OH | ID

Ohio Digital Identity Program

Providing a Secure Digital Customer Experience for Ohio's Workforce & Citizens

Category: Cybersecurity

State: Ohio

Project initiation: January 2017

Project completion: September 2018

Contact:
Derek Bridges
Department of Administrative Services, State of Ohio
derek.j.bridges@das.ohio.gov

NASCIO 2019 STATE IT RECOGNITION AWARDS

Executive Summary

Ohio's digital identity program includes user lifecycle management, identity proofing, strong authentication, coarse-grain authorization, fraud analytics, and threat monitoring. Once deployed, users who log in with their respective identity enjoy single sign-on to onboarded applications, as well as a safer, more secure experience.

Ohio's digital identity program provides an end-to-end solution that fosters a simpler, more trustworthy, and secure experience between the State and its constituents by:

- Developing a single proofed identity for citizens, businesses, or internal users than enables access to all required state resources with the assurance that the individual is who they say they are
- Automating privacy and security laws and policies compliance, including NIST, HIPAA, IRS 1075, accessibility standards per section 508 of the Rehabilitation Act, and the State of Ohio's standards for data retention
- Hosting in the cloud on a highly available and highly resilient redundant infrastructure
- Offering three levels of assurance, as well as multi-factor authentication with the level and frequency of identity authentication chosen by the individual content owners
- Delivering a set of identity services for consumption by all agencies, boards, and commissions that will simplify, decrease cost, and enable delivery of a better experience for the end user

With the successful completion of Phase 1 in September 2018, Ohio's digital identity program has brought to life its vision to provide a more secure and intuitive digital experience through enterprise identity tools and capabilities. Adoption of the state's enterprise digital identity capabilities during this initial phase yielded significant value through approximately $65M in cost avoidance, exceeding the program's expectations.

Beyond these financial benefits, Ohio's digital identity program has delivered value through increased security, operational efficiencies, centralized regulatory compliance, higher productivity, and an enhanced user experience. In addition, the program's scalable platforms and repeatable processes enabled efficient agency on-boarding and lowering barriers to and cost of adoption, resulting in adoption above and beyond the initial scope for Phase 1.

Ohio's Phase 1 pilots demonstrated the program's ability to integrate its capabilities with both high-profile / high-volume applications requiring legacy integration and an emerging class of business applications. As agencies and programs onboard to this enterprise platform, they avoid ongoing and redundant costs associated with security, privacy, and ADA solutions that would otherwise be maintained at the agency and program level while also allowing quicker reaction to policy or cyber events. In an ever-evolving digital security landscape, Ohio's enterprise identity program provides agencies and state organizations an opportunity to proactively identify and manage treat risks, produce enterprise cost savings and support a more seamless user experience all while allowing the business to maintain control over the level of authentication required.

Phase 1 Accomplishments

- **$65M** in cost avoidance
- Cost of application on-boarding reduced **85%**
- Integration of **180+** business applications
- **350,000+** citizen user accounts established
- All state agencies, boards, commissions & counties have on-boarded to identity, including **80,000+** state workforce users

Concept

As the number of customers preferring digital interactions increases, states must be diligent in keeping vital data from falling into the wrong hands. Failure to enact strong security practices is costly. On average, a security breach costs an organization $225 per record (per breach), and that is even before considering the cost to reputation and loss of customer confidence[1]. The risk for government agencies is even higher, and yet, 78% of customers indicated that the government is not sufficiently prepared to handle a cyberattack[2].

In this environment, proactive defense against security threats is key. Ohio's enterprise digital identity program focuses on leveraging digital identity as the fabric supporting an end-to-end digital user journey. The program's goal is to provide a secure and private digital identity and an intuitive and interactive user experience for Ohio's citizens, businesses, and workforce.

Ohio's digital identity platform centralizes security and compliance, allowing the organization to be holistically responsive to new threats. Security measures can be assessed and monitored by a dedicated team, and threat patterns across the enterprise can be identified. No longer is there a weak link in an underfunded, outdated or overburdened agency or departmentally-managed security protocol.

By utilizing a single set of credentials and a centralized access platform, Ohio's enterprise identity program is not only more nimble and secure, but also reduces costs. In Ohio, onboarded agencies no longer need to maintain separate security systems, reducing the overall need for infrastructure and maintenance investments.

In addition, Ohio's digital identity program helps agencies and state organizations provide a better customer experience. Through single sign-on, customers – from the State workforce to businesses to citizens – can access onboarded agency and department applications from a central location after logging in just once. Customers do not need to remember multiple usernames and passwords or navigate to multiple websites to get the information they are looking for or need.

All of this is done without constraining the ability of the business to choose the "right fit" level of authentication or security required for their customers and data. Ohio's digital identity program has implemented a variety of user authorization options, from two-factor authentication to identity proofing, depending on the level of security the agency and data requires. This allows customers to quickly and easily access their data but ensures the organization can validate the identity of the user to the level of certainty required.

Ohio's Digital Identity Guiding Principles & Capabilities

Ohioans expect their information to be secure and private. Ohio's digital identity program provides an enterprise solution that equips agencies to safeguard customer data and maintain compliance standards. Digital identity goes beyond security by also meeting customers' expectations for personalization, self-service account maintenance, and single sign-on access across state systems. The state formalized these concepts into two guiding principles:

- Security and privacy come first; securing data and information entrusted to the State is of foremost importance.
- Provide self-service and choice for customers to manage their own interactions.

[1] 2017, Ponemon Cost of Data Breach Study
[2] 2017, Aaron Smith, Attitudes about cybersecurity policy

Concept Con't

The state's digital identity program provides state agencies and organizations with capabilities that ensure that state resources and information are accessible to every Ohioan and simplifies interactions with state systems while keeping information secure and private.

Single Sign-On
Sign in once to get to everything

2-Factor Authentication (2FA)
Secure assets with second factor

Multi-Factor Authentication
Increased identity security when needed

Privileged Access Management
Greater controls for sensitive accounts

ADA-Compliant
Built-in accessibility compliance

Real-Time Analytics
Monitoring and analysis

Self-Service Portal
For integrations and users

Identity Proofing
NIST-compliant proofing

Access Logging
Full logging and history

Access Management
Control Access by roles and groups

Just-In-Time Provisioning
Add users where and when needed

User Management
Manage all users

Each user's identity is centrally maintained within a controller infrastructure managed by leading practices across a host of NIST, federal, state, and accessibility regulations and standards so agencies can focus resources on services to their constituents. This solution provides the following capabilities and key security and privacy benefits:

- Provides Single Sign-On (SSO) to internal and external applications
- Automates provisioning and de-provisioning of users in near real-time
- Expands automated user provisioning and consolidation via industry standard endpoint adapters
- Mitigates security risks associated with human intervention through self-service password reset
- Provides Multi-factor Authentication (MFA)
- Provides validation of citizen identities using Experian Identity Proofing
- Closely integrates with State SIEM for real-time threat monitoring
- FedRAMP moderate certified infrastructure
- Deploys ID as a common security platform that follows State and Federal guidelines like 800-53 and 800-63-2
- Complies with NIST FIPS 140-2 and State's ITS-SEC-01 for data encryption and cryptography
- Adheres to user accessibility standards in Section 508 of the Rehabilitation Act
- Complies with IST 800-88 standard for data destruction

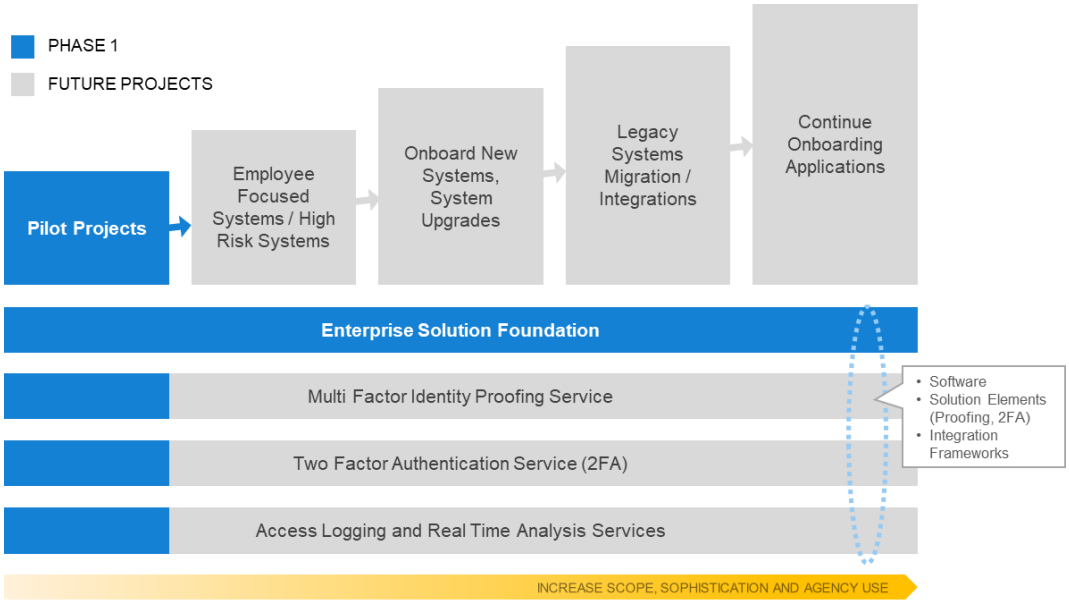
These capabilities are scalable and delivered through a self-service enablement approach, meaning agencies can quickly onboard applications, portals, websites and intranets. Capabilities such as single sign-on and built-in ADA compliance mean all Ohioans can access the critical information and services they need from anywhere and on any device. The platform's adherence to NIST, federal and state security and privacy standards means citizen interactions with on-boarded applications and portals are always supported with the latest security standards, eliminating the need for individual agencies to monitor and maintain compliance on their own.

Concept Con't

Phase 1 Overview

The goal of Phase 1 of Ohio's digital identity program, launched in January 2017, was to implement a meaningful set of pilots that would demonstrate the program's ability to integrate its capabilities with both high-profile and high-volume applications requiring legacy integration and an emerging class of business applications. Through Phase 1, Ohio's digital identity program:

- Enabled single sign-on and a single user identity/experience across state systems
- Ensured compliance with NIST, federal and state security and privacy standards
- Provided self-service for customers to securely maintain their accounts and profiles



Four pilots were planned to establish the enterprise solution foundation and implement core identities and frameworks. However, due to the success of the program, at the end of Phase 1, more than 180 applications had been onboarded within the Phase 1 timeline and budget.

Significance

The state delivered the first pilot release, a partnership with the Ohio Department of Taxation (ODT), within 6 months of program mobilization. This release established the state's enterprise digital identity foundation while simultaneously standing up the program's 24x7 fully-operational cloud-based infrastructure and service organizations. The implementations that followed built upon this foundation, resulting in a catalog of enterprise digital identity capabilities.

Releasing digital identity enterprise services

The ODT pilot marked the first wave of Ohio digital identity enterprise services and established the architectural foundation for integrating with other agency systems and applications.

The release helped ODT maintain adherence to all state and federal security and privacy standards for digital identities, as well as enabled future deployment of additional ODT capabilities and applications through the State's digital identity program.

Significance Con't

With a focus on fraud detection for Personal Income and School District tax returns, the release included capabilities aimed at benefiting citizens, taxpayers and ODT, including:

- Identity proofing for taxpayers – both through a batch process and at the individual level through an online Identity Confirmation Quiz
- Redesign of the Identity Confirmation Quiz – a responsive mobile user interface aligned with the look and feel of the State of Ohio's online presence
- Single sign-on (SSO) for employees and external workers

Launching an enterprise workforce identity solution

Through the release of the new myOhio, OH|ID Workforce established the foundation for protecting Ohio's 80,000+ internal user accounts and modernized that state's intranet portal. When the transformed myOhio was unveiled, OH|ID Workforce was launched as the state's enterprise identity solution for state and county employees, contractors, and external workers.

OH|ID Workforce delivers a secure and private digital identity to protect the state against potential data breaches. Sensitive data exists everywhere, including infrastructure, middleware and applications. Because not all data breaches are equal, OH|ID Workforce also protects against breaches to internal accounts and privileged-access accounts – high-value targets for attackers.

The launch of the new myOhio and OH|ID Workforce enhanced the security of the State's internal user accounts. The new state intranet features intuitive navigation, simplified access to on-boarded applications, and a modernized, mobile-responsive design. With OH|ID Workforce, 54,000 state employees, 15,000 contractors, and 25,000 external workers can now securely access what they need to do their jobs through one portal and one single identity.

Introducing a single citizen identity

During the Phase 1 period, Ohio launched the state's digital identity solution for citizens, requiring users to shift from a business-based to user-based identity. This change aligns with security best practices and allows for verification and tracking of individuals interacting with the state's business applications.

As a result, 350,000+ business owners, CPAs and other service providers can access and file transactions through a simplified and more secure platform, accessed via OH|ID. This also resulted in enhanced security and ability to verify and track individuals interacting with the state's business applications.

Members of Ohio's business community have been able to successfully navigate the modernized platform and file their transactions in a timely and efficient manner. As new applications are added, the ability of Ohio's businesses and citizens to access the services they need from a single, secure location increases and improves the quality of their interactions with the state.

Providing identity and access management capabilities

Through a partnership with the Ohio Department of Job and Family Services (ODJFS), Ohio's digital identity program enhanced the digital experience for users accessing the agency's online services.

Significance Con't

Through the Identity and Access Management (IDAM) initiative, ODJFS leveraged the digital identity program's core OH|ID Workforce services and the Identity Platform-as-a-Service to provide their internal and external users (customers, counties, and service providers) with a more secure, private, intuitive, and interactive experience. This included:

- Self-service password reset functionality available to more than 24,000 ODJFS state/county users
- Delegated administration enablement for more than 320 county technical points of contact deployed statewide in all 88 counties; functionality replicated across 6 Active Directory domains and 2 LDAP directories
- Automated access provisioning for two applications
- Integration of account creation between the state's HCM system and digital identity platform's ISIM Console

As a result, ODJFS now have single sign-on access for critical business applications. Users are also able to take advantage of self-service password resets through the new myOhio.

Impact

With the successful completion of Phase 1, Ohio's digital identity program has brought to life its vision to provide a more secure and intuitive digital experience through enterprise identity tools and capabilities. Adoption of the state's enterprise digital identity products during this initial phase yielded significant value through approximately $65M in cost avoidance, exceeding the program's expectations. In addition, the cost of application on-boarding was reduced by 85%, and by deploying self-service on-boarding to accelerate application integration, costs will be reduced even further.

Beyond these financial benefits, Ohio's digital identity program has delivered value through increased security, operational efficiencies, centralized regulatory compliance, higher productivity, and an enhanced user experience. Releases beyond the planned pilots for Phase 1, completed in partnership with the ODJFS, Office of Budget and Management (OBM), and other state agencies and organizations resulted in:

- On-boarding of **80,000 state workforce users**, including employees, contractors, and county workers
- Access to applications for **350,000+ constituents**
- Integration of **180+ business applications** beyond the scope for Phase 1
- On-boarding of all **88 counties**

Agency adoption of the state's digital identity capabilities suite above and beyond the initial scope for Phase 1 demonstrates the effectiveness of the program's scalable platforms and repeatable processes for both identity and user experience, enabling efficient agency on-boarding and lowering barriers to and cost of adoption. As agencies and programs onboard to this enterprise platform, they avoid ongoing and redundant costs associated with security, privacy, and ADA solutions that would otherwise be maintained at the agency and program level while also allowing quicker reaction to policy or cyber events since changes can be rolled out globally.