eBay's Journey to Passwordless with FIDO

A global commerce leader connecting millions of buyers and sellers around the world, eBay Inc. enables economic opportunity for individuals, entrepreneurs, businesses and organizations of all sizes. Because its users are at the core of its success, eBay emphasizes providing a positive and secure experience for both buyers and sellers.

As with most websites, every user's interaction with eBay begins with logging onto the site and authenticating himself, i.e., verifying that they are who they say they are. However, the typical authentication sequence using usernames and passwords impacted the user experience – and made eBay more vulnerable to bad actors at the same time. Users were constantly forgetting and resetting their passwords – a frustrating process. And with many buyers and sellers using the same password for multiple accounts on multiple sites, a breach on any of those sites could open eBay to a breach as well. eBay knew it needed to make the authentication process more secure, but not at the expense of the user experience.

Prioritizing Security and the User Journey

To add an extra layer of security to the login process, eBay implemented SMS one-time passcodes (OTPs). Even though it helped provide a more secure option, the method added costs, user friction and was still vulnerable to certain security issues.

After reviewing a variety of other options to provide a simple, easy, and secure user authentication experience, eBay decided to roll out FIDO for strong authentication across both its native mobile app and browser-based mobile and web sites.

eBay decided to build its own open source FIDO server, which they felt gave them maximum control of the user experience and the end-to-end login flow. This approach also gives eBay better ability to manage its other login options, such as social logins.

Realizing the Benefits of Standards

The strength of the FIDO Alliance and the FIDO standard, including the involvement of a wide range of major technology companies, was another significant factor in eBay's selection of FIDO.

> "Choosing the FIDO standard for eBay user authentication was about more than simply adopting a secure protocol," said Ashish Jain, head of Identity at eBay. "eBay operates in 190 markets and has a diverse set of users. We needed to make sure that any technology we choose can work consistently across various browsers and platforms"

INSIDE FIDO STANDARDS

The FIDO protocols, including FIDO UAF and 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 login, such as swiping a finger, entering a PIN, speaking into a microphone, inserting a second-factor device or pressing a button.

© 2020 FIDO Alliance. All rights reserved.

eBay's Journey with FIDO: From Push to Passwordless

As a first step, eBay implemented FIDO for second factor authentication using the FIDO UAF protocol with a push notification flow. This meant that, when a user logged into eBay with a username and password, they would receive a notification from the mobile eBay app to confirm the login. Implemented as an opt-in feature, FIDO immediately garnered significantly higher opt-in rates than the previous SMS OTP solution, validating the FIDO standard's ease of use.

Six months later, after seeing the already quick user adoption rate continue to rise, eBay decided to take the next step in passwordless authentication. In order to further simplify login flows, the company launched FIDO2 for primary authentication, no longer requiring users to take a second step to log in.

Here's how it works:

- When the user logs in as normal, eBay detects whether the device supports FIDO2. If so, the user receives a pop-up box asking them if they would like to enroll in passwordless authentication;
- If they opt in, the user is asked to enroll their facial or fingerprint biometric and is automatically enrolled;
- The next time the user logs in, all they need to do is present their biometric. No username and no password required.

Realizing Benefits for Both eBay and Its Users

Less than one year into its implementation of FIDO, eBay is already realizing its benefits: Not only are opt-in rates higher than for SMS OTPs, but also login success and completion rates have significantly improved, especially on mobile devices. eBay started to roll out FIDO2/WebAuthn on Android/Chrome and have since expanded to Mac, Windows as well as iOS. Recently, eBay has also added support for roaming authenticators, such as security keys providing another secure way to access eBay.

Looking Forward to a Completely Passwordless Future

In order to implement completely passwordless authentication, eBay must have a process in place for recovering accounts if a FIDO authenticator is lost or when a user adds a new device. In typical password authentication, users can recover their accounts through the email/password reset process, but removing a password from the equation presents a new challenge.

According to Jain, solving this issue is a priority for his team in the next six months. "Today, our users can experience much faster and convenient login experiences by opting in to FIDO," observed Jain. "But to fully realize the security benefits of FIDO, we're looking forward to disabling passwords entirely. By taking one step at a time and working as an industry to find solutions to issues like account recovery, we believe we will get there."

"Today, our users can experience much faster and convenient login experiences by opting in to FIDO, but to fully realize the security benefits of FIDO, we're looking forward to disabling passwords entirely. By taking one step at a time and working as an industry to find solutions to issues like account recovery, we believe we will get there."

Ashish Jain
Head of Identity at eBay

 © 2021 FIDO Alliance. All rights reserved.