CONCORDIUM TRUSTED AGENTS HACKATHON • 75M CCD GRANTS

APACHE-2.0 OPEN SOURCE

CROSS-CHAIN TRUSTED AGENT FIREWALL & SPONSORED X402 GATEWAY

Aegis402

Upgrading Ethereum (`eip155:*`) and Solana (`solana:mainnet`) AI agents with accountable Concordium **CIS-8004** & **CIS-8** identity, zero-PII **Verify & Access** ZKP checks, gas-sponsored **@x402/concordium** settlement, and **EU AI Act Article 12** audit dossiers.

Live Console

alphonshhhomenicmtu.github.io/aegis402-concordium/

GitHub Repository

github.com/alphonshhhomenicmtu/aegis402-concordium

1080p Demo Video

youtube.com/watch?v=0UTSsZeiQyw

01 • THE PROBLEM

Why Cross-Chain AI Agents Fail Enterprise & Regulatory Trust

UNACCOUNTABLE KEYS

Anonymous EVM & Solana EOAs

Autonomous agents act behind ephemeral `secp256k1` or `ed25519` keys with zero verifiable organizational or legal identity. Protocols face Sybil abuse and rogue key spoofing.

EU AI ACT ART. 12

Compliance vs. PII Liability

Regulators mandate verifiable recordkeeping and traceability, yet storing raw KYC documents on-chain or in API gateways creates severe GDPR and data-breach liability.

UX & GAS FRICTION

Multi-Chain Micropayment Overhead

Agents calling pay-per-request HTTP/MCP APIs struggle with multi-chain gas management, non-deterministic finality, and lack of atomic settlement.

02 • SOLUTION ARCHITECTURE

5-Stage Fail-Closed Firewall on Concordium Testnet

Every HTTP 402 or MCP tool call passes five deterministic gates before returning protected alpha or executing settlement.

STAGE 1
Cross-Chain Intent
Agent signs payload using native `ethereum_personal_sign` or `solana_ed25519`.

STAGE 2
CIS-8004 & CIS-8
Verifies active `<12802,0>` badge, `<12801,0>` key binding & card SHA-256.

STAGE 3
Verify & Access ZKP
Enforces `IdStatementBuilder` attributes (e.g., age ≥ 18) with single-use nonces.

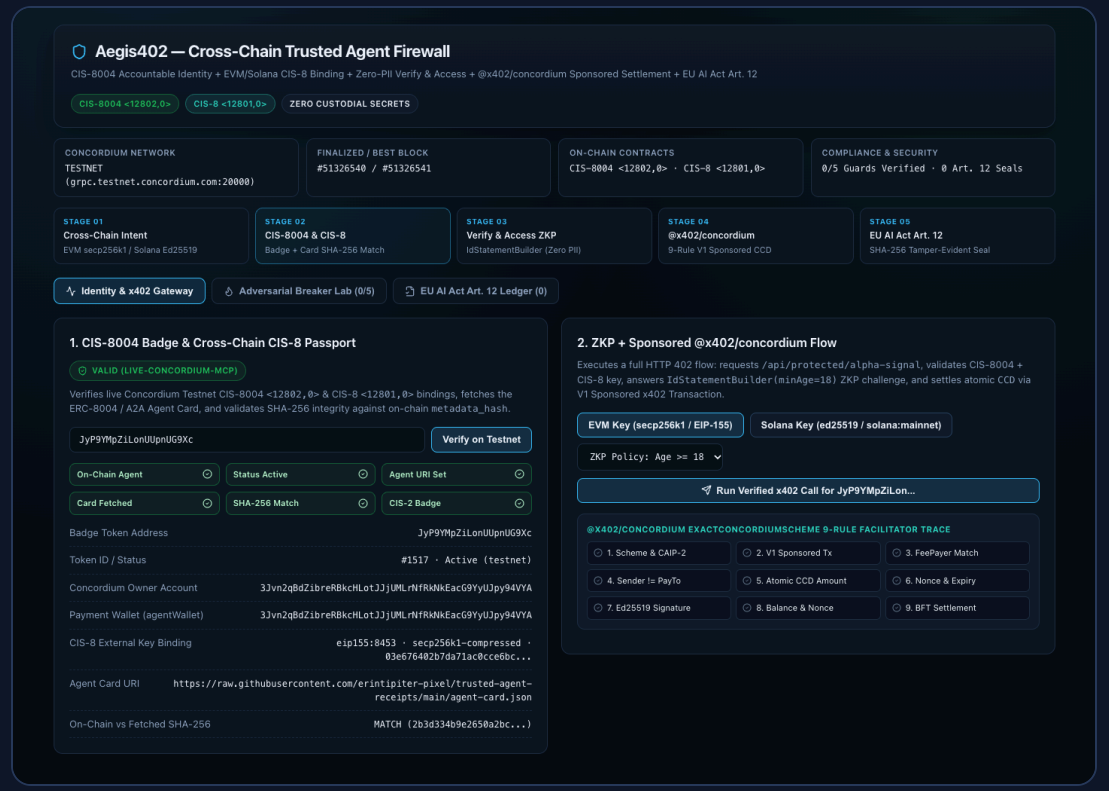
STAGE 4
@x402/concordium
9-rule sponsored facilitator settles atomic CCD via ConcordiumBFT (~10s).

STAGE 5
Art. 12 Audit Seal
Every ALLOW & DENY event is SHA-256 sealed into exportable JSON dossiers.

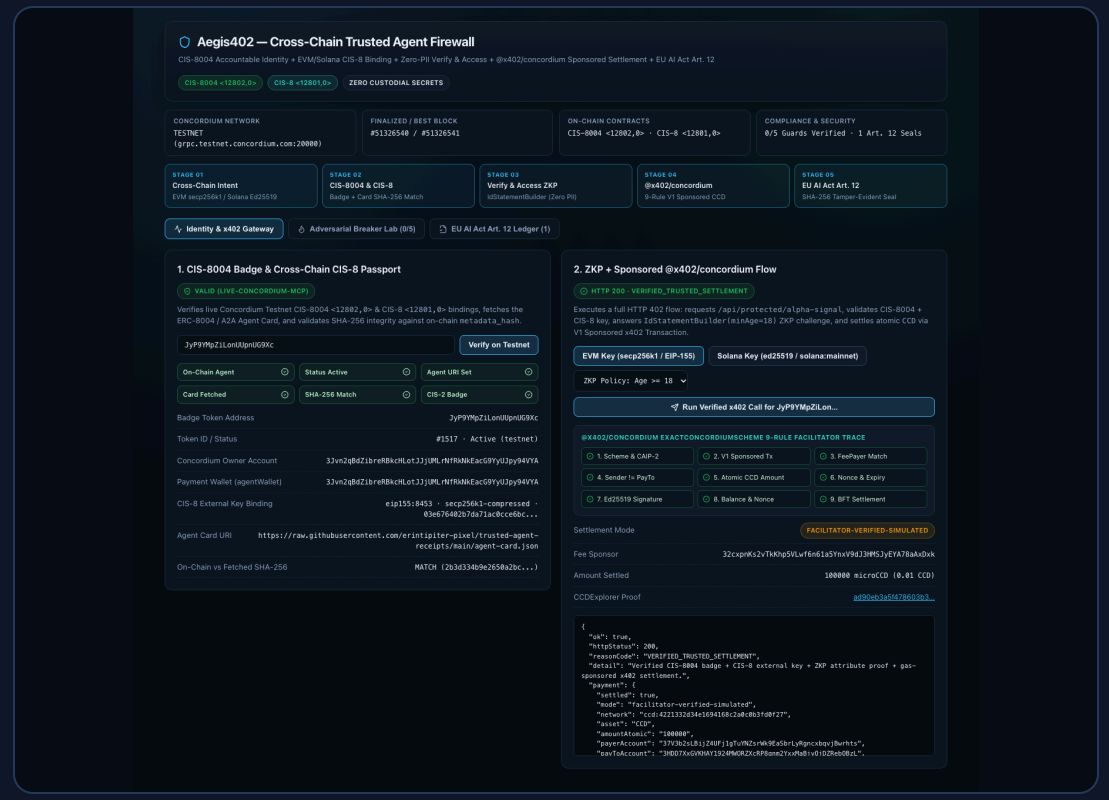
```
Testnet Genesis: ccd:4221332d34e1694168c2a0c0b3fd0f27  |  CIS-8004: <12802,0>  |  CIS-8: <12801,0>  |  Live Badge: #1517
```

03 • LIVE INTERACTIVE DEMO WALKTHROUGH

Real-Time Gateway Console & ZKP + x402 Settlement



1. Live Badge & CIS-8 Binding: Resolves Testnet badge #1517 and verifies external EVM/Solana signature.



2. ZKP + Sponsored x402 Settlement: Single-use ZKP challenge passes; `ExactConcordiumScheme` settles CCD.

9-Rule @x402/concordium Gas-Sponsored Facilitator

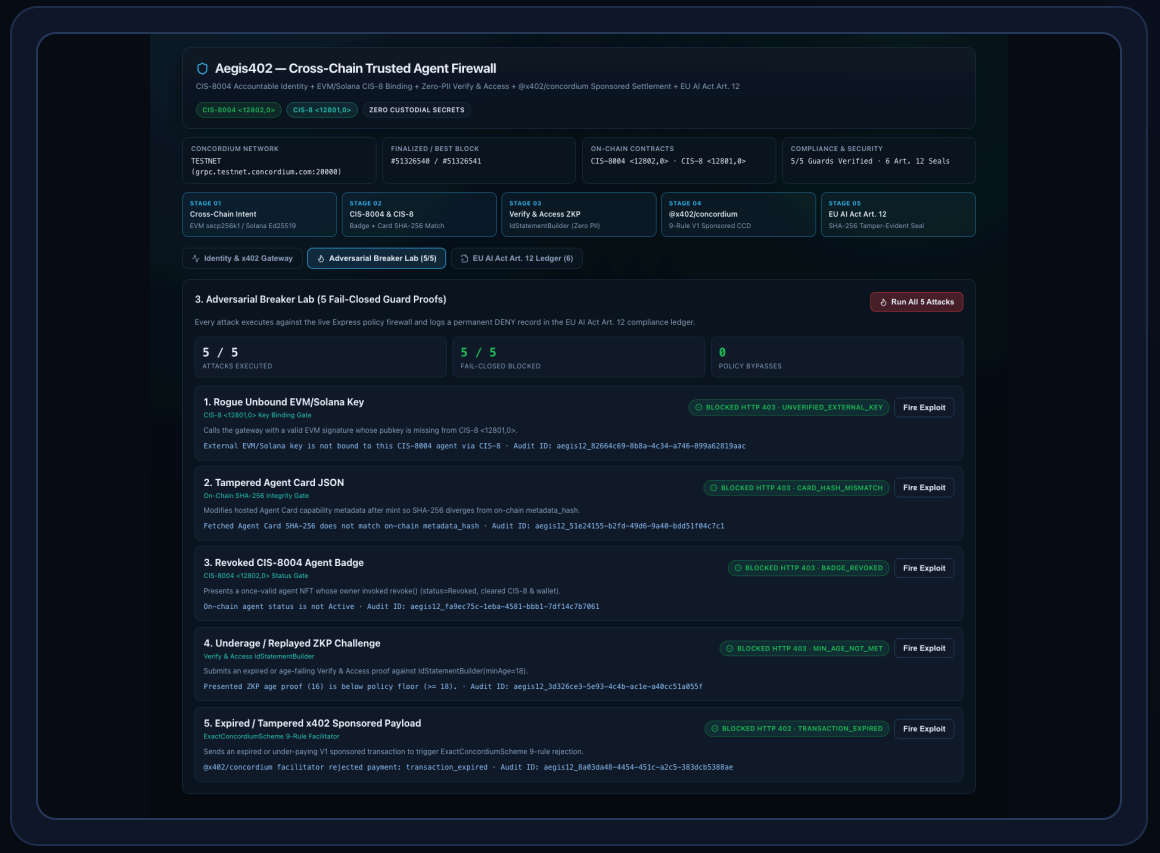
Why Sponsored V1 Transactions Matter

- Agents pay API fees in CCD or USDR without holding native gas balances across chains.
- **ConcordiumBFT** delivers deterministic ~10s finality — zero reorgs or probabilistic confirmation delays.
- Explicit mode badging (`live-testnet-bft` vs `facilitator-verified-simulated`) prevents silent mock fallback.

Enforced 9-Rule V1 Verification

CHECK	INVARIANT ENFORCED
1–3	Valid V1 sponsored payload, sponsor signature & fee budget
4–6	Exact recipient, minimum amount & non-expired `expiry`
7–9	Single-use nonce, network genesis match & atomic BFT broadcast

5/5 Adversarial Breaker Lab (0 Bypasses)



Fail-Closed Attack Matrix

ADVERSARIAL VECTOR	GATEWAY VERDICT
1. Rogue Unbound EVM/Solana Key	403 UNVERIFIED_EXTERNAL_KEY
2. Tampered Agent Card JSON	403 CARD_HASH_MISMATCH
3. Revoked CIS-8004 Badge	403 BADGE_REVOKED
4. Underage / Replayed ZKP	403 MIN_AGE_NOT_MET
5. Expired / Tampered x402	402 TRANSACTION_EXPIRED

06 • REGULATORY COMPLIANCE

EU AI Act Article 12 Audit Dossier & Zero-PII Boundary

Zero-PII Privacy Boundary

- Concordium's protocol-level ID layer issues cryptographic `IdStatementBuilder` proofs (e.g., `dob ≤ cutoff`) without exposing names, passport numbers, or raw dates.
- Gateway stores only boolean policy satisfaction + ZKP commitment hash.
- Eliminates GDPR storage liability for AI API providers.

Tamper-Evident Article 12 Ledger

- Every `ALLOW` and `DENY` decision generates a canonical SHA-256 sealed `AuditRecord`.
- Captures timestamp, external key, CIS-8004 badge ID, ZKP status, x402 tx hash, and failure reason.
- One-click JSON compliance bundle export via `/api/audit/export`.

07 • VERIFICATION & ENGINEERING RIGOR

Production-Tested Monorepo & Live Testnet Integration

9 / 9 TESTS PASS

Unit + Live Testnet gRPC

Vitest suite verifies cross-chain signers, ZKP gates, 9-rule x402 validation, and live read-only Concordium Testnet gRPC v2 + hosted MCP queries.

0 CONSOLE ERRORS

Clean GitHub Pages Console

Verified in headless Chrome across 298+ logged events and interactive Breaker Lab runs with zero runtime exceptions or 404s.

1080P WALKTHROUGH

Public Video & MCP Server

Includes `aegis402-mcp` stdio server, `aegis402-cli`, and public YouTube walkthrough (`0UTSsZeiQyw`).

08 • CONCORDIUM 75M CCD GRANTS ROADMAP

6-Month Path to Ecosystem-Wide Agentic Trust Middleware

MILESTONE 1 • M1–M2

Mainnet CIS-8004/CIS-8 & SDK

Deploy production `<10082,0>` / `<10081,0>` bindings and publish `@aegis402/sdk` + `@aegis402/express` on npm for 5-line API gating.

MILESTONE 2 • M3–M4

Multi-Facilitator x402 Relay

Launch high-availability sponsored CCD and USDR (`cis2–token`) facilitator relays with rate-limited sponsor pools for A2A/MCP servers.

MILESTONE 3 • M5–M6

Enterprise Agent Onboarding

Add periodic Merkle-root anchoring of EU AI Act Article 12 dossiers on Concordium Mainnet and onboard 10+ enterprise AI agent teams.

09 • OPEN SOURCE & NEXT STEPS

Ready for Encode Club Jury & Concordium Grants Review

Public Artifacts

- **GitHub (Apache-2.0):** `github.com/alphonshhhomenicmtu/aegis402-concordium`
- **Live Console:** `alphonshhhomenicmtu.github.io/aegis402-concordium/`
- **Grants Deck PDF:** `.../aegis402-concordium/aegis402-grants-deck.pdf`
- **YouTube Demo:** `youtube.com/watch?v=0UTSsZeiQyw`

Reproducible Commands

- `npm run typecheck`
- `npm run build`
- `npm test` (9/9 unit + live Testnet gRPC)
- `npm run demo:live-testnet -- --dry-run`