Transforming Government Experiences with Modern Identity

Highlights from a private government roundtable, hosted by the Advanced Technology Academic Research Center (ATARC), in partnership with Okta, August 2023

People interact with government in myriad ways, from standing in line at the DMV to applying for permits online. Unfortunately, each interaction typically requires a different credential, which forces users to create and manage accounts with multiple agencies. Moreover, the technology used to authenticate and verify identities is typically inefficient, insecure, and unable to scale alongside the rapid digitalization of services.

The public now expects seamless and secure digital experiences wherever they interact online. To meet these expectations and promote trust in government, modern identity solutions should be a part of every agency's modernization strategy. At a recent roundtable discussion hosted by the Advanced Technology Academic Research Center (ATARC) in partnership with Okta, federal experts discussed the strategies, opportunities, and challenges of creating a seamless identity experience in government.

Challenges with Modern Identity

Knowing someone's identity is the cornerstone of many agency missions. From maintaining strong cybersecurity postures to issuing government benefits, knowing the identity of those interacting with the government is a critical endeavor. Due to varying missions and identity requirements, agencies experience different challenges with authenticating, verifying, and trusting identities. Moreover, standardizing the identity process across government is evermore complex due to these varying requirements.

Many agencies represented at the roundtable are challenged with verifying the identities of third-party entities, especially those accessing government systems and doing business with the government. The process to verify identities is often manual in nature, requiring in many instances in-person verification.

Similarly, agencies must verify and trust the identities of individuals and organizations who share and exchange data with the government. Ensuring agencies share data with only verified and trusted entities is critical to mission security. Even so, agencies encounter instances of identity fraud frequently, and are working diligently to build systems to counteract this type of digital identity fraud. Agencies are also working to ensure the re-authentication process is seamless for users. This involves creating automated processes to update identity information without the need for customers to take repeated action.

The Need for Federated Trust of Identities

There is both a need and desire for federated trust of individual identities across federal, state, and local organizations. A federated trust environment would not only reduce the burden on the public to create multiple credentials, but would also increase security and confidence in government transactions. Programmatically, federated trust of identities would also streamline data sharing among government agencies.

Panelists discussed the use of biometrics, such as facial recognition and other technologies, as an approach to modern identity. Some agencies are already seeing success with using biometrics to improve the government experience and enhance security. However, much of the success agencies experience with biometrics is a result of controlled environments. The rate of false positive identification is still considerably high when in uncontrolled environments.

Another challenge with advanced identity technology, such as biometrics, is the possibility of customers not meeting higher-tech requirements. As the government moves towards identity federation, it will be important for agencies to consider customers' preferred channels when accessing information. Whether users have flip phones and rely on Excel spreadsheets, the government must have identity solutions for customers' digital comfort and maturity. Agencies will also need to consider whether foreign entities will allow for biometric identity verification for their citizens.

While government agencies share these identity challenges, creating standards to meet varying mission requirements will be a considerable challenge and may add another layer of frustration to the customer experience if agencies modernize identity within silos.

"We can't have an environment where none of the standards match…When we don't solve shared challenges, costs increase, trust degrades, and ultimately we're much, much less secure."

Improving Identity for the Customer Experience

Despite these challenges, the government is actively working to build a common layer of citizen-to-government identity, especially for verification. One panelist notes that there is a distinct separation between identity validation, verification, and authentication. There are many ways agencies can approach access management, all of which should reflect an agency's specific environment. But how identity is validated and ultimately trusted across agencies still remains a challenge.

There's also a distinct difference between validation and trust. To achieve federated trust in identity, agencies must be able to trust the verification process of another agency. One panelist cautions that tying validation with specific technologies, like biometrics, may be an overstep for certain use cases. There may be situations where the same level of trust can be achieved through other means. Similarly, if one agency requires biometric validation and another agency cannot, there must be another way to validate identity to achieve the same level of trust across government agencies.

Collectively, agencies will need to build multiple validation flows that meet the requirements of different missions. Ideally, this process should be standardized and accessible to all Americans, regardless of housing status, bank account accessibility, or background. The goal for agencies should be to create a digital identity that serves all Americans, protects their privacy, ensures cybersecurity, and reduces the burden on the customer.

"When agencies begin to separate aspects of identity management, smart decisions can be made to solve this problem."

Identity verification and authentication historically have been tightly coupled together. Current systems validate, authenticate, and then give access. When authentication and verification are separate processes, agencies can delegate the issued credential across agencies.

One panelist noted that when looking at data over a ten year period, 60% of government website users access the site from a mobile device. Based on user behavior when interacting with the government online, it makes sense to create a more integrated experience and leverage the phone with biometrics and other authentication methods. This may help to connect the dots between agencies and the services customers receive.

Final Thoughts

The world is changing in unpredictable ways, and the government must be able to respond quickly to complex challenges affecting large swaths of people and communities. Effective government response can become unmanageably complex very quickly in communities where digitalization is not prioritized. And unlike other countries with simple, one-layer systems of government, the United States government is layered and complex, which makes federated trust in identity a challenging issue to tackle.

Federal industry partners, like Okta, are working with agencies to ensure secure and seamless identity authentication, regardless of agency mission. Advanced technology combined with shifts in culture is how the government will begin to create a trusted shared environment to enable modern identity. A robust government resource, idmanagement.gov, recently launched to serve as the source of digital identity in government. The resources provided by idmanagement.gov should help agencies develop identity frameworks based on best practices.

LEARN MORE ABOUT OKTA'S MARKET LEADING SOLUTIONS AT HTTPS://WWW.OKTA.COM/SOLUTIONS/PUBLIC-SECTOR/COMMUNITY-IDENTITY/