



## Many Services, One State— and One Front Door

Deloitte and IBM join forces to help agencies  
modernize citizen identity and access management



Governments work to make their citizens' lives better—and today almost all of the interactions are online, either via a computer or mobile devices, where the mobile device is becoming the preferred choice. **States are trying to support the people in need with faster reaction time to make a better impact on their communities,** while at the same time they also want to provide ease of access to the citizens that need remunerated services (e.g., boating license). While supporting the population via web- and cloud-based systems to access the government services, states need to safeguard citizens' private financial and medical information, help prevent fraud, and coordinate sensitive public safety operations.

Citizens interact with government platforms in multiple ways, at multiple touch points. An identity access system that makes the process onerous gets in the way of program outcomes. These touchpoints mean different things to different people: Some look to the state for support, through programs like food supplements or Temporary Assistance for Needy Families (TANF); others have more basic needs such as paying taxes, registering a vehicle, or getting a fishing license. Some contacts involve money coming in, and some handle money going out— and if the system doesn't support both ends, the net result is counterproductive.

Having too many accounts creates more vulnerability points. Every online government platform presents “attack surfaces”—and, in many cases, the keys to entry are a matter of identity validation. Security should complement, not inhibit, functionality—because if constituents and employees find it hard to access or use a system, it can't deliver its promised value. Even a system that “works” can make it hard to get things done if it asks users to repeat their access authorizations over and over.

As digitization continues to increase, government platforms should be agile and able to adapt to fast changing landscape of digital identities. Government

agencies should blend technology expertise with an understanding of the mission objectives along with a working grasp of user experience, organizational change management, and interdepartmental interoperability. In addition to specific needs driven by each circumstance, every instance of digital citizen interaction should provide reliable self-service in a way that's intuitive and engenders trust.

These and other considerations make citizen identity and access management, or CIAM, a critical and foundational capability.

No matter what the need, each citizen comes away from a digital interaction with not only a practical outcome, but also an emotional reaction: **Did the government help me, or get in my way?**

# Deloitte and IBM: Our approach

For public entities and enterprises alike, cybersecurity is a strategic and operational risk. Addressing that risk is a long-term journey. The threats evolve along the way. As more business takes place online, more value changes hands electronically, and hackers gain in sophistication. To counter this challenge, governments need a mindset that constantly protects the citizen—and that means winning the race every day so interactions remain secure and trusted. Down that road, there are enticing possibilities. What if a state could turn services on or off based on a user's risk profile? What if the threat of password theft were to disappear because the system evolved beyond the use of passwords?

Making progress along that path starts with knowing the starting point—a maturity evaluation that takes a government's unique needs into account. From that picture, a future vision can emerge, along with specific priorities and the budgetary commitments to support them.

Through a combination of IBM's market-defining technology and Deloitte's trusted industry experience, we help government clients **effectively integrate and implement outcome-focused solutions** that accelerate their pace of modernization.

And we know that no matter how sophisticated a back-end system may become, the true measure of modernization is in the eye of the user. Government services can become more secure and easier to consume at the same time. Systems can do more than recognize people; they can recognize devices and situations so safety and access come together under a wider umbrella. With this kind of mindset, governments do more than just serve citizens—they enlist them in a relationship of trust that can help bring program benefits to more people. We take all this into account when we help organizations embrace a culture of security and harden their organization against cyber, operational, and brand-related risks.



# Deloitte and IBM: Our capabilities

When combined, Deloitte's deep government & public services (GPS) knowledge and IBM's Security solutions can help develop and implement a broad cyber risk program, streamline and automate workflows and processes, train your workforce, and—in some cases—fully manage security services.

When Deloitte and IBM help a government agency establish standards and practices for effective CIAM, they can propagate internally to all the subordinate offices and agencies that need to participate. We know technology is a critical part, but not the only part, of a citizen access solution. Deloitte leverages IBM technologies and surrounds their use with its own experience in driving adoption,

understanding shifting user behaviors, and the business of government. Then we apply that experience in taking a state's needs from strategy to implementation to operation.

Together, we help build in automation tools that enable government agencies to onboard some apps and set up new capabilities on their own as needs arise. Deloitte has demonstrated this capability in running state-wide CIAM on IBM technologies. **In two states**, our teams have brought more than **1,500 applications under the solution's management, which we implemented and operate.** These deployments provide access to more than **15 million users** and **support many departments.**

**We assist our government clients with their most pressing needs, including the modernization of legacy state government solutions and strategy, implementation, integration, and operation of solutions across cybersecurity.**

Within the specialized arena of citizen identity, Deloitte works alongside IBM serving GPS clients with broad, scalable, high-volume capabilities that draw upon the allies' proprietary technologies. Avoiding heterogenous mix of technology products means there are no cracks in the architecture and no question who owns the responsibility for performance.





Deloitte has a **deep understanding** of today's market realities in GPS, complemented by the longtime experience collaborating with IBM on GPS sector challenges.



We can help you **protect your data** in the cloud, prevent gaps in the security policies of applications, shore up systems against unauthorized users, and implement **endpoint protection** in a mobile work environment.



IBM Security solutions offer **advanced cyber risk protection**—especially for clients in data rich and heavily regulated industries—and complements Deloitte's end-to-end suite of cyber risk services.



IBM Security products supports large, **multi-million user implementations** with cloud and on-premise solutions.



IBM Security products have intelligence to help **identify, quarantine and remediate malicious activity**.

The results stemming from this alliance hasn't escaped notice in the world of government professionals. Our work for the state of Ohio has been received multiple awards from the National Association of State Chief Information Officers (NASCIO): the 2019 Cybersecurity award for Digital Identity and the 2021 Cybersecurity award for Self-service Tools & Account Transparency.



# Our joint CIAM approach in action

In most US states, **hundreds of available programs**—life-altering ones such as parole, transfer programs, and child support; conveniences such as fishing licenses, and everything in between—**rely on connected technology platforms** that most citizens interact with in some way.



In states where Deloitte and IBM have helped infuse CIAM tools and practices into these platforms, the results have gone beyond the technical challenge of streamlined secure access.



These states have seen program participation and revenue go up as the difficulty of citizen engagement has gone down.



Trust should rise as security incidents related to identity begin to decline.



Costs to service citizens are reduced as they are able to make use of self-service tools.



Citizen adoption of CIAM tools increases when the barriers to their functionalities are removed or reduced.



And central management of identity and access has made it faster and easier for officials to change settings and features, stand up new functions, or deactivate old ones in real time, with minimal disruption.

## CASE STUDIES

In a mid-western state, millions of citizen users—above 90 percent of the population, and growing—are integrated into the cloud-based CIAM solution Deloitte and IBM created. The state wanted users to interact with services across multiple agencies anytime, anywhere, on any device, via a single credential.

Using IBM Security Verify along with other IBM cloud, security, process, and integration tools, Deloitte migrated the state's identity management to a cloud-based model. The new solution now integrates with 285 applications across 16 state agencies to serve a million business users and more than 100,000 state employees and contractors in addition to most citizens.

Today, thanks to pre-defined APIs, the solution lets agencies effectively deploy modules in hours in an agile environment that meets fast-changing needs. It's now state policy that all new software, rewrites, or upgrades use the solution for front-end identity. In addition to the enhanced user experience that comes from a unified login, the system has helped the state improve security, tighten regulatory compliance, reduce infrastructure cost, and improve capacity.



To help create a required system integration module, Deloitte and IBM teamed to create HealthInteractive™, a cloud-based service business that ties a state’s newly separate Medicaid modules into a cohesive whole. In turn, HealthInteractive is paving the way to help a state to enhance its financial management and its enterprise data interchange (EDI) module, which is critical to maintaining security and HIPAA compliance. Deloitte is also delivering identity security and single-sign-on capabilities that preserve data privacy and patient confidentiality. At

launch, HealthInteractive is poised to serve almost 3 million members, most of whom are on managed care plans, as they execute more than 73 million transactions each month.

With the addition of Bureau of Motor Vehicles to its state-wide portal, Ohio ID, the state’s enterprise CIAM program, the user base has grown to as many as 12 million people. Ohio is using its citizen access system to set up an application store, similar to a commercial ‘app store’ where users can find and connect with government programs.

Arkansas engaged Deloitte to implement a full Identity and Access Management (IAM) strategy and implementation that relies on the IBM IAM solution called IBM Security Verify on IBM Cloud. The state’s new Arkansas Integrated Eligibility System (ARIES) features a Citizen Portal that gives citizens one-credential access to public services.

Citizens can set up and manage their own accounts, while behind the scenes ARIES uses IBM technology to reduce implementation and operational risks. Since its late 2020 launch, ARIES has driven efficiencies and cost savings while serving more than a million users.



## Overall, potential benefits from an effective CIAM approach also include:



An enterprise digital identity solution is the underlying fabric that enables the digital relationship between a government and its citizens.



An enterprise gains the flexibility to control costs by scaling up or down based on volume, performance, and utilization.



Ease of use facilitates quicker adoption.



An effective and comprehensive CIAM approach can bolster not only the security of a public-sector information architecture, but also its resiliency against failure and its percentage of uptime.



Security designed with user experience in mind can preserve access and effectiveness across state websites, portals, and intranets, so agencies can focus resources where they’re needed.



Trusted identity can be shared among integrated applications.





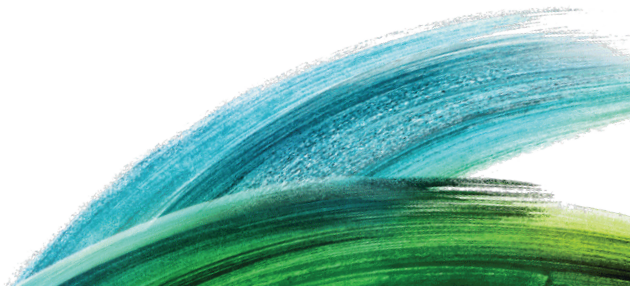
# Conclusion

Citizen identity access management is the discipline of reimagining and delivering simple and secure citizen digital identity solutions to **simplify access, reduce risk, increase trust** between agencies and constituents, and **improve user experience**. That's easy to say, but harder to achieve. Together, the trained teams at Deloitte and IBM use their combined capabilities to help governments **build trustworthy, next-generation solutions** that take CIAM from the page to everyday work.

## CONTACTS

### Dan Poliquin

Advisory Principal  
Deloitte & Touche LLP  
dpoliquin@deloitte.com



We are ready to help you embrace a culture of security and harden your organization against cyber, operational, and brand-related risks.



## Deloitte.

The combination of IBM's market-defining technology and Deloitte's trusted industry experience is more than just an alliance—it's a catalyst for your organization's digital evolution, a collaboration that works with you to implement outcome-focused solutions designed to help you accelerate your pace of modernization.

The Deloitte and IBM alliance delivers leading-edge technology solutions that are custom fit to client needs—from hybrid cloud strategies that prioritize business outcomes to AI solutions and managed services that democratize and unlock the power of data-driven insights, to advanced cyber risk solutions that protect your organization's most critical information and mitigate risk in a constantly shifting landscape. Our core service: focused innovation you can believe in, from the combined experience of two organizations you can trust.

This document contains general information only and Deloitte is not, by means of this document, rendering accounting, business, financial, investment, legal, tax, or other professional advice or services. This document is not a substitute for such professional advice or services, nor should it be used as a basis for any decision or action that may affect your business. Before making any decision or taking any action that may affect your business, you should consult a qualified professional advisor. Deloitte shall not be responsible for any loss sustained by any person who relies on this document.

As used in this document, 'Deloitte' means Deloitte & Touche LLP, which provides audit, assurance, and risk and financial advisory services and Deloitte Consulting LLP, which provides strategy, operations, technology, systems, outsourcing and human capital consulting services. These entities are separate subsidiaries of Deloitte LLP. Please see [www.deloitte.com/us/about](http://www.deloitte.com/us/about) for a detailed description of our legal structure. Certain services may not be available to attest clients under the rules and regulations of public accounting.

Copyright 2023 Deloitte Development LLC. All rights reserved.