Empowering people who serve the public®

WHITE PAPER

Improving Resident Engagement With Identity and Access Management

How Governments Can Leverage Identity and Access Management Systems for Improved User Experiences and Security

Jason Howard, Director of Software Engineering, Tyler Technologies
Michael Teeters, Senior Product Manager, Tyler Technologies

WHITE PAPER

Improving Resident Engagement With Identity and Access Management

Introduction: Is Your Government Leveraging IAM for a Secure & Enhanced Resident Experience?

This white paper serves as an introductory resource for government entities and decision-makers seeking to enhance community experiences through effective and secure Identity and Access Management (IAM) solutions. Our target audience includes government administrators, IT managers, and security professionals at city, county, and state agencies who are responsible for selecting IAM systems. The focus is on customer identity access management (CIAM) solutions that enable resident engagement and interaction with public sector services.

According to Gartner® Glossary as of July 12, 2023, 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."[1] For governments, this scales beyond the back office, and an IAM system should be part of the government-to-public technology framework. The public interacts with a wide range of digital government services, such as paying utility bills, evaluating property taxation, accessing court records, requesting public works projects, reserving recreation facilities, and much more. Each of these requires identity verification and access control. IAM systems can provide a centralized and standardized way to manage identities, access controls, and authentication across these different services, making it easier for people to access them securely. In addition, an IAM solution is the foundation of a single sign-on (SSO) experience — sign on once and have access to all participating agency or department services.

Protecting the digital identities of the public is increasingly complex due to the growth of cyberthreats. This presents a significant challenge for governments that need to balance user experience and security. Addressing this issue is crucial to foster trust in government services, safeguard sensitive information, and ensure seamless access to essential online services.

The goal of this white paper is to explore various IAM concepts and recommendations that governments should implement to improve the user experience while maintaining a high level of security. Furthermore, we aim to highlight key considerations for successful implementation.

GARTNER is a registered trademark and service mark of Gartner, Inc. and/or its affiliates in the U.S. and internationally and is used herein with permission. All rights reserved.

[1] Gartner IT Glossary, "IAM", as of July 12, 2023, https://www.gartner.com/en/information-technology/glossary/identity-and-access-management-iam.

The Evolution and Recent Trends of Identity and Access Management

The evolution of IAM in the public sector can be traced through several stages. Each stage is marked by advancements in technology, growing security concerns, and the increased demand for digital services.

Early Stage IAM: In the beginning, IAM in the public sector was primarily focused on basic user authentication and authorization. Think of simple username and password combinations. Because public sector organizations tended to operate in siloed systems, there was limited interoperability between different services.

Increased Centralization and Security Measures: As governments began to recognize the need for improved security and efficiency, they started consolidating identity management into centralized systems. They also began using additional measures such as multifactor authentication (MFA), role-based access controls, and SSO. These measures improved security and convenience for people accessing government services.

Federated Identity Management: With the need for secure and seamless data exchange between different government agencies came the development of federated identity management systems. These systems enabled the sharing of user identities and access credentials across organizational boundaries. These improvements allowed for a more integrated and efficient approach to managing individual identities.

Adoption of Cloud and Mobile Technologies: The widespread adoption of cloud and mobile technologies has transformed IAM in the public sector. Today, because of the cloud, governments can scale and deliver services more securely, efficiently, and cost-effectively. Cloud technologies have also facilitated recent trends, such as identity proofing, biometric authentication, and the use of digital identities, like smart cards.

Key Concepts of Identity and Access Management

Identity Proofing vs. Authentication

Identity proofing is the process of verifying an individual's identity prior to giving access to a system. This typically involves collecting personal information, such as name, date of birth, and social security number. That information is then compared against trusted sources like government databases, credit bureaus, or public records. The goal of identity proofing is to confirm that a user is who they claim to be. For enhanced security, proofing may also involve biometric data, such as fingerprints or retina scans.

Contrast that with authentication, which is the process of confirming that a user is the same person whose identity was established during identity proofing. This is done by verifying one or more factors, such as something the user knows (e.g., a password/PIN), something the user has (e.g., a security token), or something the user is (e.g., a fingerprint).[2] Two-factor authentication (2FA) and multifactor authentication use two or more factors, significantly increasing security.

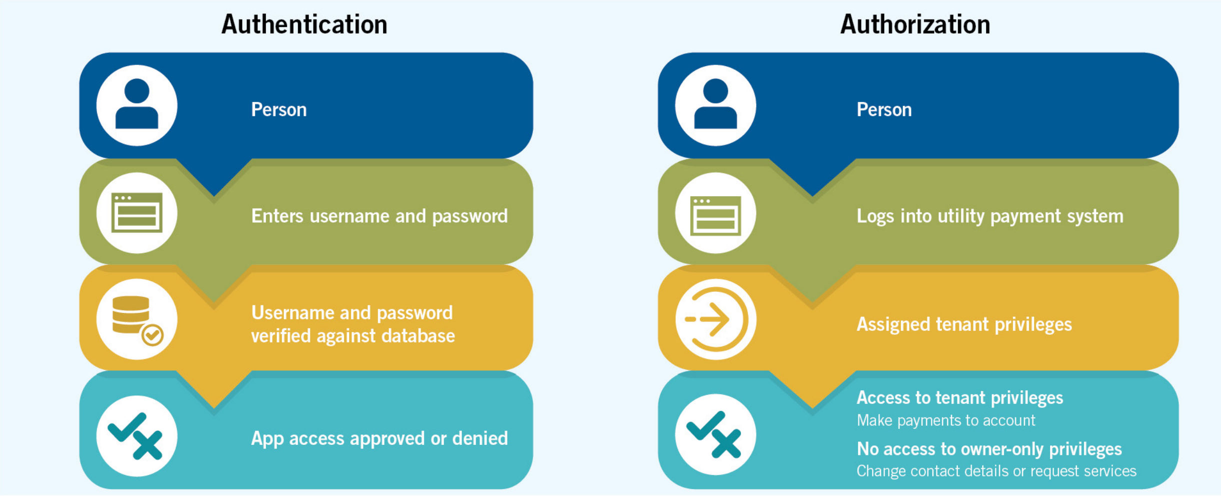
Authentication vs. Authorization

Authorization is a vital aspect of IAM that determines what actions a user can perform within a system or service after authentication. It grants or denies access to resources based on predefined rules or policies, considering the user's role, privileges, and permissions.

Role-Based Access Control (RBAC): Users are assigned roles such as registered user or guest user. Each role has predefined permissions that determine which resources they can access.

Attribute-Based Access Control (ABAC): This method looks at the user's attributes such as agency/department, location, or security level, and contextual information such as time of day or IP address to determine access. The ABAC method enables fine-grained control and adaptive policies.

Discretionary Access Control (DAC): In this method, system administrators have the authority to grant or deny access to users based on their discretion. The DAC method offers flexibility but requires manual management.


Authentication
Person
Enters username and password
Username and password verified against database
App access approved or denied
Authorization
Person
Logs into utility payment system
Assigned tenant privileges
Access to tenant privileges
Make payments to account
No access to owner-only privileges
Change contact details or request services

[2] https://csrc.nist.gov/glossary/term/multi_factor_authentication

5 Recommendations for Selecting an IAM System

When considering government IAM systems for improved 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 multifactor authentication 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 resident 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.

By addressing these five considerations, governments can create a seamless, secure, and user-friendly environment for the public to access essential services, fostering trust and satisfaction in the process.

Navigating the Transition to a Modern IAM System

As organizations plan to transition from early and mid-stage IAM systems to more advanced solutions integrating cloud and mobile technologies, several questions arise. These questions, crucial for successful adoption and gaining the full benefits of modern IAM solutions, are outlined below.

Change Management Questions To Consider

1. **Technological:** How can we seamlessly integrate our legacy systems with the modern IAM system, update our infrastructure, and ensure compatibility with new technologies? Given the potential complexity and time investment, how can we amass expertise in both existing and emerging technologies?

2. **Financial:** What level of initial investment will we need to embrace cloud and mobile technologies, including costs for new hardware, software subscriptions, and training? What are the expected ongoing maintenance and support costs, and how will these factor into our choice of IAM vendors?

3. **Organizational:** How can we address potential resistance to change, lack of internal expertise, and concerns over data privacy and security to facilitate the adoption of new IAM solutions? What strategies can we employ to coordinate efforts across various departments and agencies, given the potential challenges?

Alongside the preceding questions, it's vital to consider key public experience metrics for a smooth transition and optimal user satisfaction. This list presents common metrics, some combined for brevity.

Key Public Experience Metrics To Consider

1. **User Satisfaction and Ease of Use:** Gauge user satisfaction through surveys and feedback forms after interacting with the IAM system. Assess system intuitiveness by monitoring task completion times and helpdesk queries.

2. **Accessibility and Adoption Rate:** Evaluate the system's effectiveness for all users, including those with disabilities, through feedback and compliance with accessibility standards. Also, monitor the speed and extent of system adoption among users.

3. **Response Time and Reliability:** Measure the system's efficiency and reliability by tracking response times, the proportion of requests meeting a response time goal, and system uptime.

4. **Security Confidence:** Assess user trust in data protection through surveys and tracking the number of security incidents, reflecting confidence in the system's security.

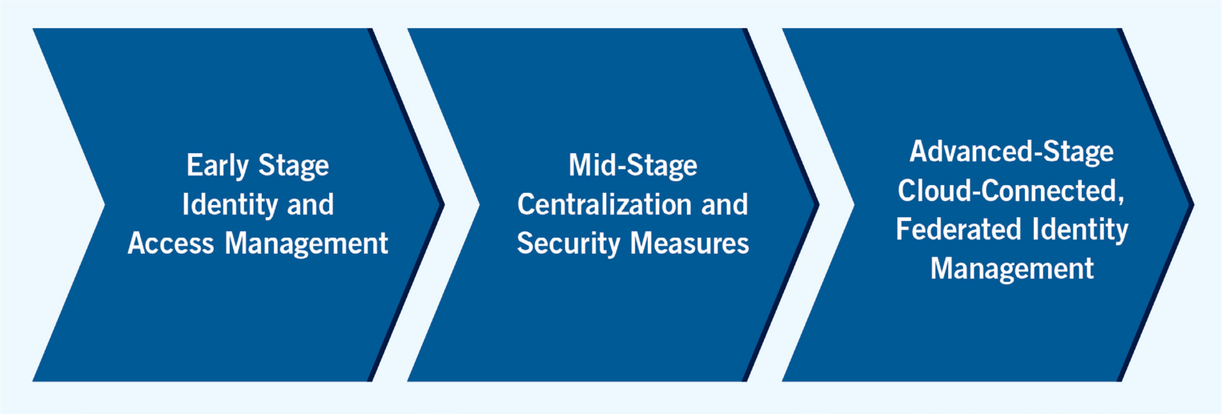
Looking Forward

The increasing reliance on online services has complicated the task of managing and protecting the public's digital identities. As a result, governments face a challenging balance between user experience and security, crucial for building trust, protecting citizens' information, and ensuring seamless access to essential services. This challenge is critical for government agencies, IT managers, and security professionals tasked with selecting IAM systems.

This white paper traced the evolution of IAM systems, from early-stage to the advanced stage incorporating cloud and mobile technologies. We examined the nuances of identity proofing, authentication, and authorization, emphasizing their implications on usability, convenience, accessibility, and security. Implementing these recommendations can lead to improved user satisfaction, increased public trust, and streamlined services, but also involves overcoming resistance to change, managing technological complexities, and considering financial impacts.

Looking to the future, further investigation is needed in areas like biometrics, AI, blockchain, and evolving privacy laws. We must continue to innovate, improving the balance between usability and security without compromising either.

We encourage our audience to critically assess their current IAM practices against the recommendations in this paper, collaborate with stakeholders, and explore additional resources to stay informed about best practices in IAM. As digital identity forms the cornerstone of community interaction, a proactive approach to IAM is not just beneficial — it's essential.



Early Stage Identity and Access Management

Mid-Stage Centralization and Security Measures

Advanced-Stage Cloud-Connected, Federated Identity Management

Additional Resources

For additional insights for government leaders on improving digital user experiences, expanding access, and boosting satisfaction with government services, visit Tyler's Resource Center at tylertech.com.

About the Authors

Jason Howard is a director of software engineering at Tyler Technologies. With over two decades of experience, he has successfully spearheaded innovative digital initiatives, enhancing citizen engagement while prioritizing privacy and security. Jason's deep understanding of CIAM strategies, coupled with his technical aptitude, has led to the successful implementation of robust identity solutions. Holding an MBA in finance and numerous technical certifications, he combines technical expertise with a keen focus on achieving favorable business outcomes. Jason remains dedicated to leveraging technology to drive continuous innovation in the public sector.

Michael "Mike" Teeters is a senior product manager with Tyler Technologies. Mike played a key role productizing Tyler's Identity Workforce and Identity Community solutions, and in launching the supporting administrative tools used by clients to manage those solutions. With a Master of Accounting degree and nearly 30 years of public sector experience — from process consulting to support team management — Mike understands the importance that CIAM solutions play in service delivery and resident engagement.

About Tyler's Solutions

More than 10,500 clients use Tyler's cloud-based solutions to enhance security, strengthen resilience, and provide the public with easy access to a wider range of services and solutions. Powered by our strategic collaboration with Amazon Web Services (AWS), we leverage the cloud to deliver a better experience for our users and constituents while reducing costs and increasing efficiency and security. Tyler's Identity cloud authentication solution is a secure, single sign-on IAM system for public sector organizations — powered by the industry-leading Okta cloud Identity-as-a-Service (IDaaS). Identity Community is one component of Tyler's emerging resident engagement platform focused on providing an end-to-end solution that simplifies connecting communities to public sector services. In contrast to general customer identity access management (CIAM) solutions, Identity Community is tailored to the needs of the public sector.

Tyler's broad geographic footprint forms a powerful network of governmental agencies. Through Tyler, these agencies create stronger connections with partner organizations and departments across local, state, and federal jurisdictions. Our proven depth and breadth of solutions set the nationwide standard for electronic efficiencies, out-of-the-box interoperability between applications, and cloud-based functionality at every level of government across public administration, justice, health, and education.

Tyler's client support teams provide clients with access to documentation, live support, online training, and more. Tyler Community is an online peer-to-peer support community that enables our clients to share knowledge about Tyler products, provides collaborative learning opportunities, and offers product support via forums, libraries, and wikis. Tyler University and Tyler Coach, our continuing education platforms, help clients improve their skills, learn new software, and keep up with the latest technology and procedures.

Contact Tyler

If you would like information about Tyler's IAM solutions, contact us at info@tylertech.com or visit 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**.

tylertech.com | 833.895.3783 | info@tylertech.com