapplies tombstones and confirms it is removed. Cross-tenant import is denied.

This does not yet delete every record across a production account. Search indexes, object stores, provider records, legal retention and backup expiry need their own adapters. Independently retained tombstones must be protected by actual custody and integrity controls; merely keeping them in the same backup does not prevent resurrection.

3. Owners control fleet updates and management

A company operator's consent assertion is no longer enough to schedule an update. The owner must authorize the specific instance and release, with an expiring grant. Scheduling consumes that grant. Installation reporting checks that the grant remains current and unrevoked.

POST /v1/fleet/updates/authorize accepts instance and release for an active owned instance. POST /v1/fleet/management/withdraw stops management, clears remotely controlled features, revokes update grants and cancels pending rollouts. Subsequent company feature changes or reactivation fail. Personal memory remains available to its owner.

This closes a reference authorization gap. It does not constitute a cryptographically verified update installer. Artifact signing, antirollback enforcement and on-device installation still need implementation and real-device validation.

4. Verification and reproducibility

The local suite now passes 55 tests. The reference API documents 40 routes. The clean-directory rehearsal passes using isolated Python and no external credentials or actions. See docs/test-results.txt and evidence/handoff-rehearsal.json for the actual output.

Run from the package root:

```
python3 scripts/validate_package.py
```

```
python3 -m unittest discover -s tests -v
```

```
python3 scripts/handoff_rehearsal.py
```

The 51 production target gates remain unrun. A passing local test is not substituted for a live provider, device, independent review or original Prime reconstruction result. The existing published Site remains edition 2.1; these backend changes are delivered in the downloadable package and are not represented as connected to that Site.

5. Genuine gates versus remaining engineering

The machine-readable specifications/gap-register.json separates local closures, missing external assets, unfinished implementation and genuine authority gates. Missing source and credentials are dependencies. Building department permissions, production schedulers, privacy adapters or update agents is engineering work; it must not be disguised as a Founder decision.

Genuine authority gates include ownership of merchant/cloud/broker accounts, approval of live financial authority, release-signing custody, lawful signatures and succession designation, and the final production release decision. Until those are resolved, preserve explicit unavailable or paper-only modes and continue independent construction work.

Further engineering remains in production authentication/data infrastructure, live company assessment and tool adapters, department-level capabilities, scheduled service operations, cross-service export/deletion, signed device distribution and independent audit custody. The current full ZoraTrade repository and canonical gateway connection are still required to integrate the existing products faithfully.

6. Acceptance of this revision

Closed locally: reviewed customer outcome delivery; owner-scoped portable memory export; deletion receipts and restore replay; owner-issued exact-release update grants; withdrawal of fleet management with pending-update cancellation.

Not claimed: complete production implementation, live AI connection, live brokerage, universal data erasure, operator-blind encryption, actual device installation or independent release certification. The revised package preserves those distinctions so a builder has a truthful continuation point.

7. Department-scoped company work

Coordination grants bind tenant, worker actor, department and expiry. Only an authority can grant or revoke them. The server selects the department from its trusted principal configuration, not a client-supplied field. Workers using the existing case-list and task-claim routes now require a current grant. Task completion checks the case department and current grant again inside the same transaction as completion. Revocation blocks a leased worker from finishing afterward.

The support worker cannot list or claim finance cases. The transport test includes both categories and verifies the denial after revocation. Direct Python Runtime methods remain a trusted internal API; they are not a remote authentication boundary. Production workload identities and tool-specific capabilities remain required.

8. Overdue work and authority inbox

The SLA sweep creates one internal escalation per unresolved case and reason after the configured age, default 24 hours. Repeated sweeps do not duplicate the escalation. The authority inbox contains pending case reviews and unacknowledged escalations. Only an authority can read or acknowledge the inbox. Resolved cases no longer appear as open escalations.

POST /v1/authority/sweep runs the check. GET /v1/authority/inbox reads the inbox. POST /v1/authority/acknowledge records the actor and reason. No external notification is sent. The local-sla-monitor service and timer are installation templates for a one-minute internal check; they have not been installed on the existing Prime host or any production system.

The worker command now requires --department. Bootstrap configures the local development worker for support, with a 24-hour grant. Renew it through the authority route instead of widening the worker role. The OS scheduler is a trusted local process; production needs its own narrowly scoped workload identity and deployment review.

9. Configurable AI assessment without execution authority

The worker can now use `--assessment canonical` with `ZORA_ASSESSMENT_URL` and `ZORA_ASSESSMENT_TOKEN` supplied through a controlled secret environment. The default remains labeled deterministic triage. Selecting canonical mode without a connection fails startup explicitly.

The adapter sends the approved company case summary, its departmental owner, case ID, server-derived company tenant and a canonical input hash. Unrelated payload fields are discarded. Allowed tools and evidence references are empty in this first binding. The provider must return exactly the expected fields and echo the request ID and input hash. Unknown fields, invented source references, empty or oversized text, mismatched correlation and HTTP redirects are rejected. Responses are capped at 32 KiB with a 25-second timeout.

Valid output is an assessment proposal requiring authority review. It cannot call a tool, mark itself resolved or authorize its own action. Failed calls retain the bounded lease/retry/dead-letter behavior. Fixture tests verify the payload boundary and the actual transition into review. A fixture is not a live AI test.

The endpoint `/v1/company/assess` is a proposed binding around the existing canonical Zora service. It is not claimed to exist today. Implement that binding using the current source, configure a service credential and gateway cost/rate policy, then validate live behavior in staging. Request-size limits are not a monetary budget guarantee. Existing model usage must be metered and reconciled before enabling unattended paid calls.

10. Worker route restrictions

Remote department workers now have a narrow route allowlist: scoped case intake/list, public evidence and task claim/finish. They cannot read the general memory endpoint, full company graph, financial trial balance, privacy export or authority inbox. Worker intake also requires the configured department and an active grant. The transport tests exercise denied routes and revoked access.

The generic continuity adapter now also rejects redirects and credential-bearing or malformed service URLs. These controls protect the configured service boundary but do not replace production identity, network egress policy, secret custody or independent security review. The server remains a loopback reference service.

11. Assessment cost reservations and reconciliation

Canonical worker calls now pass through an atomic budget reservation. An authority must configure positive integer per-call and rolling 24-hour ceilings using `POST /v1/assessment/budget`. Values are microUSD: 1 USD equals 1,000,000 microUSD. No default monetary allowance is silently granted. Missing or blocked policy prevents calls.

The reservation binds the task ID to the input hash. Concurrent reservations serialize through SQLite transactions. A completed repeat returns its cached result without another provider request; changed

input under the same ID conflicts. The request carries `max_cost_microsd`, and the response must supply a nonnegative integer `provider_cost_microsd`. Settlement releases unused allowance. If the reported cost exceeds the reservation, the actual reported amount is retained and further calls are blocked.

Timeouts, malformed responses and other uncertain outcomes keep the full reservation. These unresolved amounts continue counting even after a day passes. Retrying the same uncertain request is denied, preventing an automatic repeated charge. Existing bounded worker retries eventually expose the task for attention; reconciliation is a separate authority action.

GET `/v1/assessment/exposure` shows reserved, reported and unresolved amounts without assessment text. POST `/v1/assessment/reconcile` records the actual amount supported by a provider receipt reference. It never automatically reissues the old request. POST `/v1/assessment/unblock` requires a review note and no unresolved reservations or breaches. Increasing a limit does not clear a block. Department worker tokens cannot invoke these authority routes.

Tests cover replay, changed input, missing policy, unauthorized configuration, persistent unknown exposure, exhaustion, an over-ceiling report and authority reconciliation. The clean-directory suite passes 55 tests. These are local/fixture results, not live invoice reconciliation.

The gateway must enforce the transmitted ceiling against its actual provider pricing and token/tool limits. The local application cannot guarantee that an external provider honors that contract. Provider-reported cost is not independently verified billing; reconcile invoices before production acceptance. The actual budget amount remains an authenticated authority decision, while the engineering mechanism is now implemented.

Edition 2.6.1: sovereign operations

The local suite now passes 93 tests. Signed release staging verifies signatures, exact owner consent, expiry, platform, hashes and a local sequence floor. Staging does not install code.

Recoverable deletion includes real memory, search and object adapters, four loopback routes and a bounded worker. Unknown outcomes reconcile before another deletion; retention exceptions never claim erasure. Encrypted single-tenant restore requires retained digests and current deletion records, rejects overwrites, quarantines object bindings and leaves operations stopped.

Scoped operational health reports queue counts, expired leases, review age, unresolved cost, privacy outcomes and local audit integrity without exposing private payloads. The website publication adds saved-data download, separate history clearing and protection against late replies after privacy changes.

The live channel probe returned: `McpServerError: MCP SSE probe returned 404 from openai.org`. This blocks that connection, not independent engineering. Actual installers, provider integration, external custody and production acceptance remain open.

Read `SOVEREIGN_OPERATIONS.md` for complete setup and limitations, and `sovereign-operations.m2m.json` for the matching machine contract. Cryptographic tests use the optional cryptography 46.0.0 reproduction pin. The full master bundle also contains the updated execution ledger with source migration and 14 passing ledger tests.

Edition 2.7.0: governed execution and development separation

The current reference implementation passes 114 tests and exposes 50 documented loopback routes. Local Zora remains offline by explicit Founder instruction. No process was started or connected.

Signed ZIP application installation now writes real isolated application slots, verifies every payload file and selects only a healthy candidate. An unsuccessful candidate preserves the previous active selection. Integrity is rechecked after the health probe. This does not launch a native Zora process or constitute real-device production validation.

Company actions now bind human approval to an exact case version, connector revision and payload. Scoped workers can create actual internal work items after independent review. Uncertain results are inspected before further action; lost responses do not trigger blind duplicate execution. Five authenticated action routes accompany the implementation. External providers remain disconnected.

A separate private Cloudflare development project preserves the glass Meet Zora experience, uses a separate D1 database, and blocks the canonical gateway in code. The current website remains unchanged. Development data and secrets must not be copied into production. Production promotion requires a reviewed release candidate and separately verified identity, providers, migrations and rollback.

Read `ACTIONS_AND_INSTALLATION.md` for exact module procedures and limitations. The matching `company-actions.m2m.json` defines action states and receipt requirements. The full master directive now records the offline constraint and cloud development authorization. The entire production vision remains subject to the explicit unresolved source, provider, infrastructure and independent-acceptance gates.