The State-Endorsed Digital Identity Linkage Program

A Legislative Proposal to Combat Fraud While Protecting Privacy in Wyoming LLCs, Property Records, and Identity Verification

Prepared by David Roland
Senior Engineering Consultant
Advanced Intelligent Networks, llc
Jul 9, 2026

Abstract:

Wyoming faces persistent challenges with fraud in business filings, LLC abuse, deed and title fraud, and identity theft. The state currently lacks adequate safeguards and a clear default policy for protecting the private data it collects from residents and businesses.

While Wyoming's permissive LLC statutes have fostered a business-friendly environment, they also make it difficult to distinguish legitimate entities from anonymous shell companies. These structures are frequently exploited for money laundering, fraudulent schemes, and evading federal restrictions on foreign land ownership.

Although the Legislature has enacted useful legislation—including the Digital Identity Act (W.S. Title 40, Chapter 30) and W.S. § 8-1-102—has introduced useful definitions of Principal Authority, these provisions remain focused on commercial code protections and fall short of delivering robust personal privacy safeguards.

This legislative policy paper analyzes the current vulnerabilities and proposes targeted infrastructure reforms and draft legislation.

The recommended framework would explicitly enumerate privacy rights for individuals and businesses, create a new class of low-risk LLC designed to reduce financial institutional exposure to fraud and abuse, establish a state-endorsed Self-Sovereign Identity (SSID) system controlled by the registered Principal Authority, and incorporate algorithmic governance along with privacy-preserving technologies such as selective disclosure.

Building on Wyoming's existing leadership in digital innovation, these measures would integrate current advancements into a cohesive statutory and technical infrastructure. The result would be a modernized public data system that simultaneously strengthens digital rights, enhances transparency, deters fraud, and preserves the state's competitive advantage as a forward-looking jurisdiction for responsible business formation.

Table of Contents

Introduction....3

Scope....3

Background....3

Who Owns Your Personal Data?....3

Anonymous LLC Fraud....4

Using FinCEN Anti-Money Laundering, Know Your Customer Policy....5

FinCEN's impact on Legitimate LLCs....6

Dealing With Fraud Due To Wyoming's Missing Non-Repudiated IDs....6

Property Deeds and Title Fraud....7

Birth Records....7

Residency and Citizenship Claims....7

BOI (Beneficial Ownership Information) Filings....8

Overall Impact on Identity Theft....8

Philosophical Foundations for Legislative Reform....8

Additions to Wyoming Public Digital Infrastructure....9

Core SSID Privacy Strengths in the Proposal....9

Key Positive Applications:....10

Real Application – Formation of a Wyoming Anonymous Closed LLC....10

Summary....11

Appendix A – DRAFT....12

STATE-ENDOSED DIGITAL IDENTITY LINKAGE PROGRAM....12

Section 1....12

Section 2....13

Appendix-B....21

About the Author....21

Introduction

The intent of this document is to propose and demonstrate systems solutions to improving privacy, reducing fraud, and adopting non-repudiable assertions between entities and the Wyoming State Government.

Scope

The author has a personal interest in resolving these proposals, does not practice law, and is not being paid to submit these proposals.

This document, its assertions, conclusions and proposed methods are considered not proprietary, and are offered in the public domain, without restrictions.

This document uses commonly held assertions regarding the security of big-number cryptography implementing: one-way-hash, immutable ledgers, dual key encryption, executable Zero-knowledge Proofs, and other secure math concepts.

Background

Wyoming has a "digital identity crisis" in the widespread inability to establish and enforce strong, verifiable, and non-repudiable identities online or in key systems. It has created environments where fraud (impersonation, synthetic identities, account takeovers, etc.) becomes easy and scalable.

Without cryptographic proofs, strong biometrics tied to trusted sources, digital signatures, or hardware-backed credentials, parties can't plausibly assert “I am the owner”. Systems rely on weak, shareable, or forgeable credentials (passwords, SSNs, easily copied docs) instead of binding actions to undeniable proof. Even bank cards require a pin to counter fraud – drivers licenses don't.

The result is that state election agents, county clerks receiving deed documents, law enforcement, financial institutions, or Registered Agents, have to rely on repudiable identification, and in that moment, they do not have the ability to verify other than state issued physical documentation.

Who Owns Your Personal Data?

Although Wyoming enacted SF-0020 (“Data privacy — government entities”) during the 2026 Budget Session, which establishes baseline data privacy and minimization requirements for how state and local government entities handle residents’ personal data, the law does not recognize individuals as the owners of their personal data.

SF-0020 limits unnecessary collection, sharing, and long-term retention of personal information by government entities (with certain exceptions) and grants residents limited rights, such as access to their data and the ability to object to its accuracy or retention. **However, neither this law nor any other enacted Wyoming statute treats personal data as the individual’s personal property or explicitly establishes individual ownership over it.** Instead, it focuses on imposing responsible handling obligations on government entities.

In Whalen v. Roe (Feb. 22, 1977), SCOTUS acknowledged that the Constitution protects an “individual interest in avoiding disclosure of personal matters” and clearly recognized informational privacy as a constitutional interest (a “zone of privacy” under the Due Process Clause).

The Fifth amendment provides a clear right to refuse disclosure of personal information which should be applied against wholesale data collection. The Fourth amendment, guards against government access to personal information without probable cause. The First amendment supports refusing disclosure in contexts where revealing identities and or affiliations would chill protected expression or associations.

The US has its share of innovative regulations in the California Privacy Rights Act (CPRA), and Utah's recent SB-275 which creates a State-Endorsed Digital Identity Program (SEDI) and establishes Digital Identity Bill of Rights. Both state measures emphasize individual control, privacy, and explicit protections against compelled use or government surveillance. These acts focus on the privacy of the Principal's data, rather than Uniform Commercial Code data protection against exploiting online or digital data.

Although Wyoming established foundational legal definitions supporting privacy rights as early as 2021, the state has until now lacked the practical frameworks and incentives needed to implement them effectively. Public resistance to conventional state-issued digital identification—driven by legitimate concerns over surveillance, social scoring, and potential misuse—has underscored the need for a more privacy-respecting alternative. There is a clear and growing requirement for state-verified credentials that enable both natural persons and legal entities to securely assert verified data for governmental and non-governmental purposes, while maintaining strong privacy protections and individual or organizational control.

Anonymous LLC Fraud

Wyoming pioneered the limited liability company structure in 1977 and has long been recognized as one of the most business-friendly jurisdictions in the United States. However, Wyoming LLCs have also faced reputational challenges, including prominent mentions in the Panama Papers, due to their use in some cases for illicit purposes.

Recent legislative proposals, such as Senate File 0082, would have required registered agents to collect and retain plaintext Beneficial Ownership Information (BOI). These measures raise serious concerns. The federal government itself has acknowledged significant Fourth Amendment issues by suspending enforcement of the Corporate Transparency Act’s BOI reporting requirements for U.S. beneficial owners. Requiring registered agents to maintain sensitive ownership data would undermine the privacy protections that have long been a hallmark of Wyoming law, expose agents to substantial liability in the event of a data breach, and leave the state largely shielded from resulting damages.

Although Wyoming's Consumer Protection Act, Article 5 – Computer Security Breach (Wyoming Statutes §§ 40-12-501 to 40-12-502) is the state's primary data breach notification law. It focuses on requiring timely notice to affected residents when personal identifying information is compromised, but it provides no mechanism for exposure remidiation.

Senate File-0082 would likely fail to reduce fraud. It relies on self submitted and unsubstantiated data that could be challenged, may be inaccurate, or incomplete. Secretary Gray has also suggested it would

likely cause a potential 40% decline in Wyoming LLC registrations driven purely by privacy concerns.

Using FinCEN Anti-Money Laundering, Know Your Customer Policy

In the intricate landscape of financial security and regulatory compliance, Know Your Customer (KYC) and reporting LLC Beneficial Owner Information (BOI as suggested in SF-0082) serves as the epicenter of preventing fraud, embodying a best-practice standard that is indispensable to comprehensive due diligence. KYC is fundamentally an acknowledgment and formal commitment to uniquely identify the **Principal Authority**, the ultimate individual or entity who owns, controls, or benefits from a relationship or transaction.

At its best, KYC is a process that an institution has exerted reasonable effort to pierce through layers of intermediaries, corporate veils, trusts, or nominees to establish a clear, auditable link to the real person(s) in control. This unique identification of the principal serves as the bedrock of effective due diligence, enabling accurate risk scoring, ongoing monitoring, and accountability. Without it, fraud prevention collapses.

The trust basis in KYC verification is fundamentally about establishing a “reasonable belief” that the customer is who they claim to be. It relies on a **chain of trust** anchored in authoritative sources, legal frameworks, and multi-layered validation methods rather than absolute certainty. The primary foundation is **trust anchors,** entities or data sources whose authenticity is assumed and not derived further (e.g., government-issued IDs). The Customer Identification Program (**CIP: 31 CFR 1020.220 and related rules**) under the USA PATRIOT Act requires financial institutions to form this “reasonable belief” of true identity using these sources.

Government-issued identity documents (passport, driver's license, REAL-ID, etc.) currently serve as the strongest anchors. These are backed by state infrastructure that includes photo, biographic data, and security features. Verification involves checking document authenticity against issuer standards.

But the discontinuity in using current FinCEN policy is in depending on an authority that can and has been repudiated, especially when a human is expected to make an authenticity evaluation.

The U.S. identity system has a critical chain-of-trust problem: it treats birth certificates as the ultimate authoritative document while overlooking how easily they can be forged, even when they carry official embossed seals.

The U.S. Constitution grants state government the authority to define citizenship and residency. Congress reinforced this through the Civil Rights Act of 1866, which declared that all persons born or naturalized in the United States are citizens of the United States and of the state in which they reside. As a result, each state has a fundamental responsibility to maintain accurate records of its citizens, primarily through official birth records. Since state legislatures determine the rules for elections (including voter eligibility) every State Secretary of State’s office should maintain secure, up-to-date digital identification systems for its citizens to ensure election integrity and verifiable voter rolls.

Wyoming’s Digital Identity Act and RON rules support electronic attribution through security procedures (biometrics, cryptographic keys). This allows digital methods to carry equivalent legal weight, with trust rooted in the same government anchors plus technology safeguards (tamper-evident systems, and identity proofing).

FinCEN's impact on Legitimate LLCs

We live in an increasingly litigious society where differing opinions are often met with attempts at cancellation rather than debate. Lawfare, the weaponization of legal processes to bankrupt or silence opponents, has become normalized, driven by a troubling lack of ethics and an appetite for unchecked power.

Political candidates with deep pockets routinely file defamation suits against opponents while themselves distorting records and misleading the public. They won't hesitate to financially attack and litigate those that pushback.

As much as FinCEN wants as much exposure on the beneficiaries of LLCs, avoiding public disclosure is the reason for Wyoming's LLC laws, especially regarding anonymity, and revealing as little as possible to prevent malicious attacks.

Consider a simple example: An entrepreneur wishes to exercise their First Amendment rights by publishing a digitally distributed newsletter that critiques disinformation in political campaigns and provides factual counterpoints. They form an anonymous Wyoming Close LLC to operate the newsletter. The entity has no physical brick-and-mortar address — all operations and distribution occur through a Wyoming data center. As a legitimate business with an EIN, it seeks to monetize through subscriptions and sponsorships.

Yet here lies the contradiction: There is little practical advantage to choosing Wyoming jurisdiction if the LLC cannot obtain a bank account — largely because it lacks a physical address and because banks fear regulatory risk, even absent any criminal conduct. This blocks access to merchant services, payment processors, and legitimate cash flow, ultimately undermining both free speech and transparent financial oversight.

This is the result of regulatory overreach. FinCEN’s aggressive policies pressure banks to impose punitive restrictions, (Cheyenne State Bank, Cheyenne, WY) even in the absence of criminal activity, effectively creating choke points that undermine legitimate business. These actions appear designed, in part, to circumvent Wyoming’s strong anonymous LLC laws, which federal agencies struggle to pierce.

By limiting access to basic financial services, FinCEN’s approach harms a wide range of modern digital businesses. It casts suspicion on all anonymous LLCs, portraying them as inherently fraudulent or designed for money laundering, rather than recognizing their legitimate uses for privacy, asset protection, and free expression.

Wyoming does not have the authority to overturn these FinCEN policies, but it does have a tool, with the Division of Banking's help, to use those policies to reduce LLC fraud by following their Extended Due Diligence guidelines.

Dealing With Fraud Due To Wyoming's Missing Non-Repudiated IDs

One of the most damaging ways the absence of strong non-repudiable digital identification enables fraud is through the falsification of official state records. Without a system that cryptographically ties actions and documents directly to an individual who cannot later deny involvement, bad actors can forge, alter, or submit false records with relatively low risk of detection or accountability.

Property Deeds and Title Fraud

Deed fraud (also called home title theft or quitclaim deed fraud) has become increasingly common across the U.S. Scammers comb through public records to find properties — especially those owned by elderly people, vacant land, or homes without mortgages. They then forge the owner's signature on a quitclaim or warranty deed, often using fake notary stamps, and record it with the county recorder's office. Once recorded, the fraudulent deed transfers legal title on paper.

The criminal can then sell the property, take out a mortgage against it, or rent it out. The real owner often doesn't discover the theft until they try to sell the home, refinance, or receive a tax bill in someone else's name. Because current systems rely heavily on paper documents, scanned signatures, and in-person notarization that can be tricked with fake IDs, there is often no ironclad way to prove who actually authorized the transfer. Non-repudiable digital signatures linked to verified identities would make such forgeries far more difficult and easier to challenge.

Birth Records

Falsifying or obtaining fraudulent birth certificates is a gateway crime for broader identity theft. Criminals can use stolen or counterfeit birth certificates to:

- Obtain other government-issued IDs (driver's licenses, passports)
- Open bank accounts or credit lines
- Apply for government benefits
- Create entirely synthetic identities

In some cases, insiders have been caught producing fake birth certificates. In others, thieves use real stolen certificates or high-quality forgeries created with templates and even AI tools. Once a fake birth record exists in the system, it becomes the foundation for a long chain of fraudulent activity. Because birth records are foundational documents, falsifying them undermines almost every other form of identification downstream.

Residency and Citizenship Claims

Bad actors frequently falsify proof of residency or citizenship to access benefits, vote, obtain driver's licenses, or qualify for loans and government programs. This can involve:

- Using fake utility bills or lease documents
- Claiming residency at an address they don't actually live at (sometimes called "residence hopping")
- Falsely claiming U.S. citizenship on forms (such as employment eligibility forms or benefit applications)

False claims of citizenship carry serious legal consequences, but they are often discovered only after

the fact — if at all. Without non-repudiable digital credentials that link a person's verified attributes (citizenship status, actual residency) directly to them in a tamper-evident way, it remains relatively easy to submit false attestations.

BOI (Beneficial Ownership Information) Filings

Under the Corporate Transparency Act, many companies must file Beneficial Ownership Information with FinCEN, disclosing who ultimately owns or controls the business. While this was intended to increase transparency, the current filing system still relies on self-reported information that can be falsified. Bad actors can submit fraudulent BOI reports using stolen or fabricated personal details of beneficial owners. This allows them to hide true ownership of shell companies used for money laundering, fraud, or other crimes. Non-repudiable digital identities tied to verified individuals would make it much harder to file false ownership information.

Overall Impact on Identity Theft

When bad actors can successfully falsify or manipulate these state records without strong non-repudiation, they create a cascading effect. A single forged deed or fake birth certificate can enable years of fraudulent activity across banking, government benefits, voting, real estate, and business formation. The victim may spend months or years trying to prove they didn't authorize something — precisely because current systems often lack the technical proof that only a non-repudiable digital identity can provide.

This is why advocates in Wyoming and elsewhere argue that stronger, privacy-preserving non-repudiable digital identification systems (using cryptographic keys, verifiable credentials, or self-sovereign identity models) are needed. Such systems would allow individuals to prove control over their identity and records in a way that is very difficult to fake or deny, while still protecting personal privacy through techniques like zero-knowledge proofs.

Philosophical Foundations for Legislative Reform

Principal Authority: (W.S. § 8-1-102(a)(xviii) and (xix)), established by the 2021 Digital Identity Act (SF0039), grants natural persons and legal entities primary control over their personal or organizational digital identity. This authority includes ownership rights over associated data, along with the ability to control, disclose, and authorize its permitted uses.

State Endorsed Credentials: The State (or Notary Publics acting as state agents) may verify and cryptographically sign official credentials, providing strong authentication and verification.

State Principal Registry: New digital structures, keyed by a hashed Tax ID (or equivalent identifier), enable linkage to a W3C Decentralized Identifier (DID). This connects to a Self-Sovereign Identity (SSI) stored in an external digital data store (such as a wallet), which holds verifiable personal or organizational credentials. These credentials can be actively presented or passively queried as authorized.

State Data Dictionary: A publicly accessible, immutable ledger serves as a foundational resource, providing key components, definitions, and mechanisms to access and process digital credentials. It

includes a standardized public data dictionary that defines semantic meanings for data elements, promoting broad interoperability through widely adopted vocabularies such as schema.org and FOAF (Friend of a Friend). This dictionary encompasses structured business information definitions, including LLC operating agreements, membership lists, ownership percentages, and other records essential for regulatory compliance — such as FinCEN extended due diligence and financial institutions' cash-flow monitoring.The dictionary may also incorporate State-approved executable code to enable secure functions such as selective disclosure and the generation of derived data.

Hashed Principal Tax ID: functions as a non-repudiable identifier for state purposes, supporting activities such as land ownership records, tax accounts, voting, proof of residence or citizenship, birth records, and other official functions. It can also serve as a modern alternative to a driver's license and its derivatives (e.g., proof of age), all exercised under the Principal's Authority and subject to their usage permissions.

Additions to Wyoming Public Digital Infrastructure

In addition to the immutable public ledger hosting the Data Dictionary, the system includes two simple database tables. One table uses the hashed Tax ID (Principal identifier) as the key and returns a text field containing associated Hex values. The second table uses the hashed business registry number — assigned by the State upon business registration — as the key.

Other optional state registries, such as those for deed and residence recording as well as parental birth records, can link to or utilize the new hashed Tax ID Principal record for consistent identification and verification.

Core SSID Privacy Strengths in the Proposal

The proposal establishes a Principal Authority Registry that is explicitly described as a "secure, privacy-preserving database." Here are the key built-in protections:

- **Hashed identifiers only:** Records are keyed exclusively by a one-way cryptographic hash of the Taxpayer Identification Number (TIN), which explicitly includes SSNs, ITINs, and EINs. The state never stores the plain-text TIN.
- **Minimal data storage:** The registry holds only:
    - The hashed TIN
    - A reference to the principal's self-controlled Decentralized Identifier (DID) (to the DID-Doc which contains a public key, contact method, and WASM processor.)
    - It never stores actual credentials or personal/corporate details.
- **Full user control:** Individuals/entities retain complete ownership and control of their DID and Self-Sovereign Identity (digital wallet/repository) at all times. They can add, update, or remove their DID linkage at any time under their sole control.
- **State role is strictly limited:** The state only maintains the hashed linkage, performs verification, and provides endorsement status. It is prohibited from owning or controlling anyone's digital identity or credentials.

- **Selective disclosure & privacy-preserving verification:** Explicitly required in the duties of the Secretary of State and codified in the Digital Identity Bill of Rights.
- **Duty of loyalty:** Program operations must impose a duty of loyalty to the principal authority (not to the state or third parties).
- **No central credential repository:** Verifiable credentials stay in the principal's own wallet. The state only confirms the linkage exists.

Key Positive Applications:

1. **Dramatically reduced sensitive data exposure:**
   The state only sees the hashed EIN + DID linkage.

2. **Selective disclosure for compliance:**
   Membership and percentage influence is managed through state certified Zero-Knowledge Proof code segments without revealing unnecessary personal or ownership details. This directly supports privacy-preserving verification.

3. **Lower data breach and identity theft risk:**
   This proposal minimizes what the state holds, significantly reducing the attack surface.

4. **Ongoing record maintenance without repeated full disclosures:**
   Updates to LLC records, good standing, or ownership changes could be handled by updating credentials in the SSID wallet and obtaining fresh state/notary endorsement when needed — rather than re-submitting full documentation every time.

5. **Entity-level and individual-level flexibility:**
   LLCs maintain their own DID linked by its hashed EIN. Managers can cite member information via each Principal registry, and associated percentages. This approach keeps actual data under the principal's control.

6. **Trust without centralization:**
   Notary public endorsements (limited to identity proofing + cryptographic attestation) and Secretary of State linkage provide official state backing while the actual records remain decentralized in SSID wallets. Immutable audit logs still exist for accountability.

Real Application – Formation of a Wyoming Anonymous Closed LLC

Three main parties are involved: the Forming Party, the Registered Agent, and the State.

The Forming Party creates a Principal Authority record using their hashed Tax ID (serving as the required contact under Wyoming law). They generate a new key pair for the entity and enter a contract with the Registered Agent, sharing the new public key, their hashed Tax ID, and the proposed business name.

The Registered Agent files the formation documents, including the public key and business name. Upon approval, the State issues a business registry number, creates a registry slot, generates an access

key, encrypts it with the entity's public key, and stores it.

Anyone can view the business registry, but only the Forming Party (with the private key) can decrypt the access key — proving ownership and linking it to their hashed Tax ID record.

Simultaneously, the Forming Party creates a Private Data Store with member and operating details. Beneficial owners link their own hashed Tax ID Principal Authority accounts, providing name, ownership percentage, control type, attestation date, and DID signature.

After LLC approval, the Forming Party obtains an EIN to connect the hashed Tax ID registry to the LLC's DID. The State can verify the Tax ID via IRS letters (CP 575 or 147C) or the TIN Matching Program.

A bank account can then be opened using the EIN. With the Principal's permission, the financial institution accesses the Private Data Store for BOI information. For audits, limited query access can be granted without full permissions.

Financial services can validate distributions and flag suspicious transactions. Businesses without an EIN or Private Data Store, and members lacking Principal Authority links, are considered higher risk.

Summary

The intent of this proposal is to establish under the Secretary of State, a uniquely keyed and privacy oriented abstraction between a Principal Authority and their privately held personal data and State Endorsed credentials.

In matters of property ownership, birth records, business formation, ownership and membership structures (including anonymous LLCs), taxation, voting, and other unforeseen purposes, the Principal Authority can be uniquely referenced and identified without disclosing any tangible or sensitive personal information. At the same time, it provides a secure mechanism for the Principal Authority to be contacted, to respond to queries, to engage in selective disclosure, and to exercise the full range of functions available to both natural and juridical persons.

The positive aspects of this bill for SSID (Self-Sovereign Identity) privacy, focus on its deliberate privacy-by-design architecture. It creates a state-endorsed verification layer while keeping individuals and entities in full control of their data. Most importantly, access to credentials requires Principal Authority approval, making any institutional (state) endorsed contents of the SSID, non-repudiated.

Although Self-Sovereign Identities are often thought of as digital wallets, this is a limited view. A better description is a Private Data Store (PDS) — a secure personal vault for your information.

A typical digital wallet is usually an app on your phone that can be asked for credentials using standard query methods. In contrast, a Private Data Store can go further by allowing secure, machine-readable access to your data — including for automated systems like smart contracts — while still supporting the same credential queries. Both approaches are fully compatible with the proposed legislation and OpenID4VP standards.

Appendix A – DRAFT
STATE-ENDOSED DIGITAL IDENTITY LINKAGE ACT

SF XXX – STATE-ENDOSED DIGITAL IDENTITY LINKAGE ACT

AN ACT relating to digital identity; creating a state-endorsed digital identity linkage program within the office of the secretary of state; authorizing the linkage of decentralized identifiers to state-endorsed credentials; authorizing notaries public to perform limited endorsements; creating a registered principal registry keyed by hashed tax identifier; providing strong privacy protections and limitations on state authority; authorizing participation by legal entities; authorizing amendments to business formation processes; providing for satisfaction of physical address and beneficial ownership requirements through digital identity linkage; creating a new class of Anonymous Limited Liability Company; establishing a data dictionary ledger for cryptographic components and approved zero-knowledge proof modules; providing funding and fee authority; and providing for an effective date.

Be It Enacted by the Legislature of the State of Wyoming:

Section 1.

W.S. 8-1-102 is amended by adding new paragraphs to read:

- **(xx)** "Decentralized Identifier (DID)" means a globally unique persistent identifier that meets W3C standards and is controlled by the registered principal;
- **(xxi)** "Registered Principal" means a natural person or a legal entity that has been identity proofed and registered under this act, and has the meaning provided in W.S. 8-1-102(a)(xviii) when applicable to natural persons;
- **(xxii)** "Registered Principal Registry" means the secure, privacy-preserving database maintained by the secretary of state that creates a cryptographically verifiable linkage between a hashed taxpayer identification number and a registered principal's self-controlled Decentralized Identifier (DID);
- **(xxiii)** "State-endorsed credential" means a verifiable credential that has received official state endorsement through the linkage program established under this act;
- **(xxiv)** "Verifiable credential" means a tamper-evident digital assertion about a registered principal that complies with recognized open standards and is mathematically verifiable through cryptography, and that may be held under the sole control of the registered principal within the principal's Self-Sovereign Identity (SSID);
- **(xxv)** "Hashed Taxpayer Identification Number" means a cryptographic one-way hash of a taxpayer identification number (including a Social Security number, individual taxpayer identification number, or Employer Identification Number) verified as authentic and unique during identity proofing;
- **(xxvi)** "Business Entity Registered Number" means the unique identification number assigned by the secretary of state to a legal entity upon formation or registration;
- **(xxvii)** "Physical address requirement" means any provision of Wyoming law requiring a legal entity to provide or maintain a physical business address.
- **(xxviii)** "Anonymous Limited Liability Company" or "A-LLC" means a limited liability company formed under the Wyoming Limited Liability Company Act, W.S. 17-29-101 et seq., that elects to participate in the State-Endorsed Digital Identity Linkage Program and satisfies its

address, beneficial ownership, membership percentage, and control disclosure requirements exclusively through the mechanisms of this act, the Registered Principal Registry, and the Business Entity Linkage Registry, without public disclosure of any physical address other than the registered agent's address or of member identities or ownership percentages.

- **(xxix)** "Data Dictionary Ledger" means the immutable, cryptographically verifiable, append-only ledger established and maintained by the secretary of state under this act that contains the State's public encryption key, the semantic definitions for information elements, and all Approved WASM Modules used for zero-knowledge proofs.
- **(xxx)** "Approved WASM Module" means a WebAssembly binary that has been formally reviewed, security-audited, and officially approved by the secretary of state, then recorded on the Data Dictionary Ledger for use in generating or verifying zero-knowledge proofs from CBOR-encoded data.
- **(xxxi)** "Zero-Knowledge Proof" means a cryptographic protocol by which one party can prove to another party that a specific statement about data or credentials is true, without revealing any information beyond the validity of that statement. Zero-knowledge proofs may be used to enable selective disclosure of attributes within verifiable credentials and Self-Sovereign Identities.
- **(xxxii)** "CBOR" means the Concise Binary Object Representation data format as defined in IETF RFC 8949, used for compact, binary encoding of structured data within verifiable credentials and Self-Sovereign Identities.
- **(xxxiii)** "Verifier App" means a software application or service, authorized or operated as part of the State-Endorsed Digital Identity Linkage Program, that interacts with a registered principal's Self-Sovereign Identity (SSID) and responds to standardized OpenID queries to verify the authenticity, validity, and revocation status of signed credentials, including state-endorsed credentials.
- **(xxxiv)** "Self-Sovereign Identity (SSID)" may be implemented in various forms, including as a mobile digital wallet, a server-based or API-accessible Digital Data Store, or other technical architectures, provided that the registered principal retains sole control over the identity and any credentials contained therein.

Section 2.

A new section W.S. 9-1-XXX is created to read:

9-1-XXX. State-Endorsed Digital Identity Linkage Program.

(a) There is created within the office of the secretary of state the State-Endorsed Digital Identity Linkage Program.

(b) Duties of the Secretary of State. The secretary of state shall:

(i) Establish and maintain the Registered Principal Registry pursuant to the authority granted under W.S. 9-1-101 et seq.;

(ii) Establish objective, uniform standards for eligibility, identity proofing, endorsement, acceptance, revocation, and interoperability of state-endorsed credentials;

(iii) Provide official state endorsement by linking a verified registered principal's self-controlled DID (if provided) to one or more state-endorsed credentials in the registry;

(iv) Ensure all program operations protect privacy, support selective disclosure, impose a duty of loyalty to the registered principal, and do not grant the state ownership or control of any registered principal's digital identity or credentials;

(v) Ensure that the Registered Principal Registry provides only a verifiable linkage between a hashed taxpayer identification number and a registered principal's self-controlled DID;

(vi) Establish standards and procedures to allow legal entities to participate as registered principals, including the ability to link beneficial ownership information through verifiable credentials, consistent with W.S. 17-16-101 et seq. and W.S. 17-29-101 et seq.;

(vii) Promulgate rules necessary to implement this act, including rules governing business formation processes under Title 17 and the acceptance of public keys for optional enhanced linkage.

(c) Digital Identity Bill of Rights.

Every registered principal has the following rights with respect to digital identity:

(i) The right to own and control their personal or organizational digital identity;

(ii) The right to state endorsement of their credentials through linkage upon meeting objective standards established by law;

(iii) The right to selective disclosure of attributes and privacy-preserving verification, including through the use of zero-knowledge proofs;

(iv) The right to have state operations governed by clear legislative standards for endorsement, acceptance, and revocation;

(v) The right to have their registered principal status respected and protected by the state.

(d) Notary Public Endorsement Authority – Scope.

(i) The secretary of state may authorize commissioned Wyoming notaries public to perform notary endorsements of verifiable credentials under this program.

(ii) A notary endorsement is strictly limited to:

(A) Performing identity proofing of the registered principal, or when the registered principal is a legal entity, identity proofing of an authorized representative acting on behalf of the legal entity, using methods approved by the secretary of state;

(B) Cryptographically signing a verifiable credential presented by or on behalf of the registered principal to attest that the notary has verified the identity of the registered principal (or its authorized representative) and that the credential accurately reflects the attributes asserted;

(C) Recording the cryptographic linkage between the signed verifiable credential and the registered principal's self-controlled Decentralized Identifier (DID) in the Registered Principal Registry. The registered principal retains sole authority and control to incorporate the signed credential into their Self-Sovereign Identity (SSID).

(iii) Prohibited Acts. A notary public shall not:

(A) Create or originate the underlying content of a credential on behalf of the registered principal;

(B) Endorse any claim the notary has not personally verified;

(C) Retain copies of credentials beyond the minimum required for the notary journal and audit trail;

(D) Exercise any control over the registered principal's DID or digital wallet or Digital Data Store.

(iv) Every notary endorsement shall use a program-specific digital signing certificate, be traceable through an immutable audit log, and comply with the Wyoming Revised Uniform Law on Notarial Acts, W.S. 32-3-101 et seq.

(v) The secretary of state shall establish training requirements, maintain a public directory of authorized program notaries, and may suspend or revoke a notary's program authorization for cause.

(e) Registered Principal Registry.

(i) The secretary of state shall establish and maintain a privacy-preserving Registered Principal Registry whose sole purpose is to create a cryptographically verifiable linkage between a hashed taxpayer identification number and a registered principal's self-controlled DID.

(ii) Scope and Limitations. The Registered Principal Registry:

(A) Enables cryptographic verification that a specific DID is linked to a real, identity-proofed registered principal via their hashed taxpayer identification number;

(B) Does not store any actual credentials. The registry endorses only those specific credentials that have been expressly linked through this program. It does not endorse the registered principal's Self-Sovereign Identity (SSID) as a whole, nor does it endorse any data, credentials, or claims within the SSID that have not been specifically linked and endorsed under this act;

(C) Does not assert the truth, accuracy, or validity of any information held in the SSID except for the existence of the linkage to specifically endorsed credentials; and

(D) Stores only the minimum data necessary to maintain the linkage.

(iii) The registry may be used to support the provision of beneficial ownership information for legal entities through verifiable credentials linked to the registered principal's DID.

(iv) The registry architecture shall function as follows:

(A) The Hashed Taxpayer Identification Number points to a registry record;

(B) That record contains the registered principal's self-controlled Decentralized Identifier (DID);

(C) The DID resolves to the registered principal's Self-Sovereign Identity (SSID);

(D) The registered principal incorporates state-endorsed credentials and other verifiable credentials into their Self-Sovereign Identity (SSID), which remains under their sole control.

(v) Registered principals retain full ownership and control of their DID and Self-Sovereign Identity at all times. The state's role is strictly limited to maintaining the hashed linkage and performing verification of the linkage itself.

(f) Funding and Fee Authority.

(i) There is appropriated xxxx dollars ($xxxx) from the general fund to the secretary of state for the biennium beginning July 1, [Year], for the design, development, and initial implementation of the program and registry. These funds shall not revert.

(ii) The secretary of state may establish and collect reasonable fees for linkage services, notary endorsements, and verification queries. All fees collected shall be deposited into a separate account and are continuously appropriated to the secretary of state for administration and maintenance of the program.

(g) Privacy Protections and Limitations on State Authority.

(i) The state shall not use the Registered Principal Registry or any information obtained through the program for any purpose other than the administration of this act.

(ii) The state shall not monitor, track, surveil, or correlate the presentation or use of any DID, state-endorsed credential, or data within a registered principal's Self-Sovereign Identity.

(iii) The state shall not retain any data beyond what is strictly necessary to maintain the hashed linkage and endorsement status.

(iv) A registered principal may, at any time, request removal of their DID linkage from the registry. Upon verified request, the secretary of state shall promptly remove the linkage.

(v) Any state employee or contractor who knowingly accesses, uses, or discloses information from the Registered Principal Registry in violation of this section shall be subject to penalties under W.S. 6-5-101 et seq. and other applicable Wyoming law.

(vi) The program and registry shall be subject to regular independent audits. Audit results shall be made publicly available in accordance with the Wyoming Public Records Act, W.S. 16-4-201 et seq.

(vii) Nothing in this act shall be construed to grant the state any ownership, control, or ongoing access to a registered principal's Self-Sovereign Identity or digital wallet or Digital Data Store.

(h) Business Entity Linkage Registry.

(i) The secretary of state shall establish and maintain a Business Entity Linkage Registry to connect a legal entity's Business Entity Registered Number to a registered principal's Self-Sovereign Identity (SSID) through the principal's self-controlled Decentralized Identifier (DID).

(ii) Basic linkage under this subsection may be established after a legal entity has obtained an Employer Identification Number (EIN).

(iii) The secretary of state may establish an optional enhanced linkage process under which a person forming a legal entity may submit a public key during the formation process under Title 17. The secretary of state may generate an access key, encrypt it using the submitted public key, and store the encrypted access key. The secretary of state shall promulgate rules governing the optional enhanced linkage process, including procedures for retrieval and use of the encrypted access key by the registered principal to prove control and complete the linkage between the Business Entity Registered Number and the principal's Self-Sovereign Identity (SSID) via the Decentralized Identifier (DID).

(iv) The secretary of state is authorized to amend business formation processes under W.S. Title 17 to accept public keys for purposes of the optional enhanced linkage process described in paragraph (iii) of this subsection.

(v) The Business Entity Linkage Registry shall store only the minimum data necessary to maintain linkages and shall be subject to the privacy protections in subsection (g).

(i) Satisfaction of Physical Address and Beneficial Ownership Requirements.

(i) When forming a legal entity, if no separate physical business address is provided, the address of the registered agent may be used as the entity's address of record.

(ii) A primary contact forming a legal entity may submit their hashed taxpayer identification number to link the entity to a registered principal through the Business Entity Linkage Registry.

(iii) A legal entity that does not maintain a physical place of business in Wyoming may satisfy beneficial ownership information requirements under federal law, including those administered by FinCEN and pursuant to the Bank Secrecy Act, by making available beneficial ownership information of its members and governing documents through its linked Self-Sovereign Identity and registered principal.

(iv) Information retrieved from a legal entity's linked Self-Sovereign Identity and registered principal may be accepted by financial institutions and other regulated entities in satisfaction of beneficial ownership verification and customer due diligence requirements.

(j) Anonymous Limited Liability Company Class.

(i) The secretary of state shall establish and administer a new class of limited liability company under the Wyoming Limited Liability Company Act, W.S. 17-29-101 et seq., to be designated the "Anonymous Limited Liability Company" or "A-LLC."

(ii) **Physical Address.** An A-LLC shall have no requirement to maintain or disclose a physical business address other than the address of its registered agent. The registered agent's address maintained pursuant to W.S. 17-28-101 et seq. may serve as the entity's address of record for all purposes under Wyoming law, consistent with subsection (i) of this section.

(iii) **Membership Percentage and Principal Registry Reference Requirements.** At the time of formation and upon any change in membership or ownership percentages, an A-LLC shall provide, through the Business Entity Linkage Registry and linked verifiable credentials within the registered principals' Self-Sovereign Identity (SSID), the following information elements:

(A) Identification of each member as a registered principal, including a reference to the member's Decentralized Identifier (DID) in the Registered Principal Registry;

(B) The percentage of membership interest or beneficial ownership held by each member or registered principal;

(C) Any additional information elements the secretary of state determines by rule are necessary to verify control and beneficial ownership.

This information shall remain under the sole control of the registered principals within their SSID, shall be subject to the privacy protections and limitations on state authority in subsection (g), and shall not be included in the public articles of organization filed under W.S. 17-29-201 or in any other public record maintained by the secretary of state.

(iv) **Facilitation of Extended Due Diligence and Transaction Monitoring.**

(A) Upon verified request by a financial institution or other entity subject to customer due diligence, enhanced due diligence (EDD), or anti-money laundering obligations under the Bank Secrecy Act (31 U.S.C. § 5311 et seq.) and implementing regulations, or under Wyoming law, the registered principal of an A-LLC (or an agent or system authorized by the registered principal) may provide access to the linked verifiable credentials, membership percentage information, and registry references. Such access may be facilitated through the Verifier App or other mechanisms authorized under this act.

(B) Such information shall be made available solely for the purposes of:

(I) Performing customer identification, beneficial ownership verification, and enhanced due diligence;

(II) Understanding the nature and purpose of the customer relationship; and

(III) Conducting ongoing monitoring of cash flows, disbursements to vendors, distributions or payments to members, and other transactions.

(C) Financial institutions and other regulated entities may rely on state-endorsed credentials and linkages under this program in satisfaction of their federal and state due diligence and monitoring obligations.

(v) The secretary of state is authorized to promulgate rules and to amend business formation processes under W.S. 17-29-201, annual reports under W.S. 17-29-209, and other relevant provisions of Title 17 to implement the A-LLC class. This includes procedures for maintaining current membership and principal registry references (including via the optional enhanced linkage process using public keys authorized in subsection (h)(iii)) and for integrating updates with the Business Entity Linkage Registry.

(vi) Participation as an A-LLC is voluntary. Nothing in this subsection alters the formation, operation, or privacy features available to standard limited liability companies under W.S. 17-29-101 et seq.

(k) Data Dictionary Ledger and Approved Cryptographic Components.

(i) The secretary of state shall establish and maintain a Data Dictionary Ledger as an immutable, append-only, cryptographically verifiable record.

(ii) The Data Dictionary Ledger shall permanently record and make publicly verifiable at minimum:

(A) The State’s public encryption key;

(B) Semantic definitions for information elements used within the program;

(C) Every Approved WASM Module, including its cryptographic hash (content identifier), version number, date of approval, functional description, and the specific zero-knowledge proof circuits or verification logic it implements;

(D) All historical versions of the public encryption key, semantic definitions, and previously approved WASM modules, preserved immutably with time-stamps and cryptographic proofs of inclusion;

(E) Revocation status information for state-endorsed credentials, including cryptographic signatures of revocation events and references to revocation status lists or accumulators.

(iii) Only WASM modules that have completed a rigorous security review process (including, where appropriate, formal verification and public comment) may be designated as Approved WASM Modules and recorded on the Data Dictionary Ledger. The secretary of state shall promulgate rules establishing transparent criteria, review procedures, and revocation processes for approved modules.

(iv) Approved WASM Modules recorded on the Data Dictionary Ledger may be used by registered principals, authorized notaries, or relying parties to generate and verify zero-knowledge proofs derived from data stored or encoded in CBOR format within a registered principal's Self-Sovereign Identity (SSID) or verifiable credentials.

(v) Any zero-knowledge proof generated using an Approved WASM Module recorded on the Data Dictionary Ledger shall be considered compliant with the privacy protections, selective disclosure requirements, and limitations on state authority set forth in subsection (g).

(vi) The Data Dictionary Ledger shall be publicly accessible and independently verifiable by any party without requiring permission from the secretary of state. The secretary of state shall ensure that the ledger's integrity can be cryptographically validated at any point in time.

(vii) The secretary of state may reference or integrate the Data Dictionary Ledger with existing distributed ledger or blockchain infrastructure, provided such integration maintains the immutability, auditability, and public verifiability requirements of this subsection.

(viii) **Management of Semantic Definitions.** The secretary of state shall initially manage the semantic definitions for information elements recorded on the Data Dictionary Ledger. The agency responsible for the ongoing management and updating of such semantic definitions is yet to be determined and may be designated by the legislature or by rule promulgated under this act.

(ix) **Credential Revocation.** The secretary of state shall record on the Data Dictionary Ledger the revocation status of any state-endorsed credential. Revocation information shall be signed using the State's public encryption key recorded on the ledger and shall be made publicly verifiable. The secretary of state shall promulgate rules governing the format, timing, and cryptographic method of recording revocations, ensuring compatibility with zero-knowledge proof mechanisms supported by Approved WASM Modules.

(l) Verifier App.

(i) The secretary of state shall establish, maintain, or authorize the operation of a Verifier App as an integral part of the State-Endorsed Digital Identity Linkage Program.

(ii) The Verifier App shall:

(A) Interact with a registered principal's Self-Sovereign Identity (SSID), whether implemented as a digital wallet or Digital Data Store, to access verifiable credentials and state-endorsed credentials held under the principal's control;

(B) Respond to standardized OpenID queries, including those compliant with OpenID Connect for Verifiable Presentations (OIDC4VP) and Self-Issued OpenID Provider

(SIOP) specifications, to enable relying parties to verify the authenticity, validity, and revocation status of signed credentials;

(C) Support privacy-preserving verification methods, including selective disclosure through zero-knowledge proofs generated via Approved WASM Modules recorded on the Data Dictionary Ledger, where applicable.

(iii) The secretary of state shall promulgate rules establishing security, interoperability, privacy, and accessibility standards for the Verifier App, ensuring it operates in a manner consistent with the privacy protections set forth in subsection (g).

Section 3.

This act shall take effect July 1, [Year].

Appendix-B

About the Author

David Roland has been programming computers since 1970 and developing engineering applications since 1977. While still in college, he founded his first company, Roland Projects, becoming the first self-employed Co-op student at Rochester Institute of Technology. In 1981, he advertised his initial products in Byte Magazine.

While at Northern Telecom, Roland developed operating system applications and fault-tolerant enhancements for 911 emergency systems and voice service nodes. During this period, he conducted extensive research into real-time object-oriented control systems and returned to consulting - work that ultimately led to the creation of the DAVID™ operating system.

In 1991, Roland began contributing to the U.S. Department of Commerce's NIST North American ISDN Users' Forum. He chaired multiple working groups on compatibility and capabilities profiling and played a role in developing the U.S. national ISDN standards.

In 1996, Roland engineered another operating system for a Seiko Epson ISDN project and co-authored U.S. Patent 6,208,640. In the early 2000s, he founded SohoStar to deliver triple-play multimedia services over ISDN and later DSL.

In 2008, Roland traveled to Rwanda to develop a comprehensive national network proposal. The initiative aimed to upgrade the country's entire infrastructure into a government-owned Internet and multimedia communications network, providing voice, streaming video, and data services nationwide at a time when Internet access was not yet available in Rwanda.

The projected cost for the complete national network was $400,000. By comparison, Verizon had submitted competing offers at $400,000 per tower. The project was ultimately halted due to state corruption.

Since then, Roland has continued his engineering work, focusing on cybersecurity, decentralized communications, and transaction processing for small office, home office, and residential applications.

For the past 10+ years, his CidrPress™ platform has tracked millions of security incidents while monitoring more than 70,000 malicious agents across the globe. CidrPress protects equipment and services by detecting and terminating hacking attempts in less than one second.

Roland also provides specialized engineering services to select clients in the areas of business transactions, cybersecurity, encryption, self-sovereign IDs, and secure information gateways, servers, and appliances.