A **GOVERNMENT TECHNOLOGY** THOUGHT LEADERSHIP PAPER

No Wrong Door: Modernizing Digital Identity for Seamless Government Access

SPONSORED BY okta

State and local governments want better, faster and more efficient processes that eliminate agency silos and strengthen cybersecurity across the enterprise. Meanwhile, constituents want easy access to government services and a seamless, satisfying user experience.

But many governments rely on decades-old login infrastructure that can't address those needs. "The rising demand for mobile-first experiences, the necessity of interagency collaboration and the increase in sophisticated cyber risks are all testing the limits of infrastructures that were built long before these factors became critical," says Deb Snyder, a senior fellow at the Center for Digital Government and former chief information security officer for the state of New York. "Organizations are dealing with a patchwork of login systems, frustrated citizens and a help desk that's buried in password reset requests."

Forcing constituents to manage multiple logins across agencies doesn't just create frustration. It increases security risk.

"Agencies may have 20 different ways to log in with 20 different passwords and a mess of MFA options that don't get used," says Mat Keller, senior solutions engineer at Okta, a leading identity and access management (IAM) services provider. "This pushes users to abandon MFA and set all of their passwords to be the same. If that username and password were stolen on the dark web, bad actors could be logging into all their accounts."

The right solution is a modern IAM framework that improves the user experience, avoids disruption, strengthens security and enables interagency collaboration through a No Wrong Door model.

A Roadmap for IAM Modernization

A No Wrong Door approach means having a single, consistent login for all services, regardless of agency. For users, this creates simple, streamlined access to services. For governments, this leads to better coordination of service delivery among departments. Residents who apply for unemployment benefits, for example, could automatically be alerted about other benefits they qualify for, such as food and housing assistance.

With an IAM system — one with single sign-on capacity secured by multifactor authentication — governments can enable a true No Wrong Door approach that's more efficient and more secure for employees and constituents alike.

Here's a roadmap for modernizing IAM without disrupting existing systems.

1. Create a vision for the future.

Start at the end and work backward: Think about what an ideal government experience would look like. Map out a seamless constituent journey for accessing services across agencies.

Reach out to peer governments that have accomplished IAM modernization successfully. Talk to them about their successful strategies and lessons learned. Work with a trusted technology vendor who understands that IAM modernization is a strategy, not just a product purchase. Success requires collective commitment — very few agencies can make this journey alone.

One state completed a successful IAM modernization, but only after several failed attempts, says Steve Tout, founder and CEO of Identient, a cybersecurity firm that helps organizations implement smart identity security systems. "Success came when central IT set a clear vision and mission — and brought stakeholders with them," he says.

2. Get buy-in from all stakeholders at the beginning.

“Identity isn’t a single agency initiative; it’s a connected government imperative,” says Tout.

Gather the right stakeholders at the start to ensure buy-in. Those include IT and line-of-business leaders, information security officers, privacy leaders, budget decisionmakers and agency representatives who represent your entire enterprise. Consider including frontline staff and even constituents to help build a responsive and satisfying user experience.

3. Build a culture of innovation.

IAM modernization efforts can encounter pushback from employees. They may simply prefer the status quo. Or they may think working with an IAM partner feels like giving up internal control.

Focus on change management to help your team see the value of IAM modernization. Make sure staff understand this is a once-in-a-decade opportunity to improve public service. Address any concerns about IAM by emphasizing that when your project is based on vendor-neutral open standards, your agency is still fully in charge to authorize who is allowed to do what in your systems, whether you built or bought them.

Empathy and intentionality will help your personnel see the goal while building a culture of continuous innovation that puts constituent needs and equity at the center of every design decision.

4. Start small — and start now.

Governments that are just beginning to address their outdated, fragmented access management systems should start small and scale later. Pick a critical system, preferably one your IT team is already comfortable working with, and engage stakeholders to build consensus on requirements. Then add an identity layer to the system. Focusing on early wins builds confidence, momentum and long-term success.

5. Design an inclusive user experience.

Throughout the entire IAM modernization process, you must take a hands-on approach to accessibility when developing identity federation.

Factor in the needs of people with visual impairments, users with cognitive challenges and underserved populations with limited access to technology at home. Consider the needs of constituents who speak different languages and those with diverse abilities.

Finding the Right IAM Partner

Take these steps when evaluating vendors for your IAM project:

- Vendors will show their hand, but only if you ask them. Ask how they handle product updates, AI bias, fairness and inclusion, human review, privacy and transparency. Request documentation that demonstrates their commitments to these areas. You can also plan for and conduct private reviews that include detailed walkthroughs with the attorneys and product designers about how AI is used.

- Talk to a potential vendor’s existing customers. Inquire whether the vendor shows up as a willing partner with enthusiasm, ready to help solve problems. Ask about implementation experiences and ongoing support.

- Don’t get locked into buying a solution that doesn’t adhere with open standards, which enable consistent handling of identity, authentication, authorization and federation across different systems. Evaluate how easily these standards work in practice, not just in theory. Conduct hands-on evaluations to understand the real effort required for implementation and ongoing administration.

- Be sure to assess the vendor’s data management approach and integration flexibility. The right vendor should be able to minimize customization requirements and complexity. The best implementations are often the simplest to deploy and maintain.

Conclusion

There’s no one-size-fits-all solution to IAM. Constituents have different needs and will be at different stages in their government interactions. Technology should help — not hinder — access.

“You want to make it easy for the user,” says Keller.

This piece was written and produced by the Government Technology Content Studio, with information and input from Okta.

government technology

Produced by Government Technology

Government Technology is about solving problems in state and local government through the smart use of technology. Government Technology is a division of e.Republic, the nation's only media and research company focused exclusively on state and local government and education.

www.govtech.com

okta

Sponsored by Okta

Okta is the World's Identity Company. As the leading independent Identity partner, we free everyone to safely use any technology— anywhere, on any device or app. The most trusted brands trust Okta to enable secure access, authentication, and automation. With flexibility and neutrality at the core of our Okta Workforce Identity and Customer Identity Clouds, business leaders and developers can focus on innovation and accelerate digital transformation, thanks to customizable solutions and more than 7,000 pre-built integrations. We're building a world where Identity belongs to you.

Learn more at **okta.com**.

ADOBESTOCK/AI GENERATED