TSIT TREASURY SOLUTIONS IT

Cybersecurity by Design: Reimagining Digital ID for American Resilience

By Tricia Gallagher
June 22, 2025

Overview

The United States (U.S.) has reached a pivotal moment. As global digital infrastructure accelerates, it is no longer sufficient for U.S. cybersecurity and identity systems to merely evolve — they must be reimagined.

The recent rollback of Biden-era policies on cybersecurity and Digital Identity (Digital ID), including Presidential Executive Order 14144,[1] presents the Trump administration with an opportunity to lay the foundation for U.S. modern, secure, and privacy-preserving Digital ID infrastructure. This strategy must align with national security and financial modernization and inclusion goals, while upholding democratic values.

Digital ID systems, a critical building block for digital-asset ecosystems, are essential for modernizing payments, increasing government efficiency, enabling financial inclusion and restoring U.S. financial leadership in a fast-evolving global digital economy. To unlock these benefits, the U.S. needs a coherent national Digital ID strategy that leverages decentralized technologies, biometrics and cryptography while avoiding the surveillance risks of centralized architectures. Only then will the Trump administration truly unleash U.S. business innovation around digital assets.

Why a U.S. National Digital ID Strategy Is Urgent

The U.S. remains dangerously exposed to identity fraud, data breaches, and systemic inefficiencies. Legacy infrastructures were never designed for the speed, complexity and threat surface of today's evolving digital ecosystems. Attacks such as the Equifax and OPM breaches, and the 2023 MOVEit vulnerability, demonstrate that centralized repositories of personally identifiable information (PII) are irresistible targets for cybercriminals and hostile nation states. [2]

[1] https://www.forbes.com/sites/emilsayegh/2025/06/07/trump-drops-a-cybersecurity-bombshell-with-biden-era-policy-reversal/?utm

[2] https://www.cisa.gov/news-events/cybersecurity-advisories/aa23-158a

Further, the rise of generative AI and deepfake technologies has rendered traditional identity checks increasingly ineffective. The GAO's 2024 Science and Tech Spotlight [3] highlights synthetic-identity fraud as a mounting threat to public systems, compromising public benefits, delaying disaster aid and giving way to improper payments and federal fraud losses.

As U.S. government services migrate toward blockchain-based digital payments or decentralized finance (DeFI), identity verification must keep pace. Yet most systems still rely on outdated centralized Personally Identifier Information (PII) and credit files and knowledge-based authentication. Without reform, millions will remain excluded from services, and fraud will continue to rise.

Abroad, China is exporting a surveillance-based Digital ID model through its Belt and Road Digital Silk Road initiative. [4] This model conflicts with U.S. democratic values and is spreading rapidly across the Global South. The European Union has taken the lead in the opposite direction by deploying interoperable Digital ID wallets under its electronic Identification, Authentication and Trust Services (eIDAS 2.0) regulation designed to create a pan-European digital identity framework with robust user privacy protections and citizen control over personal data. [5] The U.S. risks falling behind unless it chooses a clear direction.

Understanding the Technology Models: Centralized, Decentralized, and the Hybrid Approach That Can Work for the U.S.

Modern digital identity systems can be broadly classified into two architectural models: centralized and decentralized (Self-Sovereign Identity, or SSI). For U.S. policymakers, understanding the distinction is essential to building secure, user-centric, and scalable identity infrastructure.

In centralized models, a single trusted authority—such as a government agency like the Department of Motor Vehicles (DMV)—issues and stores credentials in its own database. This creates a "honeypot" of sensitive data, vulnerable to breach and surveillance. Verification is performed through online query of the user's credential to

[3] https://www.gao.gov/products/gao-24-107292

[4] https://www.biometricupdate.com/202501/chinas-use-of-ai-biometrics-pose-significant-persistent-threats-dod-says

[5] https://commission.europa.eu/strategy-and-policy/priorities-2019-2024/europe-fit-digital-age/european-digital-identity_en

the central database maintained by the issuer. This model is characterized by trusted and standardized credentialling for Digital IDs, but has a high risk for breach and surveillance.

In decentralized models, credentials are issued by trusted entities—not necessarily central authorities—and stored locally on the user's mobile device. Verification is conducted via blockchain-based trust registries and cryptographic techniques rather than traditional database lookups. These systems offer the highest privacy and resilience, but require user education and technical maturity.

A hybrid model balances the best of both: centralized issuance, decentralized storage, and decentralized verification. Credentials are issued by a trusted central authority (e.g., DMV), stored in a user-controlled digital wallet (typically on a smartphone), and verified using open standards that enhance both privacy and trust.

Key technologies working together in this model include:

- **Decentralized Identifiers (DIDs):** These are unique, user-owned digital identifiers stored on a blockchain or distributed network. Instead of being issued and managed by a central entity, a DID gives the user control. When a DID is checked, it points to a "DID document" that contains the public keys and instructions needed to confirm the identity of the user or credential issuer.
- **Verifiable Credentials (VCs):** These are digital versions of things like driver's licenses, diplomas, or employee IDs. They are securely signed by the issuing authority and stored in the user's wallet. When needed, they can be shown to a verifier to prove something—without the verifier having to contact the original issuer.
- **Zero-Knowledge Proofs (ZKPs):** These allow users to prove something—like being over 18 or residing in a certain state—without revealing more than necessary. Instead of showing a full birth certificate, a ZKP lets the user prove just the fact that matters, keeping personal information private.
- **Blockchain infrastructure:** Serves as a tamper-resistant, decentralized public ledger that holds the cryptographic "receipts" needed to verify credentials and DID documents. It also hosts revocation registries—lists that show whether a credential has been suspended or canceled. Unlike traditional databases, this infrastructure has no single point of failure and offers transparency by design.

The hybrid design avoids the risks of centralized databases by keeping sensitive personal data on the user's own device rather than in government-controlled systems. If a credential (like a driver's license or identity card) needs to be canceled or suspended, the issuing authority can update a revocation list that is published on a tamper-resistant blockchain registry. One example is the W3C's Status List 2021, which allows verifiers to instantly check whether a credential is still valid, without needing to contact the issuing authority directly.

This makes revocation effectively real-time, while also preserving privacy: law enforcement or service providers can see that a credential is revoked, but they don't see the user's full identity unless strictly necessary. This approach ensures security and accountability without enabling mass surveillance. It reflects best practices recommended by institutions like the National Institute of Standards and Technology (NIST) and the World Economic Forum (WEF), which support privacy-preserving, decentralized trust models as the foundation for future Digital ID systems. [6] [7]

U.S. State-Level Digital ID Efforts Are Mostly Characterized by Centralized Storage of User Data

Today, most states are pursuing centralized or federated models where digital or mobile driver's licenses (mDLs) are stored in commercial wallets like Apple or Google where users control which data from their wallet they want to share - but these solutions rely on real-time validation from centralized state systems. [8] [9]

Only Utah is exploring or piloting a decentralized approach based on Self-Sovereign Identity (SSI), where users store verifiable credentials in their mobile wallet and prove their identity using cryptographic signatures—without a centralized database check. [10]

These initial efforts make clear the need for a coordinated U.S. federal strategy for a more secure approach for national Digital IDs where states remain the credentialing authorities and enrollment engines—they are trusted, local, and already issue vital documents like driver's licenses and voter IDs—but storage of user data or PII is decentralized. Importantly, without common standards, privacy guidelines, and technical infrastructure support from the federal level, U.S. innovation will stall.

Digital ID and Financial Inclusion: Today, modern identity systems are essential for reaching the unbanked and improving government benefit disbursements. Millions of Americans cannot open bank accounts because they lack traditional IDs or credit files. A portable, verifiable Digital ID—issued by states and backed by federal policy—would

[6] https://csrc.nist.gov/pubs/sp/800/63/4/ipd

[7] https://www.weforum.org/publications/reimagining-digital-identity-a-strategic-imperative/

[8] https://idscan.net/mobile-drivers-licenses-mdl-state-adoption/#:~:text=As%20of%20October%202023%2C%20the,these%20IDs%20at%20select%20airports

[9] https://www.dmv.ca.gov/portal/ca-dmv-wallet/mdl-privacy-policy/?utm

[10] https://www.biometricupdate.com/202304/utah-mandates-blockchain-pilot-for-digital-id-issuance?utm

unlock access to financial services, enable secure disaster aid, and accelerate the phase-out of paper checks.

Risk Mitigation Considerations

To avoid fragmentation and uphold privacy, the U.S. federal government must define common assurance levels, certify digital wallets against uniform standards, and establish interoperable revocation mechanisms. A federated trust registry—linking federal and state agencies with private-sector issuers and verifiers—can help coordinate these efforts and promote cross-jurisdictional interoperability.

Emerging fraud techniques, including deepfakes and synthetic identity attacks, must be addressed through liveness detection, AI-driven risk scoring, and hardware-based security protections. Critical biometric and behavioral data should be protected via secure enclaves—physically isolated area of a device's processor—and on-device storage, which must be mandatory to reduce exposure to centralized breaches.

To ensure both accessibility and resilience, wallets should include robust recovery mechanisms, such as social recovery, biometric fail-safes, and encrypted recovery keys.

Advances in edge computing—processing data locally on a user's device (like a phone or smart card) rather than sending it to a remote server or cloud for computation—and secure enclaves now allow fraud detection and anomaly analysis to occur locally on the device, limiting the need to transmit sensitive data. When combined with zero-knowledge proofs (ZKPs) and blockchain-based credential verification, these technologies offer a scalable path to a privacy-preserving, resilient, and fraud-resistant digital identity system.

Summary and Conclusion

Digital identity is not just a cybersecurity concern—it is a foundational pillar for economic inclusion, public service delivery, and national resilience. A U.S. strategy for Digital ID must protect privacy, enhance security, and unlock innovation in payments, identity verification, and benefits disbursement.

The Trump Administration has an opportunity to lead. By defining Digital ID as critical infrastructure, the U.S. can lay the groundwork for a system that reflects American values—one that safeguards civil liberties, resists surveillance, and restores global leadership in digital governance. The administration should take decisive, standards-based action that aligns with both market forces and public trust:

- **Issue a National Executive Order** declaring Digital Identity as critical infrastructure.
- **Establish a Federal Task Force** to define architecture standards and implementation guidelines, with input from states and the private sector.
- **Fund pilot programs** across SSA, FEMA, and state agencies using open-source, standards-based digital wallets that reflect a decentralized, user-controlled architecture.
- **Mandate open technical standards** to ensure interoperability and prevent vendor lock-in.
- **Launch a Public Trust Campaign** to frame Digital ID as a pro-privacy, pro-security, and pro-America initiative—educating the public on its benefits and protections.

Roadmap for Action (Next 12 Months)

- **Months 1–3**: Issue Executive Order and launch the federal task force.
- **Months 4–6**: Begin pilots at SSA, IRS, and FEMA with decentralized architecture and wallet interoperability.
- **Months 7–9**: Expand pilots to five states, prioritizing unbanked populations and benefit disbursement.
- **By Month 12**: Publish a National Digital Identity Strategy aligned with NIST SP 800-63-4 and principles of decentralized identity, privacy-by-design, and resilience.

By taking this path, the U.S. can shift from fragmented, insecure legacy systems to a unified, privacy-preserving digital identity infrastructure that empowers individuals and strengthens national security.