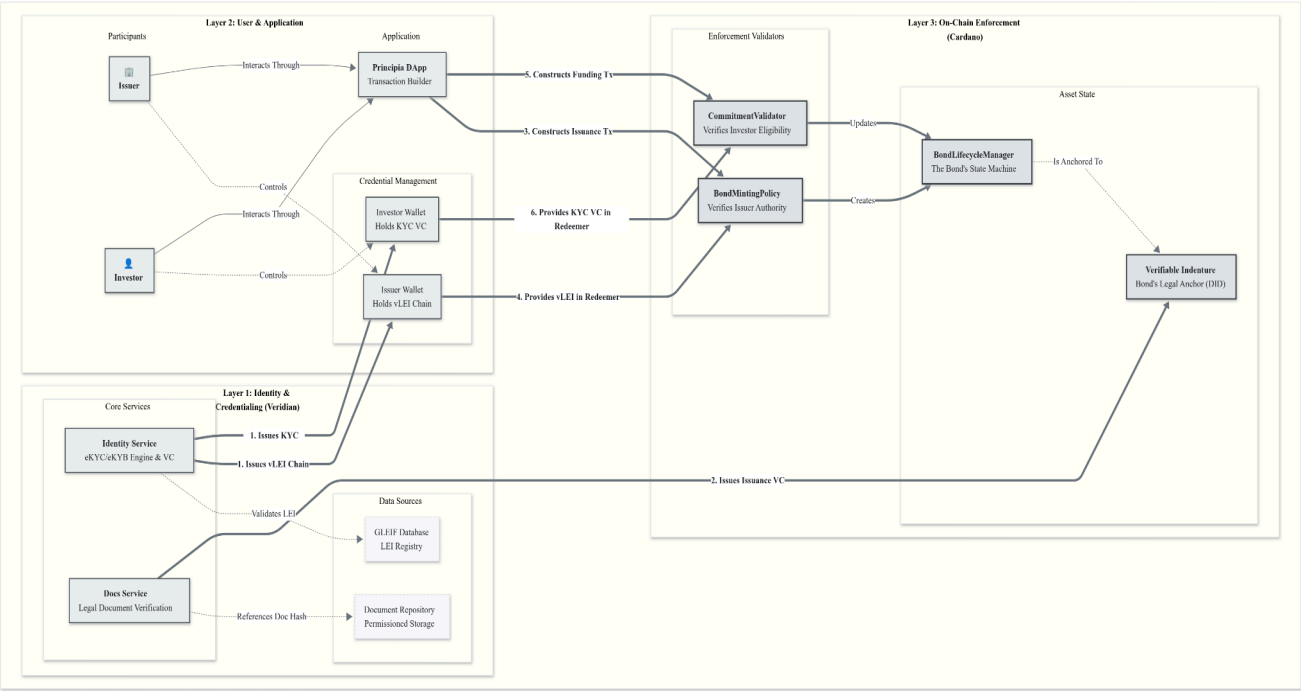
Principia Trust Engine

Overview

The Principia Trust Engine is the compliance and identity framework of the Principia ecosystem. Its purpose is to create a cryptographically-enforced, auditable link between real-world identity verification and on-chain actions. It moves beyond simple wallet whitelists to a dynamic, cryptographically secure system built on **Decentralized Identifiers (DIDs), Verifiable Credentials (VCs),** and **Verifiable Smart Contracts**. Its primary goal is to provide a practical, scalable, and auditable solution for meeting the stringent requirements of financial regulators like VARA, DIFC and ADGM.

Architecture



Core Principles

The engine's design is guided by three foundational principles:

1. **Identity as the Foundation:** All participants are represented by persistent, controllable DIDs, providing a stable identity anchor beyond ephemeral wallet addresses. Identities are issued as a vLEI and leverage the GLEIF Ecosystem Governance Framework.

2. **Verifiable Claims:** The system replaces manual whitelists with a dynamic model where users present cryptographically-signed claims (VCs) from a trusted authority to prove their eligibility at the moment of action.
3. **Direct On-Chain Enforcement:** Compliance status, verified off-chain, is directly enforced by the logic within on-chain smart contracts, creating a tight, unbreakable link between regulation and execution.

System Components & Layers

The architecture is structured into three distinct layers that work in sequence to manage identity, user interaction, and on-chain logic.

Layer 1: Identity & Credentialing (Veridian)

This off-chain layer serves as the bridge between legal entities and their digital identities. It handles all real-world due diligence and organizational credential issuance.

- **Identity Service (eKYC/eKYB):** Performs rigorous, jurisdiction-specific Know Your Customer (KYC) and Know Your Business (KYB) checks. This includes corporate document verification, AML screening, and UBO identification.
- **DID Creation:** Manages the issuance of a `did:principia` for each participant, creating a persistent digital identity.
- **Verifiable Credential (VC) Issuance:** Upon successful verification, the service acts as a trusted issuer, cryptographically signing and delivering VCs to the user's private identity wallet.
    - **For Issuers:** As a Qualified vLEI Issuer (QVI), it validates the entity's **Legal Entity Identifier (LEI)** and issues a **vLEI Credential Chain**. This chain proves the company's identity and delegates on-chain authority to specific individuals (e.g., a CFO).
    - **For Investors:** It issues a simpler VC containing claims relevant to their status, such as `kyc_status: Verified_Retail`.
- **GLEIF Validation Agent:** this is the entity that leverages its existing, regulatorily compliant client onboarding process to streamline the issuance of an LEI for a corporate client. Veridian's entire purpose is to be an identity and verification specialist, and therefore it serves the purpose as the validation agent.

Layer 2: User & Application

This layer encompasses the participants and the tools they use to interact with the ecosystem.

- **Participants:** Includes **Issuers** (corporations raising capital) and **Investors** (individuals or firms providing capital). A future role is **verifiers** to verify the authenticity of the credentials (regulator).

- **Credential Management:** Each participant controls a private wallet that holds their DIDs and associated VCs (e.g., an Issuer Wallet holding the vLEI chain, an Investor Wallet holding a KYC credential).
- **Principia DApp:** The primary user interface that acts as a "transaction builder." It helps users construct permissioned transactions by pulling the necessary VCs from their wallets to be submitted to the blockchain.

Layer 3: On-Chain Enforcement (Cardano)

This layer is where compliance is enforced directly by the smart contracts on the Cardano blockchain.

- **Enforcement Validators ("VC-in-Redeemer" Model):** This core innovation embeds verification logic directly into the financial contracts (`BondMintingPolicy`, `CommitmentValidator`). When a user submits a transaction, their VC is placed in the **Redeemer**. The validator then performs a series of checks on-chain:
    1. **Authenticity:** Verifies the VC's digital signature.
    2. **Authority:** Confirms the VC was issued by a trusted, hard-coded DID (e.g., Veridian).
    3. **Ownership:** Ensures the DID in the VC subject corresponds to a public key signing the transaction.
    4. **Validity:** Checks the relevance of the claims and ensures the VC has not expired.
- **Asset State (`Verifiable Indenture`):** To give the asset itself a legal identity, this model uses a unique DID for each bond. A master "Issuance VC" is created that links this bond DID to the cryptographic hashes of the legal documents (stored off-chain) and the on-chain parameters, creating an immutable and verifiable legal anchor for the digital asset.

End-to-End Issuance Workflow

The journey of a corporate issuer highlights how these layers interact:

1. **Onboarding (Layer 1):** The CFO of "ACME Corp" uses the Principia DApp to onboard. The Veridian service performs eKYB on ACME, validates its LEI, and issues the root vLEI credential to ACME's corporate DID. ACME then issues a delegated authority credential to the CFO's personal DID.
2. **Deal Verification (Layer 1):** ACME submits its Bond Indenture. The Docs Service hashes the legal documents and generates the master "Issuance VC," creating the bond's unique `Verifiable Indenture` DID.
3. **Transaction Construction (Layer 2):** In the DApp, the CFO initiates the bond minting. The DApp fetches the required vLEI credential chain from the CFO's wallet and places it into the transaction's **Redeemer**.
4. **On-Chain Enforcement (Layer 3):** The transaction is submitted. The `BondMintingPolicy` on Cardano opens the redeemer, verifies the entire chain of credentials to confirm the CFO's authority, and only then permits the bond tokens to be minted.

Key Design Goals

- **Security:** The model is highly secure. Stolen credentials are useless without the associated private keys needed to sign transactions, and forged credentials will fail signature verification on-chain. Credentials that become comprised benefit from key rotation to recover the credential, without the need for re-issuance.
- **Scalability:** By avoiding a centralized on-chain registry, the system is exceptionally scalable. Millions of users can be onboarded with no impact on on-chain state bloat or performance degradation.
- **Privacy:** The "VC-in-Redeemer" model is inherently private, as user credentials are only revealed for a specific transaction and not stored publicly. This architecture is also future-proofed for the potential integration of **Zero-Knowledge Proofs (ZKPs)**, which would allow users to prove their eligibility without revealing any underlying data.