Security and Identity Modernization for State and Local Government

Modern Identity Is Pushing the Boundaries of Government Services

The American public relies on digital technology daily. From online banking to distance learning, many run their lives from mobile devices to access everything. Naturally, behind the widespread adoption of consumer technology is the need for convenience and ease of use. At the same time, security is fundamental to optimal experiences. A secure Identity is at the start and center of people's confidence and ability to access entitled services and benefits. In fact, for access to data, Identity is a vital line of defense.

Individuals share an enormous amount of personal data online and with government agencies. If this data falls into the wrong hands, it can have severe consequences, including Identity theft and fraud.

The potential harm caused by these breaches can lead to significant financial and emotional damage for the individual and have repercussions in the community. To build trust with their residents, state and local governments must prioritize modern security controls to protect their personal information.

Modern Digital Government and Legacy Services

Digital technologies are always evolving to be better and faster. However, legacy applications, built years ago, aren't keeping pace. Simply put, outdated applications cannot support digital transformation. Not only are outdated services significant security risks, from a user experience perspective, they're usually found to be flawed and inadequate.

Several factors drive a modern digital government, including:

1. **Inefficient, manual systems and processes.** Administrative systems are overburdened; manual systems can't keep up with the volume of administrative paperwork. Complex legacy systems and the costs to maintain them are creating bottlenecks in communications with residents.

   In times of crisis, such as disaster recovery, individuals may need to wait weeks or even months to process their benefits, and the lost time is a considerable cost or "time tax" for the parties involved, namely, survivors, contractors, and case workers.

2. **Following the Federal roadmap.** Required actions for the federal government can create a voluntary approach and model for state and local partners to improve their digital service delivery.

3. **Expanding attack surface.** Protecting the privacy of the public is top-of-mind. The National Association of State Chief Information Officers (NASCIO) released their list of State CIO Top 10 Priorities for 2023. Number one was cybersecurity and risk management. As the technology gets easier to access and the number of users increases, so do cyber threats.

   Legacy applications are more vulnerable to attacks than systems utilizing modern Identity and Access Management (IAM). Modern IAM centralizes and manages user access seamlessly, with additional safeguards when required, and at speed. Having Identity and cybersecurity experts constantly mitigating new threats can make a significant difference.

Identity Access Management to Build Trust

"Attackers don't have any more hoops to jump through to get to my website than my users do," said Sean Frazier, federal chief security officer at Okta, when describing the need for a transparent security posture that can address the diverse users for many government apps. A modern IAM approach works on many levels to shut down intruders as quickly as possible without distracting the intended customer experience. Those steps include:

1. **Enrollment and Identity Proofing:** During online registration, people must prove that they are who they claim to be. In the past, agencies requested identifying information assuming that only the true, real-world individual would have: their social security number, date of birth, drivers license number, or other forms of personally identifying information. However, after decades of data breaches in both the public and private sectors, that approach is no longer enough.

2. **Authentication and Authorization:** At each and every sign-in, agencies must verify that the right individual is accessing the right data. Passwords are well-understood to be weak authenticators, but modern approaches like phishing-resistant authenticators and passkeys provide high assurance while simplifying the user experience.

Modern data protection tools can enable better service delivery, personalized services, and faster response times. Protecting community members' personally identifiable information (PII) can help rebuild trust with the American public and increase their interest in using government digital services.

Modern Identity for Residents

Several trends in everyday life have highlighted the need for modern Identity solutions. For starters, the public can access always-on technology, such as unsecured Wi-Fi in coffee shops, parking lots, airports, and more. This creates a dangerous opportunity for security breaches.

There are also frustrations and an increase in fraud in unemployment claims. And new technologies create challenges for many groups of people: those who lack access to them, have limited or no experience with them, or simply choose not to use them. All of these issues open the door for scammers.

These are just a few trends that are driving modern Identity and security for services.

Reasons for change	Benefits
• Outdated user experience	• Reduction in human error rates
• Expectation for government services to model private industry	• Higher retention and bolstered trust
• Vulnerable data for Americans	• Tighter data security through least privilege access
• Administrative bottlenecks	• Increase employee helpfulness and decrease paperwork

Modern Identity for the Government Workforce:

Daily cybersecurity issues impacting government services make it difficult for workforces to keep up. With fewer resources and training, they can spend long hours trying to fix issues in outdated systems. They also have to serve frustrated community members looking for solutions.

Modernizing government services and systems can dramatically increase the efficiency of the workforce. Eliminating administrative bottlenecks and automating manual processes can free up massive hours for agencies to focus their time, resources, and energy on service delivery that's in tune with people's needs.

Modern Identity and Access Management Advantages

Government agencies are committed to restoring public trust, starting with a solid foundation of modern Identity and access management. "Okta's mission is all about making Identity and access simple for the government," explained Steve Caimi, Okta's Director of Public Sector Product Marketing. "So, when you think of Identity as a cloud, it can deliver all the capabilities that make Identity management universal, easy, and reliable."

Identity and access management systems are categorized as High Impact under the Federal Security Modernization Act (FISMA). Okta's modern Identity platform achieved FedRAMP High Impact Level Authorization. It is built exclusively for the federal government and its partners. The platform enables agencies to adopt the cloud and allow online services to be continuously delivered to the public with the highest level of security and privacy.

Trust also depends on delivering digital service excellence for the people being served. Apps and mobile devices are simple, intuitive, and widely adopted by the public. Using these digital tools and devices is critical for the government to serve communities effectively.

In a modern digital government, trust is rebuilt through convenient, easy-to-use services that work consistently and quickly for people of all abilities. At the same time, their identities are secure, and their data remains private.

Modern Identity to Improve the User Experience

Agencies can create better experiences for their workforce, as well as the communities they serve.

Unique benefits to Okta's modern Identity platform include:

- Okta is a truly **independent and neutral** Identity platform with more than 7,000 integrations in the Okta Integration Network. Okta securely manages apps and multi-cloud environments across a single Identity platform and supports government standards and industry protocols.
- Okta delivers **simplified** experiences for agency developers, employees, partners, and community members. User registration and login are friction-free, and agencies can get a central admin console to manage all users, apps, and policies.
- Okta's solution is **customizable**. Okta can handle any workforce or customer Identity use case and enhance agency security. The platform includes fully built API endpoints to customize the configuration, user authentication, and access control.
- As a cloud service provider committed to the government, Okta is StateRAMP Ready via reciprocity of our FedRAMP Moderate **Authorization**.
- Learn more about our approach at the Okta Trust Center.

Okta: Modern Identity and Security for State and Local Government

Modern Identity securely connects communities with a digital government and workforce using the always-on services they demand. Rebuilding trust depends on easily accessible, reliable, and secure government services.

Getting Identity right is critical today, yet it can be challenging. With a trusted partner like Okta, your agency can create better experiences for community members while you improve your security, compliance, and uptime through modern Identity.

Learn more about Okta at: www.okta.com/publicsector