

Reclaiming Digital Identity

Verifiable Credentials (VCs) & Decentralized Identifiers (DIDs)

A Promising But Premature Policy Mandate

William Peracchio · IGA-236: Cybersecurity, Technology, Policy & Law · Harvard Kennedy School · Spring 2026

THE PROBLEM

Who Controls Your Digital Identity?

Today's identity infrastructure relies on a handful of corporate intermediaries and centralized government databases. When you log in with Google or use a national ID registry, you depend on an institution to vouch for you — and that institution collects data on every interaction. These structural failures result in:

**Surveillance by Design**

OAuth/OIDC notifies the identity provider on every login. Cross-site behavioral profiles are built invisibly, without user consent or knowledge.

**Catastrophic Breach Risk**

Centralized credential databases are high-value targets. The 2017 Equifax breach exposed 146M Americans' identity data in a single incident.

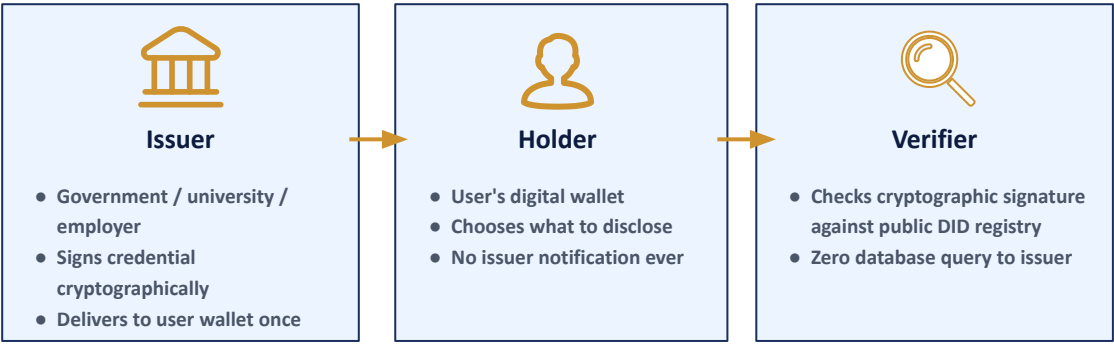
**No Selective Disclosure**

Proving you are over 21 requires revealing your full name, address, and birthdate — data irrelevant to the transaction.

HOW IT WORKS

The VC + DID Model

Verifiable Credentials (W3C 2022) and Decentralized Identifiers create a three-party architecture that eliminates the central intermediary entirely:



KEY INSIGHT: After initial issuance, verification is purely peer-to-peer. The issuer never learns when or to whom you present a credential.

REAL-WORLD DEPLOYMENTS

It's Not Vaporware

EU eIDAS 2.0

Mandates W3C-compatible digital identity wallets for all 450M EU citizens. Target: 2026.

This is the most ambitious deployment of VC/DID infrastructure to date.

Time: 2024-Present | [Link to Current Status](#)

US DHS / CBP

Piloted verifiable digital travel credentials for border processing, reducing reliance on centralized biometric databases.

Time: 2018-2023 (Pilot) | [Link to Current Status](#)

Microsoft Entra

Verified ID deployed in enterprise contexts for employment and education credential verification — production scale.

Time: 2022-Present | [Link to Current Status](#)

GLEIF

Global Legal Entity Identifier Foundation issues organizational VCs for corporate identity, replacing paper-based KYC in finance.

Time: 2014-Present | [Link to Current Status](#)

SIGNIFICANT BARRIERS TO ADOPTION

Why a Mandate Would Be Premature

**Wallet UX & Key Recovery**

Shifting custody to users also shifts risk. If a user loses their wallet or private key, recovery is non-trivial. There is no mature, standardized recovery mechanism — a fundamental problem before mass adoption is responsible.

**DID Method Fragmentation**

Multiple competing DID methods (did:web, did:key, did:ion, did:ethr) create interoperability gaps. Mandating adoption before convergence on common methods would recreate current silos in a new form.

**Legacy Transition Costs**

Federal agencies run identity systems built on decades-old infrastructure. Transition costs — technical, organizational, and political — are enormous. Political will is a prerequisite, not a technical problem.

**Accountability Gaps**

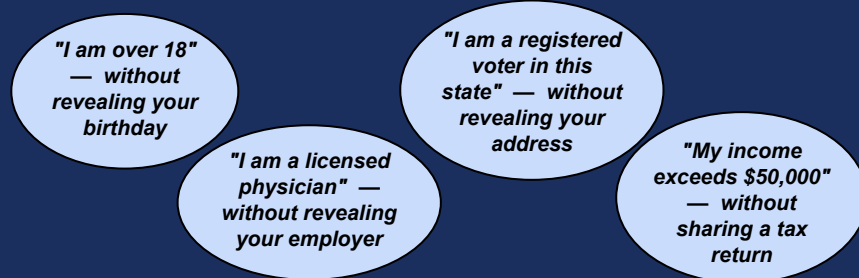
Pseudonymous credentials can make it harder to enforce court orders, revoke access from bad actors, or conduct lawful investigations. Governance frameworks must resolve this tension before broad deployment.

THE FRONTIER

Zero-Knowledge Proofs

VCs already improve dramatically on today's model — but ZKP-enabled credentials take **Selective Disclosure** to its logical conclusion: **Derived Disclosure**. The formal academic term is anonymous credentials, dating to Chaum (1984) and now being standardized for the post-quantum era.

Instead of revealing an attribute (through some complicated cryptography beyond the scope of this paper), you prove a predicate about it:



Already in Production: zk-SNARKs (Zcash), BBS+ signatures (MATTR), zkLogin (Sui)

POLICY RECOMMENDATION

Invest, Standardize, and Pilot — Not Mandate Yet

VCs and DIDs represent a genuine architectural improvement over the status quo. But the barriers to full adoption around the world are real. A federal mandate today would risk locking in immature standards and creating new inequities for users without technical sophistication.

The appropriate policy posture is targeted investment and staged adoption:

1 Fund Interoperability Research

Direct NIST to designate 2–3 approved DID methods for government use and fund convergence work.

Without a common standard floor, VC adoption will fragment along vendor lines — recreating today's silos in a new form.

2 Launch Targeted Federal Pilots

Authorize DHS, SSA, and State to run time-limited VC/DID pilots for high-friction, low-risk credentials (professional licenses, education records).

Gather evidence on UX, security, and equity before broader rollout.

3 Enact an Issuer-Tracking Prohibition

Classify credential presentation logging by issuers as a privacy violation under federal law, with FTC enforcement.

This can be done now, independently of adoption pace, and prevents future surveillance creep regardless of which system wins.