Sovereign Digital Identity

A system that creates a unique identity for interaction on the Blockchain

Executive Summary

This white paper proposes a Sovereign Digital Identity (SDI) that returns control to the citizen, reduces repetitive paperwork, and protects privacy by design. The solution combines Decentralized Identifiers (DID) and Verifiable Credentials (VC) with minimal disclosure presentations and zero-knowledge proofs (ZKP) to validate conditions (e.g., "over 18 years old") without exposing sensitive data.

The WIRA Wallet generates the DID and keys on the device and stores the credentials in the app's encrypted storage protected by Keystore/Keychain; it is only unlocked during user action (PIN/biometrics). Verifications can be off-chain (portals/apps) or on-chain (attestation/traceability contracts). No PII is written on-chain: verifiable references (CIDs) and events are anchored.

VC issuance is done with our own Issuer compatible with Polygon ID and the iden3comm messaging protocol. Each VC includes a statusPointer (location of the public status list + index) so third parties can verify if it is active/suspended/revoked without seeing its content. To operate on the blockchain, Account Abstraction (ERC-4337) with Smart Accounts and Paymasters is used. Recovery in case of device loss employs Shamir Secret Sharing in Carnet+PIN (2-out-of-2) and Guardians (n-out-of-s) modes. The result is an interoperable, auditable platform aligned with Bolivian regulations.

1. Introduction

This White Paper proposes a Sovereign Digital Identity (SDI) platform for Bolivia based on three principles: user control, security by design, and minimal disclosure. The WIRA Wallet generates the decentralized identifier (DID) and its keys on the device itself and stores the holder's credentials in the app's encrypted storage, protected by Keystore (Android) / Keychain (iOS). This storage is temporarily unlocked in memory only when the user authenticates (PIN or biometrics), and after the operation, the key is erased from memory; clear-text information is never stored on the phone. With these credentials, the wallet builds presentations with cryptographic proofs that reveal only what is essential to authorize an action (affirming that evidence belongs to a person or process) without exposing personal data.

Verification can occur off-chain in portals (frontends) and backends (servers) or on-chain, in smart contracts. The on-chain layer is limited to managing and operating the holder's Smart Account and executing domain contracts like attestation and traceability, but no personal data (PII) is recorded on the chain. To simplify the experience, Account Abstraction (ERC-4337) is used: the wallet signs UserOperations and can use Paymasters to sponsor network fees under defined policies, preventing the citizen from manually managing gas.

1.1 Context

In Bolivia, access to public and private services often requires the same personal information repeatedly (repeated KYC). There is no data portability between institutions, and centralized repositories concentrate the risk of leaks. This dynamic increases costs and times, discourages digital adoption, and exposes citizens to impersonation.

Furthermore, in processes requiring traceability and attestation—for example, the upload and validation of minutes, or certifications of origin and quality in production chains—verifiable evidence (signatures/hashes/status of validity) and records auditable by third parties without friction are often lacking. Distrust between actors and irregular connectivity lead to duplicate verifications and manual tasks, introducing operational friction: more steps, more waiting, higher costs, and a greater likelihood of error.

The proposed SDI addresses these points with:

- Portable verifiable credentials (VC) controlled by the user.
- Minimal disclosure presentations with expiration and recipient.

- On-chain operations without PII and with low-friction experiences like sponsored gas.
- Traceability evidence such as files and metadata published on IPFS and attested in contracts.

1.2 Project Objective

General Objective:

Design and implement an SDI platform that returns control to the holder, minimizes exposure of personal information, reduces operational friction, and respects the Bolivian legal framework.

Specific Objectives:

- Develop and publish WIRA WALLET with local generation of DID and keys, encrypted bundle (app's encrypted storage protected by Keystore/Keychain) to custody credentials () and minimal operational metadata, presentations with nonce, recipient, and expiration. Also, a local history interface visible only to the user.
- Operate Issuer Nodes for credential issuance and claims through our own Issuer (currently the only one), publishing the validity status compactly and retaining only minimal audit metadata, without storing personal attributes.
- On-chain execution with Smart Accounts (ERC-4337) and Paymasters applying sponsorship policies suitable for already operational attestation and traceability flows.
- Secure off-chain evidence pipeline, including capture and OCR through our own backend (to avoid exposing API keys), file hashing and publication on IPFS, linking that evidence with on-chain attestations when the process requires it.

1.3 Problem and Opportunity

Current Problem: Data repetition, silos between institutions, risks from centralized storage, high friction in verifications, and limited traceability reduce trust and audit capacity.

Opportunities with SDI: Portability of attributes controlled by the user, immediate verification with minimal disclosure presentations and queryable validity status, reduction of time and costs by eliminating redundant steps, smaller attack surface by keeping PII off-chain and encrypted on the device, and verifiable traceability/attestation (evidence on IPFS + on-chain events) that strengthen the auditability of civic and productive processes

and improve competitiveness in markets requiring verifiable certifications of origin and quality.

2. Technical Foundations

2.1 Decentralized Identifier.

WIRA Wallet generates a key pair on the device and derives a DID compliant with compatible methods. The public DID document publishes the active verification keys. The private key never leaves the device.

2.2 Verifiable Credentials in JSON-LD.

A VC is a claim signed by a trusted issuer about the holder's attributes. It is issued in JSON-LD or SD-JWT (depending on the chosen schema) and includes:

- Proof of origin and integrity (issuer's signature).
- Status Pointer to a compact public list of validity status (active/suspended/revoked).

The wallet stores the VC in the app's encrypted storage protected by Keystore/Keychain. Our own Issuer based on Polygon ID validates the received evidence and returns the VC signed with its issuer DID.

2.3 Verifiable Presentations with Zero-Knowledge.

When a verifier requests something, the wallet builds a Verifiable Presentation (VP) that contains only what is required (selective disclosure) and can include zero-knowledge proofs (ZKP), on the BJJ curve for range or membership proofs. Each VP incorporates:

- nonce (unique request identifier),
- aud (domain/recipient),
- expiration (TTL).

This prevents reuse and correlation of presentations.

2.4 Secure Messaging with iden3comm.

Issuance and presentation are conducted via iden3comm, with end-to-end encryption and mutual authentication between WIRA Wallet and the Issuer or Verifier. The backend acts as a transport gateway without access to content.

2.5 On-Chain Execution with Account Abstraction.

On-chain operation is done with a Smart Account compatible with ERC-4337 (EntryPoint v0.7). The wallet signs UserOperations with its local key and sends them to the EntryPoint. If there is sponsorship, a Paymaster covers fees under policies. This model reduces operational steps and avoids exposing PII on the chain.

In the case of traceability/attestation, on-chain contracts register CIDs of evidence (IPFS) and emit verifiable events. However, ZK verification logic and VC status checks occur off-chain.

3. Technical Architecture

3.1 Identity Layer.

The holder's identity originates on their own device. WIRA Wallet locally generates the key pair and derives a DID (decentralized identifier). From that DID, a DID document is published with the active verification keys. The private key associated with the DID does not leave the phone: it is only used to sign when the user authenticates and the operation requires it. In parallel, the app maintains a key (privkey) for on-chain operation linked to the holder's Smart Account, which will be deployed at the time of the first transaction.

3.2 Credentials Layer.

Issuance by the Polygon ID Issuer Node, encrypted storage in WIRA Wallet locally (bundle), on-demand presentation, and compact status lists or equivalent mechanisms for revocations and expirations. Each VC includes a "status" pointer to a compact public list maintained by the issuer (e.g., bitstring or merkle map) to mark validity, suspension, or revocation.

Verifiable Credentials (VC) are currently issued from our own Issuer node based on Polygon ID and encoded in JSON-LD to provide semantics and compatibility with standard verifiers. Each VC includes the issuer's signature and a status pointer to a public StatusList of the

issuer, where any third party can check if the credential is active, suspended, or revoked. The VC is not stored on servers; it is kept only on the holder's device within a locally encrypted bundle (app's encrypted storage protected by Keystore/Keychain), and the issuer preserves minimal metadata in its internal database without PII.

3.3 Privacy Layer.

Verification is designed for minimal disclosure. Upon a request, Wira builds a Verifiable Presentation (VP) that contains only the strictly necessary attributes and adds anti-correlation controls: a unique nonce per request, an explicit recipient, and a short expiration. When the case warrants it, the VP incorporates zero-knowledge proofs (ZKP) to demonstrate conditions without revealing values in clear text. All peer-to-peer exchange is conducted via iden3comm, with end-to-end encryption.

3.4 On-Chain Execution Layer.

On-chain operation is limited to what is necessary for traceability and attestation cases: the holder's Smart Account (ERC-4337) signs and sends UserOperations to the EntryPoint, and attestation contracts record references and emit verifiable events. No PII is recorded on the chain. To simplify the experience, a Paymaster can sponsor gas under policies so the user does not have to manage fees.

3.5 Integration Layer.

The platform exposes an evidence pipeline oriented towards traceability and attestation: the app captures images and data, OCR/validations are executed (without exposing API keys on the client), the hash is calculated, and files/metadata are published on IPFS, obtaining its CID (immutable content identifier). This CID is linked on-chain through attestation contracts from the app (frontend): all on-chain operations are initiated and signed in WIRA Wallet with local keys; the backend never signs or sends transactions on behalf of the user, nor does it custody keys. Third-party portals verify by combining: the on-chain event (who attested and when), retrieval on IPFS using the CID (ensures that the read content is exactly what was attested), and when applicable, querying the credential status in the issuer's public StatusList indicated by the VC's statusPointer. No PII is exposed on the chain.

3.6 Storage and Custody Scheme

Three pieces are stored on the user's device:

- The DID seed/key
- The private key (privkey) used by the Smart Account
- The VCs in the app's encrypted storage protected by Keystore/Keychain.

This bundle is encrypted with AES-256-GCM using a DEK (Data Encryption Key) which is in turn protected with a KEK derived from the user's PIN and a secret from the device's secure storage (Argon2id-type derivation). The bundle is temporarily decrypted in memory when the user authenticates, and after the operation, the key is erased from memory; clear-text information is never stored on the phone. Recovery in case of device loss is implemented with Shamir Secret Sharing (SSS): the bundle's recovery secret is fragmented for the Carnet+PIN (2-out-of-2) and/or Guardians (n-out-of-s) schemes, so the user can regain access without any single actor being able to do so alone.

4. Flows

4.1 Onboarding and Issuance.

When installing WIRA Wallet, the user locally generates a master seed. From this seed, two keys are derived: the identity key which is the DID for the credentials layer, and the private key privkey which will be used for on-chain operation. With this private key (privkey), the predictive address of their Smart Account (ERC-4337) is calculated via the factory; the contract is not yet deployed.

To request an identity or role VC, the app captures images of the ID card and face and sends only these images to our own backend for OCR and liveness (we avoid exposing API keys on the client). Minimum attributes are derived from the result (names, surnames, date of birth). The app signs a request and sends it encrypted via iden3comm to our Issuer. The Issuer validates the evidence and issues the VC (JSON-LD) with its signature and a status pointer included within the VC itself (credentialStatus / statusPointer), which references the issuer's public StatusList (active/suspended/revoked).

The VC is stored only on the device within an encrypted bundle that is the app's encrypted storage protected by Keystore/Keychain. This bundle is encrypted with a key derived from the user's PIN plus the device's secure storage; each time the user acts, the app temporarily unlocks the bundle to read/sign and then reseals it. The Issuer retains only minimal audit metadata without PII.

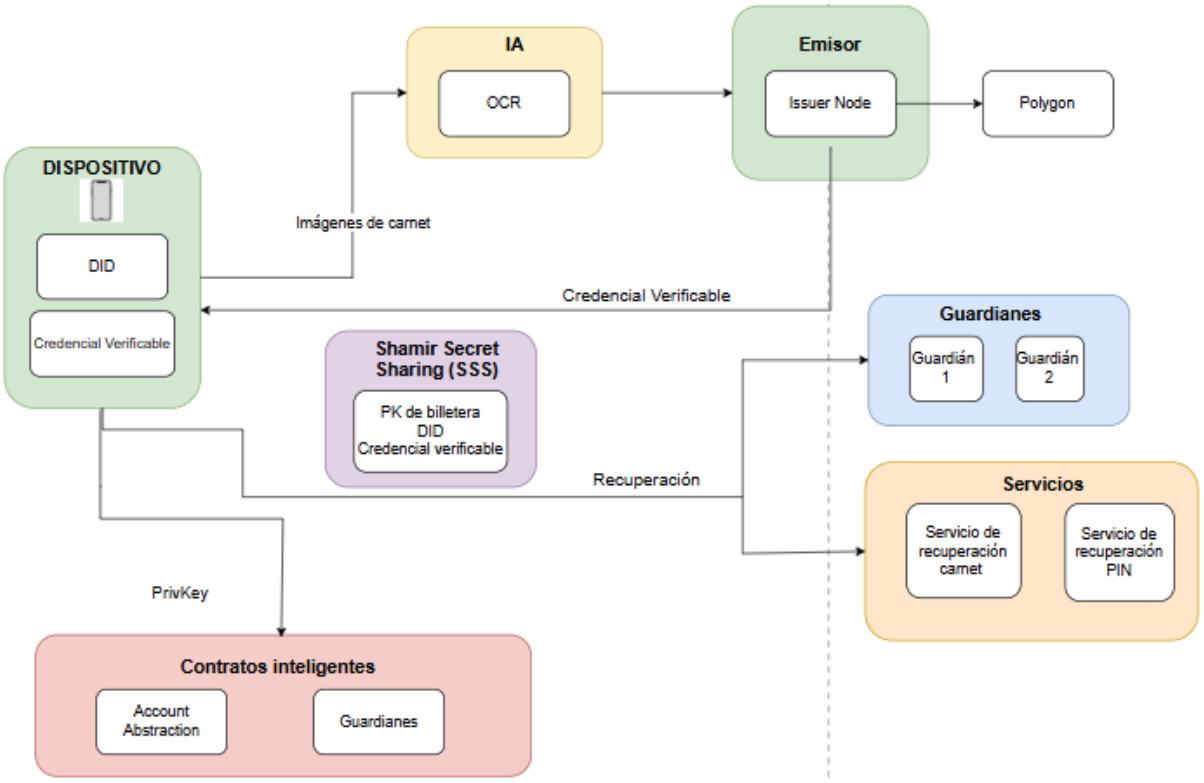

Figure 1: System Components and Interactions of the SDI System

4.2 Off-Chain Presentation and Verification.

When a third party requests to verify something—for example, "this person is accredited as a witness" or "this certificate of origin is valid"—WIRA Wallet transparently shows what is being asked, for what purpose, and for how long. If the user accepts, the app builds a Verifiable Presentation (VP) with minimal disclosure, including nonce (unique identifier), aud (recipient), and expiration. The verifier validates the signature of the referred VC's issuer and consults the public StatusList indicated by the statusPointer. Thus, it obtains the necessary guarantee without seeing personal data or the complete VC.

4.3 On-Chain Verification and Execution.

For attestation and traceability operations, the app builds a UserOperation (ERC-4337) and signs it locally with the user's private key. The UserOperation is sent to the EntryPoint, and the Smart Account (which was already deployed during registration) executes the call to the contracts, such as registering or updating evidence, issuing or supporting an attestation. On-chain events provide a verifiable record of who acted and when.

When there is gas sponsorship, the app directly requests authorization from the 4337-compatible Paymaster, and if the Paymaster's policy allows it, it covers the fee. In all cases, no PII is sent to the chain: only references (such as IPFS CIDs).

4.4 Encrypted Backup and Recovery.

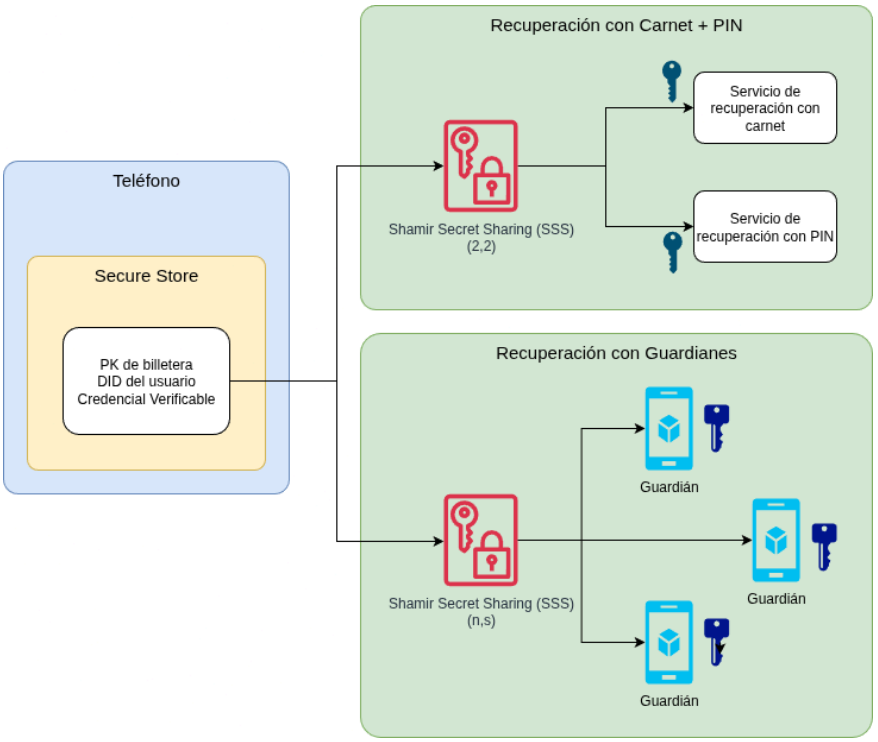

Figure 2: Account Recovery

The user's data (DID key, Smart Account private key (privkey), and VCs) reside in the phone's encrypted bundle. If the user enables recovery, Shamir Secret Sharing (SSS) is applied to the bundle's decryption secret:

Carnet+PIN Scheme (2-out-of-2): Two shares are generated; one is associated with the ID card verification service (the user resends photos of ID card/face when recovering) and the other with the PIN recovery service. With both shares, the secret is recomposed, and the bundle is decrypted.

In the Guardians scheme, the user registers s guardians (trusted persons or devices) and defines a threshold n. The bundle's decryption secret is fragmented with Shamir Secret Sharing (SSS) into s parts (shares), and each guardian receives their share. No one can recover alone.

To recover, the user gathers at least n shares. The app recomposes the secret, decrypts the encrypted bundle, and restores DID/VC/private key (privkey) on the new device, resealing it upon completion. If the threshold is not reached, recovery is not possible.

5. Privacy and Security

The design assumes adversaries with physical access to a lost or stolen device, communication interception, impersonation attempts, and correlation analysis between requests. Defense is layered: keys are born and custodied on the device, credentials are stored in an encrypted bundle that is temporarily decrypted in memory only when the user authenticates (PIN or biometrics) and is resealed after the operation; clear-text is never stored. Messaging between parties uses iden3comm with end-to-end encryption and mutual authentication. Presentations include recipient (aud), unique identifier (nonce), and expiration, which blocks reuse and reduces correlation. A credential's status is consulted through a compact public list (StatusList), without needing to expose the VC's content. Access recovery is based on independent factors (SSS/guardians) so that no party alone can reconstruct the secret.

5.1. Protected Personally Identifiable Data.

The solution avoids exposing PII to open records or third parties. VCs are kept only on the holder's device, within the encrypted bundle; VPs reveal only what is necessary for the requested purpose (minimal disclosure) and never include the complete VC.

5.2 Non-Correlation and Non-Reuse.

Each VP incorporates nonce, aud, and expiration. This prevents replay (reuse of a presentation outside its context or time window) and makes it difficult for different verifiers to correlate to the same holder.

5.3 Status and Revocation Without Exposing Content.

The issuer maintains a public StatusList (compact and signed list) where each position represents a credential's status: active, suspended, or revoked.

Each VC carries within it a statusPointer that indicates where to consult that list (e.g., a URL or a CID on IPFS) and which index corresponds to the credential. In verification, the third party only consults that status; it does not need access to the complete VC or personal data.

5.4 Multi-Factor Recovery.

If the user enables recovery, Shamir Secret Sharing (SSS) is applied to the bundle's decryption secret:

Carnet + PIN (2-out-of-2): Two "shares" are generated. One is associated with the service that validates ID card/face (the user resends photos when recovering), and the other with the PIN service. Both shares are needed to reconstruct the secret and decrypt the bundle on a new device.

Guardians (n-out-of-s): The user registers s guardians (trusted persons or devices) and defines a threshold n. s shares are generated; each guardian receives theirs (encrypted). With at least n shares, the app recomposes the secret locally and restores DID/VC/private key (privkey). No guardian can recover alone.

6. Regulatory Alignment in Bolivia

- Digital signature and probative validity: Use of digital signature and legal validity of electronic documents according to Law 164 and its regulations; compatibility with the certification infrastructure (Root CA/ATT, public/private ECPs).
- Official identification: Role of SEGIP as authority for CI and RUI; coexistence of derived credentials (SDI) that do not replace the CI but can prove attributes signed by authorized issuers.
- Interoperability: Integration with the State Interoperability Platform for institutional queries/validations, regulatory traceability.
- Data protection: Adherence to principles of lawfulness, purpose, minimization, security, and ARCO rights, preparation for future Personal Data Protection Law, consent and revocation mechanisms.
- Issuers retain only: schema identifier, issuer DID, issuance timestamp, status pointer, and a hash of credentialId. They do not store personal attributes.

7. Priority Use Cases

7.1 Commerce and Traceability.

Certificates of origin and quality as VCs issued by authorized bodies. Evidence (photos, analyses, guides) are published on IPFS, and their CID is noted on-chain through attestation

contracts. A buyer or regulator verifies: who/when certified (on-chain event), that the read file is identical to the attested one (same CID), and that the certifier's credentials are still valid (StatusList). Result: end-to-end traceability without PII.

7.2 Civic Participation.

Roles such as polling station witness, delegate, or observer are accredited with role VCs. Minutes and evidence such as images are uploaded to IPFS; their CIDs are attested on-chain to establish authorship and temporality without publishing personal data.

The public audits the integrity and sequence of evidence (same CID, order of on-chain events). The authority, with legal basis, can request the holder to provide a presentation proving that the evidence belongs to that role/process, without revealing more PII than strictly necessary. This reinforces civic trust, reduces disputes about authenticity, and provides traceability for each step of the process.

8. Design Principles

8.1 Holder Sovereignty

Keys and DID are generated and custodied on the device. Credentials reside in an encrypted bundle that is decrypted only when the user acts (PIN/biometrics) and is resealed upon completion. Consent is granular, explicit, and revocable, and the user can review a local history of presentations.

8.2 Minimal Disclosure

Each verification reveals only what is strictly necessary (e.g., ">18 years" instead of the birth date). VPs integrate nonce, aud, and expiration to prevent reuse and correlation. When applicable, zero-knowledge proofs (ZKP) are used to demonstrate conditions without exposing values.

8.3 Zero-Knowledge Proofs (ZKP)

The wallet can generate ZKP (range or membership proofs) on compatible schemas (BBS+/SD-JWT, among others), allowing a third party to verify that a condition is true without learning the clear data. This reduces the attack surface and PII leakage.

8.4 Interoperability

W3C DID/VC standards and StatusList (signed public lists) for status are adopted. Compatibility with BBS+, JSON-LD, and compact status structures is maintained.

8.5 Blockchain-Based

The chain is used where it adds verifiable value: holder's Smart Accounts (ERC-4337) and attestation contracts that anchor evidence CIDs and emit events. PII is never written on the chain. VC verifications (signatures, status in StatusList) and ZKP occur off-chain.

8.6 Security by Design

Zero-trust model between components. Iden3comm for end-to-end encryption, non-custody of keys, explicit validation of recipient and time windows, and revocation/key rotation policies for issuers/verifiers published in the Trust Registry.

8.7 Multi-Layer Security.

Encrypted bundle (AES-256-GCM) with random 256-bit DEK.

KEK derived from PIN + device's secure storage (Argon2id-type derivation) to protect the DEK.

Recovery without custodians with Shamir Secret Sharing (SSS): Carnet+PIN (2-out-of-2), or Guardians (n-out-of-s) registered by the user.

Rotation and revocation of issuer/verifier keys and publication of their signed StatusList.

9. Conceptual Framework

9.1 Issuer.

Accredited entity (public or private) that validates evidence and issues signed Verifiable Credentials (VCs) with its issuer DID. It publishes its StatusList (public list of credential status) and its manifesto in the Trust Registry, so any verifier can validate signature and validity without accessing PII. Currently operated with our own Issuer based on Polygon ID.

9.2 Holder.

Person or organization that controls a DID and custodies their VCs locally in WIRA Wallet within an encrypted bundle. The holder decides what to share, with whom, and for how long. When a service requests verification, the wallet generates a Verifiable Presentation (VP) with minimal disclosure.

9.3 Verifier.

Service or entity that requests attributes or proofs ("over 18", "valid witness role"). It verifies: the VC's signature (origin), the status in the issuer's StatusList referred to by the VC's statusPointer (active/suspended/revoked), and the integrity and anti-replay parameters of the VP (nonce, recipient, expiration). With this, it decides whether to grant the service/benefit without seeing PII.

9.4 Verifiable Credentials.

Signed claims about the holder's attributes, encoded in JSON-LD or SD-JWT. Each VC includes:

- Proof of origin and integrity (issuer's signature).
- Validity metadata (dates/conditions).
- CredentialStatus / statusPointer: pointer to the issuer's public StatusList, where it is checked if the credential is active, suspended, or revoked.

VCs are not stored on servers: they are kept only on the holder's device, encrypted in the bundle.

9.5 Decentralized Identifier (DID)

Cryptographic identifier whose DID documents publish the active verification keys and service endpoints. The associated private key never leaves the device: it is used to sign only when the user authenticates and the operation requires it.

9.6 Verifiable Presentations (VP)

Packages built by the wallet with subsets of one or more VCs and, when applicable, zero-knowledge proofs (ZKP) to demonstrate conditions without exposing clear values. Each

VP incorporates nonce (unique identifier per request), aud (explicit recipient), and exp (expiration), which prevents reuse and correlation.

9.7 Account Abstraction.

The holder's identity can operate on-chain through a Smart Account (ERC-4337). The app signs UserOperations locally and sends them to the EntryPoint. A Paymaster (optional) can sponsor gas under policies. The on-chain layer is used for attestation/traceability (events, CIDs) and does not record PII.

9.8 Status Management

The issuer publishes a signed public list that marks, for each VC, whether it is active, suspended (reversible), or revoked (definitive). Compact compatible formats are used for efficiency and privacy:

- Indexed bitstring (each index represents a VC).
- Merkle map (key = hash(credentialId), value = status) with signed Merkle root.

The statusPointer included in the VC indicates where to consult that list (URL/CID/DID-URL). The verifier only learns the status, not the VC's content.

9.9 Backup and Recovery.

VCs and keys reside in an encrypted bundle on the device. Optionally, the holder enables recovery using Shamir Secret Sharing (SSS) on the bundle's decryption secret:

- Carnet+PIN (2-out-of-2): The user recovers by providing photos of ID card and face (for share 1) and their PIN (share 2).
- Guardians (n-out-of-s): The user registers s guardians and defines a threshold n. Each guardian receives a share; to recover, ≥ n shares are gathered.

The DID is not regenerated: the original bundle is restored. If the user does not reach the threshold, recovery is not possible.

9.10 Trust Registry

The Trust Registry is a public directory without PII that is initially operated and where each Issuer/Verifier publishes its DID, the fingerprint of its public key, and the CID of its signed

JSON manifesto. An on-chain contract anchors this data and registers additions, rotations, and suspensions with multisig, leaving a public audit trail. With that manifesto, any verifier knows which keys to use, where to consult the issuer's StatusList (credential validity status), and which endpoints (iden3comm) to invoke. The flow is: extract the issuer's DID from the VC, then read the CID from the contract, retrieve and validate the manifesto with the DID's signature, verify the VC's signature, consult the StatusList indicated by the statusPointer. Thus, cryptographic guarantees are obtained without seeing personal data or the complete VC.

10. SDI Wallet Design

- Key Functions. WIRA Wallet generates the DID and keys locally, custodies VCs in an encrypted bundle, issues Verifiable Presentations (VP) with minimal disclosure, signs on-chain operations via Account Abstraction, and backs up/recovers via SSS (Carnet+PIN and/or Guardians). Includes local history (visible only to the user) with date, destination, and scope of each presentation.
- Security and Custody. The bundle is encrypted (AES-GCM) with a DEK protected by a key derived from the PIN and the device's secure storage. The bundle is unlocked only during an action, and the key is immediately erased from memory. Signing always occurs on the device. Recovery requires a threshold of shares; no actor can restore alone.
- Accessibility. Offline mode, static and dynamic QR codes for verification portals, multilingual support in Spanish and English.
- Compatibility. Android and iOS, SDK for third parties, Iden3comm for presentations where required.

Appendix A. SWOT (Bolivia)

Strengths

- There is a legal framework in Bolivia regarding digital signature, legal validity of electronic documents, and data protection.
- The system is designed to protect people's data and empower them over what to share.
- Local fintech ecosystem and active blockchain communities.

Opportunities

- It can be proposed to local governments or institutions, although we do not know the demand and which specific niches would demand it.
- Certification and traceability in agriculture/livestock/mining for export.
- Alignment with regional standards (MERCOSUR) in data protection.
- It is a mechanism to link crypto wallets to a person's identity, and for them to recover this wallet closely tied to their identity, without the need for complicated keys and proofs, using account abstraction.
- Institutional weakness in Bolivia may create demand for decentralized solutions if people ultimately understand the blockchain concept.
- Citizen distrust in data exchange between institutions, but if they understand the concept, it could be a way to win them over.

Weaknesses

- We are not sure who is interested in protecting their data; we do not know the scope and demand for a solution that protects users' data.
- Connectivity gap and digital literacy in different population strata; a tool that facilitates understanding is necessary.
- Citizen distrust in data exchange between institutions.

Threats

- Regulatory changes and political polarization that delay adoption.
- More sophisticated cyberattacks and identity fraud.

- Risk of excessive surveillance if the privacy principle is broken.
- Fragmentation of standards (many systems with identities) if each actor creates closed solutions.

Appendix B. Business Model Canvas

Market Segments

- The digital identity application or its system is a product to sell to:
- Local, regional governments
- Even institutions that want to include their own advanced features.
- The use of our digital identity as a differentiator or tool would have clients such as:
- NGOs or institutions that want to pay directly to beneficiaries, for example, through a traceability or certification system.

Main Value Proposition

- Crypto wallet related to a digital identity, with the ability for the user to sign smart contracts, develop reputation, and receive funds directly addressed to their identity.

Channel

- The channel to distribute the digital identity application is the Android and Apple stores.

Customer Relationship

- Communication from LinkedIn, to selected profiles.
- Traditional communication with quinoa unions, business leaders, and similar.
- Digital advertising, TikTok targeted at politicians, municipal candidates, etc.
- Communication, being B2B, should be personalized, with many virtual or in-person meetings with management or similar.

Revenue Sources.

- Revenue sources for the identity and oracles project are closely related; they would be:
- Sale or rental of government systems.
- Sale or rental of traceability systems.
- Tokenization platform and charging for membership to list cryptos, information control systems, compliance, etc.

- Sale or rental of customized systems linked to our digital identity.

Key Activities

- Identify market niches that have a latent need for digital identity and its benefits, and are willing to pay for it or implement it even if it is not an official tool.
- Implement the system in pilot mode in these institutions, until full customer satisfaction is achieved, so that it can be reused or something similar done in other use cases.
- Advertise the service.

Key Resources

- Patent on the intellectual property of our system, however adapted to software licenses.
- A coherent and secure system with blockchain signature, digital identity, and ZK proofs.
- Funding and team to maximize the possibility of finding market niches and working with them, with little funding until a minimum system is achieved that creates enough value to later advertise it.

Key Partners

- Business leaders willing to implement innovative systems with the investment, challenges, and problems that implies, but with the vision of achieving real differentiating features for their companies.
- Early adopters of systems, investors, or clients of traceability products, who know the technology and value products supported by it.
- Politicians who want to implement the technology as a political tool and who are then willing to provide the necessary funding and follow-up.
- Sales partners, who help create business strategies, close sales with projects and institutions.

Cost Structure

- Cost of servers, maintenance, and improvement of systems.
- Legal costs, adapting municipal laws, lobbying to achieve these things.

- Costs of time and money to implement the systems and adapt them for easier user adoption.
- Costs of partners who help close these deals.

Appendix C. References and Compliance (Practical Summary)

- Digital Signature and Probative Validity: Law 164 and its regulations; recognition of ATT as Root Certification Authority; coexistence with private and public ECPs.
- Official Identification: Law 145 (SEGIP/SEGELIC); RUI Regulations; practices for derived credentials without replacing CI.
- Interoperability: Supreme Decree 3525 and guidelines for publishing/consuming services; traceability mechanisms.
- Data Protection: Draft bills/PL under discussion; recommendations for immediate adequacy (consent, minimization, PIAs).
- Standards: W3C DID/VC, StatusList 2021, SD-JWT-VC,.

Appendix D. Glossary

- VC (Verifiable Credential): claim signed by an issuer that can be cryptographically verified.
- DID (Decentralized Identifier): verifiable and resolvable cryptographic identifier without a single central authority.
- VP (Verifiable Presentation): set of credentials/proofs presented by the holder to a verifier.
- BBS+ / CL / SD-JWT: cryptographic schemes for selective disclosure and/or ZKP applicable to VC.
- BJJ: curve used in certain ZK proofs (e.g., ranges/membership).
- Smart Account (ERC-4337): contract account that signs UserOperations via EntryPoint; can use Paymasters to cover gas according to policies.
- CID (Content Identifier): immutable identifier of content on IPFS; ensures that what is retrieved is exactly what was published.
- Trust Registry: catalog of accredited issuers and verifiers, with public metadata on policies and DIDs.
- DEK: Data Encryption Key, random key used to encrypt the bundle on the device with AES-256-GCM.
- Keystore/Keychain: secure storage of the OS (Android/iOS) that protects keys and cryptographic material; used to derive/store the KEK that wraps the DEK with which the app's storage is encrypted.
- KEK: Key Encryption Key, key derived from PIN + secure hardware (Keystore/Secure Enclave) with Argon2id to wrap the DEK.
- Status List: compact structure signed by the Issuer that indicates the validity of VCs without revealing their content.
- iden3comm: messaging protocol of the iden3/Polygon ID ecosystem for credential issuance and verification flows. End-to-end encryption and authentication between issuer, holder, and verifier.
- statusPointer: pointer within a VC that indicates where the issuer's public StatusList is (URL/CID/DID-URL) and which index to consult to know if the credential is active, suspended, or revoked.
- privkey: holder's private key used to sign UserOperations (ERC-4337) from the wallet; generated and remains on the device, within the encrypted bundle.

- ERC-4337, EntryPoint, UserOperation, Paymaster: Account Abstraction components for signing and paying gas without EOA.
- Guardians: actors or factors that, under a threshold policy, help recover the DEK (they do not access VCs).
- Status Management. Each VC includes a status pointer to a public list signed by the issuer.
- Bitstring: array of bits where the index assigned to the VC indicates its status (0 active, 1 not active). Revoking is changing the bit and republishing the signed list or its CID on IPFS/Ceramic.
- Merkle map: key-value map hash(credentialId) → status with signed Merkle root; verification uses membership proofs without downloading the entire list.
- ZKP (Zero-Knowledge Proof): proof that certifies a condition (e.g., "over 18") without revealing the underlying data.