FIDO Alliance White Paper:

Accepting FIDO Credentials in the Enterprise

October 2020

Editors:

Dean H. Saxe, Amazon Web Services
Pamela Dingle, Microsoft
Salah Machani, RSA

© 2020 FIDO Alliance. All rights reserved.

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 and advanced open and scalable standards 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.

Enterprises that accept FIDO credentials are participating in a digital credential exchange. This white paper is intended for CISOs and IT professionals who are considering deploying FIDO across their enterprise. In this paper, we provide a high-level overview of the most common digital exchange – the authentication exchange. We will examine the participants, protocols, and decisions that enterprises must make regarding the creation, management, and usage of FIDO credentials.

What Does it Mean for an Enterprise to Accept FIDO Credentials?

FIDO credentials are created and used via a standardized authentication mechanism that significantly reduces the risk of machine-in-the-middle attacks and account compromise. From an end user perspective, roaming (external devices) or platform embedded hardware (both referred to as FIDO Authenticators) are leveraged to authenticate to enterprise resources. This idea may not seem revolutionary, but consider that FIDO Alliance and W3C Web Authentication standards integration enables seamless access by end users on the most popular combinations of operating system, hardware, and browser. It is this promise of vendor-agnostic tools, coupled with rapid authentication, improved user experience, and the phishing-resistant cryptographic properties of FIDO credentials that make FIDO Authentication a compelling option for enterprises.

The enterprise's main goal in enabling a FIDO Authentication mechanism is to eliminate password-only user authentication from the enterprise by way of delivering ubiquitous second-factor, multi-factor, passwordless, and/or usernameless authentication capabilities. This will not only reduce the risk of account compromise due to credential reuse, phishing, and machine-in-the-middle attacks, but will also provide superior user experience and increased productivity.

The primary mechanism for enterprise relying parties (RPs, e.g. web applications) to request a credential to be created or fetched is the W3C Web Authentication specification[1], commonly referred to as WebAuthn. WebAuthn allows the enterprise's services to interact with an end user's FIDO Authenticators, using the browser as a trusted intermediary. The browser, in turn, negotiates with platform authenticators, such as built-in fingerprint readers, or roaming authenticators, via transport mechanisms like USB, Near Field Communications (NFC), or Bluetooth. As a WebAuthn RP, the enterprise services rely on the public key credentials authenticator to strongly authenticate users to their services.

The following section will explore how credentials are created and used for authentication.

[1] https://www.w3.org/TR/webauthn/

© 2020 FIDO Alliance. All rights reserved.

Creating and Fetching Credentials

FIDO Authenticators can store many credentials. Each credential is "origin-bound", meaning that each credential is scoped only to a given origin, i.e. 'example.com'. Credentials are created and fetched (used for authentication) by calling JavaScript functions in the browser; the names and parameters of these functions are standardized within the WebAuthn specification. While the end-to-end experience is generally consistent, there are a small number of choices that an enterprise can make to limit the situations in which authenticators should create credentials, or to require that certain factors be present during authentication. The considerations for credential creation and use are discussed below.

Common Enterprise Credential Creation Requirements

User Verification and Presence Requirements

All FIDO Authenticators require a user gesture – a tap, PIN entry, or presenting a biometric – prior to creating or fetching a credential. These gestures prove that a human is present in the transaction (tap) or uniquely verify the owner (biometrics or a FIDO Authenticator PIN). Enterprises can optionally require user verification (UV) in addition to user presence (UP) at the time of creation or usage of a credential.

Not all authenticators support user verification and not all use cases require it. In use cases where the FIDO credential is used as a second factor in conjunction with a password, UP is enough, and the FIDO Authenticator is a possession factor in this transaction. This is a common deployment pattern for enterprises migrating to FIDO Authentication from traditional second factor mechanisms. Additionally, in speed-sensitive, highly constrained environments such as warehouse employees and first responders who wear gloves, a single-factor UP-only flow (e.g. FIDO Authenticator as a bearer token) may be acceptable, if the security and usability tradeoffs are adequately balanced.

When user verification is utilized, FIDO Authentication represents multiple factors: the device is a possession factor and the gesture is either an inherence factor (biometric) or knowledge factor (PIN). UV is primarily used in passwordless and usernameless flows where security and convenience are paramount.

Which Authenticators are Acceptable?

In certain use cases, enterprises may need to limit the type of authenticators that can create credentials. The WebAuthn RP may require that a credential only be created by a roaming authenticator, platform authenticator, or based upon other authenticator properties defined in the FIDO Metadata Service (MDS).

These decisions will have implications on the user's overall authentication experience. For example, requiring only platform authenticators would mean that no external devices could be used to authenticate. While this might be important for an air-gapped use case, for a more general use case, users will be unable to authenticate if the platform authenticator device becomes unavailable. A roaming authenticator cannot be used as an inexpensive backup device in these cases. On the other hand, roaming authenticators may be the only practical option, such as in the cases of shared-machine login or physical access control systems. However, in most general-purpose authentication use cases, the best practice is to allow all modalities to be used to create/use credentials.

Typically, enterprises limit authenticators by FIDO certification levels, regulatory compliance, security characteristics, and functionality.

Credential Discoverability

Finally, FIDO credentials may be "discoverable". Discoverable credentials are capable of being used to identify the user (e.g. a username) and authenticate the user in a single step. Discoverable credentials eliminate username entry (e.g. identifier-first flows, aka usernameless) from authentication workflows and may be used in both passwordless (first factor) and password-enabled (second factor) flows.

© 2020 FIDO Alliance. All rights reserved.

When using discoverable credentials, the user visits an RP which requests the discoverable credentials. The user presents their FIDO Authenticator and a gesture (typically UV), the RP discovers credentials through standard WebAuthn APIs, and authenticates the user. Optionally, the user may have to enter a password or present another type of authenticator or gesture to complete a second-factor flow.

Considerations Outside of the Web Browser Paradigm

In addition to using FIDO credentials through a web browser, there are non-web enabled use cases that can take advantage of FIDO Authentication. The most prevalent examples include native applications on smartphones, tablets and laptops which may utilize the native biometric hardware on the user's device such as on Android, iOS, Windows 10, and macOS. The native application acts as a FIDO Relying Party and uses a hardware-backed FIDO2 roaming or integrated platform authenticator.

The latest set of FIDO protocols is called FIDO2 and includes both WebAuthn and CTAP2 specifications – the latter of which is utilized for roaming FIDO Authenticators. FIDO2 enables several new enterprise use cases for FIDO Authenticators such as for desktop and domain logon. In this case, a desktop logon agent acts as a FIDO client and communicates with a FIDO2 Authenticator using platform-specific APIs (e.g. Windows Hello). In such an instance, FIDO2 credentials may be used directly to unlock the desktop and create a user session, or indirectly to unlock legacy credentials such as X.509 certificates, which in turn are used to unlock the desktop and create a user session.

Similar use cases for FIDO Authenticators outside of a web browser include heritage remote access protocols such as RADIUS and ssh. In these scenarios, FIDO Authentication is typically performed out-of-band with a roaming or platform FIDO Authenticator as a second factor following in-band first-factor authentication using a password or a certificate stored on disk. As of the release of OpenSSH 8.2, FIDO2 and U2F are directly supported by the ssh daemon.

Other creative implementations of FIDO that enable passwordless or second-factor authentication include using FIDO for physical access control systems, logon to major server operating systems, access to hosted virtual desktop environments, access to Kerberos services, privilege elevation on systems, access to network appliances, VPNs and firewalls.

© 2020 FIDO Alliance. All rights reserved.

Summary and Conclusion

Enterprises can adopt W3C WebAuthn on their web applications or enterprise single sign-on service to enable a FIDO Authentication mechanism and reduce the risk of account compromise due to credential reuse, phishing, and machine-in-the-middle attacks. However, before adopting a FIDO Authentication strategy, enterprises must consider their end goals, as well as the steps to achieve them. Architects should consider a phased rollout, first taking common, known user experiences such as second-factor authentication and switching heritage protocols to FIDO-based protocols. As users adapt and enterprise penetration of FIDO Authentication grows, consider more advanced deployments, including discoverable credentials and passwordless flows, and deployment to all enterprise staff. Finally, all deployments must consider mechanisms for access continuity in the case of loss or breakage of a FIDO Authenticator. The mechanisms to resolve access continuity challenges will be highly dependent upon the enterprise risk tolerance and the nature of the business (e.g. on-premises vs. remote employees).

For further information, the following resources are available to allow enterprises to dig deeper into technical details:

- FIDO Alliance White Paper: FIDO Enterprise Adoption Best Practices – FIDO and PKI Integration in the Enterprise (April 2019): This white paper is aimed at enterprises and government agencies looking to expand their authentication capabilities to include FIDO technology, and have FIDO work in conjunction with other authentication systems such as a Public Key Infrastructure (PKI), Kerberos, and Lightweight Directory Access Protocol (LDAP) that may be in place at the organization.
- FIDO Alliance White Paper: Enterprise Adoption Best Practices – Managing FIDO Credential Lifecycle for Enterprises (April 2018): This white paper provides guidance to IT and security professionals on how to manage FIDO Authentication credentials throughout their full lifecycle.
- FIDO Alliance White Paper: Enterprise Adoption Best Practices – Integrating FIDO & Federation Protocols (December 2017): This white paper outlines how the FIDO standards compliment federation protocols. It also provides guidelines on how to integrate the two in order to add support for FIDO-based MFA and replace or supplement traditional authentication methods in federation environments.

Acknowledgments

The authors acknowledge the following people for their valuable feedback and comments:

- John Bradley, Yubico
- John Fontana, Yubico
- Bill Leddy, Visa
- Eric Le Saint, Visa
- Andrew Shikiar, FIDO Alliance
- Shane Weeden, IBM

© 2020 FIDO Alliance. All rights reserved.