Prisma DIDs – Executive Summary

Version: 1.0

Date: December 2025

Status: Production-Ready Specification

Overview

Prisma DIDs is a Cardano-native decentralized identity system that enables self-sovereign identity and verifiable credentials using existing Cardano wallets. The system provides W3C-compliant DIDs and privacy-preserving credentials at a fraction of the cost of existing solutions.

Problem

Current decentralized identity solutions for Cardano face significant barriers:

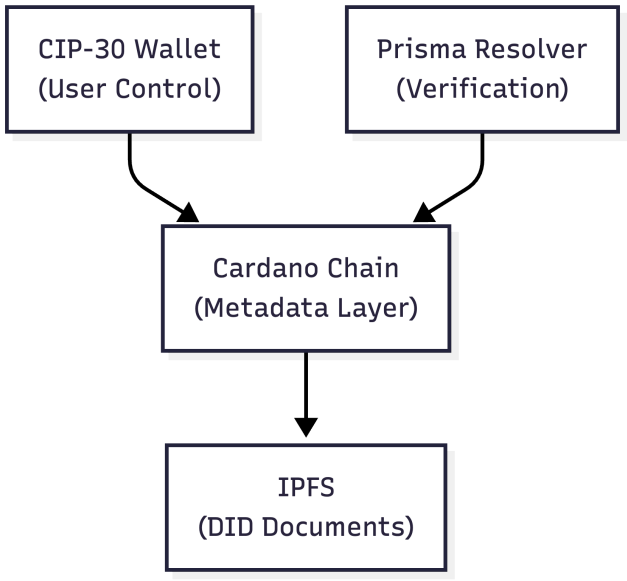
Challenge	Impact
Heavy Infrastructure	Existing methods (e.g., `did:prism`) require dedicated nodes and backend services
Complex Integration	Specialized SDKs and complex setup processes
Centralized Dependencies	Resolution often relies on centralized services
High Costs	Smart contract-based approaches have 10-100x higher transaction fees

---

Solution

Prisma DIDs leverages Cardano's native capabilities to provide a lightweight, accessible identity layer:

Core Architecture



Key Differentiators

Feature	Prisma DIDs	Traditional Solutions
Cost per Operation	~0.17-0.25 ADA (~$0.10-0.15)	$1-10+
Infrastructure	Wallet + IPFS + lightweight resolver	Dedicated nodes, backends
Time to Integrate	Minutes (SDK import)	Days to weeks
Wallet Support	Any CIP-30 wallet (Eternl, Lace, Nami, etc.)	Often proprietary

---

Technical Approach

DID Method: `did:cardano`

DIDs are derived from Cardano stake addresses, providing:

- **Persistence:** Stake addresses remain constant across wallet operations
- **Security:** Native cryptographic binding via stake key signatures
- **Interoperability:** Standard bech32 format (`did:cardano:stake1u9...`)

On-Chain Registry

All DID and VC events are stored as CIP-20 transaction metadata:

Label	Purpose
L_DID (199674)	DID lifecycle: create, update, revoke
L_VC (199675)	VC anchoring: issue, validate, revoke

Verifiable Credentials

Three credential formats supported:

Format	Privacy Level	Use Case
SD-JWT	Selective Disclosure	Standard credentials with field-level privacy
Ed25519	Full Disclosure	Simple attestations, low overhead
BBS+ (planned)	Unlinkable Presentations	Maximum privacy, zero-knowledge proofs

> ***Revocation: SD-JWT credentials use the `jti` (JWT ID) as the on-chain identifier, enabling revocation checks regardless of which claims are disclosed in a presentation.***

Standards Compliance

Standard	Implementation
W3C DID Core 1.0 (https://www.w3.org/TR/did-core/)	Full compliance
W3C VC Data Model 2.0 (https://www.w3.org/TR/vc-data-model-2.0/)	Full compliance
IETF SD-JWT (https://datatracker.ietf.org/doc/draft-ietf-oauth-selective-disclosure-jwt/)	Selective disclosure
CIP-10/20/30 (https://cips.cardano.org/)	Cardano integration

Use Cases

Primary: Contribution Credentials

The initial deployment targets **Action Learning Journey (ALJ)**, where organizations issue verifiable credentials for:

- Learning module completions
- Project contributions
- Skill attestations
- Community participation

Broader Applications

Domain	Application
Education	Certificates, course completions, skill badges
Employment	Work history verification, reference attestations
Governance	Voting eligibility, delegation credentials
Supply Chain	Product authenticity, certification chains

Cost Analysis

Operation	Estimated Fee
DID Create	0.17-0.20 ADA
DID Update	0.18-0.22 ADA
DID Revoke	0.17-0.20 ADA
VC Anchor	0.17-0.20 ADA

Monthly estimate (100 DIDs, 500 VCs): ~115 ADA (~$70 at $0.60/ADA)

Security Model

Threat	Mitigation
DID Hijacking	Only stake key holder can sign events
Event Forgery	Ed25519 signatures verified on resolution
Chain Tampering	Blockchain immutability + prev pointer chain
Replay Attacks	Version numbers prevent replay
Credential Forgery	On-chain anchoring + issuer DID verification

---

System Architecture

Per the technical specification, the system separates **global infrastructure** from **forkable components**:

Global Infrastructure (Prisma-operated)

Component	Purpose	Scope
DID Dashboard	Universal DID management	All Cardano users
DID Indexer	DID resolution and validation	All `did:cardano` identities

Forkable per Organization

Component	Purpose	Scope
VC Interface	Credential issuance/verification	Per organization
VC Indexer	VC status and revocation lookups	Per organization

This separation enables:

- A single, shared DID infrastructure for all Cardano users
- Organization-specific credential systems with custom schemas and indexers
- Decentralized VC ecosystems without relying on Prisma infrastructure

---

Documentation

Document	Description
TECHNICAL_DESIGN.md (./TECHNICAL_DESIGN.md)	Full normative specification
TECHNICAL_DESIGN_1.6.md (./TECHNICAL_DESIGN_1.6.md)	Latest versioned spec
CARDANO_INTEGRATION_PLAN.md (./CARDANO_INTEGRATION_PLAN.md)	Cardano integration specification
POC_PLAN.md (./POC_PLAN.md)	Implementation roadmap and tasks
ADR-001 (./adr/001-metadata-anchoring.md)	Architecture decision record

---

Contact

Project: Prisma DIDs

Repository: https://github.com/prisma-collective/enrol