Whitepaper

Bring secure, frictionless customer experiences to government faster with modern CIAM

The public sector's path to modern Customer Identity and Access Management

The way government interacts with the public continues to evolve dramatically. Websites used to be a way to publish basic, static information. But the explosion of modernization and the growing demand for omni-channel experiences has changed all that. Today, users are always connected. Some 85 percent of U.S. adults owned smartphones in 2021, according to the Pew Research Center. Three-quarters owned desktops or laptops and over half owned tablets. These users need to connect in a multitude of ways to access digital services and consume dynamic content.

Consumers are accustomed to a seamless, consistent, and high-quality experience in the commercial world, and they expect it from their government as well, regardless of the device or channel they use. They also expect those experiences to be secure and private. As security and data breaches continue making headlines, the American people are demanding better protection of their personal information and more security around their digital experiences. Agencies not meeting these demands risk losing people's confidence and trust, leaving some behind. Failing to meet these needs online forces the American public to seek costly, time-consuming alternatives such as phone, office visits, or mail.

Over a decade ago, the federal government recognized the need for greater security through Identity management by instituting the Federal Identity, Credential, and Access Management (FICAM) architecture. FICAM comprises the tools, policies, and systems that allow an organization to manage, monitor, and secure access to protected resources. Identity and Access Management has become critical to the government's success in delivering services to the public. In 2019, the U.S. Office of Management and Budget (OMB) updated the FICAM policy to require agencies to create their own Identity, Credential, and Access Management (ICAM) teams. And in 2022, OMB required agencies to provide phishing-resistant Multi-Factor Authentication (MFA) as an option for public users by the end of Fiscal Year (FY) 2024.

To meet the high expectations of today's government users, reduce development time of digital experiences, and eliminate potential security gaps, government agencies need to put employee, public, and other user Identity use cases front and center. In order to accomplish this, the need for enterprise-managed Identities is front and center for public sector organizations.

The power of cloud-based CIAM

CIAM systems securely capture and manage a user's Identity and profile data, and manage their access to applications and services. In government, many agencies are saddled with legacy systems to address legacy requirements. To address modern requirements many have resorted to using a hodgepodge of tools that are inflexible, inconsistent, expensive to maintain, and difficult to secure. The result has been a dissatisfying and fragmented user experience. Multiple applications require the American people to use different credentials, for different contexts, at different times. This frustrating and complicated approach discourages people from interacting digitally with government services.

Agencies can modernize their approach by implementing a cloud-based Identity solution, delivering agility, flexibility, speed to market, and scalability. Okta, the leading cloud-based Identity platform, supports the main capabilities of a modern CIAM solution:

- Frictionless user experience
- Fast deployment
- Centralized access management, including Identities both within and outside of existing directories
- Secure and highly scalable
- FedRAMP Moderate and High authorized platforms

Frictionless user experiences

Public and government users expect the same frictionless experiences across all their devices that they receive as consumers. That requires agencies to know and understand their customers. The cloud enables organizations to create secure, scalable repositories designed specifically to store and manage user information. And as you build out registration, login, or other common user web-based workflows, you should be able to customize those activities to user needs.

In the public sector, those users could be the American people, internal agency employees, former employees, users at other agencies, and many others. For example, CDO Technologies relied on Okta to raise the Air Force's security position by transitioning its entire Human Resources (A1) data center to the cloud. This effort helped to centralize Identity and Access Management for up to 5 million users annually, including active Air Force personnel, reservists, contractors, civilian employees, and retirees.

Fast deployment

A cloud-based CIAM solution allows developers to quickly and securely leverage new and updated tools to modernize services to the American public. To help them focus on core application logic, gain greater development agility, and develop apps faster, Okta provides tools that make it quick and easy for developers to integrate Okta Identity and security capabilities. That includes robust application programming interfaces (APIs) with easy-to-use software development kits (SDKs) and configurable prebuilt components using open standards that span a wide array of modern programming languages. Okta also provides extensive documentation, wizards, quick start guides, and API management integration. You can even add modern Identity capabilities into an app in less than 15 minutes by simply putting a hosted customizable Okta widget in front of your apps and portals.

These tools focus developers on building core services for your agency's apps and other digital experiences. They no longer have to worry about designing and coding common hacker-proof workflows to handle registration, sign-in, account recovery, forgotten passwords, MFA enrollment, and more. Nor do developers need to worry about keeping up with evolving Identity and security requirements. With Okta's CIAM platform, developers are more agile and productive — and needed security and privacy features are built in.

Case study: CDO Technologies

Tasked with advancing the privacy of 5 million U.S. Air Force users, CDO Technologies relied on Okta to raise the Air Force's security position by transitioning its entire Human Resources (A1) data center to the cloud, including 33 systems and 200 applications. Due to extensive experience, industry expertise, and proven capability, CDO chose Okta to assist with security, user experience, and value delivering the following benefits:

- Centralized IAM across 33 systems and 200 applications
- The ability to tailor information access according to user location
- Streamlined auditing and reporting tools
- Improved user experience anywhere in the world with simple, streamlined multi-factor authentication (MFA)
- Robust tools for analyzing user behavior across a broad portfolio and uncovering anomalies as they occur
- The ability to hand over the administration of individual applications to owners throughout the organization

Read the full case study:
www.okta.com/customers/cdo-technologies

Centralization of access management

As the number of users increases, it's essential to centralize access control decisions. Making and managing decisions on an app-by-app basis is inefficient and time-consuming. It can also leave an agency vulnerable to security gaps due to access and security policies being applied inconsistently from one app to another.

With CIAM, you can consistently and securely implement policies in the most frictionless manner possible. Understanding where to apply additional security requires contextual access management that considers what app is being accessed, authentication attempts, location of access, time of access, strength of password, anomalies in user behavior, devices being used, IP addresses, impossible travel scenarios, and more. Additionally, Okta's administrative user interface gives you one place from which to manage all users, apps, groups, devices, APIs, and policies.

Case study: Centers for Medicare & Medicaid Services and the U.S. Digital Service

The Centers for Medicare & Medicaid Services (CMS), an agency within the Department of Health and Human Services, administers the nation's major healthcare programs including Medicare, Medicaid, and the Children's Health Insurance Program (CHIP). It also oversees Healthcare.gov and quality standards related to the Health Insurance Portability and Accountability Act (HIPAA), long-term care facilities, and clinical labs.

As part of its shift to a value-based payment model, CMS worked with the U.S. Digital Service (USDS) to build a Quality of Payments Program (QPP) interface. The QPP replaced three government programs, each with its own Identity management system. In addition to simplifying and securing access to the appropriate information, CMS wanted a system that ensured that the best healthcare providers received the greatest benefits.

CMS and USDS adopted an API-first approach, connecting to clinical data registries that already contained information on healthcare quality and outcomes. CMS chose Okta to manage Identity and access because of its industry leadership and well-documented APIs. Okta API Access Management allows CMS developers to focus on streamlining the provider experience, while Okta securely controls access to the QPP website and API.

Key benefits of the project:

- 15 percent of Medicare claims are now submitted via the Okta-enabled API
- One website and API to gather information about healthcare quality and outcomes
- A modern Identity infrastructure, with improved security, reliability and scalability
- A streamlined user experience, delivered on time and within budget
- Read the full story: www.okta.com/CMS

Secure and highly scalable

Critical to the experience that any organization provides to its users is the ability to secure access to its applications and sensitive data. You need to protect the American public's personally identifiable information (PII) as well as comply with relevant regulations. Identity and Access Management is the foundation for security risk mitigation, and cloud-based CIAM plays a critical role in helping agencies lock down security, whether those applications are in your data centers or in the cloud.

However, having secure access is counterproductive if users find the experience of digital access too difficult and frustrating. Ideally, you want the right people to have the right access to the right resources with minimal friction. With cloud-based CIAM, security and great usability no longer have to be on opposite ends of the spectrum. Okta allows you to leverage a broad set of authentication factors combined with authentication threat intelligence and contextual response capability in adaptive multi-factor authentication (aMFA) to create secure, frictionless customer access experiences. This includes the ability to introduce responsible password-less authentication ranging from simple SMS to biometric options instead of less trustworthy passwords that can be compromised.

Furthermore, many application owners struggle to apply consistent and compliant security policies across all applications. They use an active directory for internal users and have to adapt other approaches for users outside their internal network. With Okta's Universal Directory, they can combine all user profiles into one secure, unified user directory across all applications, enabling single sign-on for users while ensuring security through multi-factor authentication.

To provide improved situational awareness, Okta dashboards and reports give you real-time visibility into your CIAM ecosystem. Okta also makes syslog data available to various analytics solutions, further enabling your response team to investigate and remediate issues quickly.

Identity and Access Management is the foundation for security risk mitigation, and cloud-based CIAM plays a critical role in helping agencies lock down security, whether those applications are in your data centers or in the cloud.

FedRAMP authorized platform

Okta has an official authorized status with the Federal Risk and Authorization Management Program (FedRAMP) of High Authority to Operate (ATO) as well as Moderate ATO. This means that federal agencies can leverage the Okta Identity Cloud and its features and capabilities, including Okta Universal Directory, to maintain external identities in a highly extensible first-class user store, allowing federated access to your applications without the need to create, manage and license Active Directory accounts. In addition, agencies can take advantage of Okta's Identity-proofing integrations, creating an even more powerful layer of security.

Beyond FedRAMP, Okta takes a comprehensive approach to securing its own infrastructure that spans its hiring practices, architecture, data center operations, and software development. It employs SOC 2 Type I and Type II processes to successfully audit its operational and security processes. It has achieved Cloud Security Alliance (CSA) Security, Trust, & Assurance Registry (STAR) Level 2 Attestation. Its ISO 27001:2013, ISO 27018:2014 certifications, and HIPAA Compliant Service attest to Okta's commitment to providing a secure service to its customers and to securing PII in the cloud.

Case study: Directorate of Defense Trade Controls

The Directorate of Defense Trade Controls (DDTC), part of the U.S. Department of State, has transformed the digital experience for its users. DDTC ensures that the commercial export of defense articles and services advances U.S. national security and foreign policy objectives. When DDTC decided to digitize its paper-based case management system, the agency realized that modernizing its CIAM component would prove demanding.

Over 13,000 external organizations are registered with DDTC as manufacturers, exporters, and brokers for defense services and defense articles. These organizations submit license applications to allow exports and temporary imports of munitions and technical data on the U.S. Munitions List. Before migrating to the cloud, DDTC struggled to figure out how to manage CIAM for so many collaborators. The cloud enabled DDTC to deliver CIAM in a fraction of the time it would take if they were to build a solution from scratch.

Key benefits of the project included:

- The consolidation of eight legacy Identity databases into one for all CIAM needs
- A 360-degree-view of user activity across all applications and an understanding of exactly who sees what information
- Significantly better security while delivering a seamless experience for license applicants

Modern CIAM with Okta Identity Cloud

Built for the modern era, the Okta Identity Cloud enables government to deliver secure, consistent digital experiences to its workforces, partners, suppliers, and public community. It's a holistic IAM solution that seamlessly incorporates and unifies Workforce Identity and CIAM capabilities into a single technology platform that can transform the digital experiences of the American people and agency employees alike.

Okta's simple-to-use APIs and out-of-the-box tools enable developers to create seamless experiences while giving IT and security teams a central place to manage security policies. Okta's API Products serve as Identity building blocks for any agency's mobile or web applications, providing three core services to accelerate digital transformation:

- **Embeddable Authentication:** Okta's prebuilt UI widgets let you create frictionless and secure user experiences with common user flows such as login, registration, and password reset, or build completely customized experiences with Okta's APIs.
- **Embeddable Authorization:** You can control which APIs your users and developers can access using Okta's API Access Management. You can also customize claims and scopes, as well as insert external attributes using Okta's token extensibility.
- **User and Policy Management:** Okta lets you manage users and security policies programmatically via APIs or from a user-friendly admin console. You can also create single sign-on (SSO) experiences and manage the user lifecycle with automated onboarding and offboarding.

About Okta
With more than 7,000 out-of-the-box integrations, Okta makes it easy to bring Identity to various elements of your agency infrastructure.

Born in the cloud and supporting best-of-breed technology, Okta Identity Cloud helps ensure success in digitally engaging users of all types — be they citizens, employees, contractors, or other agency stakeholders — while increasing security, increasing efficiency, and reducing costs.

To discover more ways in which Okta can help modernize and secure your organization, visit www.okta.com/okta-public-sector.