FIDO Alliance White Paper:

FIDO Authenticator Lifecycle Management for IT Administrators

April 2021

Editors:
Salah Machani, RSA Security
Tim Cappalli, Microsoft
Shane B Weeden, IBM

© 2021 FIDO Alliance. All rights reserved.

Abstract

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, the FIDO Alliance has established a series of best practices and how-to white papers that align 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 the enterprise.

Audience

This white paper targets IT administrators and Enterprise Security Architects considering deploying FIDO Authenticators across their enterprises and defining lifecycle management policies.

© 2021 FIDO Alliance. All rights reserved.

Contents

© 2021 FIDO Alliance. All rights reserved.

Introduction

The FIDO Alliance recognizes that company security policies are unique and dictated by company demands and industry. In this white paper, we provide an overview of the different types of authenticators and guidance on managing them in the enterprise. We intend to guide companies to align their authenticator lifecycle management policies with their security policies and risk tolerance.

For clarity, an authenticator is a physical or software element in possession of the end user that supports operations to securely create credentials and generate assertions. A credential is a public/private key pair generated by an authenticator. The private key is never shared outside the authenticator's secure operational boundary. During credential registration, the credential ID and public key are shared with the Relying Party (RP) for which they have been created. This document covers the lifecycle management of authenticators. For more details on the lifecycle management of FIDO credentials, please refer to the Managing FIDO Credential Lifecycle for Enterprises white paper.

Using FIDO Authenticators in the work environment

FIDO Authenticators are used in the enterprise to address many authentication use cases, including desktop login, web single sign-on (SSO), and mobile app sign-in. They can be used in two-factor authentication (2FA) and passwordless authentication ceremonies. Authenticators come in different form factors and types, including platform authenticators and cross-platform roaming authenticators. The forthcoming "Choosing FIDO Authenticators for the Enterprise Use Cases" white paper describes in more detail the different FIDO use cases in the enterprise and the recommended authenticator type for each use case.

This paper will cover the following authenticator deployment scenarios:

- Scenario 1: the enterprise allows for the use of platform authenticators only
- Scenario 2: the enterprise allows for the use of roaming authenticators only
- Scenario 3: the enterprise allows for the use of a mix of platform and roaming authenticators

The lifecycle management of authenticators differs in each scenario. When planning for FIDO rollout, enterprises must examine and understand each deployment scenario's benefits and pitfalls.

In Scenario 1, the authenticator is bound to the user's device. Upgrading and replacing the device will result in the loss of the ability to use existing FIDO credentials. Credentials cannot be transferred from one authenticator to another authenticator. Users will have to register new credentials using the new platform-bound authenticator.

In Scenario 2, the lifetime of the authenticator is independent of the device. The user may replace an authenticator, use a secondary/backup authenticator, and register new credentials using a new authenticator without upgrading the device and vice versa. The likelihood of losing or misplacing the authenticator in this scenario is higher than in Scenario 1. The user may be required to register two or more authenticators for recovery scenarios.

© 2021 FIDO Alliance. All rights reserved.

In Scenario 3, the enterprise has the benefits and the pitfalls of both Scenarios 1 and 2. Some users may use platform authenticators, some may use roaming authenticators, and some may use both depending on their function and the use case. When both types of authenticators are allowed, the user can bootstrap a FIDO credential in one authenticator type using the second authenticator type (typically, a roaming authenticator is used to bootstrap and enroll FIDO credentials in the platform authenticator).

Deploying and managing FIDO Authenticators

Onboarding new employees

Enterprises may adopt different authenticator registration and identity binding models when onboarding new employees.

- Delegated: a trusted authority such as an IT administrator, an HR representative, a payroll clerk, or the employee's manager issues a FIDO Authenticator to the new employee and registers a FIDO credential on behalf of the employee that is limited in scope. For example, the user can only use the credential to log in to the desktop machine or a self-service registration portal. The trusted authority may set a temporary PIN for user verification and request the user to change the PIN on first-time use[1]. Once the authenticator is handed or shipped to the user, the user uses it to complete the self-service registration processes and anchor them to an internal identity process.
- Self-Service: the new employee visits a self-service registration portal and registers a new authenticator. The FIDO Authenticator may be employee-owned or company-owned, handed or shipped to the employee during the onboarding process. In this model, the employee undergoes a remote identity proofing process at registration time or uses a temporary registration code or password to prove ownership of their enterprise identity.

Rolling out FIDO Authenticators to existing employees

When rolling out FIDO Authentication, employees may leverage their existing authenticators as trust anchors for FIDO registration. Depending on the enterprise's risk tolerance, existing authenticators may include other types of authenticators of equivalent or lower assurance levels. Examples of other authenticators include smart cards, one-time password (OTP) tokens, and Out-of-Band (OOB) mobile authenticators. To preserve the authentication assurance level provided by FIDO Authentication, we recommend authenticating users at the highest assurance level possible when registering new FIDO credentials for an account. The employee visits a self-service registration portal, signs in using a valid multi-factor authenticator, and then registers a FIDO credential using their authenticator.

Offboarding employees

When an employee leaves a company, the IT administrator must ensure that their FIDO credentials are revoked to prevent any intentional or accidental access to the employee account and company assets. The company policy may require offboarded employees to return their authenticators. Such a policy is generally applicable to platform FIDO Authenticators on company-owned devices and company-owned roaming authenticators. IT may choose to reset returned authenticators and assign them to other users.

[1] Enforcing PIN replacement is possible with CTAP 2.1.

© 2021 FIDO Alliance. All rights reserved.

Replacing lost FIDO Authenticators

The Alliance recommends parties relying on FIDO, including enterprises, to require multiple FIDO Authenticators per user to prevent account lockout situations when an authenticator is lost. Similarly, enterprises may require users to register and bind non-FIDO multi-factor authenticators to their accounts in addition to FIDO Authenticators and use them as a fallback[2] when a FIDO Authenticator is lost. However, registering multiple authenticators per user may not be desired for cost, server limitations, or security policy reasons. Enterprises must have processes and alternative user verification methods in place to recover access to accounts and replace lost authenticators when a backup authenticator is not available. These processes should align with the enterprise risk management strategy, the authentication use cases, and the desired user experience. Enterprises can choose from multiple methods, including:

- The help desk revokes[3] credentials that are bound to the lost authenticator and orders a new authenticator for the employee for self-registration using a registration code or a remote identity proofing method.
- Similarly, a manager vets the employee's identity and assists the employee in the recovery/authenticator replacement process.
- The employee undergoes a remote identity proofing orchestration process that may include multiple verification steps such as government ID verification, mobile ID verification, remote biometrics verification, etc., and self-registers a replacement authenticator.
- The employee authenticates to a trusted identity provider, possibly using FIDO Authentication, before registering and binding a replacement FIDO Authenticator to their enterprise identity.
- The employee leverages another multi-factor cryptographic authenticator. The employee uses an alternative non-FIDO strong authentication technique if available. They can then self-service the revocation of existing credentials associated with the lost authenticator, and the subsequent registration of new credentials.

Bring Your Own Authenticator vs. Company-Owned authenticators

The FIDO Alliance recognizes that company security policies are unique and dictated by the demands of the company and the industry. The intent here is to provide guidance that can be consumed by organizations in a manner that is aligned with the company's existing security policies and risk tolerance.

[2] This is generally considered a less-secure approach primarily because most alternative-to-FIDO approaches do not offer the same phishing-resistant capabilities supported by FIDO.

[3] To facilitate revocation of credentials, the enterprise RP may track additional data to identify the lost authenticator that created the credential. Such data includes registration nickname, last use time, attestation data, credential creation time, etc.

© 2021 FIDO Alliance. All rights reserved.

We can leverage some of the terms that are often used when talking about Bring Your Own Device (BYOD) scenarios. When hardware authenticators are provided by the organization, we can classify them into two buckets: Company Owned, Business Only (COBO), and Company Owned, Personally Enabled (COPE). As the names may suggest, a COBO authenticator is intended for work/school accounts only, while a COPE authenticator can also be used for personal accounts. However, there is no standardized mechanism to prevent a COBO authenticator from being used for personal accounts. Enterprises are recommended to treat COBO and COPE authenticators the same way. FIDO Authenticators present an opportunity for users to help improve their personal digital security posture throughout their entire digital life.

Considerations for BYOA

Bring Your Own (BYO) deployment models have become popular over the past decade as they allow users to leverage the devices and platforms they prefer to use. BYO can result in hardware cost savings but may result in increased support costs if a well-designed BYO support model is not already in place. While FIDO certification ensures interoperability of authenticators, clients, and RPs, the initial configuration of authenticators may vary across vendors. Upcoming features that enable credential management and biometric enrollment may ease some of these concerns by providing a common interface, but as with any new features, it will take some time for them to become widely available.

There are three major scenarios for BYOA:

1. Users are required to provide their own authenticator(s) and will be eligible for help desk support.
2. Users can use their own authenticator(s) and will be eligible for help desk support.
3. Users can use their own authenticator(s) but will not be eligible for help desk support.

Scenario 1 saves on hardware costs but may increase support costs. Note that in some locales, employees cannot be required to use personal devices without compensation for hardware and/or time so this scenario may not be applicable based on local laws and/or social norms.

Scenario 2 provides a good balance for users and may save some hardware costs, but support costs will likely be higher as both company-provided and BYO authenticators will need to be supported by the help desk.

Scenario 3 is essentially the "we're not going to block it" scenario. Savvy users that are leveraging their FIDO Authenticators in their personal life can continue to do so at work but will not be entitled to help desk support for their authenticator.

Realistically, all deployments will require some availability of company-provided authenticators as there will always be users who are not willing to purchase or use a personal device. There is also the case where a visitor needs organizational access and may not have an authenticator of their own. Contractors are a great example of this. Long-term contractors may need to be assigned a company-owned authenticator just like an employee.

© 2021 FIDO Alliance. All rights reserved.

Considerations for Company-Owned authenticators

Devices that are issued by an organization often carry a higher support guarantee for end users. By issuing the same hardware roaming authenticators to all users or allowing the user to pick from a supported set, frontline IT support staff may find it easier to assist users in the event of an issue. This common support model comes with a potentially large upfront monetary cost, with recurring expenses for new users and organizational growth. These costs can potentially be minimized by requiring users to return their authenticator(s) when their relationship with the organization changes, allowing authenticators to be reset and reused. A full factory reset of the authenticator before reassignment is critical to ensure all previous credentials and configurations are removed.

A cost-benefit analysis should be performed to determine if the shipping and handling costs for returning an authenticator are greater than the cost of purchasing new authenticators. In large global deployments, these costs may be prohibitive, making it cheaper to allow the user to keep the hardware authenticator.

For organizations that wish to associate a specific hardware roaming authenticator with a user, Enterprise Attestation (EA) can help. EA allows an authenticator's unique hardware identifier to be disclosed to an RP based on a client-side enterprise policy configuration, a configuration in the authenticator, or after explicit user consent. EA also enables a hardware authenticator manufacturer to create special authenticators for an organization that has an immutable list of RP ID burned into the hardware with a flag that allows the device identifier to be disclosed via EA. This enables a smart card-like experience where a login session is bound to an authenticator which is associated with a user.

When discussing mobile devices, devices are often lumped into company-owned and BYOD. The other important dimension is unmanaged vs. managed. Managed devices, regardless of ownership, often have additional capabilities for provisioning and deprovisioning, including the potential management of a FIDO Authenticator app.

Generally, company-owned authentication devices such as smart cards and OTP tokens are restricted to COBO. This restriction does not apply to company-owned FIDO Authenticators. FIDO2 Authenticators are not bound to a specific identity or identity provider. They can be used to generate and register credentials with any FIDO RP and bind them to any identity, providing a flexible experience for users.

As there is no standardized way to prevent an authenticator from being enrolled with another RP, users in both COBO and COPE deployments should be informed and educated about the potential risk of using a company-provided authenticator with personal accounts. These risks include the potential loss of access to personal accounts that are protected solely with the company-owned authenticator.

© 2021 FIDO Alliance. All rights reserved.

Conclusion

The lifecycle management of authenticators has a fundamental importance in the enterprise to maintain workforce productivity and manage security risks. Generally, it is the responsibility of IT managers and security architects to define policies and processes for the use of authenticators and how they are managed after acquisition and throughout all stages of the lifecycle, including the initial bootstrap and binding to enterprise identities, replacement after loss or damage, reset and reassignment, or disposal after an employee leaves, etc. IT managers and security architects should consider defining clear policies and processes for the following:

- Allowed and disallowed authenticators in the work environment. For example, the policy can specify the type of authenticators (platform vs. roaming), makes and models, security capabilities, etc.
- Allow or disallow employees to bring their own authenticators
- Return company-owned authenticators during employee offboarding
- Reset and reassign or dispose of returned company-owned authenticators
- Technical support for employee-owned authenticators
- User identity verification during the registration of authenticators and bootstrap of FIDO credentials
- Allowed alternative authentication methods for emergency access in the event of a lost authenticator to ensure user access continuity
- Revocation of credentials and the replacement of lost authenticators

These policies and processes should be defined during FIDO rollout planning and aligned with the company risk tolerance and business objectives.

For further information and additional considerations for FIDO deployment in the Enterprise, refer to the following white papers:

- Accepting FIDO Credentials in the Enterprise
- Considerations for Deploying FIDO Servers in the Enterprise

Acknowledgments

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

- John Fontana, Yubico
- Max Hata, NTT DOCOMO
- Anna Sarnek, RSA
- Kevin Turner, HYPR

© 2021 FIDO Alliance. All rights reserved.