accenture

Digital identity

Creating an environment of trust

Traditional IAM and Digital Identity are complementary tools that meet the same goals. Both are relevant in helping organizations develop trust, ensure privacy, increase security, provide an excellent user experience, and accelerate the business. As the lines of digital and reality mold into one encompassing experience, we have a great opportunity ahead.

As the world evolves to expand digital experiences and blend them with authentic in-person interactions, the importance of using the best standards from each discipline increases. Over the past 20 years, organizations have significantly invested in their IAM capabilities to allow their employees to do their job safely and ensure their partners can consume business services, and consumers can consume digital services. The biggest challenges I see in organizations in adopting a digital identity mindset are:

- Organizations do not have the appetite to implement another IAM solution. IAM solutions are complex and require months to years to roll out to an entire organization. Digital.
- Who is the source of truth for verifiable credentials? We've seen conglomerates form in specific industries and cross-industries to have a shared credential. For example, we see European banks and Telcos for conglomerates to share the same credential to consumers of their services. These are still siloed credentials.
- The scale of some of the underlying Digital Identity technologies has yet to be proven. Some organizations have Billions of daily transactions to authenticate and authorize users, machines, and services.

I believe these challenges can and will be overcome, and the industry is already in action. For our first challenge, we are seeing major organizations like Apple, Google, and Microsoft work together to embed open standards into their software and devices that facilitate secure user authentication and authorization using an open standard called FIDO 2.0.

Another essential standard for authentication, OIDC, was recently updated for the issuance and verification of verifiable credentials. This is important because almost every leading IAM software vendor supports these standards and will update their software to support the enhanced version. This will allow organizations to utilize Digital Identity capabilities using their existing IAM investments.

For our second challenge, we can leverage the concepts of e-passports and e-government-issued credentials. This emerging technology takes advantage of existing cryptography standards to safely identify a user. Combining these verifiable credentials into an identity wallet controlled and managed by users is critical. Identity wallets must allow users to authorize personal data for a given entity for a period of time and have confidence that personal data is anonymous and only used for the given transaction and discarded securely after the transaction. I also feel strongly that adoption will increase if these e-passports and government-issued credentials could take advantage of open standards such as FIDO 2.0 and OIDC.

Traditional IAM software is proven to meet today's scale and tomorrow's realities and the integration that I just described will mitigate scale concerns.

Consider a significant challenge almost all businesses face around fraud and business email compromise. Business email compromise (BEC) is a type of cybercrime in which attackers use email to deceive or trick individuals or organizations into transferring money, revealing sensitive information, or performing other malicious actions. BEC attacks typically involve impersonating or spoofing email addresses, domains, or user accounts to make fraudulent emails appear legitimate. Traditional IAM systems cannot prevent BEC.

One way to use verifiable credentials to prevent BEC is to use them to authenticate the identity of email senders and recipients. By requiring verifiable credentials to be presented before allowing access to sensitive information or systems, organizations can significantly reduce the risk of BEC attacks that rely on impersonation or fake identities.

For example, an organization could require all employees to present a verifiable credential, such as a digital certificate or a biometric authentication token, before sending or receiving emails related to sensitive financial transactions or confidential data.

As highlighted in Accenture's 2023 Tech Vision, we feel the time is now for organizations and businesses to enhance their existing IAM roadmaps to take advantage of Digital Identity capabilities. Organizations that can get both to work together will be industry leaders.

Damon McDougald
Identity and Access Management Lead
Accenture Security
damon.mcdougald@accenture.com

LEGAL NOTICE & DISCLAIMER: © 2023 Accenture. All rights reserved. Accenture, the Accenture logo, and other trademarks, service marks, and designs are registered or unregistered trademarks of Accenture and its subsidiaries in the United States and in foreign countries. All trademarks are properties of their respective owners. All materials are intended for the original recipient only. The reproduction and distribution of this material is forbidden without express written permission. The opinions, statements, and assessments in this report are solely those of the individual author(s) and do not constitute legal advice, nor do they necessarily reflect the views of Accenture, its subsidiaries, or affiliates.