Empowering people who serve the public®

tyler technologies

ISSUE PAPER

Changing Resident and Business Engagement: The Case for Centralized Digital Identities

How States Can Leverage Identity and Access Management (IAM) for Seamless Cross-Agency User Experiences

Ron Thornburgh, Vice President of Digital Government Policy & Advocacy
Michael Teeters, Senior Product Manager
Nick Winston, Senior Director of Product Strategy

ISSUE PAPER

Changing Resident and Business Engagement: The Case for Centralized Digital Identities

Introduction: Does Your State Offer a Seamless User Experience?

In an era characterized by digital transformation, state governments face the challenge of evolving to meet the changing needs and expectations of their residents and businesses. Just as consumers have become accustomed to personalized online shopping and banking experiences, the public expects the same level of convenience and customization from government services. A crucial aspect of this digital evolution involves the establishment of a centralized identity system, serving as a single, robust profile for each user across different governmental departments and online services.

Intergenerational research supports a user-centric approach to e-government, finding that easy-to-use digital experiences improve government interactions across all age groups. [1] Survey results from the National Association of State Chief Information Officers (NASCIO), indicate that the second-highest priority for state CIOs in 2023 is improving digital government services.[2] Gartner predicts that by 2026, "total experience" strategies that bring coherence to traditionally siloed government approaches will increase customer satisfaction by 50%.[3]

This issue paper serves as a resource for government organizations and decision-makers seeking to enhance online resident experiences through seamless and secure identity and access management (IAM) solutions.

The Core Challenge States Are Trying to Solve

The central problem that states are grappling with involves establishing a centralized identity for each user that streamlines their interactions across a vast array of state services. At its core, the goal is to create a single authentication method and identity store (username/password) for all applications and services. However, the ambitions of most states extend far beyond simply providing a consistent sign-on experience. States aim to develop a comprehensive and robust profile for each user, capturing a multitude of details that define their relationship with various agencies.

Each profile would include a "global" section with widely used details like address and phone number. More detailed, "domain or agency" sections would hold agency-specific information or linkages to agency-owned data, such as vehicle details for the DMV or licensing details for professional licensing boards. The ultimate vision is to leverage this multifaceted identity to accelerate government interactions, bypassing the need to repeatedly provide the same information for different forms and allowing individuals to utilize saved payment methods for all state services.

Further, states envision creating a more personalized, targeted, and proactive digital relationship by using the information contained within these profiles. By linking experiences across disparate governmental sectors, users could view all their receipts in a single location, receive consolidated notifications, and much more. This approach promises not only a more user-friendly and intuitive experience, but it also has the potential to enhance governmental efficiency and improve public service delivery.

[1] https://www.tylertech.com/resources/resource-downloads/how-local-governments-can-reach-each-generation

[2] https://www.nascio.org/resource-center/resources/state-cio-top-ten-policy-and-technology-priorities-for-2023/

[3] https://www.gartner.com/en/newsroom/press-releases/2023-04-17-gartner-announces-the-top-10-government-technology-trends-for-2023

IAM vs. CIAM

IAM and CIAM (Customer Identity and Access Management) are both approaches to managing digital identities, but they cater to different user groups and have different focus areas. For governments, IAM scales beyond the back office, and an IAM system should be part of the government-to-public technology framework.

Gartner defines IAM as "a security and business discipline that includes multiple technologies and business processes to help the right people or machines to access the right assets at the right time for the right reasons, while keeping unauthorized access and fraud at bay."

IAM primarily caters to internal users within an organization like employees, contractors, and partners. It focuses on controlling user access to critical data within the organization, usually through a zero-trust lens that limits access to applications and digital resources. Key features typically include single sign-on (SSO), multi-factor authentication (MFA), and lifecycle management.

Meanwhile, the term CIAM, on the other hand, refers to managing external customers. While it shares some functionalities with IAM, such as SSO, authentication, and authorization, it has additional capabilities tailored to customer interaction.

Because the public interacts with a wide range of digital government services, such as paying for licenses, filing taxes, accessing court records, reserving recreation facilities, and much more, CIAM systems need to manage identities at a larger scale and offer a seamless user experience. Key considerations include ease of use, self-service capabilities (like password reset or profile updates), and maintaining high performance even with a large number of users.

Moreover, because customers are accessing public-facing applications, CIAM solutions must handle consent and preference management to comply with consumer privacy regulations. CIAM solutions are often designed to gather user data that can be leveraged to enhance customer service.

The central problem that states are grappling with involves establishing a centralized identity for each user that streamlines their interactions across a vast array of state services.

Enabling Other Dimensions of Resident and Business Engagement

Centralized digital identities are a catalyst for digital transformation across five dimensions of engagement:

1. **Personalized Web and Mobile Experiences:** Using unique profiles, states can deliver personalized online services. For instance, a resident who frequently uses state park services might receive updates about new parks, events, or reservation availability, enhancing their digital journey.

2. **Connected Digital Services and Forms:** Leveraging digital identities, states can create a unified service experience. An automated system could pre-populate forms with relevant information, such as pre-filling a driver's license renewal application, expediting transactions, and making the process more convenient.

3. **Centralized Payments System:** This system simplifies transactions by allowing stored payment methods for recurring or scheduled payments across multiple agencies. For example, a resident could automate payments for vehicle registration while simultaneously processing a one-time state park reservation fee, increasing efficiency and ease of use.

4. **Cross-agency User Interests and Notifications:** States can send personalized notifications based on a user's interests. An individual who is a licensed professional could receive notifications about relevant regulatory changes or continuing education opportunities, enhancing their overall experience.

5. **Robust Digital Records and Permissions:** Centralized identities can create a digital repository for important documents, like professional licensing records or voter registration status, offering secure and streamlined access and management. Additionally, controlled access permissions ensure data privacy and security, enhancing public trust.

In an era driven by data, these dimensions also form a foundation for meaningful data analytics, enabling states to draw valuable insights to further enhance the digital experience.

Five Considerations for Selecting a Statewide IAM System

When considering a centralized IAM system for improved user experiences, it's recommended to keep the following five factors in mind:

1. **Usability and Convenience:** Select an IAM system with a focus on user-friendliness and intuitive interfaces, branded with your government seal, that foster an easy-to-use experience for the public. For example, simplify registration and login processes, and provide step-by-step guidance for users.

2. **Accessibility:** Make sure that the IAM system is accessible to all users, such as ensuring that accessibility features like screen reader compatibility and adjustable text sizes are available. While requirements may vary by jurisdiction, inclusive design is a best practice.

3. **Security and Privacy:** Prioritize security measures to protect user data and maintain privacy. Implement multi-factor authentication (MFA) using methods like email, SMS codes or authenticator apps, encryption, and role-based access controls to safeguard against unauthorized access and data breaches. Comply with cloud security standards and adopt privacy-enhancing technologies to further protect user information.

4. **Interoperability and Single Sign-On (SSO):** Enable seamless data exchange and integration with existing systems across multiple departments and agencies. For example, a resident could use one digital identity to access services from the department of motor vehicles, tax office, and public health department. Adopt open standards and application programming interfaces (APIs) to facilitate cross-agency collaboration and streamline the user experience. Implement SSO to simplify the login process across multiple applications.

5. **Scalability:** Select an IAM system with scalability in mind to accommodate growing numbers of users and services over time. Utilize cloud-based solutions and modern technologies to ensure the system can expand and adapt to evolving requirements. For example, self-service capabilities allow users to request password resets and other actions to reduce customer support tickets.

Conclusion

As digital interaction becomes the norm, balancing user experience with security is crucial. Ensuring seamless access to services while protecting residents' information is fundamental for trust-building and efficient service delivery. Given digital identity's centrality to user interaction, a proactive approach to IAM isn't just beneficial — it's essential.

For additional insights on improving digital experiences, visit Tyler's Resource Center at tylertech.com.

ABOUT TYLER TECHNOLOGIES, INC.

Tyler Technologies (NYSE: TYL) provides integrated software and technology services to the public sector. Tyler's end-to-end solutions empower local, state, and federal government entities to operate efficiently and transparently with residents and each other. By connecting data and processes across disparate systems, Tyler's solutions transform how clients turn actionable insights into opportunities and solutions for their communities. Tyler has more than 40,000 successful installations across nearly 13,000 locations, with clients in all 50 states, Canada, the Caribbean, Australia, and other international locations. Tyler has been recognized numerous times for growth and innovation, including Government Technology's GovTech 100 list. More information about Tyler Technologies, an S&P 500 company headquartered in Plano, Texas, can be found at tylertech.com.