eBook

Leveraging Identity

A Public Sector Guide
for External Services

Contents

Introduction

Government and education organizations today are tasked with providing a vast number of services to the American people — a core principle of which is to ensure those services reach the right people, and that the data provided by residents or staff is safe from malicious actors. Whether government-to-consumer (G2C), government-to-government (G2G), or government-to-business (G2B) and education business models alike, ensuring all external-facing Identity services are secure and user-friendly can bolster trust, fight fraud, and much more.

From providing services to the American public to engaging with business customers and mission partners, public sector organizations support a wide range of external interactions. Too often, individuals and business partners today must struggle through multiple Identity systems in order to engage with government. That erodes the end-user experience, and impedes an agency's ability to meet its mission. Federal civilian and defense agencies, state and local governments, and higher education alike: All must provide a secure and seamless Identity experience for their external stakeholders.

Introduction

"Whether we are talking about the government's customer as the American public, another government agency, or a business partner, people want to avoid retelling the same information and want to avoid getting stuck in a digital queue while confirming their Identity," said Patrick Chu, federal civilian director for Okta, the leading independent Identity partner trusted by government organizations and educational institutions to provide secure connections between people and technology.

While it's vital that staff be able to access applications and information without hassle, secure access with a seamless experience has never been reserved for just the workforce. The external Identity journey is vital to ensuring smooth interactions for those outside an organization who need access to services or information. And this is more important now than ever, given that customer service has emerged as a priority at the highest levels. The Executive Order on Transforming Federal Customer Experience and Service Delivery[1], for example, challenges public-sector organizations to be more responsive — and that starts with an improved Identity experience in support of more simple end-user engagements.

[1] https://www.whitehouse.gov/briefing-room/presidential-actions/2021/12/13/executive-order-on-transforming-federal-customer-experience-and-service-delivery-to-rebuild-trust-in-government/

Introduction

$25.6b

Growth from 2022–2027
The global Identity and Access Management market is expected to grow from $13.4 billion in 2022 to $25.6 billion by 2027.

"Agencies should continually improve their understanding of their customers, reduce administrative hurdles and paperwork burdens to minimize 'time taxes,' enhance transparency, [and] create greater efficiencies across government," according to the Executive Order (EO).

With the global Identity and Access Management market expected to grow from $13.4 billion in 2022 to $25.6 billion by 2027[2], there's growing awareness of the key role Identity plays, not only in enabling seamless service delivery, but also in securing IT systems and data. The National Cybersecurity Strategy[3], for example, makes it clear that strong digital Identity solutions, including those applied to public-facing systems, are foundational to security.

[2] https://www.marketsandmarkets.com/Market-Reports/identity-access-management-iam-market-1168.html?gclid=EAIaIQobChMIzO3il7KO_gIVtcmUCR3e7wk5EAAYAyAAEgJ3ZPD_BwE

[3] https://www.whitehouse.gov/briefing-room/statements-releases/2023/03/02/fact-sheet-biden-harris-administration-announces-national-cybersecurity-strategy/

An Urgent Need

There's an urgency to the Identity situation in the public sector. Many agencies and universities still depend on legacy custom-built customer Identity solutions. Often these have been implemented without considering security features such as Multi-Factor Authentication, threat detection, or reporting.

As technology continues to dominate interactions with government, IT teams are finding it increasingly difficult to manage access on an app-by-app and customer-by-customer basis. For example, when a university has different Identity tools for managing student applications, submitting student aid, and applying for student work, things quickly become unwieldy.

There's also the user experience to consider. As government seeks to serve every member of the American public — from business owners to members of the military to those seeking benefits services and beyond — agencies need intuitive logins that are accessible even to less tech-savvy users. Importantly, the first interaction most public sector organizations have with the American public is via log-in services. When those services are complicated and threat-prone, many of these impressions start out on the wrong foot.

An Urgent Need

At a time when trust in government is already at record-low levels, it erodes public trust even further when government agencies fail to provide simple, effective login and Identity management services. Pew Research reports that just two-in-ten Americans say they trust the government in Washington to do what is right “just about always” or “most of the time” — and failure to act now will only compound the problem going forward.[4]

Technology is becoming ever more pervasive. That means the systems supporting the customer experience must be adaptable enough to accommodate emerging and perhaps unforeseen future interactions.

With cloud-based systems, government can take a new approach to Identity, taking advantage of scalable, future-ready tools, like Single Sign-on — tools that allow agencies for example to personalize external engagements. Such an approach would reduce the administrative burden that threatens to overwhelm IT teams and would deliver the kind of seamless interactions that the American public, students, and other key external stakeholders want and expect.

[4] https://www.pewresearch.org/politics/2022/06/06/public-trust-in-government-1958-2022/

Federal Civilian

When people interact with federal civilian agencies, there's a growing expectation that their experiences will be seamless and straightforward: checking their benefits should be as easy as checking their bank balance. To that end, "government should find a way to modernize its Identity systems so that consumers can … validate their credentials in the online world — and do it in a way that protects privacy and guards against Identity theft," according to the advocacy group The Better Identity Coalition.[5]

The Challenge

Legacy Identity approaches make it complicated and time-consuming for the American public to engage with government.

Individuals looking to access services may find themselves providing the same information multiple times to multiple government agencies or even within a single agency. They may run into a range of authentication and authorization experiences, all of which add time and complexity to their interactions.

There are government-to-government Identity issues as well. Agencies are tasked to deliver inter-governmental support, such as the proper distribution of data or access to needed systems. The Department of Veteran Affairs, for example, needs access to research data from the National Institutes of Health in order to promote effective care[6], while the Office of Personnel Management needs to collect telework data[7] from across multiple agencies in order to drive effective policy-making[8]. Outdated authentication processes can get in the way of such efforts.

Businesses turn to government economic and financial data as well for regulatory guidance and procurement opportunities. These interactions with government can become problematic, especially when legacy Identity systems make it difficult to access these resources and information.

All these hurdles generate frustration on the part of stakeholders. Moreover, the inability to gain smooth and easy access interrupts an agency's ability

[5] https://www.betteridentity.org/five-key-initiatives

[6] https://veterans.joinallofus.org/en#:~:text=What%20is%20All%20of%20Us,get%20sick%20or%20stay%20healthy

[7] https://chcoc.gov/sites/default/files/2022-Data-Call-HR-Directors-Memo1208.pdf

[8] https://www.whitehouse.gov/wp-content/uploads/2023/04/M-23-15.pdf

Federal Civilian

to deliver important services on behalf of the American people. “If they can’t avoid providing these bad experiences, the government risks falling short on their mission delivery,” Chu said.

The Goal

As stated in the EO on Customer Experience, government “must be held accountable for designing and delivering services with a focus on the actual experience of the people whom it is meant to serve.”

The EO makes this not just a question of mission objectives but posits smooth interactions with government as a foundational idea: “Strengthening the democratic process requires providing direct lines of feedback and mechanisms for engaging the American people in the design and improvement of Federal Government programs, processes, and services.”

It sets a high bar for agencies that serve the American public in high-stakes areas such as travel and health, as well as agencies with financial or security responsibilities. The goal here is to deploy Identity in such a way as to facilitate not only secure but also seamless interactions — to strike a balance between the need to protect privacy and security, on the one hand, and the need to make government readily accessible to all, on the other.

To that end, federal civilian agencies — especially High Impact Service Providers (HISPs) like the Transportation Security Administration (TSA), United States Department of Agriculture (USDA), U.S Department of Health and Human Services (HHS), and the Internal Revenue Service (IRS) — must meet various goals and mandates that call on them to shift their focus around security and access[9]. While many agencies have already begun to apply Human-Centered Design (HCD) methods with the aim to coordinate service delivery based on some of the most critical moments in people’s lives, it’s crucial that they maintain momentum[10] as they move away from solutions built around existing funding streams or organizational structures and turn instead toward more effective and efficient systems that prioritize the user experience.

[9] https://www.performance.gov/cx/hisps/

[10] https://www.whitehouse.gov/omb/briefing-room/2023/03/03/fact-sheet-biden-harris-administration-launches-nine-life-experience-projects-to-streamline-service-delivery-for-the-american-people/

Federal Civilian

For agencies that serve other agencies and those that interact with business partners, “the goal is to facilitate information exchange in a secure and seamless manner,” Chu said. In doing so, agencies position themselves for future success. “When an agency can provide access to critical resources from anywhere in the world, while also validating who has access to what, they can better operationalize how they run support which could ultimately lead to more staff and funding.”

“When an agency can provide access to critical resources from anywhere in the world, while also validating who has access to what, they can better operationalize how they run support which could ultimately lead to more staff and funding.”

Patrick Chu
Director, Federal Civilian, Okta

Identity in Action: CMS transforms the American healthcare system. Okta secures and streamlines Identity.

The Challenge

The government faces Identity challenges that go beyond just log-in and account creation. For the Centers for Medicare and Medicaid Services (CMS), the challenge lay in connecting multiple clinical data registries.

Under the Medicare Access and CHIP Reauthorization Act (MACRA), CMS was tasked to consolidate three existing websites into a single user experience, as well as building an information-gathering API, connecting the website to clinical data registries.

Because each existing site had its own legacy Identity management system — mostly built in-house — login and account creation presented significant hurdles. The team also needed to design an information-gathering process that would help CMS shift the focus toward performance-based compensation strategies.

The Solution

The complex task “led them to choose Okta for an API-first approach,” said Stephanie Davidson, federal civilian director for Okta.

The new Quality Payment Program (QPP) empowers CMS to collect evidence, payments, and other required data in a secure portal. The interface has been instrumental in transforming the U.S. healthcare system, as it shifts emphasis toward a value-based payment model and away from traditional fee-for-service. Okta API Access Management allows CMS to focus on streamlining the provider experience.

By taking this approach, “they were able to design an information-gathering process that ensures the best providers receive the greatest benefits,” Davidson said. “Other agencies that need to securely connect layers of access can benefit from a similar deployment.”

Department of Defense

The Department of Defense (DoD) interacts with a broad and varied user base. Mission partners such as other federal agencies, suppliers, or allied nations "often need to access shared data and resources in order to execute military operations and defend the nation," said Sabrina Lea, director of DoD and Intelligence Community at Okta. Among these, there are many who do not have access to the Common Access Card (CAC), DoD's most-used form of authentication.

The Challenge

Government-to-business use cases include "the suppliers and contractors of the Defense Industrial Base (DIB), whose contributions to military operations range from logistics and supplies to contracted labor and support. These businesses require access to web portals, mission applications, and other shared systems in order to support the Department," Lea said.

When it comes to the mission partner environment, the DoD Instruction 8110.01 emphasizes the importance of "effective information sharing,"[11] and calls for "Identity, credential, and access management policies that support secured, available, and accurate electronic information sharing."

[11] https://www.esd.whs.mil/portals/54/documents/dd/issuances/dodi/811001p.pdf

Department of Defense

But this is not easily achieved. Various populations may encounter different authentication protocols, even when accessing the same systems. "If modern Identity solutions are not adopted, these stakeholders — and the administrators who serve them — will have to deal with different user experiences, different security controls, and limited interoperability across Department resources," Lea said.

The DoD CIO's office has recognized the challenge[12], noting that "[i]n order to interact with these mission partner entities, authentication services must be able to consume mission partner credentials by leveraging a persistent, unique identifier" consistently and effectively.

The Goal

On the public-facing side, DoD needs to find a way to eliminate access barriers across the non-CAC community, especially in support of engagements with new recruits, spouses, and other external stakeholders. DoD needs to streamline and simplify access, connecting these populations to necessary healthcare, education, and human resources services and information more effectively, while still protecting sensitive data.

In its engagements with others in government, defense organizations need to move away from legacy Identity solutions that cause disparate, workaround user experiences. The DoD also needs to ensure that contractors and other key suppliers in the DIB have the access they need to meet mission-critical demands in a timely manner. In fact, the Government Accountability Office has warned that too few new companies are joining the ranks of defense contractors, with many saying that administrative burdens make it too hard to engage with DoD. Even suppliers already working with DoD may be reluctant to bid on DoD contracts due to "lack of access to and communication from DoD," RAND reports.[13] It's essential that DoD adopt an approach to Identity that allows it to break down the access barriers across supplier communities, while still ensuring the security of sensitive information and systems.[14]

"With a modern Identity platform, DoD can fully embrace mission elasticity, avoiding workarounds or disparate user experiences for users trying to access personally-identifiable or mission-critical information," Lea said.

[12] https://dodcio.defense.gov/Portals/0/Documents/Cyber/DoD_Enterprise_ICAM_Reference_Design.pdf

[13] https://www.rand.org/pubs/research_reports/RR267.html

[14] https://www.nationaldefensemagazine.org/articles/2022/2/4/pentagon-struggles-to-attract-new-entrants-into-industrial-base

Identity in Action: Tasked with advancing the privacy of 5 million U.S. Air Force users, CDO Technologies relies on Okta to raise the organization's security position.

The Challenge

CDO Technologies was charged with moving the entire Human Resources (A1) data center for the U.S. Air Force to the cloud, including 33 systems, 200 applications, and 5 million users. These systems don't just serve staff and military personnel, however. They also need to support the needs of military recruiting, military universities, family services, and veterans.

A1 users include all active Air Force personnel, as well as ancillary and non-active-duty users. In an effort to put all users under the same Identity umbrella, the CDO team deployed solutions from both Okta's workforce Identity and customer Identity product lines.

"The A1 project follows the complete lifecycle of an airman throughout their career and transition to civilian life," Lea said. "During this time, an airman can change locations, status, and roles, and the Air Force can analyze user behavior across a broad portfolio to uncover user login patterns as they occur. Additionally, the airman's dependents can now access Department resources in a modern and secure way."

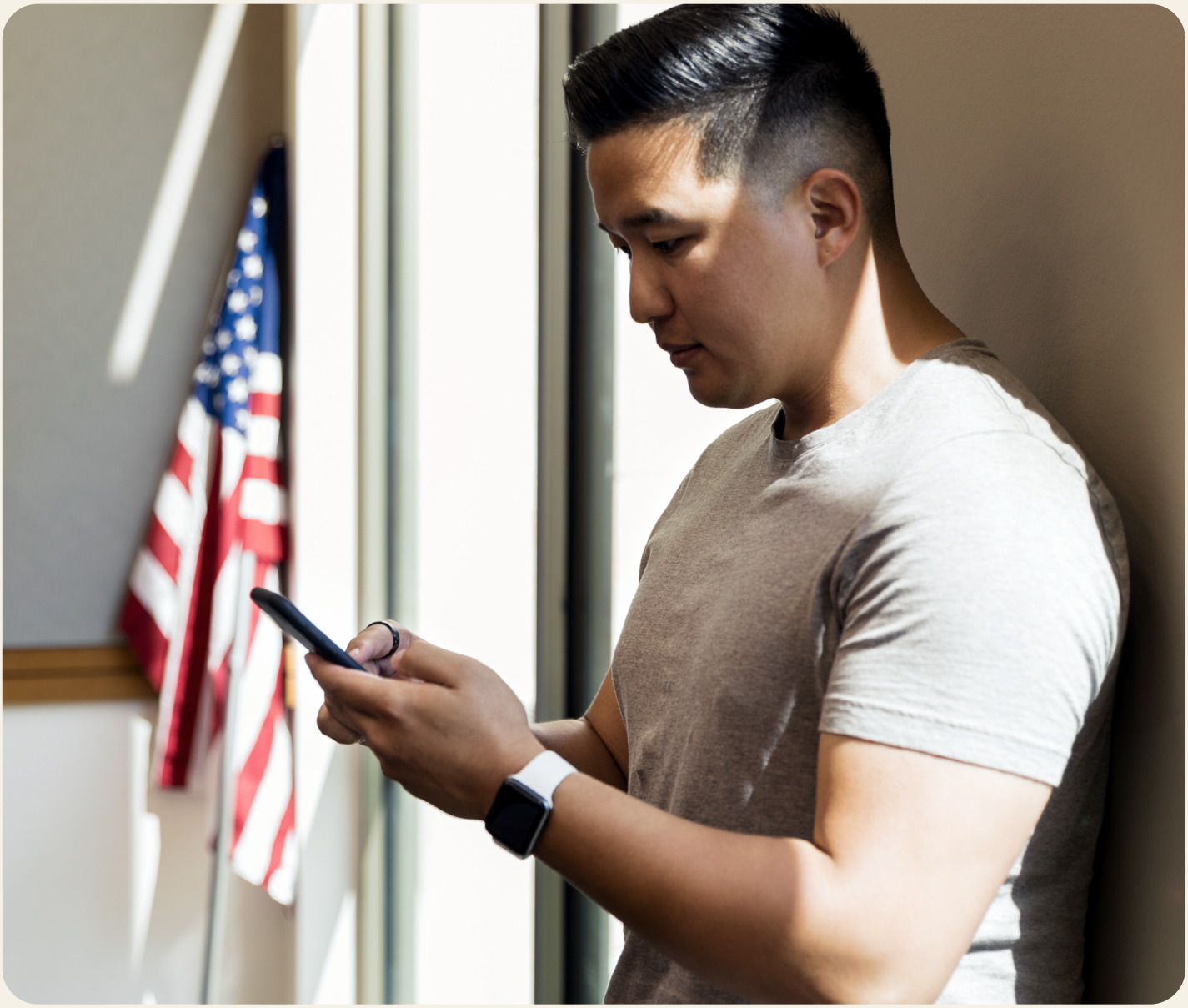
The Solution

The project shifted some 200 applications to the cloud, tapping Okta Adaptive Multi-Factor Authentication for Identity and access management. Those who don't have CAC access can use Okta Verify, a Multi-factor Authentication (MFA) app that lets users verify their Identity when they sign in to Okta, making it less likely that someone pretending to be the user can gain access to the account.

Ultimately, with the help of Okta, users have a seamless experience, and Air Force administrators can tailor application access depending on user location. "By turning to Okta, other DoD organizations who have a diverse user population can benefit from a similar deployment," Lea said.

200

The A1 project shifted some 200 applications to the cloud, tapping Okta Adaptive Multi-Factor Authentication for Identity and access management.



okta

“With a modern Identity platform, DoD can fully embrace mission elasticity, avoiding workarounds or disparate user experiences for users trying to access personally-identifiable or mission-critical information.”

Sabrina Lea
Director, DoD and Intelligence Community, Okta

State and Local Government

In state and local government, effective Identity solutions are key to supporting interactions with residents and delivering vital services. When people go online to look up real estate tax information, renew a driver's license, or pay a government fee, they want that interaction to be seamless and stress-free. The National Association of State Chief Information Officers (NASCIO) has said that effective Identity and access management "is essential to enabling effective, relevant, and secure interaction and services between state government and its employees and constituents."[15]

The Challenge

Historically, the process of applying for or renewing benefits or engaging with other functions of state government, such as licensing and permits, "has been time-consuming, confusing, and complicated," said Erika Messerschmidt, senior manager of solutions engineering for Okta.

Government-to-government transactions, as well as engagements with the business community, have likewise been plagued by manual, paper-based processes. And recent circumstances have made a difficult situation worse.

[15] https://www.nascio.org/wp-content/uploads/2022/10/2022-State-CIO-Survery-_a.pdf

State and Local Government

"For example, states continue to struggle with pandemic backlogs due to the intense burdens on Unemployment Insurance (UI) systems," Messerschmidt said. That pressure, in turn, has been exacerbated by an uptick in fraud exploits aimed at state and local governments. "Using the Identity of another person and using fake Identity information are two fraud schemes that contributed to the fraud and breakdown of federal-state relief programs," Messerschmidt adds.

> "Using the Identity of another person and using fake Identity information are two fraud schemes that contributed to the fraud and breakdown of federal-state relief programs."
>
> **Erika Messerschmidt**
> Senior Manager of Solutions Engineering, Okta

On the upside, these trends have generated momentum around state and local Identity efforts.

"Recent federal initiatives and legislation have established the risk of getting Identity verification wrong and are responding with strategy and funding to support stronger preventative steps," Messerschmidt said. "There's now a collective effort across government to modernize efforts and improve service delivery to benefit the intended person."

The Goal

When the American public interacts with state and local government, they expect a level of ease and intuitiveness that's at least on par with what they encounter in their digital private-sector engagements.

State and Local Government

“That is always in the back of the mind for most government officials,” Messerschmidt noted. “State and local governments are working through complex bureaucratic structures that can slow down the development and deployment of digital services,” she said — but that does not excuse them from the responsibility of elevating that end-user experience.

Trust in government is low, and it’s vital that state and local authorities have in place Identity systems that deliver a seamless experience while still ensuring the safety of personal information. Individuals want it, and the businesses that interact with government increasingly are demanding it.

“To deliver the frictionless, seamless, and most importantly secure experience desired, you’ll want a central view of identities to easily manage user access and without the need for multiple usernames or passwords,” Messerschmidt said.

Identity in Action: Larimer County Enhances Digital Services with Okta and Auth0

The Challenge

Larimer County, Colorado faced a situation familiar to many government organizations.

With an IT infrastructure built up over time, the county had a disparate infrastructure that relied too heavily on Active Directory Federation Services (AD FS) and didn't provide sufficient support for the county's cloud-based apps. IT had to shoulder a heavy workload, and the county found it difficult to serve residents efficiently and securely.

The county needed a new means to enable citizen access to a range of digital services.

The Solution

To simplify and streamline access to cloud-based apps, the county adopted a number of Okta's Workforce Identity products. This improved access not only for employees, but also for citizens looking to access the county's expanding inventory of digital services.

State and Local Government

To extend Identity capabilities to its citizens, the county leveraged Okta's Auth0's flexible customer Identity solution. A drop-in solution that adds authentication and authorization services to applications, Auth0 enables an organization to rapidly integrate authentication and authorization for web, mobile, and legacy applications.

By taking this route, the county was able to provide citizens with seamless access to county services via their social media logins, while also centralizing authentication.

Looking ahead: By consolidating its infrastructure with Okta, the county was able to add an extra layer of security and automated provisioning, ensuring that stakeholders can always securely access the services they need.

In the future, the county will be able to use Okta and Auth0 to provide citizens with a more convenient, customized digital experience. In addition, Larimer County plans to improve its security posture by gaining more control off-network server access and leveraging new Multi-Factor Authentication features.

Higher Education

When it comes to Identity and Access Management (IAM), higher education faces a unique situation. According to the Association of College and University Auditors (ACUA), "the openness of the educational and research environment in higher education, the large numbers of users entering and leaving your institution annually, the many different types of users"[16]— including employees, students, affiliates, and vendors — all come together to create "unique challenges to ensuring an effective and efficient IAM control environment."

The Challenge

In higher education, it's important to provide all campus users with a secure and seamless digital experience. That gets complicated when users must interface with multiple systems, often encountering varied authentication protocols. They might, for example, have to use different credentials to access learning modules, academic records, tuition and payment information, and other campus resources.

In their interactions with outside scholars and other academic institutions, schools are seeking to facilitate seamless collaboration while also addressing the security concerns that arise with present workaround solutions. And in their engagements with the business community, colleges may be looking to coordinate more efficiently with employers in order to support high job-placement rates. Commercial partnerships and other ties that can help to strengthen the institution's reputation may be held up by outdated security practices.

The intrinsic openness of the campus environment inevitably complicates efforts around Identity. Schools want to promote a free and open exchange of ideas and, in the digital age, that means they must facilitate access to key data and applications.

"Colleges and universities accept many visiting students, faculty, and staff for various reasons," Messerschmidt said. "At the very least, these visitors will need Wi-Fi access, and they will likely need readily available access to other systems as well, whether in pursuit of research projects or other academic objectives."

[16] https://acua.org/Training-Networking/Webinars/Identity-and-Access-Management-in-an-Academic-Envi

Higher Education

Too often, “these visitors may need a separate username and password to access systems, or they could potentially ‘borrow’ credentials from another student or faculty member,” Messerschmidt said — a common workaround that jeopardizes security.

The Goal

In modernizing the approach to Identity, many schools will be looking to ease the burden of IT staff, who may be spending untold hours provisioning and managing identities under current legacy solutions. They’re looking to free up time and talent to devote to higher-order technology needs.

All this becomes even more urgent as schools adapt their operations to the needs of the post-pandemic era.

“Administrators, more specifically CISOs and CIOs, strive to create a seamless learning experience, especially in the current hybrid learning environment,” Messerschmidt said. “A student’s location should most definitely be taken into consideration, but they should be able to use their ‘home’ credentials versus creating multiple accounts.”

“Administrators, more specifically CISOs and CIOs, strive to create a seamless learning experience, especially in the current hybrid learning environment.”

Erika Messerschmidt
Senior Manager, Solutions Engineering, Okta

Identity in Action: Helping University of Notre Dame's students and IT team work smarter

The Challenge

The University of Notre Dame is a leading research institution with more than 18,200 students, faculty, and staff. The technology its stakeholders use to learn, teach, research, and collaborate has grown rapidly in recent years, creating an opportunity for the institution to modernize its approach to Identity management and provide its campus users with a secure, seamless experience.

"Notre Dame's digital infrastructure expanded rapidly, and their homegrown Identity and access management system — which dated back more than two decades — could not scale to address the required operational efficiency or potential data breaches," Messerschmidt said.

"The growth in their Identity and access management systems resulted in having to balance security and user experience, neither of which should be competing with the other," she said.

Operational efficiency and vulnerability to data breaches became time-consuming challenges. The university needed to modernize and automate IT workflows. The institution wanted an IAM solution with seamless, scalable integrations to tackle the unique challenges within the higher education sector and a sprawling IAM system. School leadership also wanted greater visibility into daily IAM activities and smoother account provisioning.

The Solution

Notre Dame turned to Okta as an Identity partner that could provide trusted expertise and a solid foundation. To ensure the implementation of the Okta Identity Cloud would be frictionless for all of its users, the school worked with Okta to seamlessly transition its diverse stakeholder groups to the new system. At the initial go-live, all users made the change to Okta Single Sign-on and Okta Verify for Multi-Factor Authentication in a smooth and seamless deployment.

Looking Ahead

With rising expectations around customer experience, and a growing cybersecurity threat, Identity is a front-and-center concern in the public sector. “Nearly every organization today needs a way to have visibility and control into who has access to what,” according to the Identity Defined Security Alliance.[17]

Going forward, public sector entities will need to find robust solutions to Identity for both workforce as well as public and community users.

There’s certainly an economic incentive here. The American Enterprise Institute, a public policy think tank, notes that cyber-criminals “are constantly looking for holes in online Identity verification—a key reason why the US government lost $163 billion in unemployment-related fraud during the pandemic.”[18]

Government and higher education need to look to the future of Identity in order to support their digital transformation efforts. Legacy solutions haven’t been able to keep pace with the transition to the cloud: They don’t scale well, nor do they integrate with cloud systems to support a seamless user experience.

What does a modernized Identity solution look like? It needs to deliver:

- **A cloud-based approach to external-facing Identity:** The adaptability of a cloud-based solution allows developers to quickly deploy new or updated tools, such as social authentication, so that they reach the public more quickly.
- **A centralized approach to access management:** By bringing all access points and administrative decisions under one roof, a modernized solution eases the burden on administrators, freeing up valuable IT talent for higher-level tasks.
- **Comprehensive access policies based on criteria like user profiles and group memberships,** including requirements to recognize and control segmented access rights for different scenarios. With automation technology, policy engines can deliver stronger Identity

$163b

The American Enterprise Institute notes that cyber-criminals “are constantly looking for holes in online Identity verification—a key reason why the US government lost $163 billion in unemployment-related fraud during the pandemic.”

[17] https://www.idsalliance.org/modernizing-identity-governance/

[18] https://www.aei.org/technology-and-innovation/modernizing-the-federal-identity-system-highlights-from-a-conversation-with-jordan-burris/

Looking Ahead

hygiene: If a student changes a department, for example, or a staff member audits a course, those permissions are updated accordingly.

- **Ability to apply additional security based on contextual access management:** This allows administrators to manage Identity more finely, looking at what app is being accessed, authentication attempts, location of access, time of access, the strength of the password, anomalies in user behavior, devices being used, IP addresses, impossible travel scenarios, and more.

A leader in customer Identity, Okta helps government and education organizations of all levels, delivering robust solutions in support of public sector organizations. Its solution include:

- **Universal Directory:** Enables organizations to manage data from multiple sources, granting access that's filtered and published to those with the proper security permission to access it.
- **Okta Verify:** A Multi-Factor Authentication app that makes it less likely that someone pretending to be the user can gain access to the account.
- **Adaptive MFA:** Protects Identity and access to data wherever your users go and wherever your data lives.
- **API Access Management:** Allows you to secure your APIs with Custom Authorization Servers, custom scopes, claims, policies, and rules to determine who can access API resources, regardless of the API gateway.

Learn more about how Okta can help ensure Identity and access management is seamless and secure for your external services!

Continue here →

okta

Okta Inc.
100 First Street
San Francisco, CA 94105
info@okta.com
1-888-722-7871