

Web3User Permission Lab — System Mindmap & Architectural Tree (Milestone 6.4 Visual Summary)

Built Architecture vs. Planned Roadmap · Version 0.3.0 · 23 October 2026 · M0–M6.3 Complete · M6.4 Locally Validated · Unpublished

1. PRODUCT VISION & SCOPE

- **Goal:** Explicit, testable, auditable off-chain permissions for Web3 actions.
- **Target Users:** Smart wallets, ERC-4337 bundlers, dApps, autonomous AI agents.
- **Decision Triad:**
 - **ALLOW:** Complies with all allowlists, limits, and timestamps.
 - **DENY:** Explicit policy violation (target, recipient, amount, expiry).
 - **UNKNOWN:** Missing, malformed, or unsupported transaction calldata.
- **Hard Exclusions:** Zero token launch, zero custody, zero on-chain deployment.

2. CORE EVALUATION ENGINE [BUILT]

- **Module:** `src/policy.ts` (deterministic TypeScript, 0 dependencies).
- **Supported Action:** `ERC-20 transfer(address,uint256)` (selector: `0xa9059cbb`).
- **Calldata Parser:** Exact 68-byte validation, strict 12-byte zero padding.
- **Lossless Arithmetic:** `uint256 BigInt` decoding; avoids float precision loss.
- **Policy Rules:** Target contract & recipient allowlists, per-action cap, validity.
- **Enforcement Boundary:** Evaluator issues decisions; does not submit transactions.

3. CRYPTOGRAPHIC CAPABILITIES [BUILT]

- **Binding Digest (V1):** SHA-256 over canonical length-prefixed request & policy.
- **Asymmetric Signing (V2/V3):** Ed25519 digital signatures via `node:crypto`.
- **V3 Artifact Schema:** version (3), `authId`, `keyId`, `issuedAt`, `expiresAt`, `policyId`, `revision`, `digest`, `sig`.
- **Length-Prefixed Serialization:** `web3user-signed-authorization-v3\n` with `name:length:value\n` format (prevents delimiter injection).
- **Cryptographic Boundary:** Evaluator signs authorization artifacts; wallet signs EVM transactions with `Secp256k1`.
- **Verification Invariant:** Signatures verified strictly BEFORE storage writes.

4. PERSISTENT STORAGE & GOVERNANCE [BUILT]

- **Storage Engine:** SQLite via `node:sqlite` (WAL mode, `busy_timeout = 5000`).
- **Two-Phase State Machine:** `issued` -> `consumed` with version discriminator.
- **Single-Use Replay Prevention:** Atomic UPDATE; duplicate consumptions return DENY.
- **Key Registry:** Active, retired, revoked statuses; enforces chronological invariants.
- **Policy Store:** Monotonically increasing revision numbers preventing rollbacks.
- **Monotonic Clock:** Transaction-locked high-water mark rejecting backward time jumps.

Web3User Permission Lab — System Mindmap & Architectural Tree (Milestone 6.4 Visual Summary)

Concurrency, Recovery, Roadmap & Summary Legend · Version 0.3.0 · M0–M6.3 Complete · M6.4 Locally Validated

5. CONCURRENCY, CONTENTION & RESILIENCE [BUILT]

- **Contention Retries:** 5-attempt / 250ms budget with randomized exponential backoff.
- **Non-Spinning Sleep:** Synchronous `Atomics.wait` on `SharedArrayBuffer` (`sleepSync`).
- **Safe TTL Arithmetic:** Subtraction-first calculation prevents integer overflow up to `Number.MAX_SAFE_INTEGER`.
- **Multi-Process Race Barrier:** 4-process IPC rendezvous barrier synchronizing simultaneous consumption attempts; strictly enforces 1 ALLOW and 3 DENYS.
- **Process Crash Recovery:** Verified SQLite WAL automatic rollback upon reopen when worker is terminated abruptly (`SIGKILL` / `exit(1)`) mid-transaction.
- **Durability Boundary:** Verifies process-crash recovery; physical power loss durability depends on OS fsync and hardware write caches.

6. STATIC WEBSITE PREVIEW & HOSTING [BUILT]

- **Bundle Directory:** `website-preview/` (responsive dark theme, verified stats).
- **Artifacts:** White paper v0.3.0 & project mindmap v0.3.0 PDFs in `assets/`.
- **Hosting Candidates:** Cloudflare Pages or GitHub Pages (static preview URL).
- **Domain Strategy:** `web3user.tech` unconfigured; zero DNS modification until approval.

7. TOOLS & VERIFICATION HARNESS [BUILT]

- **TypeScript Compiler:** Static type enforcement (`npx tsc --noEmit` passes clean).
- **Vitest Test Runner:** 238 passing tests across 14 test suites.
- **Persistent Replay Demo:** Verified isolated two-step ALLOW -> DENY runner.
- **Dependency Health:** Clean npm audit status; zero known vulnerabilities.
- **Git Baseline:** Commit `f1bed7f51e6a3ccb024b17a86993faf07bc48349`.

8. DEVELOPMENT ROADMAP

- **M0–M3 COMPLETE:** Foundation, ERC-20 evaluator, unit tests, private repo.
- **M4–M5 COMPLETE:** Length-prefixed canonical binding & SQLite two-phase store.
- **M6.1–M6.2 COMPLETE:** Ed25519 V2/V3 signing, key registry, monotonic revisions.
- **M6.3 COMPLETE:** Concurrency hardening, monotonic clock rollback protection.
- **M6.4 LOCALLY VALIDATED (UNPUBLISHED):** Safe TTL arithmetic, multi-process race barriers, process crash recovery verification (238 tests).
- **M7 PLANNED:** Cumulative spending budgets across rolling time windows.
- **M8 PLANNED:** Adversarial property testing, fuzzing, and malformed ABI corpora.
- **M9 PLANNED:** Independent third-party security audit & controlled public demo.

MINDMAP LEGEND & ARCHITECTURAL NOTES

- **Milestone Status Hierarchy:** Milestones M0–M6.3 are complete in Git history. Milestone 6.4 is locally validated in the working tree subject to documented verification evidence (238 passing tests, clean TypeScript compilation, and verified crash recovery); uncommitted and unpublished. Milestones M7–M9 are planned.
- **Committed HEAD vs. Working Tree:** Baseline HEAD is commit `f1bed7f51e6a3ccb024b17a86993faf07bc48349`. Milestone 6.4 validation includes uncommitted and untracked changes in the local working tree.
- **Security & Durability Boundaries:** The evaluator issues off-chain Ed25519 authorization artifacts; it does not custody private keys, sign EVM transactions, or submit to blockchain networks. Process-crash recovery (SQLite WAL rollback) is verified, but physical power-loss durability is not claimed. Custom domain DNS activation is deferred.
- **Visual Summary Note:** This PDF is a condensed visual summary. Complete narrative details, schemas, and rationale are documented in the companion Markdown source (`docs/web3user-project-mindmap-v0.3.0.md`).