FIDO Alliance White Paper:

CXO Explanation: Why Use FIDO for Passwordless Employee Logins?

July 2020

Editors:
Nicholas Steele, Cisco Systems
Salah Machani, RSA
Shane Weeden, IBM

Abstract

Today, secure access to online applications and services has evolved into a framework reliant on devices, public key cryptography and biometrics to replace the shared secrets of aging passwords. Since 2013, the FIDO Alliance has developed open and scalable advancements to eliminate phishing and other security attacks. To introduce these improvements and to educate employees throughout corporate management and IT security, FIDO Alliance has developed a series of best practices and how-to white papers that match the Alliance's goals with the responsibilities and titles of technology professionals. This work is dedicated to eliminating passwords and securing the simple act of logging on within all companies.

This white paper answers the most common questions from CXOs about the value proposition of FIDO Authentication and how the FIDO2 passwordless framework addresses the authentication needs and challenges of companies for the modern workforce. The goal of this document is to guide executive leaders within an organization as to why they should invest in FIDO2 deployment for their employees.

CXO Frequently Asked Questions

What is FIDO Authentication and where does FIDO2 fit in?

FIDO Authentication is an approach to strong authentication that uses standard public key cryptography techniques instead of shared secrets to provide stronger authentication and protection from phishing and channel attacks. FIDO is designed from the ground up to protect user privacy; login credentials and biometrics, when used, never leave the user's device. This is all balanced with friendly and secure user experiences through a simple action at login using an authenticator, either built into their device (such as fingerprint or facial biometrics) or external (such as a FIDO Security Key).

FIDO Authentication can be delivered through three sets of protocols published by the FIDO Alliance: FIDO Universal Second Factor (FIDO U2F), FIDO Universal Authentication Framework (FIDO UAF), and FIDO2 (Client to Authenticator Protocols and Web Authentication). FIDO2 brings passwordless capabilities to the web and is well suited for enterprises that are looking to start on a path towards passwordless for their desktop applications; FIDO2 is the focus of this brief.

What is new in the FIDO2 approach and why will it be successful?

FIDO combines some of the best security properties given to us by past second-factor authentication frameworks along with the added benefit of making sure user credentials are cryptographically strong and unique for each web application that a user may have to access for their job. FIDO thwarts phishing, which is a compelling concern for many enterprises, by making sure that user credentials are specific to a given web application and that the credentials never leave the user's possession. We believe that this approach will allow for a faster, simpler, and more secure login experience.

FIDO2 provides all the benefits of FIDO Authentication while extending supported login experiences, including using a mobile device as an external authenticator, and providing enterprises with the ability to go passwordless and experience username-less login as well. Importantly, the W3C WebAuthn API component of FIDO2 has allowed FIDO Authentication support to be built directly into all major web browsers and operating systems, which eases implementation in the enterprise.

What problems does FIDO solve for my business?

Passwords are challenging for everyone involved. They are difficult for users to remember, and vulnerable to theft and reuse. In fact, most breaches on the internet stem from stolen or weak user passwords. Additionally, dealing with lost passwords can be a large expense for enterprises and their helpdesk workers. FIDO can be used to replace passwords entirely or be used as a second-factor authentication method on top of existing schemes. FIDO reduces the risks that have plagued passwords since their inception. Passwords are shared secrets that, if stolen, can give attackers access to a person's account and the information inside. This problem has led to the popularity of multi-factor authentication (MFA), which has helped address some of the shortcomings of passwords – but some approaches (such as SMS OTP) remain vulnerable to technical and/or social engineering attacks.

FIDO takes a new approach for MFA to address both the security and usability concerns of passwords. FIDO uses public-key cryptography in order to create strong and unique credentials for every site with which a user needs to authenticate. Instead of a password, a user's authenticator creates a public and private key and shares the public key with a given web application, while the private key is securely stored inside a piece of hardware, such as a security token or a secure storage space on the user's phone. This private key is unextractable and not stored in a central location like with passwords. Biometric authentication may also be used with FIDO-enabled authenticators to ensure that the keys being accessed are being directly accessed by a certain user.

FIDO aims to strengthen user and enterprise security by making authentication to web applications a more secure process while decreasing user friction.

How else is secure authentication dealt with today, and what are the limits of these practices?

Currently, most organizations rely on passwords to authenticate users. While enterprises can reduce the number of times a user needs to enter their password by using Single sign-on (SSO) or account federation, users may still pick weak passwords, re-use the same password across multiple applications, or share their passwords which could result in breaches without the application of password policies or additional user training. To help mitigate weak user credentials, many enterprises opt to use smart cards, MFA applications, or two-factor authentication (2FA) tokens, which, while helpful in mitigating the risk of credential theft, also introduce administration and management challenges and poor user authentication experience – and are still susceptible to more sophisticated replay or man-in-the-middle attacks.

Who cares? If FIDO2 deployment is successful for an organization, what difference will it make?

The organization adopting FIDO2 will experience profound improvements in the following areas: security, cost, and user experience.

- **Security:** The majority of breaches succeed through stolen, reused, or weak passwords. FIDO2 introduces a viable alternative to password-based authentication for web-based applications. FIDO authenticators enable users to have a faster and more secure login by managing credentials on their behalf.
- **Cost:** Breaches resulting from compromised passwords are expensive to both the bottom line and an organization's reputation. In addition, password-based authentication systems require costly support services to deal with their inherent limitations (e.g. password resets, security training, and second-factor authentication deployments).
- **User experience:** Users have already experienced the simplicity of gesture-based authentication on their phones and laptops via fingerprint or facial recognition. The same user experience can be brought to your users for website and enterprise application login with FIDO2.

What are the challenges associated with deployment?

Deployment can be difficult without user education and resources. Passwordless login is still a new concept to most of the workforce, and many people could be either confused by the new mechanisms they must use or hesitant to rely on biometric technology. It is important that adopters consider user education early on to get their users started with FIDO. Legacy support may be an issue for your organization, so planning for how to adapt your organization's current identity solutions could require time. If you are not relying on SSO as an authentication gateway, implementing FIDO2 may be difficult without native support for your enterprise's applications. If your organization plans to deploy FIDO Security Keys and has not done so already, it is important to plan a management cycle for these devices and how they are provisioned to users and eventually decommissioned.

How long will it take to get started?

Our recommendation is to plan a pilot–three to six months should be enough to get something deployed and start getting employee feedback. Your mileage will vary depending on your existing enterprise authentication infrastructure.

If you use a commercial product or service for web access management, enablement may be as straightforward as working with your vendor to turn it on. If you have a federation-based SSO system which includes some form of extensibility framework for multi-factor capabilities, start by adding FIDO2 registration and authentication to that system as an additional multi-factor capability. For those with a grander vision and advanced operational capability, challenge your team to offer complete alternative-to-password authentication experiences. Otherwise, save this challenge for a later phase of adoption.

What does success look like?

A reasonable expectation is that employees will be able to authenticate to enterprise applications with a safer AND more desirable user experience than what they are using today. Authentication will be safer because weak or reused passwords do not expose application access to attackers, and it will be more desirable because your employees have the option of using fast and intuitive authentication experiences just like you use for unlocking your phone or laptop today.

If many of your enterprise applications can be accessed safely with the touch of a button, wouldn't you consider that a big step in the right direction for both enterprise security and employee productivity?

Where can I find more information?

For additional information, see case studies at https://fidoalliance.org/content/case-study/ and white papers on FIDO deployment in the enterprise at https://fidoalliance.org/white-papers/. You can find more details on the benefits of deploying FIDO to consumers at https://loginwithfido.com/provider.

Summary

Today, most organizations rely on passwords for user login, which is a form of authentication that can potentially be a threat to your business and users. Passwords can be stolen, leaked, phished, or shared among users, and the cost of dealing with password hygiene and password loss can be high. Adopting passwordless authentication with FIDO2 for your enterprise can greatly increase user security, while also decreasing the friction of login for your users. Passwordless is still a new concept to many users, so early education for users will be important. We recommend a time-boxed pilot around three to six months, and to work with your web access management team or vendor to craft an adoption solution that works for your enterprise. With a successful rollout of FIDO2, your users should be able to experience a faster, simpler, and more secure login experience than previously with passwords.

Acknowledgments

The authors acknowledge the following people (in alphabetical order) for their valuable feedback and comments:

- Karen Chang, Egis
- Norman Field, Strongkey
- John Fontana, Yubico
- Bill Leddy, Visa
- Nick Mooney, Cisco Systems, Inc.
- Megan Shamas, FIDO Alliance