Digital Law Framework

A Trust Architect's Contribution to State Digital Policy

by Christopher Allen <ChristopherA@LifeWithAlacrity.com>

A Supplement to The Architecture of Autonomy

September 3, 2025

Status: Community Draft for Comments (Not for Publication)

Preface

I am a technologist, not a lawyer or legislator. My perspective comes from decades designing cryptographic systems that millions use daily, including TLS 1.0, which secures web communications, and contributing to decentralized identity standards. This experience has given me insight into how technical architecture shapes legal possibilities.

In recent years, I've had the privilege of advising Wyoming legislators on digital asset and identity legislation, helping translate between technical reality and legal frameworks. This document emerged from those conversations and similar discussions with policymakers seeking practical approaches to digital law.

This framework offers model legislation that states can adopt to clarify how existing legal principles apply to cryptographic systems. It is intended as a companion to my longer work, "The Architecture of Autonomy," focusing specifically on implementable statutory language rather than broader policy analysis.

These model acts reflect what I've learned: that good digital law doesn't require understanding every technical detail, but does require recognizing which technical distinctions have legal significance. My hope is that legislative staff will find this useful as states navigate the intersection of law and cryptography.

This document is US-centric, reflecting American legal traditions and federalist structure. International readers may find the principles useful but will need to adapt them to their own legal systems.

I'm actively seeking feedback from all parts of the community - technologists, policymakers, legal scholars, and practitioners. What have I missed? What unintended consequences might arise? Please share your thoughts at ChristopherA@LifeWithAlacrity.com.

Christopher Allen
September 2025

Policy Explainer: A Four-Layer Framework for Digital Law

This package contains four coordinated acts:

- Cryptographic Secret Protection Act (foundational - must be adopted first)
- Digital Signature and Assent Act
- Cryptographically Verifiable Records Act
- Digital Identity Recognition Act

While the acts build upon each other, states have flexibility in adoption. The Cryptographic Secret Protection Act serves as the foundation, establishing core definitions and standards for all cryptographic systems. States seeking minimal implementation should begin with the Secret Protection Act and the Verifiable Records Act, as those primarily guide courts rather than creating new governance structures.

Why This Matters

Law has not kept up with cryptography. Current state and federal statutes (E-SIGN, UETA, identity pilots) mix together different functions: signing, authenticating records, and proving identity. This creates legal ambiguity and slows innovation.

The **Digital Law Framework** provides a clear, future-proof structure that states can adopt in whole or in part.

The Problem with Current Law

When E-SIGN was passed in 2000, "electronic signature" meant clicking "I agree" or typing your name. Today we have:

- Multi-signature wallets requiring 3-of-5 approvals
- Zero-knowledge proofs that verify facts without revealing data
- Verifiable credentials that selectively disclose attributes
- Blockchain records that prove timing and integrity
- Post-quantum cryptography preparing for future threats

Current laws force these innovations into outdated categories, creating uncertainty for businesses and courts.

Why Layering?

By separating distinct functions into independent layers, we achieve:

- **Legal clarity**: Each layer has one job, making interpretation straightforward
- **Technology neutrality**: Works with current and future cryptographic methods
- **Incremental adoption**: States can adopt one layer at a time
- **No vendor lock-in**: Prevents monopolies while enabling innovation

What Each Layer Does

Layer 0: Cryptographic Secret Protection Act*(foundation)*

- **Problem it solves**: Courts ordering people to decrypt data or surrender private keys
- **Solution**: Protects cryptographic secrets just like Fifth Amendment protects self-incrimination
- **Real impact**: Your Bitcoin keys, password manager seeds, and biometric templates stay private

Layer 1: Digital Signature & Assent Act

- **Problem it solves**: Uncertainty whether multi-sig wallets, threshold signatures, or AI agents can legally sign
- **Solution**: Makes ALL digital signatures legally valid if there's intent
- **Real impact**: Smart contracts, DAO votes, and automated systems can execute binding agreements

Layer 2: Cryptographically Verifiable Records Act

- **Problem it solves**: Courts rejecting blockchain records as hearsay or requiring expensive expert witnesses
- **Solution**: Makes cryptographically verifiable records self-authenticating evidence
- **Real impact**: Blockchain receipts, git commits, and timestamped logs accepted without testimony

Layer 3: Digital Identity Recognition Act

- **Problem it solves**: State identity monopolies and unclear authority for digital credentials
- **Solution**: Recognizes ANY verifiable credential while grounding authority in existing agency law
- **Real impact**: Your university, employer, or bank can issue credentials the state must recognize

What Each Layer Contains

- **Layer 0: Cryptographic Secret Protection Act** - Protects private keys, seeds, zk-proofs, and other secrets - Prohibits compelled disclosure of cryptographic secrets - Prevents economic coercion through cryptographic control- Prevents behavioral surplus extraction- Establishes standards framework for all cryptographic systems- Prefers minimal disclosure (ISO principle) using methods such as public keys, zk-proofs, selective disclosure techniques, or elided proofs - Prevents government hardware mandates
- **Layer 1: Digital Signature & Assent Act** - _Did they agree?_ - All digital signatures valid - Multi-sig, revocation recognized - Protects against duress-based signatures- Identity questions not included

- **Layer 2: Cryptographically Verifiable Records Act** - _Is the record authentic?_- Self-authentication & admissibility - Records are tamper-evident and portable- Defers identity questions upward
- **Layer 3: Digital Identity Recognition Act** - _Who agreed?_ - Agency law (principal/agent) - Recognition of verifiable credentials - Essential service obligations- State does NOT monopolize ID

Core Protections Against Platform Abuses

The framework specifically addresses documented platform harms:

- **Economic Coercion**: Essential services cannot demand cryptographic secrets
- **Behavioral Extraction**: Platforms cannot use secrets for surveillance without consent
- **Adhesive Contracts**: Courts must scrutinize "consent" when no alternatives exist
- **Infrastructure Monopoly**: No entity can control multiple verification layers
- **Exit Prevention**: Users retain rights to export data and reputation even after revocation
- **Legibility**: Technical decisions affecting rights must explain who/what/how to appeal

Why States Should Act Now

1. Competitive Advantage: Early adopter states will attract crypto businesses, fintech startups, and digital innovation hubs. Wyoming's blockchain laws brought in $500M+ in economic activity.

2. Legal Certainty Reduces Costs: Businesses currently spend millions on legal opinions for basic digital operations. Clear law eliminates this friction.

3. Protect Citizens' Rights: As more life moves online, citizens need protection from forced decryption and recognition of their digital credentials.

4. No State Spending Required: Unlike identity system procurements that cost millions, this framework costs nothing, it just clarifies existing law.

Common Objections Addressed

"This is too technical for judges"The framework uses familiar legal concepts: agency law, evidence rules, and contract principles. The technology works in the background.

"What about law enforcement?"Layer 0 preserves existing warrant and subpoena powers for records and communications—it only protects the cryptographic keys themselves.

"This could enable crime"Criminals already use encryption. This framework ensures law-abiding citizens and businesses have legal clarity.

"We need uniform federal law"Federal law moves slowly. States can lead, as they did with electronic signatures before E-SIGN.

Real-World Impact: Before and After

Corporate Governance

- *Before*: "Are DAO votes legally binding? Can smart contracts be corporate bylaws? Nobody knows."
- *After*: Multi-signature treasury controls and on-chain voting are explicitly valid corporate acts.

Property Records

- *Before*: "We need to maintain parallel paper records because blockchain might not be admissible."
- *After*: Blockchain property records are self-authenticating evidence in court.

Identity Verification

- *Before*: "Only government ID accepted. Your employer badge or university credential doesn't count."
- *After*: Any cryptographically verifiable credential is legally recognized.

Digital Estate Planning

- *Before*: "If you die, your family may be forced to surrender your keys to access your assets."
- *After*: Estate executors can use zero-knowledge proofs to establish authority without compromising keys.

Implementation Roadmap

Phase 1: Pass Layer 0 (Secret Protection)

- Immediate protection for citizens' digital assets
- Establishes standards framework for entire package
- No infrastructure needed
- Sends signal that state understands cryptography

Phase 2: Add Layers 1-2 (Signatures & Records)

- Enables blockchain business operations
- Clarifies digital evidence rules
- Still no infrastructure required

Phase 3: Complete with Layer 3 (Identity)

- Full modern digital law framework
- Competitive advantage complete
- State leads in digital innovation

Model Success: Wyoming

Wyoming passed similar laws piecemeal:

- 2018: Blockchain records authorized
- 2019: Digital asset property rights
- 2021: DAO LLC recognition
- Result: 30+ crypto companies relocated, $500M+ economic impact

This framework accomplishes more, faster, with clearer legal structure.

Why Not a Digital Assets Law?

Many states, led by Wyoming, have passed complex digital asset statutes defining categories like "digital consumer assets," "digital securities," and "virtual currency." This has created:

- **Fragmentation**: Each state defines categories differently
- **Complexity**: Multi-part statutes requiring constant updates
- **Regulatory confusion**: Overlapping federal proposals add uncertainty

Our approach: Digital assets are simply property controlled by cryptographic secrets. Our framework already protects them:

- Layer 0 protects the keys that control assets
- Layer 1 validates transfers via smart contracts
- Layer 2 makes blockchain ownership records admissible
- Layer 3 recognizes authority to transfer

If your state needs explicit digital asset language, add this minimal provision to existing property law:

DIGITAL ASSETS AS PERSONAL PROPERTY(1) A digital asset is personal property.(2) Control of a digital asset is established by possession of the cryptographic secret that grants power to transfer the asset.(3) Transfer of control constitutes transfer of the property right.(4) This section does not alter characterization for tax, securities, or other regulatory purposes.

This avoids complex taxonomies while providing legal clarity. But the four-layer framework may be sufficient without any digital asset definition. It provides the infrastructure for digital assets to function within existing property law.

The framework also protects against platform-specific abuses documented in recent years, from arbitrary account freezes to behavioral data extraction, through its anti-coercion provisions and legibility requirements.

Addressing the Architecture of Extraction

These laws specifically combat the "six inversions" that platforms use to undermine user rights:

- Possession becomes privilege → Protected by cryptographic secrets
- Contract becomes coercion → Courts scrutinize adhesive agreements
- Enforcement becomes absolutism → Legibility requirements ensure accountability
- Power becomes invisible → Infrastructure monopolies prohibited
- Exit becomes erasure → Data portability guaranteed
- Identity becomes commodity → Principal authority preserved

The framework restores human agency without mandating specific technologies or creating new bureaucracies.

Call to Action

Every month of delay means:

- Businesses choosing other states
- Citizens vulnerable to forced key disclosure
- Courts making inconsistent digital evidence rulings
- Innovation happening elsewhere

The Digital Law Framework is ready for introduction. No appropriation needed. No agencies to create. Just clear, modern law for the digital age.

Next Step: Contact [legislative sponsor] to introduce the framework or individual acts in the upcoming session.

PART 0. CRYPTOGRAPHIC SECRET PROTECTION ACT

SECTION 1. SHORT TITLE.

This [act] may be cited as the **Cryptographic Secret Protection Act**.

> **Drafting Note:** A state legislature may rename or omit the short title consistent with codification practices.

SECTION 2. DEFINITIONS.

(1) **"Cryptographic secret"** means information that provides the basis for cryptographic security, including but not limited to private keys, secret shares, recovery seeds, biometric templates, or other forms of knowledge or data used to control access, create signatures, or generate cryptographic proofs.

(2) **"Compelled disclosure"** means any order, subpoena, demand, mandate, or condition requiring a person to reveal, surrender, or otherwise provide a cryptographic secret.

(3) **"Minimal disclosure method"** means a cryptographic process, consistent with the ISO principle of data minimization, that allows a party to prove a fact without revealing the underlying cryptographic secret.

(4) **"Cryptographic capability"** means the ability to use a cryptographic secret to perform operations such as signing, encryption, decryption, or proof generation.

(5) **"Essential service"** means a service necessary for participation in economic or civic life, including but not limited to banking, payment processing, government benefits, employment platforms, and dominant digital platforms as may be designated by [appropriate regulatory authority].

(6) **"Behavioral surplus extraction"** means the collection of data beyond that necessary for service provision, used to predict or influence behavior without user awareness or meaningful consent.

SECTION 3. GENERAL PROHIBITION ON COMPELLED DISCLOSURE.

No court, agency, or person may compel an individual or entity to disclose a cryptographic secret in any civil, criminal, administrative, or legislative proceeding.

No person shall be compelled to use their cryptographic capability to create a signature, proof, or attestation against their will.

No financial institution, payment processor, or essential service provider may condition access to services on disclosure of cryptographic secrets, except as provided in Section 4.

No person shall be compelled to use their cryptographic capability to authorize transactions or transfers under duress, including economic duress.

Cryptographic secrets shall not be used to enable behavioral surplus extraction without explicit, revocable consent.

The existence, custody, or control of a cryptographic secret may not be used as the basis for contempt, sanction, adverse inference, or penalty for refusal to disclose.

Digital methods recognized under this act shall not discriminate against persons with disabilities. Alternative methods of equal legal effect must remain available.

This act shall be interpreted to maximize individual autonomy and self-determination while minimizing coercive or unconscionable technical designs. Technical implementations should preserve meaningful choice and resist designs that create dependence without recourse.

Technical implementations shall be evaluated not only on cryptographic merit but on their support for human dignity, comprehension, and meaningful control.

When technical systems make decisions affecting legal rights or obligations, they must provide legible explanations of:

- What entity made the decision
- By what authority or rule
- With what avenue for appeal

Courts shall apply a presumption against economic and technical coercion when interpreting this act.

SECTION 4. LIMITED EXCEPTIONS.

Compelled disclosure of a cryptographic secret may be ordered only if a court finds, by clear and convincing evidence, that:

- no minimal disclosure method or less intrusive alternative is reasonably available; and
- the disclosure is narrowly tailored to access specific property, rights, or data lawfully subject to the proceeding.

Any such order must:

- specify the precise secret or scope required;
- limit use of the disclosed information to the proceeding for which it was compelled;
- provide protective measures to minimize dissemination; and
- require destruction or sealing of the disclosed secret once its use is complete.

SECTION 5. GOVERNMENT HARDWARE OR SERVICE MANDATES.

Nothing in this state's law shall be construed to require the use of government-issued or government-mandated hardware devices, software, or services for the generation, storage, or use of cryptographic secrets.

A person may freely choose lawful methods or tools for custody and use of cryptographic secrets.

SECTION 6. PRESUMPTION IN FAVOR OF MINIMAL DISCLOSURE.

A minimal disclosure method is presumed sufficient to satisfy any legal requirement of proof if it demonstrates the fact in question with cryptographic integrity.

Minimal disclosure methods include, but are not limited to:

- presentation of a public key corresponding to a private key;
- production of a zero-knowledge proof demonstrating possession of, or a property of, a cryptographic secret;
- provision of a selectively disclosed credential or attribute from a verifiable credential;
- presentation of a cryptographic commitment or elided proof that may be later revealed or un-elided.

A court or agency must accept such a method unless it makes specific findings that the method is unreliable in the particular case.

When multiple disclosure methods exist, courts and agencies shall prefer the method revealing the least information necessary to satisfy the legal requirement.

SECTION 7. STANDARDS FOR ALL CRYPTOGRAPHIC SYSTEMS.

(a) PRESUMPTION OF VALIDITY. Systems implementing any act in this package shall be presumed valid if they demonstrate compliance with ANY of the following:(1) Technical standards adopted by recognized international bodies;(2) Open standards developed through transparent, multi-stakeholder processes;(3) Industry customs and practices that have achieved substantial adoption; or(4) Open source implementations that have undergone public security review.

(b) RECOGNIZED STANDARDS BODIES. Standards bodies are recognized if they meet ALL of the following:(1) Maintain open membership and transparent governance;(2) Publish specifications without discriminatory licensing;(3) Include diverse stakeholder representation; and(4) Document security and privacy considerations.

(c) INDUSTRY CUSTOMS. Following the law merchant tradition, courts may recognize cryptographic practices that satisfy ALL of the following:(1) Are regularly observed by a substantial portion of the industry;(2) Have existed long enough to demonstrate stability;(3) Are documented through open source implementations or public specifications; and(4) Do not conflict with express statutory requirements.

(d) SAFE HARBOR FOR INNOVATION. Cryptographic systems qualify for safe harbor if they meet ALL of the following:(1) Implement recognized cryptographic primitives;(2) Undergo public security review through bug bounty programs or security audits;(3) Publish source code or detailed specifications;(4) Demonstrate interoperability with at least one other implementation; and(5) Employ cryptographic agility to enable migration when algorithms are compromised or deprecated.

(e) RECOGNITION ACROSS JURISDICTIONS. Cryptographic systems authenticated under another jurisdiction's comparable law have the same effect here unless contrary law applies.

(f) BURDEN OF PROOF. The burden to demonstrate unreliability of a system meeting these criteria falls on the challenging party.

SECTION 8. RELATION TO OTHER LAW.

Nothing in this [act] alters obligations under existing discovery, evidence, or investigative procedures, except to limit compelled production of cryptographic secrets as provided herein.

This [act] supplements protections under [the state constitution] and the Fifth Amendment to the United States Constitution.

Minimal disclosure methods described in this [act] may be used in connection with records, signatures, or identity credentials recognized under related Acts.

This act operates independently but may be used in conjunction with the Digital Signature and Assent Act, Cryptographically Verifiable Records Act, and Digital Identity Recognition Act. Combined use does not create requirements beyond those in each individual act.

Standards for all cryptographic systems are established in Section 7 of this act and apply to all acts in this package.

SECTION 9. NO APPROPRIATION; NO UNFUNDED MANDATE.

This [act] does not of itself appropriate money.

Nothing in this [act] requires the state to procure or operate cryptographic hardware, software, or services.

SECTION 10. SEVERABILITY.

If any provision of this [act] or its application to any person or circumstance is held invalid, the invalidity does not affect other provisions or applications of this [act].

COMMENTARY (for drafters and courts)

- Expands on [Wyoming HB0041 (2022)](https://www.wyoleg.gov/Legislation/2022/HB0041) to cover all cryptographic secrets.
- Codifies the ISO minimal disclosure principle with examples.
- Prevents compelled disclosure while allowing narrowly tailored exceptions.
- Bars government hardware mandates.
- Supplements constitutional protections under [U.S. Const. amend. V](https://constitution.congress.gov/constitution/amendment-5/) and state equivalents.
- Protects against compelled use of cryptographic capabilities.

- Prevents economic coercion through denial of essential services, addressing concerns from cases like *Totem Marine Tug & Barge, Inc. v. Alyeska Pipeline Service Co.*, 584 P.2d 15 (Alaska 1978).
- Ensures accessibility without mandating specific implementations.
- Establishes presumption against coercion as interpretive principle, following established canons of construction.
- ESTABLISHES STANDARDS FRAMEWORK for all cryptographic systems in this package, including recognition of open standards, industry customs (following UCC § 1-303), and safe harbors for innovation.
- No fiscal impact.

PART I. DIGITAL SIGNATURE AND ASSENT ACT

SECTION 1. SHORT TITLE.

This [act] may be cited as the **Digital Signature and Assent Act**.

> **Drafting Note:** A state legislature may rename or omit the short title consistent with codification practices.

SECTION 2. DEFINITIONS.

(1) **"Electronic signature"** means an electronic sound, symbol, or process attached to or logically associated with a record and executed or adopted by a person with the intent to sign. (2) **"Digital signature"** means an electronic signature produced by cryptographic or other verifiable methods that ensure authenticity, integrity, and non-repudiation. (3) **"Composite signature"** means a signature created by combining multiple methods of verification, including but not limited to cryptographic keys, biometrics, passcodes, or devices. (4) **"Multi-party signature"** means a digital signature requiring approval from more than one person or device, including threshold or quorum-based methods. (5) **"Principal"** means a person or entity granting authority to another person, device, or system to act on their behalf. (6) **"Agent"** means a person, device, or system authorized by a principal to affix a digital signature on the principal's behalf. (7) **"Economic duress"** means financial pressure that overbears a party's will, including threats to withhold essential services, payment processing, or access to funds.

SECTION 3. LEGAL EFFECT.

A digital signature has the same legal effect as a handwritten signature, provided it is affixed with intent and attached to or logically associated with the record.

The validity of a digital signature establishes assent but does not by itself establish identity. Questions of identity are governed by the Digital Identity Recognition Act.

Digital methods recognized under this act shall not discriminate against persons with disabilities. Alternative methods of equal legal effect must remain available.

This act shall be interpreted to maximize individual autonomy and self-determination while minimizing coercive or unconscionable technical designs. Technical implementations should preserve meaningful choice and resist designs that create dependence without recourse.

Technical implementations shall be evaluated not only on cryptographic merit but on their support for human dignity, comprehension, and meaningful control.

When technical systems make decisions affecting legal rights or obligations, they must provide legible explanations of:

- What entity made the decision
- By what authority or rule
- With what avenue for appeal

Courts shall apply a presumption against economic and technical coercion when interpreting this act.

SECTION 4. MULTI-PARTY AND COMPOSITE SIGNATURES.

A record signed by a multi-party signature has the same legal effect as if each required signer had affixed an individual signature.

A composite signature is valid if the combined methods reliably demonstrate assent under the circumstances.

SECTION 5. AGENCY AND DELEGATED SIGNATURES.

A digital signature affixed by an agent within the scope of authority granted by the principal binds the principal.

The law of agency applies, including rules concerning authority, ratification, and revocation, unless displaced by this [act].

SECTION 6. REVOCATION AND EXPIRATION.

A digital signature remains effective until revoked, expired, or compromised.

Revocation or expiration does not affect the validity of signatures affixed before.

Emergency revocation is permitted only to prevent imminent harm or ongoing fraud. Non-emergency revocation requires:

- Specific notice of grounds for revocation
- Opportunity to cure defects where applicable
- Right to retrieve or export data before revocation takes effect
- Documentation of revocation grounds in tamper-evident format

SECTION 7. SIGNATURES UNDER DURESS.

A digital signature affixed under duress, including economic duress, may be voidable at the option of the coerced party.

Courts shall consider whether economic pressure through control of essential services rendered genuine consent impossible.

Courts shall scrutinize digital signatures for genuine consent when:

- The signing party had no meaningful alternative
- Terms were non-negotiable and adhesive
- Refusal would result in exclusion from essential services

SECTION 8. STANDARDS.

Standards for systems implementing this act are governed by the Cryptographic Secret Protection Act, Section 7, which applies to all cryptographic systems under this package.

SECTION 9. NO EXCLUSIVE METHOD.

This [act] does not require or limit the use of any particular technology for signatures.

SECTION 11. RELATION TO OTHER LAW.

This act operates independently but may be used in conjunction with the Cryptographic Secret Protection Act, Cryptographically Verifiable Records Act, and Digital Identity Recognition Act. Combined use does not create requirements beyond those in each individual act.

SECTION 12. NO APPROPRIATION; NO UNFUNDED MANDATE.

This [act] does not of itself appropriate money and does not require agencies to procure or operate systems.

[OPTIONAL] SECTION 13. ADMINISTRATION AND RULEMAKING.

An agency may adopt rules to implement this [act] within existing appropriations, provided such rules are technology-neutral and nonexclusive.

SECTION 14. SEVERABILITY.

If any provision is held invalid, the remainder is unaffected.

COMMENTARY

- Distinguishes assent (signature) from identity.
- Explicitly covers multi-sig and composite methods.
- Recognizes agency signatures under principal–agent law.
- Provides optional safe harbors without locking in technology.
- Cross-references Identity Act for identity questions.
- Protects against signatures made under economic duress, applying principles from *Austin Instrument, Inc. v. Loral Corp.*, 29 N.Y.2d 124 (1971).
- Requires due process for non-emergency revocations.
- Ensures accessibility without mandating specific implementations.
- Establishes presumption against coercion as interpretive principle.
- No fiscal impact.

PART II. CRYPTOGRAPHICALLY VERIFIABLE RECORDS ACT

SECTION 1. SHORT TITLE.

This [act] may be cited as the **Cryptographically Verifiable Records Act**.

> **Drafting Note:** A state may omit this section if codification practices do not include short titles.

SECTION 2. DEFINITIONS.

(1) **"Verifiable record system"** means any system that uses cryptographic methods to establish authenticity, integrity, and chronology of digital records. (2) **"Verifiable record technology"** means computer software or hardware enabling such systems. (3) **"Digital record"** means information stored in electronic form, including data, documents, contracts, or communications. (4) **"Portable format"** means a standardized, machine-readable data structure that preserves cryptographic proofs and enables verification across different systems.

SECTION 3. SELF-AUTHENTICATION.

A digital record registered in a verifiable record system is self-authenticating if accompanied by a declaration stating time of entry, retrieval, regular maintenance, and reliance.

Digital methods recognized under this act shall not discriminate against persons with disabilities. Alternative methods of equal legal effect must remain available.

This act shall be interpreted to maximize individual autonomy and self-determination while minimizing coercive or unconscionable technical designs. Technical implementations should preserve meaningful choice and resist designs that create dependence without recourse.

Technical implementations shall be evaluated not only on cryptographic merit but on their support for human dignity, comprehension, and meaningful control.

When technical systems make decisions affecting legal rights or obligations, they must provide legible explanations of:

- What entity made the decision
- By what authority or rule
- With what avenue for appeal

Courts shall apply a presumption against economic and technical coercion when interpreting this act.

SECTION 4. BUSINESS RECORDS PRESUMPTION.

Such records are presumed admissible unless circumstances suggest untrustworthiness.

SECTION 5. DEFAULT PRESUMPTIONS.

Unless rebutted:

- A record verified through valid technology is authentic.
- The recorded date/time is the date/time added.
- Indication of originator does not establish authority; that is governed by the Identity Act.
- Agreed presentation format is sufficient.
- The existence of a record in a verifiable system does not authorize its disclosure beyond what existing law permits.
- No single entity may control multiple layers of verification infrastructure (storage, retrieval, validation, or distribution) for the same record system.

SECTION 6. LIMITATIONS.

Presumptions extend only to authenticity, integrity, and chronology, not truth or legal status.

SECTION 7. SCOPE.

Applies to contracts, property, governance, identity interactions, and communications.

SECTION 8. STANDARDS.

Standards for systems implementing this act, including recognition across jurisdictions, are governed by the Cryptographic Secret Protection Act, Section 7, which applies to all cryptographic systems under this package.

SECTION 9. PORTABILITY.

A holder of a verifiable record has the right to export that record in a standardized, machine-readable format that preserves cryptographic proofs of authenticity.

Verifiable record systems shall support standard export formats that maintain the integrity and verifiability of records when transferred between systems.

Emergency revocation is permitted only to prevent imminent harm or ongoing fraud. Non-emergency revocation requires:

- Specific notice of grounds for revocation
- Opportunity to cure defects where applicable
- Right to retrieve or export data before revocation takes effect
- Documentation of revocation grounds in tamper-evident format

SECTION 10. NO MANDATE; NO VALIDATION.

Nothing requires adoption of such technology or validates underlying activity merely because recorded.

SECTION 11. RELATION TO OTHER LAW.

This act operates independently but may be used in conjunction with the Cryptographic Secret Protection Act, Digital Signature and Assent Act, and Digital Identity Recognition Act. Combined use does not create requirements beyond those in each individual act.

SECTION 12. NO APPROPRIATION; NO UNFUNDED MANDATE.

This [act] does not of itself appropriate money and imposes no obligation to procure or operate systems.

[OPTIONAL] SECTION 13. ADMINISTRATION AND RULEMAKING.

An agency may recognize formats or evidentiary methods within existing appropriations, provided such recognition remains technology-neutral and nonexclusive.

SECTION 14. SEVERABILITY.

If any provision is invalid, the rest remains effective.

COMMENTARY

- Anchors admissibility and evidentiary presumptions.
- Explicitly defers identity authority questions to the Identity Act.
- Cross-references Signature Act for integrated use.
- Provides optional safe harbors without forcing technology.
- Clarifies that technical storage doesn't override privacy law.
- Ensures portability of records with cryptographic integrity.
- Requires due process for non-emergency revocations.
- Ensures accessibility without mandating specific implementations.
- Establishes presumption against coercion as interpretive principle.
- No fiscal impact.

PART III. DIGITAL IDENTITY RECOGNITION ACT

SECTION 1. SHORT TITLE.

This [act] may be cited as the **Digital Identity Recognition Act**.

SECTION 2. DEFINITIONS.

(1) **"Digital identity"** means a set of attributes, credentials, or identifiers representing a principal in electronic form. (2) **"Credential"** means a verifiable digital attestation or token supporting a digital identity. (3) **"Principal"** means the person or entity represented. (4) **"Agent"** means a person, device, or system authorized to use a digital identity. (5) **"Issuer"** means an entity that creates and provides a credential. (6) **"Verifier"** means an entity that relies on a credential. (7) **"Essential infrastructure provider"** means an issuer providing identity services necessary for access to employment, government benefits, financial services, or other essential services as designated by [appropriate regulatory authority].

SECTION 3. LEGAL RECOGNITION.

A cryptographically verifiable identity or credential has the same legal effect as physical identification.

Recognition is not limited to state-issued systems.

This [act] does not authorize creation of a single, centralized identity system.

Digital methods recognized under this act shall not discriminate against persons with disabilities. Alternative methods of equal legal effect must remain available.

This act shall be interpreted to maximize individual autonomy and self-determination while minimizing coercive or unconscionable technical designs. Technical implementations should preserve meaningful choice and resist designs that create dependence without recourse.

Technical implementations shall be evaluated not only on cryptographic merit but on their support for human dignity, comprehension, and meaningful control.

When technical systems make decisions affecting legal rights or obligations, they must provide legible explanations of:

- What entity made the decision
- By what authority or rule
- With what avenue for appeal

Courts shall apply a presumption against economic and technical coercion when interpreting this act.

SECTION 4. AGENCY BASIS.

Agency law applies to digital identity. Acts within authority bind the principal; unauthorized acts do not, unless ratified.

SECTION 5. ISSUERS AND RELIANCE.

Issuers represent that credentials were issued to the stated principal.

Verifiers relying in good faith may treat credentials as valid unless untrustworthy.

Issuers may be liable for knowingly or negligently false credentials. Liability is limited to actual damages from reasonable reliance. No issuer is liable for uses beyond the stated scope of the credential.

When an issuer provides identity services as essential infrastructure for access to other services, employment, or government benefits, the issuer bears heightened duties of:

- Reasonable notice before credential revocation
- Transparent appeals processes
- Data portability upon request
- Protection against arbitrary denial of service

Essential infrastructure includes but is not limited to: payment processing, employment platforms, government service access, and dominant social platforms as designated by [appropriate authority].

SECTION 6. REVOCATION AND EXPIRATION.

Credentials may be revoked or expire by their terms. Past uses remain valid unless otherwise provided.

Revocation information may be published in any publicly accessible, tamper-evident format. Good faith reliance on recent verification creates a safe harbor even if subsequently revoked.

Emergency revocation is permitted only to prevent imminent harm or ongoing fraud. Non-emergency revocation requires:

- Specific notice of grounds for revocation
- Opportunity to cure defects where applicable
- Right to retrieve or export data before revocation takes effect
- Documentation of revocation grounds in tamper-evident format

Digital identity systems shall support indefinite persistence unless:

- The principal explicitly requests termination;
- Required by court order with due process; or
- Technical compromise necessitates migration to preserve security.

Issuers shall provide migration paths when technical evolution requires system changes.

Revocation or termination of credentials must not prevent:

- Export of user-generated content or relationship attestations
- Proof of prior standing or reputation

- Migration of cryptographically-signed history

SECTION 7. INTEROPERABILITY.

This state recognizes digital identities consistent with widely adopted open standards.

Credentials recognized in other jurisdictions have the same effect here unless contrary law applies.

Identity verification should minimize real-time dependencies. Systems that require contacting external services for each verification ("phone home" behaviors) are disfavored unless necessary for revocation checking or fraud prevention.

Offline verification methods are preferred where technically feasible.

Portability (moving identity between systems) and interoperability (systems working together) serve different purposes. This act recognizes both as valid but distinct design choices.

SECTION 8. STANDARDS.

Standards for systems implementing this act are governed by the Cryptographic Secret Protection Act, Section 7, which applies to all cryptographic systems under this package.

SECTION 9. NO MANDATE OR EXCLUSIVE CONTROL.

Nothing requires adoption of a digital identity.

Nothing grants exclusive control of identity systems to the state or any provider.

SECTION 10. FINANCIAL IDENTITY PROTECTION.

Digital identity used for financial services receives heightened protection. Financial service providers shall not:

- Freeze identity-linked accounts without due process
- Share identity credentials with other providers for blacklisting
- Require waiver of identity rights as condition of service

SECTION 11. RELATION TO OTHER LAW.

This act operates independently but may be used in conjunction with the Cryptographic Secret Protection Act, Digital Signature and Assent Act, and Cryptographically Verifiable Records Act. Combined use does not create requirements beyond those in each individual act.

SECTION 12. NO APPROPRIATION; NO UNFUNDED MANDATE.

This [act] does not of itself appropriate money and does not require the state to operate identity systems.

[OPTIONAL] SECTION 13. ADMINISTRATION AND RULEMAKING.

An agency may designate open standards or recognition criteria for credentials within existing appropriations, provided such designations remain technology-neutral and nonexclusive.

SECTION 14. SEVERABILITY.

If any provision is invalid, the remainder is unaffected.

COMMENTARY

- Frames identity in agency law (principal ↔ agent).
- Follows [Utah's model](https://le.utah.gov/xcode/Title46/Chapter1A/46-1a.html) of recognition without centralization.
- Balances issuer liability with verifier good faith reliance.
- Covers verifiable credentials, DIDs, federated IDs, and future cryptographic attestations.
- Explicitly bans a state monopoly identity system, following principles from *hiQ Labs, Inc. v. LinkedIn Corp.*, 31 F.4th 1180 (9th Cir. 2022) regarding anticompetitive platform behavior.
- Standards framework established in Cryptographic Secret Protection Act, Section 7 applies to all identity systems.
- Clarifies revocation mechanisms without mandating infrastructure.
- Limits issuer liability to encourage participation.
- Establishes heightened duties for essential infrastructure providers.
- Protects financial identity from arbitrary exclusion.
- Discourages "phone home" verification patterns.
- Requires due process for non-emergency revocations.
- Ensures accessibility without mandating specific implementations.
- Establishes presumption against coercion as interpretive principle.
- No fiscal impact.