Government's Role in the Growing Digital ID Market

By Eugene Le Roux
VP, Digital Government

Digital access to conventional services is expected today. Once a convenience, COVID restrictions made digital transactions a necessity for all types of commerce including government services.

However, accelerating adoption of digital services without well-designed user authentication increases the risk of fraud and bad actors that prey on unsuspecting consumers. Therefore, identifying the consumer has become essential for digital transactions. Biometrics-authenticated Digital Identification (DID) is increasingly prevalent in commercial, financial and government applications.

GROWTH OF BIOMETRICS IN IDENTITY RESOLUTION

Long trusted to secure facility access, biometrics now safeguard transactions on mobile financial apps, desktop systems and online platforms. Logging in with face recognition (provided it is liveness enabled and matched against an original trusted source) is more secure and convenient than knowledge-based criteria, one-time passwords and cumbersome back-end processes.

Adoption of face recognition accelerated during the pandemic as demand for remote, touch-free services intersected with advancements in fast, reliably accurate biometric algorithms. Many airlines and airports have automated preboarding processes using face recognition of travelers who opt in to use DID. Biometrics that can be used to secure digital wallets can verify identity in a variety of venues.

Several states are implementing or investigating official mobile driver's licenses (mDLs), and the Transportation Security Administration is testing using biometrics to process TSA PreCheck passengers who are also enrolled in American Airlines Mobile ID.

NEC is one of several third parties independently developing and supporting the technology used for DID. The National Institute for Standards and Technology (NIST) tests the accuracy of biometric algorithms against standard IAL2, but the government needs to establish a more encompassing national framework to ensure that independent systems meet interoperability and other standards.

The Biden administration has been asked to establish such a framework. In a letter to the administration, six groups with a shared interest in DID recommended that Biden's promised Executive Order include steps to accelerate the deployment of mDLs and the development of remote identity proofing solutions that meet standard IAL2.

"NIST made clear long ago that knowledge-based verification tools are not sufficient for identity proofing," the letter says in part. Among four points, the letter asks that the Executive Order "direct NIST to create a Digital Identity Framework of standards and best practices to help agencies at all levels of government establish attribute validation and other digital identity services in a way that is standardized and sets a high bar for security, privacy and equity."

FRAMEWORK ESSENTIALS

We believe federal standards must include **four key pillars** – authentication, accessibility, interoperability and data protection.

- **Authentication** now involves validating documents and needs to include matching live capture images of the applicant against ID images on record. Identity proofing is now only performed in person, but steps should be taken to establish trusted remote identity proofing with 1:1 and 1:n matching accuracy of face biometric algorithms.
- **Accessibility** is needed to make official driver's licenses and IDs more equally attainable. Certain populations have greater difficulty obtaining IDs. Remote identity proofing can help address transportation issues by providing access through mobile apps or government kiosks at additional locations. Kiosks and apps also make it easier to update addresses and other personal data.
- **Interoperability** is necessary for all agencies and jurisdictions to access vital information when it is needed. Just as anyone can read a physical ID card, all jurisdictions need to be able to decipher data on a cryptographic driver's license. Using a single Digital Trust Service with all state decryption keys is vital to signal reader technology that an mDL is authentic and belongs to the holder.
- **Data protection** is critical to protect personally identifiable information. Privacy by Design standards are important both to the mDL holder and any relying agency that wants to avoid risks associated with storing and safeguarding personal information.

DID AROUND THE WORLD

Several countries are ahead of the U.S. in developing frameworks for Digital ID programs, and there has been significant coverage of existing systems and attempts.

Estonia was an early pioneer, pairing digitalsignatures with physical ID cards in 2002. All Estonians are issued a state-issued eID, which has been updated over the years to use on smartphones and through an app called Smart-ID.

Germany automatically activates an electronic ID with every physical ID card issued to citizens over the age of 16. Less than half of the population has used the option: More than 62 million Germans have an ID card, but the chip is active in only 25 million cards.

Australia's DID is optional and entirely app-based. Participants set up and manage a DID through the myGovID app, choosing between a basic ID with limited information and limited access, a standard ID with document validation or a strong ID adding live capture face recognition.

The UK attempted a DID program in 2016, intending that Gov.uk Verify would be the standard way for citizens to prove their identity and access all online government services. Registration involved in-person identity proofing at a post office. Enrollment was anticipated to take 5-15 minutes, but sometimes took hours or failed entirely.

URGENCY FOR STANDARDS

The U.S. need to work quickly to establish its framework, because DID providers are already responding to burgeoning demand. People want the convenience, privacy and security that DIDs provide. Both commercial and government organizations want biometrics to help protect against ID and benefit fraud.

People who opt in for DID need only their face to log into several secure services. Personal information is secured on their mobile phone and they can share only what is needed for a transaction.

For example, a government-issued DID such as an mDL can be used to authorize age-restricted purchases without revealing unnecessary personal information. The DID holder controls their privacy by choosing to display just their ID photo and "over 21" status, rather than showing a card with their name, address, birthdate and weight.

Just as TSA PreCheck's enrollment of 1.3 million people shows that people want the convenience of streamlined screening, we believe the Mobile ID test will prove interest in rapid biometric verification.

Without a framework, DID implementations will continue to fragment across an expanding ecosystem. Interoperability is important, because reader technology needs to be able to decipher data from an issuer using different technology to generate and encrypt biometric signatures.

GETTING STARTED

The U.S. government established the Internet Engineering Task Force, the organization responsible for technical standards for the Internet Protocol suite (TCP/IP). The task force now operates independently under an international non-profit organization and cooperates with other standards bodies.

Standards organizations working toward interoperable 5G Open RAN technologies have private companies as contributing members of working groups that test standards and technologies.

A public private partnership could combine the two approaches. NIST already establishes standards for biometric technologies and is well suited to direct the process.

NEC has a robust R&D budget and continually invests in improvements. We are also committed to meeting standards and contributing to industry work groups. We welcome the opportunity to participate in the development of an interoperable DID ecosystem with reliable authentication, accessibility and data protection.

Join the ecosystem.

NEC has a Digital Identity Platform trusted by government agencies as well as financial and commercial organizations. It is built on Privacy by Design standards, and its face biometrics algorithm is highly rated by NIST.

Contact NEC to visualize your Digital ID solution and begin your journey forward.