What is Digital Identity?

CONTRIBUTING AUTHOR — SEPT. 2024

Elizabeth Bynum Sorrell
Senior Research + Engagement Manager, Digital Benefits Network

GEORGETOWN UNIVERSITY | beeckcenter social impact + innovation | Digital Benefits NETWORK

The Digital Benefits Network (DBN) began researching digital identity in public benefits in 2022. We started this work because we recognize that digital identity presents challenges for public benefits applicants, beneficiaries, and state agencies. Our research so far has included:

- Landscape research documenting authentication and identity proofing practices in initial online benefits applications;
- A guide to federal government activities related to digital identity; and
- A review of promising digital identity design patterns.

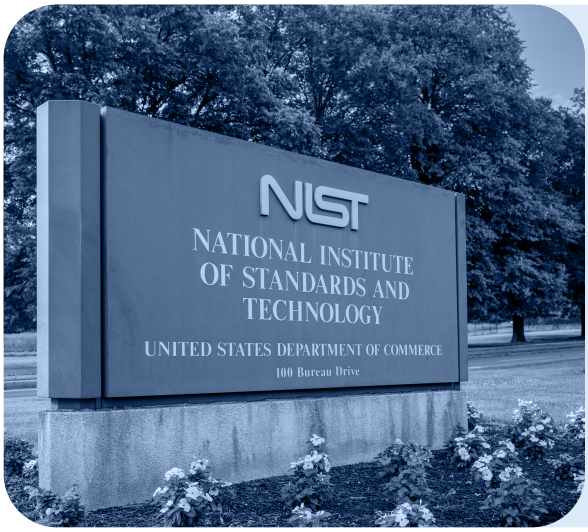
To improve digital identity in public benefits, practitioners need information about the broader landscape. In this updated primer, we:

- Introduce the concept of digital identity, and
- Provide brief snapshots of digital identity-related developments internationally and in the U.S.

Defining Digital Identity

When we talk about digital identity, we're talking about how we can tell someone else about ourselves online. In the United States, the National Institute of Standards and Technology (NIST) issues guidelines for managing digital identities. In their most recent draft guidelines, NIST explains:

> "A digital identity is always unique in the context of an online service. However, a person may have multiple digital identities and while a digital identity may relay a unique and specific meaning within the context of an online service, the real-life identity of the individual behind the digital identity may not be known."



Let's put this in context.

When you want to access a service online, you may need to create a specific digital identity. For example, you might make a username and account to place an online shopping order. That username or account represents you when you interact with that retailer online. But creating an account or username doesn't mean a service provider knows who you are in the real world. As NIST has also noted, you might represent yourself online in many, distinct ways. Think for a moment about the number of accounts you have across the internet.

In some higher risk interactions, where sensitive information or funds are exchanged, it may be useful for a service provider to know who is accessing a system. When a service provider wants to know who you are in real life, they may use identity proofing and authentication processes to:

- Link a digital identity to a real-world person, and/or
- Confirm that the same person is accessing a service each time.

IDENTITY PROOFING	AUTHENTICATION
"The process by which a credential service provider (CSP) collects, validates, and verifies information about a person." - NIST Identity proofing aims to establish confidence that someone is who they claim to be. If identity proofing is being used, your user experience might involve answering questions about your credit history or uploading a selfie and images of your photo identification. For more information, see our Glossary.	"The process by which a claimant proves possession and control of one or more authenticators bound to a subscriber account to demonstrate that they are the subscriber associated with that account." - NIST Authentication is how a service provider tries to confirm that a person accessing an account is the same person each time. The user experience might involve creating an account and then entering a password or pin, or inputting a one-time passcode, when coming back to that service. For more information, see our Glossary.

Identity proofing and authentication can present opportunities (for example, enabling individuals to transfer information from one application to another or supporting the pre-filling of forms, etc.). But identity proofing and authentication can also create barriers for users who may face internet access issues, document access issues, and/or language access issues, or lack consistent email or device access.

In our primer on Digital Identity + Public Benefits, we describe how identity proofing and authentication show up in benefits applications. In that primer, we also explore equity and security concerns related to common identity proofing methods: use of biometrics and knowledge-based verification. When people talk about digital identity, though, they may also be talking about other processes, like the creation of digital identification credentials—or digital IDs—and government identification programs.

International Snapshot

National Digital Identity Programs + Identity for Development

In 2021, the World Bank estimated that 850 million people lacked official identification. The United Nations' Sustainability Goal 16.9 aims for everyone to have a legal ID by 2030. Digital identification is often framed as a way to close this identification gap. Many countries already have or are exploring national digital identity systems (e.g., Estonia, Indonesia, Nigeria, and Ukraine, among others). There are also international efforts to develop digital identity standards; for example, the European Union's Digital Identity Framework Regulation.

The World Bank's Identity for Development (ID4D) agenda promises financial inclusion and other benefits. But global NGO leaders and academics have raised human rights concerns. Civil society groups worry that digital identification programs exclude some populations. Academics also point to the potential for surveillance and exclusion if digital identification systems become the only entry points to services. Another important consideration is the degree of centralization in a system. Blockchain and other distributed ledger technologies could give users more control over their information. But social science researchers argue that these technologies are not inherently more empowering.

India's Aadhaar is one of the better known digital identification systems. The government-backed system issues unique, 12-digit identification numbers linked to biometric data. Following its launch, academics have raised concerns about misuse of Aadhaar data. Social scientists have also explored how Aadhaar could exclude citizens who cannot register. Technical glitches in Aadhaar's system have also blocked individuals from receiving needed benefits. Those issues complicate claims that Aadhaar can promote inclusion or reduce corruption.

U.S. Snapshot

Digital Identity Standards Development + Mobile Drivers' Licenses

NIST issues guidelines for identity proofing, authentication, and federation. In the guidelines, NIST provides requirements for federal systems. State, local, tribal, and territorial governments are not required to follow NIST guidelines, but may make reference to the guidelines as they offer a technical framework that may not be available elsewhere. Many private companies also rely on or refer to the NIST guidelines. NIST updated its digital identity guidelines in 2017 and is currently revising them. For more on the process, visit NIST's website.

Mobile drivers' licenses (mDLs) are the main way government-issued credentials are being digitized in the U.S. A mobile driver's license is a digital representation of a driver's license on a mobile device. As industry groups point out, mobile driver's licenses could enable consumers to use government-backed credentials online. However, civil liberties groups worry that mDLs could exclude individuals who do not have devices and create new pathways for tracking. Civil liberties groups also suggest that mDLs could make identification requests easier and more frequent, and have expressed concerns about the role of third-party vendors. Still, mDLs could enable users to choose what information they share. For example, when making an age-restricted purchase, someone with an mDL could choose to share only information about their age.

According to the American Association of Motor Vehicle Administrators (AAMVA), more than half of U.S. states have deployed or are exploring mDLs. The International Standards Organization (ISO) has developed standards for using mDLs in person (ISO/IEC 18013-5) and is developing standards for online, "unattended" use cases (ISO/IEC 18013-7). NIST is also testing these standards and recently announced the organizations collaborating to explore mDL implementation for their first use case, financial services. Strong standards will likely be key for mDL success. For example, in 2022, security researchers demonstrated that credentials for an Australian digital driver's license program could be forged.

The U.S. does not have a national identification program or card, however the federal government has invested in shared authentication and identity proofing infrastructure. Login.gov provides a shared digital infrastructure for authentication and identity proofing and all federal agencies can use it. The service also partners with state and local governments (for example with state workforce agencies through the Department of Labor). Following a 2023 report from the General Services Administration's Office of Inspector General (OIG), Login.gov updated their documentation to say that the services "continue to work toward achieving certification of compliance with [NIST's] IAL2 standard from a third-party assessment organization." In a reversal of their previous stance, Login.gov announced plans to add facial matching to the service as one identity proofing pathway. Login.gov is piloting that approach as well as increased in person-verification options in 2024.

For a point-in-time, deeper dive on federal-level activity related to digital identity in the United States, check out our "Logging In and Providing Proof: A Guide to U.S. Government Actions on Digital Identity" from March 2023.

Conclusion

The status quo around digital identity presents challenges in the public benefits sector and beyond, as data breaches and identity theft are persistent issues. We recognize that these challenges cannot be solved by one sector alone. As we have previously written, we think the U.S. needs a national digital identity strategy, backed by standards that take into account equity, accessibility, privacy, data protection, potential harms and disparate impacts, evolving security threats, and future technologies.

Navigating digital identity choices requires government agencies to evaluate tradeoffs between the need for identification and privacy and surveillance risks. Effective, equitable implementation of new identity technology may be facilitated through design justice approaches that engage and incorporate user experiences, and establish clear data protection standards. Through our work, the DBN aims to empower state benefits administrators to evaluate digital identity approaches. We believe state agencies should use resources like the NIST Digital Identity Guidelines and risk management model to determine whether and at what level authentication and identity proofing solutions are necessary for a given benefits program context.

GET IN TOUCH

In our future work on digital identity, we will focus on the public benefits space, while keeping the larger landscape in mind. To engage with the DBN on this topic, please visit our Digital Identity Community of Practice page, or reach out via digid@georgetown.edu.