simpler
stronger
authentication

Case Study:

State of Michigan's MiLogin Adopts Passkeys

"FIDO Drives Strong Authentication Results for the State of Michigan's MiLogin"

The State of Michigan's Department of Technology, Management & Budget (DTMB) is a principal department of the state's government responsible for providing a wide range of support functions to other state agencies.

The department's broad spectrum of responsibilities includes technology services, labor market information, facilities management, financial services, procurement, retirement services, real estate management, the Michigan public safety communication system, fleet and records management, and more.

The DTMB also plays a crucial role in cybersecurity for the state, providing resources and tools to protect against cyber threats and manage the State's IT infrastructure. One of the DTMB's efforts is the MiLogin digital identity solution, which enables over 10 million users to access state government services securely and conveniently.

DTMB was looking to secure MiLogin, Michigan's application that allows users to access multiple state applications and services with a single user ID, with strong authentication that improves user experience and decided to go with passkeys, based on FIDO authentication.

> *Passkeys are a password replacement that provide faster, easier, and more secure sign-ins to websites and apps across a user's devices. Unlike passwords, passkeys are resistant to phishing, are always strong, and are designed so that there are no shared secrets.*

Key Objectives

The State of Michigan aimed to address several key objectives with the integration of passkeys:

Enhance the digital user experience.

The goal was to streamline the digital user experience, particularly in providing users with seamless access to critical state government services. DTMB aimed to simplify the login process, making it more user-friendly and efficient.

Reduce help desk support dependency.

Recognizing the strain on help desk resources due to login access issues, DTMB sought to reduce users' need to access help desk support. By implementing changes to enhance the login process, the goal was to empower users to navigate.

Fortify security resilience.

There is no shortage of risk and vulnerabilities associated with traditional username and password authentication. A key objective was to fortify the system against security threats and phishing incidents, by adopting advanced FIDO strong authentication to mitigate the risks commonly exploited by bad actors seeking unauthorized access.

The Importance of Open Standards and Interoperability

Before deciding to implement passkeys, the DTMB explored a proprietary passwordless login solution offered by a cloud-based identity-as-a-solution (IDaaS) provider. However, the solution lacked the interoperability required.

The DTMB determined early on in its process that open standard and interoperability were critical and required components of its strong authentication strategy.

A standards-based approach provides interoperability across popular device types and web browsers, maintains vendor neutrality, allows for cost savings through community adoption, and a pathway to adopt future innovations in the FIDO ecosystem.

The Solution: FIDO Drives Results

Passkeys checked all the boxes for the DTMB, utilizing open standards and an interoperable approach for authentication.

The DTMB found that passkeys provide the following advantages:

- Passkeys are based on open standards, ensuring interoperability without necessitating additional software for users to download.
- Multiple vendor support for FIDO standards and the tech’s rapid adoption promotes the long-term continuity of FIDO authentication as a service.
- FIDO standards accommodate various authenticator types (such as biometric sensors, hardware keys, etc.) across desktop and mobile devices, catering to the DTMB’s user base’s diverse authentication requirements.
- Prioritizing user and ecosystem partner security, passkeys provide strong phishing resistance.

MiLogin’s Path to Passkeys

The DTMB’s passkey rollout involved a meticulous process to ensure a seamless, secure transition.

Extensive research on passwordless authentication solutions was conducted, engaging the DTMB’s cybersecurity review board in the evaluation process. Upon selecting passkeys for further exploration, the DTMB delved into the analysis of various FIDO options and sought feedback from the National Institute of Standards and Technology (NIST).

Working together with Deloitte, which is the DTMB’s trusted systems integrator for the State’s enterprise digital identity solution, a comprehensive strategy was planned for the design, development, and implementation phases.

In the design phase, insights from the FIDO Alliance's usability study results were working into screen and workflow designs. Findings from the DTMB’s MiLogin human-centered design usability study were also used to create a user experience tailored to address the diverse needs of various personas.

The development phase focused on integrating MiLogin with FIDO authentication methods, accompanied by the creation of animated user help guides and tutorial videos to drive greater user adoption.

Post-implementation, the DTMB monitored production metrics and gathered feedback from end-users, ensuring the success of the implementation and identifying areas for functionality enhancements in future releases.

MiLogin's Impressive Passwordless Results

Within the first six months of release, MiLogin achieved impressive results for the State of Michigan:

- 100,000+ customer devices enrolled in passkeys
- ~18,000 new passkey enrollments per month
- Increased FIDO-based logins with zero reported issues
- Decreased help desk initiated password resets with 1,300 fewer calls related to password resets in a single month.

"I am proud that our MiLogin team has brought passwordless authentication to our public digital identities. Passwordless brings additional protections to our public digital identities, and helps protect our systems from account takeover attempts such as brute force and password spray attacks."

- Jayson Cavendish, Chief Security Officer, State of Michigan, DTMB

The Road Ahead for Passwordless in the State of Michigan

The State of Michigan anticipates a significant increase in passkey adoption, targeting over 10 million public users. They also plan to implement passwordless authentication for their workforce, integrating with their state directory services solution.

FIDO authentication is a part of the State of Michigan's Zero Trust Identity strategy to establish a secure identity in citizen interactions with state services. It will also improve the user experience, generate cost savings for the state, and increase adoption of the State's digital identity solution by diverse state agency partners.

So what advice does the DTMB have for other other organizations? The State of Michigan recommends understanding diverse user bases and use cases, prioritizing user experience, and incorporating usability studies, clear end-user messaging, and a well-designed communication plan for a successful FIDO authentication implementation.