Alendra Institutional Verifiable Credential Engine (AIVCE)

AN OPEN-SOURCE ENTITY-VERIFICATION LAYER FOR THE XRP LEDGER

REFERENCE ROOT: ALENDRA.XYZ · PAYSTRING: ALENDRA$BITHOMP.COM

APPLICANT ENTITY NATASHA PELAK & ASSOCIATES, LLC	PROJECT LEAD NATASHA PELAK	REQUESTED FUNDING $75,000 · MILESTONE-BASED
SAM.GOV UEI P6LCJBMBQEE6	CAGE CODE 220B9	CERTIFICATION WOSB · SAM ACTIVE · EST. 2011

Federal identity, verifiable on-ledger.

Institutional adoption of the XRP Ledger — particularly for real-world assets, payments, and regulated finance — is bottlenecked by a structural gap: the entities institutions must trust exist in siloed federal registries (SAM.gov, the DLA CAGE system), while on-chain accounts carry no native cross-reference to those registries. Today, confirming that an XRPL account genuinely belongs to a registered, certified enterprise requires centralized intermediaries or manual audit.

AIVCE closes that gap with a lightweight, fully open-source verification layer built on primitives the ledger already has: bi-directional domain attestation (AccountSet Domain field ↔ `/.well-known/xrp-ledger.toml`), an enterprise credential extension to the standard toml schema carrying machine-readable federal identifiers (CAGE, UEI, WOSB status, NAICS), the XRPL Credentials/DID capabilities for attestation-based access under Permissioned Domains, and PayString for human-readable routing. No new token. No custodial service. A public-good standard any entity can self-deploy.

The applicant is its own first proof. Natasha Pelak & Associates, LLC is a real federal entity — WOSB-certified, SAM.gov-active, CAGE 220B9 — whose principal also operates the alendra.xyz research root. AIVCE ships with live reference implementations across three sovereign roots (personal lab, federal contractor entity, and consumer venture), demonstrating the standard at every institutional scale from day one.

Why this matters to the XRPL ecosystem now

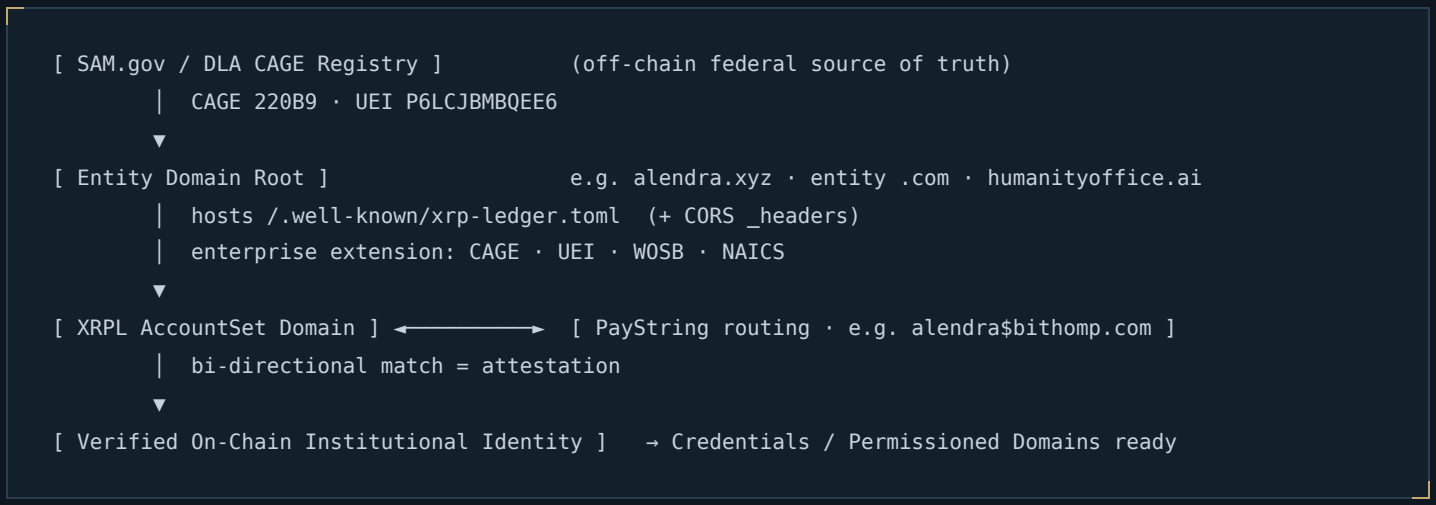
Entity verification is the precondition for institutional RWA and payments adoption — the 2026 funding program's stated priority areas. Every tokenized asset issuer, stablecoin counterparty, and enterprise payment participant faces the same question AIVCE answers: *how does anyone verify who is actually behind this account, using open protocols instead of a phone call?* AIVCE makes the XRP Ledger the first major chain where a government-registered enterprise identity is verifiable end-to-end with no intermediary.

PROGRAM ALIGNMENT · 2026

Submitted through the unified XRPL funding application for consideration across Grants and Accelerator tracks. Request ($75,000) sits within the published $50K–$200K program range. Milestones below are structured to the program's model — a minority of funding on development milestones and the substantial majority (~70%) on adoption and on-chain growth metrics. Open-source deliverables under a permissive license throughout.

One standard, sovereign roots.

AIVCE deliberately rejects the single-registry model. Each entity anchors its *own* domain root — the same domain its regulators, customers, and counterparties already know — so the attested identity an explorer shows matches the identity the off-chain world verifies. Alendra.xyz serves as reference implementation and specification home, not as a central authority.



Milestones — development-weighted 30%, adoption-weighted 70%

PHASE	TIMELINE	DELIVERABLES & METRICS	FUNDING
Phase I BUILD	Months 1–3	Production reference roots live (alendra.xyz + two sibling roots); enterprise toml extension specification published; open-source CAGE/UEI→toml mapping templates and validator CLI released on GitHub; bi-directional AccountSet verification demonstrated on Testnet and Mainnet.	30% · $22,500
Phase II ADOPT	Months 4–7	Adoption metrics: ≥10 external entities self-deploy verified roots using the toolkit; explorer/wallet compatibility confirmed (Bithomp, XRPScan, Xaman); lightweight open-source API cross-referencing public SAM.gov records ships; DNSSEC + edge-deployment automation released.	40% · $30,000
Phase III SCALE	Months 8–12	Growth metrics: ≥25 cumulative verified entity roots incl. defense-supply-chain contractors from the applicant's federal practice; SDK release; Credentials/Permissioned-Domains integration pattern published; independent security review; full developer documentation.	30% · $22,500

Budget

CATEGORY	SCOPE	ALLOCATION
Engineering	xrpl.js integration, toml tooling, validator CLI, API service, SDK (native XRPL transactions — no smart-contract layer required)	$45,000
Security review	Independent review: CORS/endpoint hardening, domain-isolation testing, key-management practices audit	$15,000
Legal & governance	Entity-asset custody documentation, license selection, specification governance	$10,000
Infrastructure	Edge deployment, DNSSEC enforcement, uptime monitoring	$5,000
	Total requested	$75,000

A federal entity as its own testnet.

Team & eligibility

Natasha Pelak — Project Lead. Principal of Natasha Pelak & Associates, LLC (WOSB, est. 2011); fifteen years across federal compliance consulting (CMMC, DFARS, FOCI), cybersecurity program production (OWASP NY/NJ under formal MOU at Microsoft 11 Times Square; Thomson Reuters C-suite governance panelist), and InfraGard membership since 2017. The firm's active defense-supply-chain advisory practice supplies the Phase III adoption pipeline: real contractors with real CAGE codes who need exactly this verification layer.

Engineering delivery via contracted XRPL developers under the project lead; security review independently sourced. All open-source deliverables published under a permissive license from the project GitHub organization.

Proof of architecture

Per program evaluation criteria, the application is accompanied by: the system-design schematic (p.3), the production toml templates for all three reference roots, the deployed reference sites, and — prior to submission — a public GitHub repository containing the toml kit, validator tooling, and deployment documentation. The applicant's own SAM.gov record (UEI P6LCJBMBQEE6) provides independently checkable ground truth for every claim in the reference implementation.

Risk governance

- Zero-secret policy. No private key, seed, or authorization token ever appears in a toml file, repository, or deployment pipeline.
- Entity asset isolation. Each root's XRPL accounts are held by the corresponding legal entity, with custody documented in operating agreements; personal, institutional, and venture accounts never commingle.
- No custody, no token. AIVCE holds no user funds, issues no asset, and introduces no intermediary — it is a verification standard plus tooling, minimizing regulatory surface.
- Spoofing resistance. Verification is bi-directional by design; the toolkit's validator rejects one-sided claims, and documentation teaches integrators to do the same.
- CORS correctness. All attestation endpoints ship with explicit `Access-Control-Allow-Origin` headers and deployment linting, eliminating the silent-failure class that breaks explorer crawls.

What the ecosystem receives

An open standard and toolkit that lets any registered enterprise — starting with U.S. federal contractors, extending to any jurisdiction with a public registry — make its identity verifiable on the XRP Ledger with no intermediary. Infrastructure for the institutional adoption the 2026 program exists to accelerate, delivered by an applicant who is, herself, the first verified entity.

SUBMISSION CONTACT

Natasha Pelak · natasha@natashapelak.com · alendra.xyz · Natasha Pelak & Associates, LLC · UEI P6LCJBMBQEE6 · CAGE 220B9