November 10, 2022

ISSUE BRIEFING: Digital Identity

The Issue: Digital identity is the digital representation of a subject. It must be unique in a given context, and it can be but is not always linked to a real person or entity. Digital identity helps governments and other organizations offer services online.

What does digital identity entail?
There are two fundamental components of digital identity: **authentication** and **proofing**. It is important to emphasize authentication is not proofing, and proofing is not authentication.

What is authentication?
Authentication allows users to pick up where they left off when making a return visit to a service (i.e., USER123 has returned). Authentication has nothing to do with being a real person or a specific person. It is only about return visits.

Authentication binds authenticators to an account. Authenticators include:

- Something you know, such as a password or security question,
- Something you have, such as a security key or cellphone, and/or;
- Something you are, such as fingerprints or your face.

Multi-factor authentication (MFA) or two-factor authentication (2FA) is when two or more authenticators from two different categories (know, have, are) are required. To be clear, requiring two authenticators from the same category is not MFA.

What is proofing?
Proofing confirms a digital identity is linked to a real and specific person (i.e., USER123 is this specific Jane Doe). It has nothing to do with returning to a service.

Proofing is rarely required online because it is burdensome, lacks affordable and accessible market solutions, and is often unnecessary. It only needs to be used when you truly need to know with whom you are interacting online or, in other words, when it would be a problem to give something, such as data, to the wrong person.

Proofing is necessary when you want to give someone sensitive information that they did not give you. Proofing includes three steps:

- Resolution: Of all the Jane Does, which Jane Doe are we talking about?
- Validation: Is this Jane Doe a real person?
- Verification: Am I actually interacting with this specific Jane Doe?

How do we decide what digital identity practices to implement?
Like every other element of running your organization, decisions around digital identity must be based on risk management. There are risks associated with imposing too many requirements on your customers, and there are risks associated with not imposing enough requirements to deter bad actors. Too much proofing also carries privacy and liability risks. Organizations should avoid collecting and holding personal data they do not need.

Decisions around authentication and proofing should be based on the service you are providing:

- Do users need to make return visits? Do they need to pick up where they left off? (Authentication)
- Do customers need to access sensitive data or services they did not give to you and you must not provide to the wrong person? (Proofing)

What are the trends in digital identity today?

- When it comes to authentication, passwords remain the most popular. While knowledge-based authentication seems to be trending downward, the use of biometrics is on the increase. Using physical tokens is only feasible in certain scenarios.
- Many organizations interested in implementing proofing have difficulty finding market solutions that meet their needs. Though the market continues to innovate, current solutions can be expensive and pose implementation challenges, particularly for certain populations[1].
- When proofing is implemented, it is usually through driver's license or passport checks. This method is imperfect for many applications but is one of the only options presently available.
- Federation is trusting a third party that has already done authentication and/or proofing. So far, there have been successful examples of federation for authentication, and some experts hope to see federation grow to include proofing.

Examples of digital identity in practice:

- Login.gov (General Services Administration)
- Mobile Driver's License (American Association of Motor Vehicle Administrators)
- Remote Electronic Notarization (NASS)

Acknowledgments:
NASS thanks Dr. Mike Garcia for his extensive contributions to this issue briefing. NASS also thanks the sponsors of our 2022 webinar on digital identity that made this issue briefing possible:

[1] Factors related to the digital divide, accessibility issues, and bias in facial recognition algorithms contribute to this.