fido ALLIANCE

U.S. General Services Administration's Rollout of FIDO2 on login.gov

The General Services Administration's (GSA's) login.gov provides single sign-on for the U.S. public and federal employees to interface and transact with federal agencies online. With one account, users can access services like the federal government's job board, USAJOBS, and the Department of Homeland Security's Trusted Traveler Programs, such as Global Entry. In addition to enabling users to access federal government services more easily, login.gov handles software development, security operations, and customer support. This allows agencies to focus on their core missions, while reducing costs and improving security. It also allows the login.gov team to focus on protecting one service instead of many, and to adopt best practices for security and account management.

THE CHALLENGE:

Balancing Security, Convenience, and Cost

As the U.S. government continues to modernize e-government services for both federal employees and the public, there is a challenge to provide these services in a manner that is secure, user-friendly, efficient, and cost-effective. With phishing attacks on the rise, it was imperative for the government to support "phish-proof" multi-factor authentication (MFA) technology.

THE ROAD TO FIDO:

GSA's Evaluation Process for login.gov

The GSA evaluated several options for authentication for login.gov with three main priorities: security, cost, and compliance.

Security

One of the options for MFA GSA examined was SMS one-time passwords (SMS OTPs).

They found that SMS OTPs were a popular MFA option for users. Although convenient, SMS OTPs introduce avoidable security risks to users; this includes malware inadvertently downloaded onto a mobile phone that could monitor the user's text messages. Additionally, GSA experienced a lot of issues with phishing, especially targeting accounts that were controlling bank information and personally identifiable information, including the user's date of birth and Social Security Number. For login.gov, GSA wanted to offer a secure alternative to SMS OTPs that could prevent phishing, and began evaluation of FIDO2 authentication standards.

Overview

The Challenge

With phishing attacks on the rise, it was imperative for the government to support "phish-proof" multi-factor authentication (MFA) technology that was also user-friendly, efficient and cost-effective.

The Solution

After evaluating several options for authentication for login.gov, the government decided to support FIDO2 through the use of FIDO security keys and built-in FIDO authenticators like Windows Hello biometrics. Through comparison to other options, they found FIDO to check the box for security, usability, cost and compliance.

The Results

GSA rolled out authentication with FIDO2 in September 2018. With initial adoption equating to about 2,000, or 0.2%, of new users, GSA made it a requirement for users to register a second MFA option. As a result, the number of new FIDO2 security keys increased to 17,000 per month. In late June 2019, there were about 27,000 FIDO2 keys registered and the adoption rate has increased to about 3% of all new users, representing a significant increase from initial rollout.

FIDO2 is a set of strong authentication standards that enables users to leverage common devices like on-device biometrics and FIDO security keys to authenticate to online services with phishing-resistant cryptographic security. The FIDO2 specifications are the World Wide Web Consortium's (W3C) Web Authentication (WebAuthn) specification and FIDO Alliance's corresponding Client-to-Authenticator Protocol (CTAP).

After reviewing the FIDO Alliance's FIDO2 standards, GSA found that FIDO2's phishing resistance made it the most appropriate approach to address its security challenges.

Reduce Costs

In addition to security concerns, GSA found SMS OTPs quite expensive to manage. Without alternatives, those expenses would continue to escalate as more and more users are onboarded to login.gov.

With FIDO2, GSA could leverage a "bring your own FIDO security key" approach, making it more cost effective. The federal government does not sell or provision authenticators, but enables the use of authenticators previously provisioned.

Compliance

NIST's Digital Identity Guidelines - Authentication and Lifecycle Management (Special Publication 800-63B) is the guidance that federal agencies must adhere to as it pertains to authenticating users to its networks. The 2017 guidance reclassified SMS OTPs as a "restricted" authentication technology. This means that agencies need to offer users at least one alternate authenticator that is not restricted. They also must provide users with meaningful information on the security risks of the restricted authenticator (SMS OTP) and availability of alternatives. FIDO standards provide a secure alternative that meets NIST guidelines for high assurance strong authentication.

FIDO2 Development

Prior to development, GSA utilized a Google developer resource on enabling strong authentication with FIDO2 WebAuthn on developers.google.com. To assist with server-side processing, GSA leveraged a WebAuthn-ruby gem on GitHub. That greatly benefited and expedited the development including back-end processing. In addition, GSA used the W3C reference material for further clarification on any issues encountered.

All of GSA's code for login.gov is on open source and it's on GitHub under a repo 18F/ identity-idp. Because it is a standards-based authentication technology, implementing support for FIDO2 was extremely fast. It took a small team of three developers just two weeks to develop and move into production.

INSIDE FIDO STANDARDS

The FIDO protocols, including the FIDO2 specifications, use standard public key cryptography techniques instead of shared secrets to provide stronger authentication and protection from phishing and channel attacks.

The protocols are also designed from the ground up to protect user privacy. The protocols do not provide information that can be used by different online services to collaborate and track a user across the services, and biometrics, when used, never leave the user's device.

This is all balanced with a user-friendly and secure user experience through a simple action at log in, such as swiping a finger, entering a PIN, speaking into a microphone, inserting a second-factor device or pressing a button.

Facial scan

Fingerprint

Local PIN

Security Key

Deployment and User Experience with FIDO2

GSA rolled out authentication with FIDO2 in September 2018. login.gov supports FIDO2 through the use of FIDO security keys and built-in FIDO authenticators like Windows Hello biometrics. For users, these are all referred to as "security keys" during user onboarding. The process for setting up FIDO2 at login.gov works like this:

1. When a user is creating a login.gov account, they enter their email address and create a password. Login.gov will first send an auto-generated email for the new user to confirm their email address.
2. Then, they are instructed to select and set up MFA from a menu of options, including SMS OTP, FIDO2 security keys, and backup codes.
3. To set up FIDO2, the user will select the "Security Key" option.
4. The user can create a nickname for their security key.
5. They are prompted to either insert a hardware security key into their computer and touch it or, if their device has a supported built-in authenticator, be prompted to use it by looking into the camera or touching a biometric sensor (for two examples).
6. The user is presented with a "success screen" and then they can access their login.gov account.

Many users take advantage of the "Remember Device" option when signing in. For example, if the user is using a laptop and checks "Remember Device," they will not need MFA on that laptop again for another 30 days.

Support of Non-FIDO2 Security Keys

During testing, the development team discovered that several hardware security keys were failing. They found that the majority of the failures were because they were not FIDO2-compliant. After considering to add support for non-FIDO2 security keys, the decision was made not to support them because it would have considerable time and effort than simply implementing WebAuthn. GSA plans to revisit support for non-FIDO2 keys at a later date. A listing of FIDO2 Certified authenticators can be found on the FIDO Alliance website.

FIDO User Adoption: On the Upswing

Initially, users registered about 2,000 new FIDO2 keys per month, which equates to about 0.2% of new users. In analyzing authentication statistics, GSA found that more users were choosing mobile/SMS OTP options for MFA more often. In May 2019, GSA began requiring new users to register a second MFA option to increase awareness and adoption of FIDO2. That change increased the number of new FIDO2 authenticators to 17,000 per month. This number increased to 27,000 just in the month of June and the adoption rate increased to about 3% of all new users, representing a significant increase from initial rollout. GSA is considering the same requirement for existing users, but is looking at doing so without hindering the user experience.

As of June 2019, login.gov onboards about one million new users per month and that is expected to grow as agencies continue to add additional services. GSA has high expectations for the use of built-in authenticators to increase adoption, because it does not require users to acquire a separate FIDO security key.

Future Improvements for Increased Adoption

One of the challenges login.gov has faced is user education. Specifically, informing users that they have the option to enroll with FIDO2 and educating them about what FIDO is and how to set it up. It can be a challenge to accomplish this without confusing the set of users who are not able to set up FIDO, either because they don't have a FIDO2 security key or don't have a built-in authenticator.

Another area that GSA is working on is the onboarding process and the use of the term "security key" for all FIDO authenticators. User research is currently underway as of September 2019 around prompting users to set-up whatever their device is named rather using the security key language. Preliminary findings indicate that it would help adoption to keep the security key option for users who have the physical security key and then adding additional options for users with built-in authenticators i.e. "use your Android phone," or "use your Windows Hello device," etc. This will help give users clarity around their options so they will be more likely to set it up.

Another enhancement under consideration is a feature called "MFA Checkup." This is to address the real-world problem that occurs when users change their smartphone and lose their backup codes. Login.gov would display a screen informing the user of the methods available or provide the user with the option to replace a method.

Ultimately, GSA sees these actions to streamline user communications and make user authentication options more clear as key to increasing user adoption and help both GSA and end users realize the full security, usability and cost reduction benefits that FIDO Authentication provides. As one of the first governments to offer FIDO Authentication for login to e-government services, GSA strives to be a model for other governments to follow.