Exponent®

THOUGHT LEADERSHIP

PUBLISHED 3Q 2019

Balancing Convenience and Security in Phone-Based Digital Identities

July 25, 2019

For over twenty years, the identity community has recognized that digital identity is the most secure form of identity. Computers can validate that a digital identity once created - remains valid, has not been altered, was issued by the proper authority, and is currently being held by the person to whom it was issued. This is in contrast to physical identities, like a driver's license, for which the primary mode of authentication is simple visual inspection of the credential and the bearer of the credential. Digital identities are typically held inside tiny digital vaults, known as secure elements, that are contained in government ID cards, chip credit cards, and passports that can be read electronically.

In recent years, individuals, agencies, and businesses have increasingly sought to replace electronic IDs with digital solutions on mobile phones. With their immense computing power, mobile phones can eliminate the need to carry a physical wallet or even a phone sleeve for credit cards and IDs. However, with convenience comes great risk and responsibility. Depending on the implementation, mobile phones may not be as secure as the single-purpose vaults found in current electronic IDs. If improperly secured, a mobile device can become a treasure trove of data that adversaries can exploit for financial or other gain.

Phone-based digital identities can achieve high levels of user convenience, security, and privacy if done well. Several considerations can help both government and commercial entities navigate trusted mobile device implementations including safeguarding biometric information; applying the three pillars of identity to build trust; and navigating an evolving regulatory environment.

Safeguarding Biometric Information

Mobile phones increasingly feature biosensors for user authentication. Fingerprint authentication, which matches a template generated from a user's full fingerprint, and facial recognition are the two primary biometrics in use today. While biometric authentication is secure and considerably more convenient than the use of strong passwords, it has a different threat model and corresponding risk landscape. Unlike passwords that can be easily changed if compromised, the risks associated with a stolen, unchangeable biometric are considerably higher. For this reason, all biometric data and computations on a mobile phone should be safeguarded in a secure area.

Device manufacturers can better safeguard biometric information by relying on a trusted execution environment (TEE) with secure key storage implemented in a mobile phone's hardware. These methods are a very effective, but as a device security measure, the full use of these features is often not available to third-party developers and their applications. For developers it is even more critical that full security architecture assessments are performed to ensure adequate user protections for their application's threat model.

Applying the Three Pillars of Identity to Build Trust

In addition to protecting biometric information, phone-based digital identities should also promote trust. A person or system to whom an ID is presented must be able to trust that the ID is valid, has not been altered, and is in the possession of the correct individual. The most secure ID systems combine the three pillars of

Balancing Convenience and Security in Phone-Based Digital Identities

identity: something a user has (e.g., a physical credential), something a user knows (e.g., a PIN number), and something a user is (e.g. a biometric). With secure spaces to store credentials, pin entry devices, and multiple biosensors, mobile phones have a unique ability to apply all three pillars of identity without the need for external support.

Our team at Exponent frequently partners with the U.S. government and select commercial entities to write, review, and test specifications for mobile credentials. Our goal is to ensure that a device can perform to desired security and privacy requirements both by itself and as a component within a broader system. Our work is informed by over twenty years of experience ensuring the durability and reliability of smart cards and other credentials. We actively participate in the American National Standards Institute (ANSI) and International Organization for Standardization (ISO) working groups on identification cards and related technologies and help write standards specific to physical characteristics, test methods, and interoperability. By applying this learning to the credentials stored in a digital device, our team can help our partners build trust in their digital identity solutions.

Navigating an Evolving Regulatory Environment

The regulatory, policy, and legal aspects of ID credentials that reside on a mobile device often pose a larger challenge than the technical execution of the system. Exponent is currently working with commercial entities, U.S. states, and the federal government on efforts to standardize security and privacy requirements. Within the identity community, there is a recognition that companies must work together on interoperable solutions if mobile-based credentials are to be useful both nationally and globally.

Some local legislation has been passed in this realm, including the Generic Data Privacy Regulation (GDPR), which came to into force in the European Union in May 2018. This legislation recognizes that companies need a proactive approach to engineering privacy-enhancing and secure solutions and implementations. Companies that fail to implement solutions in a privacy-enhancing and secure manner can face legal, financial, and brand-reputation risks.

While international standards for security and privacy requirements are not yet well-defined, we expect to see progress in this area over time. Our team at Exponent continues to work with both government regulators and commercial entities to provide input into what these standards could ultimately look like.

How Exponent Can Help

Exponent's multi-disciplinary team of engineers, data scientists, and privacy experts has been a leader in the digital identity community for over two decades. We can help manufacturers optimize the security, privacy, interoperability, durability, and reliability of current or future mobile devices and applications as they become a key, if not primary, ID management credential that users employ daily.

John R. Fessler, Ph.D., P.E.
Mechanical Engineering
Principal Engineer
Orange County
(949) 242-6005
jfessler@exponent.com

Brad A. McGoran, P.E., CSCIP, CSCIP/G, GIAC, ACE-M
Statistical & Data Sciences
Principal Engineer
Menlo Park
(650) 688-7013
mcgoran@exponent.com

Christopher Williams, Ph.D., CISSP
Statistical & Data Sciences
Manager
New York
(212) 895-8140
cwilliams@exponent.com