JORDAN SHAPIRO

Digital ID: the secure and private future of identification Part 1: Introduction

January 2024

Executive Summary

Digital identification is coming to America.

With the proliferation of computers, smart phones, and internet access, many services that were once only available in person or through traditional means have moved online. This digital transformation has made it easier for people to access a wide range of services, such as banking, shopping, communication, entertainment, and even healthcare, from the comfort of their homes or on-the-go.

Digital services offer more transparency, faster information sharing, and better engagement with citizens.[1] But there is one major problem with digitalization: how to prove who you are online securely. Without structures to confirm identity online, there are no checks on fraud for online services. Online identity verification is not just a government problem, private companies, too, find themselves at the forefront of the online identity challenge. New regulations are placing companies in charge of verifying online identity, especially for young users.

The key solution to this challenge being adopted around the world is the digital ID.

The European Union, India, Singapore, Estonia, Panama, the United Kingdom, and Nigeria are just some of the countries pursuing or implementing their own versions of digital identification.

A digital ID is similar to other forms of identification, containing essential information such as a photo, name, address, date of birth, and expiration date. However, it introduces a significant advancement. Unlike conventional physical licenses, digital IDs are designed to be easily read by machines through means like a QR code, a wireless chip, or even biometric authentication, akin to unlocking a smartphone.

Digital IDs replace low-tech and less private means of online identity verification. They do this by using encryption, and other privacy preserving technologies to only sharing essential information, not the entire document.

The U.S. is pursuing digital identification. However, unlike the countries above, the US lacks a national identification system, which results in a fragmented digital ID landscape.

[1] "Digital and Effectiveness," June 20, 2023, https://uca.hal.science/hal03620113/file/Digital%20and%20effectiveness.pdf.

This fragmentation means that Americans don't have a single, standardized way to verify their identity online.

Instead, local, state, and federal government agencies and departments choose different online verification methods. These processes typically require citizens to provide sensitive information such as answering multiple-choice questions about past addresses and vehicles or uploading identity documents to government websites via secure identity management systems (which inherently excludes the millions of Americans without any form of identification). They lack privacy, are insecure, and sometimes are easily forgeable.

The absence of uniformity poses a significant challenge: there is no universal method for proving our identities online, essentially leaving Americans without a digital identity verification at all.

Digital IDs are a key tool to manage online fraud, youth online safety, and even online banking and government service delivery.

However, these benefits can only be fully realized in a private, secure, accessible, and interoperable system. Currently, none of the U.S. offerings boast all of these qualities.

Lacking these protections, digital IDs can become repositories for personal data for hackers and bad actors to exploit.

Furthermore, when identification is integrated with essential public and private services, it must be available to all.

Billions of people around the world have digital IDs. Looking abroad at other digital ID systems we can find the best practices and challenges to avoid.

This paper explores the outlook for the United States's fragmented approach to digital IDs relative systems around the world. First, it will introduce digital IDs. Next, it will examine the benefits and opportunities of digital driver's licenses in America and abroad. The third section explores the challenges requiring data privacy, cybersecurity, accessibility, and interoperability. Finally, it will look at digital IDs abroad and in the U.S. to highlight lessons learned and provide recommendations to Congress for the next steps.

The key recommendations are as follows:

- Congress needs to pass data privacy protections at the national level so everyone's mDL data is protected anywhere they use their digital ID.
- Congress needs to standardize the underlying technical frameworks, called application programming interfaces (APIs) and software development kits (SDKs), so every digital ID has the same security and interoperability across state lines.

- Congress needs to ensure no one gets left behind by opening pathways to access digital IDs even without a physical ID card.

U.S. Identification Challenges

More than most other sectors, the public sector is responsible for offering identity documents and authenticating recipients of government services. Building on this responsibility, digital IDs become the key component to verify identity and streamline the online service delivery process.

The United States, however, struggles with identification.

Whereas most countries provide a single national ID card to all citizens, the US pursues a decentralized approach whereby every U.S. state (and territory) offers a state-specific ID card called driver's licenses or non-driver ID cards. The process is onerous, particularly for under-documented and undocumented folks. This is in contrast to places like Estonia, which provides an ID card from birth.

This system is mirrored in the shift toward digital IDs.

Countries like Singapore, Estonia, and India all provide national digital IDs for every citizen.

The US approach, however, relies on already having documentation or a physical ID card to be able to verify online.

For Americans who do have access to physical ID cards, the online verification challenge doesn't end there.

As U.S. states are in charge of providing identification, they are also in charge of digitalizing identity verification. Every state appears to be pursuing its own unique method.

California and Louisiana offer the ability to add a driver's license to a smartphone app. New York's Department of Motor Vehicles requires uploading identity documents via a secure online system run by Okta, an identity management company. The federal government offers a system similar to New York's but via a different identity management company, id.me. Maryland, Colorado, and others are partnering with Apple to add driver's licenses to smartphone mobile wallets.

With so many systems, there is little room for interoperability or the ability to use a digital ID in all places where it's needed. Giving so many different companies access to identity documents isn't private and it isn't secure.

And still, not every state offers a digital option, leaving millions of Americans behind.

To be clear, digital IDs are not without their own privacy, security, and access concerns, which will be explored in successive sections. However, globally, billions of people already use digital IDs, allowing lawmakers to appropriate the best practices and learn from the challenges.

The next section outlines unpacks the use cases for digital IDs.

Digital IDs around the world

Stay tuned for Part 2