LANDANO

Design specification: Landano Veridian prototype

Author: Dorus van der Kroft - dorus@landano.io

Sep 9, 2025

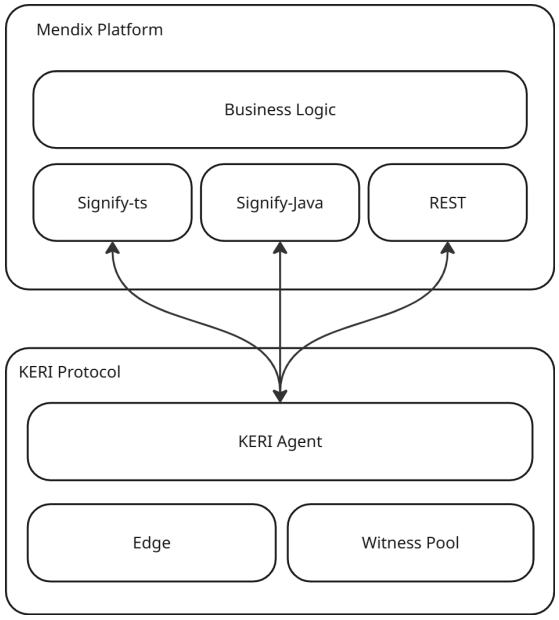
V1.1

Introduction

The Landano project is using Cardano NFTs to notarize land rights in jurisdictions that need better land registry solutions.

Landano is prototyping the use of the Cardano Foundation ID wallet with its platform. The Cardano Foundation ID Wallet implements the KERI (Key Event Receipt Infrastructure) protocol. This is a decentralized identity system built around the concept of self-certifying identifiers (Autonomic Identifiers known as AIDs) that are cryptographically bound to controlling keys.

The Landano platform is built in the Mendix Low-Code platform, and the prototype is implemented using:
- signify-ts for client-side identity and credential management within the Mendix Native app.
- cf-signify-java for backend verification and credential processing within the Mendix web backend.



This document specifies the design of the prototype system. We are testing three basic use cases as a proof of concept:
1. Verify Landano user identity
2. Verify user ownership of Landano NFT
3. Verify ADA wallet balance belongs to an ID wallet holder

Use cases

1. Verify Landano User Identity

In the jurisdictions where we are piloting our solution, a village chief and their representatives have the right to approve land administration transactions for their community. This use case represents this scenario.

We want to demonstrate that a particular user has the credentials to act as a representative for their chief. The chief has the constitutional authority to approve land transactions and is considered to be the root of trust.

1. Chief has an AID and is an issuer as the root of trust

The Chief has been given a Mendix account and uses their personal ID Wallet (Veridian or similar) to generate and manage their Autonomic Identifier (AID).

The wallet connects to the Cardano Foundation's KERIA instance via signify-ts, maintaining the Chief's cryptographic keys securely on their device.

Note on Root of Trust Bootstrapping

In the current pilot, each village chief acts as a root of trust by issuing credentials to their representatives. While this model works at a community level, it introduces a bootstrapping problem: how does a verifier know that a given AID truly belongs to a legitimate chief? For broader scalability, this root of trust may need to be anchored by a trusted attestation party, such as a government registry, traditional authority council, or an NGO that validates chiefs' AIDs. This ensures that verifiers can rely on a federated set of trusted issuers rather than individual chiefs alone.

2. Chief representative creates AID

The Chief Representative creates their AID using signify-ts through the Cardano Foundation ID Wallet on their device.

3. Mendix orchestrates credential issuance from Chief to Representative

The credential issuance follows the IPEX (Issuance and Presentation Exchange) protocol with Mendix acting as the orchestrator:

- Mendix prepares the credential details (representative's AID, attributes, permissions) based on business rules and data entry
- Mendix sends an IPEX Apply message to the Chief's wallet requesting credential issuance
- The Chief receives a notification in their Veridian wallet showing the proposed credential details
- The Chief reviews and approves the issuance request directly in their wallet

- Upon approval, the Chief's wallet uses signify-ts to create and send the ACDC credential to the Representative via IPEX Grant
- The Representative receives and stores the credential in their ID Wallet
- Mendix receives confirmation of successful issuance and updates its records

This approach ensures the Chief maintains full control of their signing keys while Mendix handles the business logic, approval workflows, and audit trail.

4. Verifier requests presentation

The Verifier (via Mendix backend using signify-java) initiates a presentation request using the IPEX Apply protocol. The Representative's wallet (using signify-ts) receives the request, creates a presentation of the ACDC, signs it with their AID, and returns it via IPEX Offer. The

Verifier validates both:

- The Chief's original signature on the ACDC credential
- The Representative's signature on the presentation

This dual verification ensures the Representative possesses a valid credential from a legitimate Chief and controls the AID associated with that credential.

This completes the first use case scenario for the prototype wherein we verify a Landano user’s identity and credentials.

2. Verify User Ownership of Landano NFT

In the Landano system, users own Cardano NFTs that prove their rights in relation to specific plots of land. This use case represents a scenario where a third party verifies that the user is in control of a Landano NFT.

The system performs comprehensive ownership verification to ensure the user controls both the identity and the blockchain asset through a dual-signature binding stored immutably in the NFT metadata:

Initial Binding (During NFT minting):

- When a Landano NFT is minted, the system generates a binding message containing the AID, Cardano wallet address, NFT identifier, and timestamp
- The user signs this identical message with both their ID wallet (proving AID control) and their Cardano wallet (proving wallet control)
- Both signatures are embedded directly in the NFT metadata along with the AID, creating an immutable record of the legitimate owner
- This dual-signature proof demonstrates that at minting time, the same person controlled both the AID and the Cardano wallet

Ownership Verification (Each time access is requested):

- Query the Cardano blockchain to retrieve the NFT and its complete metadata
- Extract the AID and both binding signatures from the NFT metadata
- Verify the user controls the claimed AID by requesting a fresh signature from their ID wallet
- Check that the NFT is still held by the original wallet address specified in the binding
- Validate both stored signatures against the binding message to ensure the cryptographic proof remains intact
- Only grant access if the NFT is held by the original wallet and the user can prove control of the bound AID

Property Transfer Control: Since property rights cannot be transferred by simple wallet-to-wallet NFT transfers, any legitimate ownership change must go through a smart contract that:

- Verifies the current owner's identity through both wallet and AID signatures
- Updates the NFT metadata with the new owner's AID and fresh binding signatures
- Records the transfer authorization and relevant legal documentation
- Ensures the previous owner's binding is properly terminated

This approach ensures that property rights remain correctly tracked and legally compliant, preventing unauthorized transfers through simple wallet movements.

3. Verify ADA Wallet Balance belongs to an ID Wallet Holder

In addition to verifying identity and NFT ownership, the prototype also demonstrates how to prove control over an ADA wallet and its balance in relation to a KERI-based ID Wallet. This is useful in scenarios where users must show they have sufficient ADA to complete a transaction or service.

The system enables a verifier (e.g., government official) to confirm that a Cardano wallet belongs to a specific ID wallet holder:

Verification Process:

- ID holder claims ownership of a Cardano wallet address
- Verifier generates a challenge message: "I, holder of AID [AID], own Cardano wallet [address] [timestamp]"
- ID holder signs this message with their ID wallet (proving AID control)
- ID holder signs the same message with their Cardano wallet (proving wallet control)
- ID holder provides both signatures to the verifier
- Verifier validates both signatures are correct for the claimed AID and wallet address
- If both signatures verify, the verifier can query the ADA balance using the Cardano Mendix Plugin
- Verifier sees the confirmed balance of the verified wallet

This proves to the verifier that the ID holder actually controls the Cardano wallet they claim to own.

Key Components:
- Mendix (frontend and backend platform for Landano)
- signify-ts (edge signing inside the ID Wallet app)
- cf-signify-java (backend verification and credential processing)
- Cardano node/Blockfrost (on-chain balance query)

Implementation

Milestone 1

During the first milestone we will prove the preliminary integration between the Landano/Mendix plugin and the KERI protocol by having a user prove they hold a certain credential and tying the results of this verification to the user account in the Mendix application. Initially we will use the REST endpoints of the KERI Agent to get a better understanding of the process flows of the KERI protocol.

Milestone 2

In this milestone we'll implement the 3 different use cases as outlined earlier. We will also shift from a REST endpoint integration towards a full signify implementation so we are no longer dependent on credential-server API endpoints that are exposed but instead make use of the KERI endpoints as defined in the protocol.

As we will need integration with the Cardano blockchain we'll add the Cardano Mendix Plugin to the project to be able to create wallets, read wallet information and be able to sign transactions and messages.

After the full implementation of the use cases we will develop all the test cases necessary to proof the system is working properly and execute on these test cases.

Milestone 3

Milestone 3 will be used to fix the findings of the test phase ending milestone 2. The documentation outlining the use cases and how to implement identity handling using the KERI protocol in a Mendix context will be written.

After this the solution will be published in the Mendix marketplace so it becomes available for the 400,000 Mendix developers world wide.