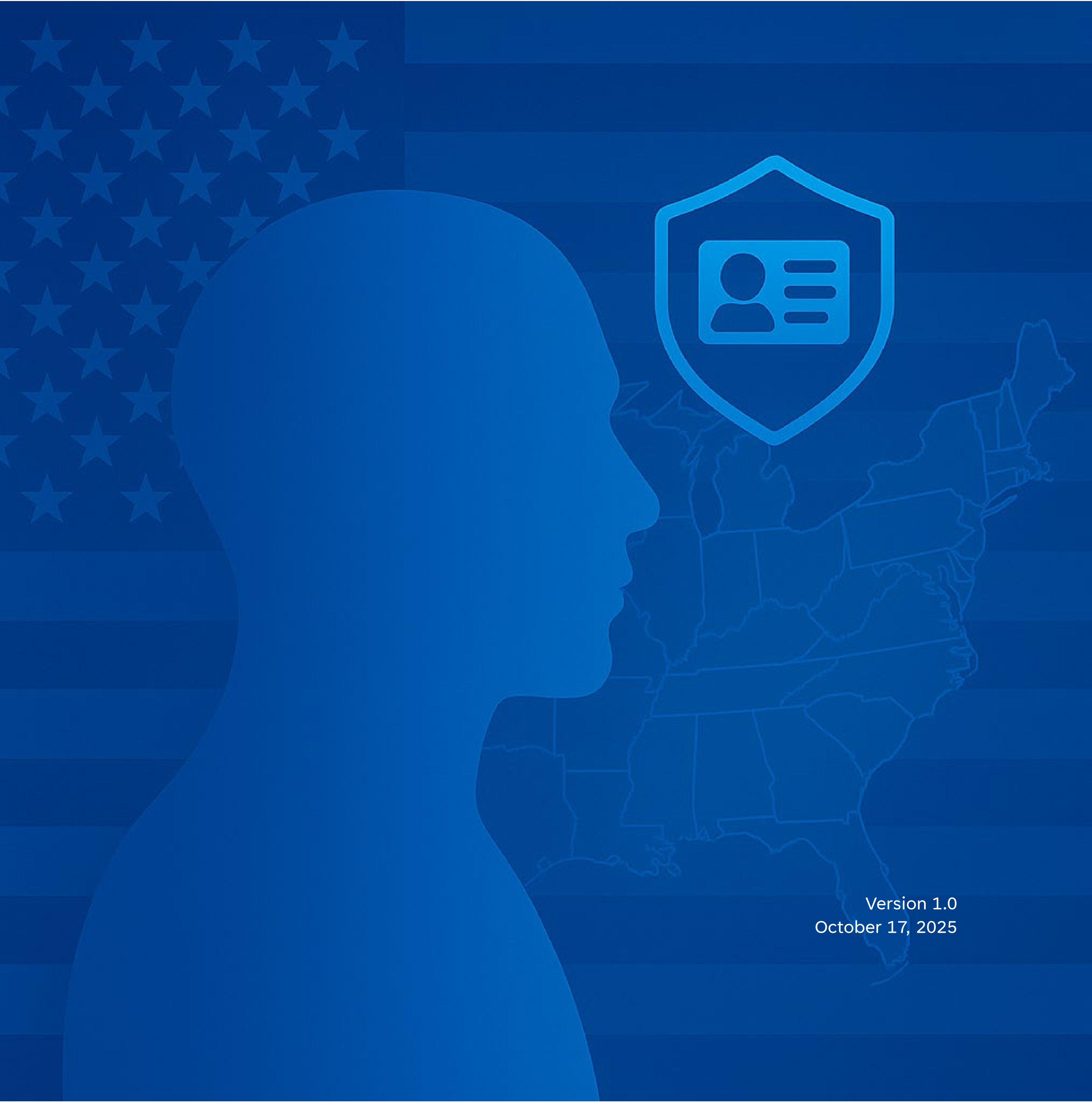

Version 1.0
October 17, 2025

STATE-ENDORSED DIGITAL IDENTITY

PROTECTING LIBERTY IN THE DIGITAL AGE

utah govops

SUMMARY

State-Endorsed Digital Identity, or SEDI, is a constitutionally-based model meant to restore trust and protect liberty in the digital age. It is the first rights-first framework for digital identity, founded on the American value that identity is inherently decentralized and innate to the individual and not created by governments or corporations. SEDI requires that individuals fully control their digital identifiers. In this framework the state endorses and protects identity, rather than creating or owning an individual's identity.

Many of the digital identity systems currently designed and implemented in the United States do not include a comprehensive governance framework. These systems have either neglected or intentionally rejected the concept of individuals' rights. While these systems often seek to solve real challenges such as fraud, child safety, impersonation prevention, efficiency creation, and interoperability, the risks to individuals' rights are profound. Public distrust in digital identity has grown globally in response to systems capable of government tracking, surveillance, profiling, and scoring, which transform digital identity into a means of control. Public trust erodes when digital identity systems are hastily rolled out and do not allow for the public discourse required for such foundational infrastructure.

SEDI offers a different path, one that honors an individual's autonomy and will be a digital export of freedom to the world. Through comprehensive governance, open standards, digital authenticity and autonomy-respecting architecture, SEDI enables individuals to prove facts about themselves securely and privately, without tracking or surveillance, and only if, how, and when they choose. SEDI treats digital identity as critical public infrastructure, essential for national security, ensuring that both democracy and the free market can thrive in the digital age. States are invited to join Utah in the SEDI Consortium, to create a better digital identity and future that harmonizes an individual's rights with a state's responsibilities.

THE CHALLENGE: TRUST HAS COLLAPSED ONLINE

The internet has transformed how people live, work, and communicate. It connects billions of people across continents, supports global commerce, and powers innovation. To date this progress has been primarily driven by commerce, entertainment, and social networks. Yet a trustworthy way for individuals to prove who they are does not exist.

In the physical world, trust is reinforced by an individual's image, voice, and official documents. In the digital world, those natural and institutional signals of trust vanish. In their absence, governments and corporations attempt to fill the void, building—either intentionally or unintentionally—digital identity systems that control, surveil, profile, objectify, score and monetize our behaviors and personal data, as seen in China and other authoritarian nations.

Today, identity online is fragmented across countless accounts and systems but unified by the trackable profiles that technology companies, data brokers, and governments create. This digital ecosystem has fueled fraud, data breaches, impersonation, manipulation, and disinformation, eroding public trust. With the rise of generative AI, new techniques such as *deepfakes* allow attackers to dramatically reduce their costs and conduct even more sophisticated attacks, using digitally doctored photos, videos, and audio streams that took days or weeks to produce, can now be done in minutes. This trend will only accelerate impersonation fraud.

The absence of a secure, privacy-preserving identity layer has become more than an inconvenience; it has become a national vulnerability that puts at risk individual security, trust in democracy, and the free market economy.

WHY SEDI IS NEEDED

For more than a decade, technologies and standards, such as ISO/IEC 18013-5/-7 (mobile driver's license), OpenID Connect, OAuth 2.0, KERI, SAML, and W3C Verifiable Credentials have advanced the technical capabilities of digital identity worldwide. Organizations who have adopted these technologies have not addressed some of the most essential questions concerning individual rights, comprehensive governance, and constitutional safeguards. SEDI fills that gap, ensuring that digital identity is designed to serve people.

A CONSTITUTIONAL FOUNDATION FOR DIGITAL TRUST

SEDI begins with a foundational principle: identity belongs to the person, not the government. The government's role is not to create or control identity but to endorse and protect it as a matter of public trust.

This reflects the founding idea of the United States, that all just powers of government derive from the consent of the governed. SEDI recognizes it is the role of the state to act as a trusted endorser, verifying an individual's asserted identity and then issuing an endorsed credential mathematically bound to a digital identifier that the individual alone controls.

A hierarchy of values is used to establish priorities for SEDI requirements, the highest being to protect individual rights (including privacy), safeguard children and the vulnerable, and strengthen families and communities. Operational goals such as interoperability, efficiency, convenience, or private-industry profits are recognized as legitimate but subordinate to these higher values and may never justify compromising them.

SEDI BASICS

1. **Comprehensive Legal Framework -** Before implementing any digital identity system, states should establish a comprehensive legal and governance framework that protects an individual's rights and ensures accountability. The SEDI Model provides the structure and principles to define this framework. It requires that states adopt:

    - clear governance structures;
    - comprehensive program requirements;
    - enforceable standards for how digital identity systems operate;
    - open standards and open protocols;
    - explicit provisions for transparency;
    - separation of duties;

- a right to paper;
- enforcement mechanisms;
- and independent audits.

2. **Individual Control** - With SEDI, an individual creates a globally unique digital identifier using cryptography that they alone control. After verifying the individual's real-world identity, the state digitally signed credential that endorses, not creates, the individual's identity, which is cryptographically (mathematically) bound to the provided identifier. The individual's identifier can be thought of as a keyring, a foundational digital starting point to which verifiable credentials can be attached. Licenses, permits, certifications, and other credentials are like keys a person might add to their ring, all under their exclusive custody and control within a digital wallet of their choosing.

3. **Privacy** - SEDI implements a decentralized, peer-to-peer approach. Credentials stored in a user-controlled wallet can be verified with mathematical proofs, eliminating the need for privacy-invasive 'phone-home' checks to a central authority, issuer, database or proxy. Individuals can prove facts (such as age) without revealing unnecessary details (such as sex, height, or address). No tracking by other parties is permitted when a SEDI credential is used.

4. **Parental Rights and Delegation** - With SEDI, parents are able to manage their children's digital identity and any associated credentials. In today's digital world, identity and data are too often used to exploit children rather than protect them. SEDI gives parents the technical tools to protect their children from those who would misuse their identity or personal data for profit or manipulation. It also enables delegation, allowing a legally appointed guardian to act on behalf of a vulnerable adult.

5. **Critical Public Infrastructure and Security** - SEDI expects digital identities to be under constant attack by nation-state actors, and some will be compromised. SEDI breaks new ground in security, providing both individuals and government with powerful means to detect compromise, contain any intrusion, and fully and rapidly recover. SEDI credentials are verifiable offline and can continue to function securely during outages, disasters, or attacks.

6. **Backward Compatibility** - SEDI is backwards compatible with existing technologies in the digital identity ecosystem. This ensures that individuals, states, and organizations can transition toward full SEDI compliance without disruption or loss of functionality. Backward compatibility makes SEDI both principled and practical, allowing advancement while maintaining continuity.

SEDI OPPORTUNITY

The benefits and capabilities of SEDI will be profound, providing a foundation for individuals and businesses to derive utility and for the free market to create new value-added solutions, including:

- Proof of identity;
- Replacement of usernames, passwords;
- Consent, permission, and agreement;
- Delegation;
- Management of personal data;
- Agentic AI;
- Government records (birth certificates; school transcripts, property records);
- Age verification;
- Peer-to-peer communication;
- Change of address.

Above all, SEDI is a rights-first, decentralized identity model that will empower individuals and families to control their data and privacy, protect children from digital exploitation, and safeguard democratic trust. SEDI will strengthen states and the free market generally by reducing fraud, enabling secure and efficient transactions, and fostering innovation. Most importantly, it will project freedom to the world, demonstrating that America can lead the digital age by example, anchoring technology in liberty and constitutional order.

A CALL TO ACTION

Utah invites every state to join the State-Endorsed Digital Identity Consortium to create a better digital identity and digital future together.

CONNECT WITH THE TEAM

Marvin Dodge
Executive Director, Utah Department of Government Operations (DGO)
marvindodge@utah.gov

Alan Fuller
Chief Information Officer, DGO, Division of Technology Services
alanfuller@utah.gov

Christopher Bramwell
Chief Privacy Officer, DGO, Utah Office of Data Privacy
christopherbramwell@utah.gov

Joe Jackson
Chief Technology Officer, DGO, Division of Technology Services
joe@utah.gov

Micah Vorwaller
Deputy Chief Privacy Officer, DGO, Utah Office of Data Privacy
mavorwaller@utah.gov

George McCewan
Privacy Architect, DGO, Utah Office of Data Privacy
mcewan@utah.gov

LEARN MORE ABOUT THE SEDI CONSORTIUM

Email us at SEDI@utah.gov to learn more about the SEDI Consortium.