FIDO Alliance White Paper:

Choosing FIDO Authenticators for Enterprise Use Cases

March 2022

Editors:

Salah Machani, RSA Security

Norman Field, HYPR

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 is intended for IT administrators and Enterprise Security Architects who are considering deploying FIDO Authenticators across their enterprise and defining life cycle management policies. In this paper, we provide an overview of the different use cases for multi-factor authentication and the FIDO Authenticator choices administrators have. The intent is to help and guide administrators in choosing the right authenticator types for their specific environment.

Contents

Key Properties of FIDO Authenticators 5

Authenticator Types 5

Roaming Authenticators 5

Platform Authenticators 5

FIDO Protocol Versions 6

User Presence 6

User Verification 6

Discoverable Credential 7

Enterprise Attestation 7

Enterprise Use Cases 8

Use Case 1: User registration and enterprise identity binding flow 8

Example 1 - Registration of existing IT users with the enterprise FIDO server 9

Example 2 - Registration of new IT users who do not yet have a corporate account 9

Use Case 2: Web Authentication using FIDO as second factor 11

Use Case 3: Web Authentication using FIDO as a first factor (passwordless) 12

Identifier-first flow 12

Identifier-less flow 12

Use Case 4: Desktop/laptop logon using a roaming FIDO Authenticator as a second factor 13

Use Case 5: Passwordless desktop/laptop login using FIDO 14

Use Case 6: Log on to a remote computer using FIDO 15

Use Case 7: Authentication for relying parties during federation 16

Use Case 8: FIDO Authentication over SSH 17

Use Case 9: Tap-and-Go authentication for first responders, factory employees, and others 18

Use Case 10: Physical access using FIDO 19

Appendix: Choosing Authenticators Per Industry 20

Banking, Financial Services, and Insurance (BFSI) 20

Manufacturing 21

Aviation, Airlines 21

Acknowledgments 21

Tables

Table 1: Use Case 1 Properties 10
Table 2: Use Case 2 Properties 11
Table 3: Use Case 3 Properties 13
Table 4: Use Case 4 Properties 14
Table 5: Use Case 5 Properties 15
Table 6: Use Case 6 Properties 16
Table 7: Use Case 7 Properties 17
Table 8: Use Case 8 Properties 18
Table 9: Use Case 9 Properties 19
Table 10: Use Case 10 Properties 20

Key Properties of FIDO Authenticators

The FIDO Authenticator represents the user-facing portion of the FIDO Authentication standard. During both registration and authentication, the user must interact with the authenticator to confirm possession of the authenticator and/or to verify their identity. The authenticator is also responsible for protecting key materials generated during the registration process. To achieve the full potential of improved user experience over password authentication, an enterprise deployment must carefully consider what authenticators best fit the business, how authenticators get rolled out to the user population, and how they will be managed in the long run.

This section describes the key technical properties required to support enterprise use cases.

Authenticator Types

FIDO Authenticators can be classified into two types: *roaming authenticators* and *platform authenticators*. While each of these authenticator types performs the same role in the FIDO standard, they appear quite different to the end user.

Roaming Authenticators

For those with casual knowledge of FIDO Authentication, the roaming authenticator is the first thing that comes to mind. In particular, it conjures an image of a USB device plugged into a computer with a flashing light demanding to be touched. This is an accurate depiction of a roaming authenticator, but it is also not the complete picture.

The roaming authenticator is software implemented in a device that can be separated from the client device (i.e. the computer running the web browser). The roaming authenticator attaches to the client device over protocols such as USB, *Bluetooth® low energy technology*, or NFC. This means that even smartphones can act as authenticators for a separate client device. In this way, the roaming authenticator allows the user to carry the credentials associated with one relying party (RP) to authenticate on multiple computers.

Platform Authenticators

While roaming authenticators may be the first thing someone imagines when thinking of FIDO, platform authenticators have the benefit of ubiquity. A platform authenticator is simply an authenticator implemented in a computing device playing the role of the client in the FIDO standard. Common implementations include biometrics for user verification as well as special hardware chips for protecting cryptographic key materials (e.g. Secure Execution Environment, Trusted Platform Module (TPM), or a Secure Element (SE))[1]. If the user is performing the authentication gesture with the same device running the browser, that would be considered authentication with a platform authenticator.

The great benefit of platform authenticators for deploying FIDO to the enterprise is that virtually everyone has one already.

[1] Common commercial biometric implementations that can leverage platform authenticators include TouchID and FaceID from Apple, Android Fingerprint and Windows Hello.

FIDO Protocol Versions

FIDO consists of three protocol versions for strong authentication to web and non-web applications: Universal 2nd Factor (U2F), Universal Authentication Framework (UAF), and FIDO2.

There are more than 380 FIDO® Certified[2] makes and models of FIDO Authenticators from different vendors. While the three versions use a common public-key based authentication framework, there are subtle differences that make one version more suitable than another to address a particular use case or deliver a particular user experience.

- FIDO Authenticators supporting U2F are intended to be used as second-factor authenticators in a two-factor authentication scheme in addition to the first factor (generally, the user's password).
- FIDO Authenticators supporting UAF are intended to be used as first-factor authenticators in a passwordless authentication scheme, specifically in native applications, namely mobile apps.
- FIDO2 Authenticators are intended to be used as first-factor authentication for web applications supporting the W3C Web Authentication (WebAuthn) JavaScript API and non-web applications supporting CTAP2 protocol.

User Presence

User presence (UP) is a simple form of authorization gesture where a user interacts with an authenticator to prove human presence by simply touching it, shaking it, or pressing a button (depending on the authenticator form factor, other modalities may also exist). A test of user presence is typically required when an authenticator is used as a second factor of authentication. User presence does not constitute user verification. An authenticator that can perform user presence tests may also be capable of user verification using biometrics or a memorable secret such as a password or a PIN.

User Verification

User verification (UV) is typically required when an authenticator is used as the first factor for passwordless authentication. It can be initiated through various authorization gesture modalities; for example, through a PIN or password entry, or biometric scans (fingerprint, face recognition, iris recognition, etc.). The intent of user verification is to distinguish individual users.

[2] https://fidoalliance.org/certification/fido-certified-products/

Discoverable Credential

A Discoverable Credential, also known as Resident Credential or Resident Key, enables passwordless authentication flows. It is a public key credential source whose credential private key is stored in the authenticator, client, or client device. A WebAuthn RP can specify at credential creation time if discoverability of credential is required, preferred, or discouraged[3]. An authenticator that supports Discoverable Credential is not expected to offload the key storage to WebAuthn RP server. It can select the credential private key given only an RP ID, possibly with user assistance (e.g. by providing the user a pick list of credentials scoped to the RP ID). A Discoverable Credential can also enable the "Identifier-Less" authentication flow - a passwordless flow that does not require the user's identifier/username to log in even when the user logs in from a new machine. Enterprises implementing the identifier-less authentication flow should check with their authenticator vendor if the authenticator model supports Discoverable Credentials.

Enterprise Attestation

FIDO2 Authenticators supporting the CTAP2.1 protocol can have an enterprise context. FIDO2 Authenticators with an enterprise context enabled can be controlled (pre-configured and/or managed by the enterprise, in a similar fashion to managed Bring Your Own Device (BYOD)). There can be only one enterprise context per authenticator. An authenticator with enterprise context enabled can still be used for personal accounts. The enterprise will not be able to manage or get the list of the user's personal credentials or RP IDs and the user's privacy remains protected. The enterprise context allows enterprises to control which relying parties can request an enterprise attestation[4] that includes uniquely identifying authenticator information (such as the AAGUID).

The enterprise attestation allows RPs to verify not only the authenticity and integrity of the authenticators used in the enterprise environment, but also to:

- Verify that users are using authenticators that are pre-assigned to them, or
- Track authenticators and know who is using which authenticator

To enable the enterprise context, enterprises work directly with their authenticator vendor in order to source their enterprise attestation capable authenticators. An enterprise attestation capable authenticator may be configured to support either or both of the following configuration options:

[3] Web Authentication: An API for accessing Public Key Credentials - Level 2 (w3.org)

[4] The enterprise attestation can be enabled if the following conditions are met: (1) the browser supports WebAuth Level 2 API, (2) the platform supports CTAP2.1 and (3) the Authenticator supports CTP2.1 and enterprise context.

1. Vendor-facilitated Enterprise Attestation (EA): the customer enterprise works with an authenticator vendor to enable EA for their exclusive use. The customer may request the authenticator vendor to configure the authenticators with the enterprise's RP IDs. The Authenticator returns the EA only when requested by those RP IDs. If enterprise attestation is requested for any RP ID other than the pre-configured RP ID(s), the attestation returned along with the new credential is a regular privacy-preserving attestation, i.e. NOT an enterprise attestation.
2. Platform-managed Enterprise Attestation: a platform-management policy determines whether an origin (RP) can request EA. The platform must be enterprise-managed and can enforce the policy by vetting the RP ID. Enterprises can re-enable EA via vendor-supplied management tools. When requested by authorized origins, the platform-managed EA-capable authenticators return the EA. Users can disable EA functionality by doing a hard reset on the authenticator, but the enterprise can re-enable it from a managed platform.

Enterprise Use Cases

FIDO authenticators can be used in the enterprise to address the need for strong authentication for many use cases. This section provides the most common use cases:

- Use Case 1: User registration and enterprise identity binding flow
- Use Case 2: Web Authentication using FIDO as second factor
- Use Case 3: Web Authentication using FIDO as a first factor (passwordless)
- Use Case 4: Desktop/laptop logon using a roaming FIDO Authenticator as a second factor
- Use Case 5: Passwordless desktop/laptop login using FIDO
- Use Case 6: Log on to a remote computer using FIDO
- Use Case 7: Authentication for relying parties during federation
- Use Case 8: FIDO Authentication over SSH
- Use Case 9: Tap-and-Go authentication for first responders, factory employees, and others
- Use Case 10: Physical access using FIDO

Use Case 1: User registration and enterprise identity binding flow

Enterprises go through considerable effort to vet users before onboarding them into the corporate IT infrastructure. Once vetted, a user is given credentials, typically in the form of a username/password, that allow them to access corporate IT assets commensurate with their role. However, because passwords are easily compromised, using passwords for authentication devalues all the hard work placed on vetting the user in the first place. Passwordless authentication with FIDO preserves the value of the vetting, which takes place as part of user onboarding.

When adopting FIDO Authentication for the enterprise, there are two processes that need to be established:

1. Registration of existing IT users with the enterprise FIDO server
2. Registration of new IT users, who do not yet have a corporate account

Both cases are described below.

Example 1 - Registration of existing IT users with the enterprise FIDO server

Converting corporate users from password-based authentication to passwordless authentication using FIDO Authenticators requires educational outreach. However, from a technical standpoint, the process is relatively simple.

Prepare the following infrastructure:

- Establish (and distribute, if necessary) the set of authenticators supported by the enterprise.
- Leverage the identity provider (IdP) self-service web portal or create an internal web application accessible to authenticated enterprise IT users only. The portal or web application takes advantage of the vetting that took place during onboarding and guides the user through a FIDO registration process, which involves binding one or more authenticators to the corporate identity of the user.

Once the infrastructure is in place, users may register for FIDO by following these steps:

1. Open a web browser supported by the enterprise.
2. Access the FIDO registration web application and authenticate using the corporate credentials.
3. Follow the instructions for registering an authenticator. Depending on the type of authenticator, this will require either a user presence check (physical gesture) or a user verification check (biometrics, PIN, etc.).
4. After registering the first authenticator, the best practice would be to have a second authenticator registered to address the case where the first authenticator is lost or damaged.
5. The user now has the ability to log in to FIDO-enabled corporate web applications.

Example 2 - Registration of new IT users who do not yet have a corporate account

While it is certainly possible to continue to onboard corporate users with username/password credentials and then direct them to the above procedure for FIDO registration, keeping this workflow in place perpetuates the life of passwords in the enterprise. Establishing a passwordless onboarding process opens the door for a password-free and hence phishing-free corporate IT infrastructure.

The days of requiring in-person onboarding of new corporate IT users are over. By now most companies have procedures for onboarding users without having them visit the security office at corporate HQ. Those established procedures can now be used to initiate onboarding users for FIDO Authentication. The procedure would roughly follow these steps:

1. Distribute authenticator(s) to users.
2. Establish a website for new corporate IT user registration, which is accessible on the internet. The critical aspect of this website is to securely identify the user. There are many ways to do this (e.g. identity proofing, one-time codes, hiring manager assistance, etc.), which are beyond the scope of this document. Whatever policy is adopted here, it should leverage or improve upon what is currently used to onboard enterprise users.
3. The user visits the onboarding website and is challenged to identify themselves by whatever means the enterprise has deemed appropriate.
4. Once identified, the user is prompted for a user presence or a user validation check.
5. The user is presented with the option to register more than one FIDO Authenticator.

Table 1: Use Case 1 Properties

Authentication Mechanism	**FIDO2**	**U2F**
Client	Web browser[5]	Web browser
Gesture	UV recommended UP optional	UP required
Transport Protocols	USB, NFC, or Bluetooth LE	USB, NFC, or Bluetooth LE
Platform Authenticator	Windows 10+, MacOS, Chrome OS, Android, iOS, iPadOS	Chrome OS, Android, iOS, iPadOS
Roaming Authenticator	Security key, mobile device	Security key
Required Protocol Extensions	May require enterprise attestation by policy	N/A

Users have to be logged into the enterprise website before the FIDO key is registered. The challenge is which mechanism we should adopt to log in to the enterprise website.

[5] At the time of writing, the following web browsers support FIDO2/WebAuth: Chrome, Firefox, Edge, Safari, Opera. Chrome, Firefox and Opera support U2F.

Use Case 2: Web Authentication using FIDO as second factor

The user, an employee of example.com, sees that the corporate intranet site (RP) supports FIDO2 Authentication. The user uses their existing credentials to bootstrap a new FIDO Authenticator using a web browser. After bootstrapping the new authenticator, the user logs in with their new FIDO Authenticator as follows:

1. The user navigates to the login page.
2. The user enters their username and password. After accepting the username and password, the user is prompted to present a FIDO Authenticator.
3. The user presents a FIDO Authenticator. After presenting the authenticator, the user is prompted for a user presence gesture (e.g. tap).
4. The user provides a gesture as proof of presence and completes the authentication process.

The FIDO Authenticator in this case can be a U2F Authenticator or a FIDO2 Authenticator.

The client can be any web browser supporting the FIDO2 protocols (i.e. WebAuthn and CTAP2). Proof of user presence, in this case, is required. Presence can be verified using a simple gesture such as a tap. User verification using a PIN or a biometric is typically optional. This use case can be supported with or without enterprise attestation.

Table 2: Use Case 2 Properties

Authentication Mechanism	**FIDO2**	**U2F**
Client	Web browser	Web browser
Gesture	UP recommended, UV optional	UP required
Transport Protocols	USB, NFC, or Bluetooth LE	USB, NFC, or Bluetooth LE
Platform Authenticator	Windows 10, MacOS, Chrome OS, Android, iOS	N/A
Roaming Authenticator	Security key, Mobile device	Security key
Required Protocol Extensions	May require enterprise attestation by policy	N/A

Use Case 3: Web Authentication using FIDO as a first factor (passwordless)

The user, an employee of example.com, sees that the corporate intranet site supports FIDO2 Authentication. The user uses their existing credentials to bootstrap a new FIDO Authenticator using a web browser. After bootstrapping the new authenticator, the user logs in with their new FIDO Authenticator. The enterprise can choose to implement two different passwordless authentication flows using Discoverable Credentials:

Identifier-first flow

- The user enters a username to which the RP responds with a prompt to present a FIDO Authenticator with a user verification gesture (e.g. biometric or PIN). The RP response must not include the user's allowed list of credentials[6].
- The user performs the gesture, completing the authentication process.
- Subsequent authentication events may only require a FIDO Authenticator if the username is stored by the browser (e.g. using cookies) between sessions.

Identifier-less flow

- To authenticate, the user navigates to the RP which prompts the user for a FIDO credential.
- The user presents a FIDO Authenticator that supports resident credentials without first entering a username. If there are multiple resident credentials, the user may have to choose a specific credential via a browser interface element. The user completes authentication with a user verification gesture.

The FIDO Authenticator must be a FIDO2 Authenticator. The client can be any web browser supporting the FIDO2 protocols (i.e. WebAuthn and CTAP2). When used as a first factor, user verification is typically required or desired. User presence is implied when user verification is processed. To support the identifier-less flow, the credential must be discoverable. Enterprise attestation is not required.

[6] To protect the user's privacy, the RP must authenticate the user first (using a password, a long-lived secure session cookie or some other authentication factor) before returning the allowed list of credentials.

Table 3: Use Case 3 Properties

Authentication Mechanism	**FIDO2**	**UAF**
Client	Web browser, Native Application	Native Application
Gesture	UV recommended, UP optional	UV recommended, UP optional
Transport Protocols	USB, NFC, Bluetooth LE	Push Notifications or QR code
Platform Authenticator	Windows 10, MacOS, Chrome OS, Android, iOS, iPadOS	N/A
Roaming Authenticator	Security key, Mobile device	Mobile device
Required Platform Extension	Discoverable Credential Required, Enterprise Attestation Optional	N/A

Use Case 4: Desktop/laptop logon using a roaming FIDO Authenticator as a second factor

Description: User uses a domain password as a first factor and a roaming FIDO Authenticator as a second factor to log on or unlock a desktop/laptop computer. The computer may be a Windows, MacOS, or Linux machine and may or may not be connected to the network (offline access).

This use case would typically involve a user login to a machine issued by the enterprise. In addition to the typical domain login, the machine has been configured to use FIDO as a second factor. The roaming authenticator may have been issued by the enterprise or the user may have registered a personal authenticator.

The user logs in with their desktop as follows:

1. The user is presented with the desktop login screen.
2. User enters their username and password. The desktop validates the credentials.
3. After the desktop validates the username/password, the user sees a prompt to present an authenticator to complete the second-factor authentication.
4. User presents a FIDO Authenticator. After presenting the authenticator, the user may be prompted for a gesture (e.g. touch or fingerprint).
5. Upon providing the gesture (if required) as proof of presence, the user is logged into the desktop operating system.

Table 4: Use Case 4 Properties

Authentication Mechanism	**FIDO2**	**U2F**
Client	Native OS Credential Provider or Custom Credential Provider Local OS and/or Agent/Credential Provider	Custom Credential Provider
Gesture	UP recommended, UV optional	UP required
Transport Protocols	USB, NFC, or Bluetooth LE	USB, NFC, or Bluetooth LE
Platform Authenticator	N/A	N/A
Roaming Authenticator	Security key, Mobile device	Security key
Required Protocol Extensions	HMAC secret	N/A

Use Case 5: Passwordless desktop/laptop login using FIDO

Description: User uses a roaming FIDO2 Authenticator to log in or unlock a desktop/laptop computer. The computer may be a Windows, MacOS, or Linux machine. The authenticator may be used to log on to or unlock the computer in offline mode or in online mode.

Table 5: Use Case 5 Properties

Authentication Mechanism	**FIDO2**
Client	Local Operating System Agent/Credential Provider
Gesture	UV required
Transport Protocols	USB, NFC, or Bluetooth LE
Platform Authenticator	Windows 10+
Roaming Authenticator	Security key, Mobile device
Required Protocol Extensions	N/A

Use Case 6: Log on to a remote computer using FIDO

Description: User uses a FIDO Authenticator to log in to a remote computer. The FIDO Authenticator may be used as a second factor after the user enters the password. In this case, the user uses FIDO to authenticate and sign into the local machine, runs the remote desktop client on the local machine, and signs in automatically to the remote machine without having to re-authenticate.

Table 6: Use Case 6 Properties

Authentication Mechanism	**FIDO2**	**U2F**
Client	Local Operating System Application (RDP Client, custom logon agent)	Local Operating System Application (RDP Client, custom logon agent)
Gesture	UP recommended	UP required
Transport Protocols	USB	USB
Platform Authenticator	Windows 10, MacOS	Windows 10, MacOS
Roaming Authenticator	Security key, Mobile device	Security key
Required Protocol Extensions	HMAC secret extension required	N/A

Use Case 7: Authentication for relying parties during federation

Enterprises often contract out to third parties for services such as health insurance, financial services, and many other services outside the core function of the enterprise. In such cases, federated single sign-on is used to securely transfer identity from the enterprise - acting as an Identity Provider (IdP) - to the third-party service - acting as a Service Provider (SP).

Typically, the enterprise IdP evaluates the access policy and performs multi-factor authentication (MFA) to authenticate the user at the required assurance level before issuing an assertion about the user's identity to the third-party service. In this case, the IdP acts as the FIDO RP and performs FIDO authentication or delegates FIDO authentication to a 3rd party MFA provider / FIDO RP before issuing the assertion.

In cases where the IdP performs a non-FIDO primary authentication method and issues an assertion about user identity, the SP may determine that assertion requires a second-factor authentication to protect the data in their purview. In this case, the SP performs additional authentication using a FIDO-based mechanism or redirects the user back to the IdP with a request to re-authenticate the user with a FIDO-based authentication to supplement the prior non-FIDO-based authentication.

Table 7: Use Case 7 Properties

Authentication Mechanism	**FIDO2**	**U2F**
Client	Web browser	Web browser
Gesture	UP recommended, UV optional	UP required
Transport Protocols	Bluetooth LE, NFC, USB, Out of Band Mobile Authenticator	USB, NFC, Bluetooth LE, Out of Band Mobile Authenticator
Platform Authenticator	Windows 10, MacOS, Chrome OS, Android, iOS, iPadOS	Windows 10, MacOS, Chrome OS, Android, iOS, iPadOS
Roaming Authenticator	Security key, Mobile device	Security key
Required Protocol Extensions	Discoverable Credential preferred May require enterprise attestation by policy	N/A

Notes: This use case is used to raise the authentication assurance associated with a federation event by requiring a second factor during federation to the RP. The IdP in this case does not support multi-factor authentication (MFA).

Use Case 8: FIDO Authentication over SSH[7]

Description: Secure Shell (SSH) is widely used by systems administrators and developers to remotely access machines dispersed throughout the enterprise network. The release of OpenSSH 8.2 introduced support for FIDO Authentication to the secure shell protocol. OpenSSH introduced new key types *ecdsa-sk* and *ed25519-sk* and added support for those key types in the SSHD server as well as the various SSH utilities.

Using one of the above key types while the authenticator is attached, the command *ssh-keygen -t <keytype>* generates a public private key pair. After generation, this key may be used like any other supported key in OpenSSH. However, in order to use the private key for remote login, the FIDO Authenticator must be attached to the client machine, so that the user may perform the required gesture for authentication.

[7] https://cryptsus.com/blog/how-to-configure-openssh-with-yubikey-security-keys-u2f-otp-authentication-ed25519-sk-ecdsa-sk-on-ubuntu-18.04.html

If a user needs to frequently move between machines, the *ssh-keygen -O resident* option can be used. This is supported by the authenticators adhering to the FIDO2 standard and allows the private key to be retrieved from the authenticator. The command *ssh-keygen -K* downloads all available resident keys from the authenticator attached to the host and writes the corresponding public/private key files to disk.

Table 8: Use Case 8 Properties

Authentication Mechanism	**FIDO2**
Client	SSH/SSHD distributed with OpenSSH 8.2 or greater
Gesture	UP, UV (Biometric, PIN)
Transport Protocols	USB, NFC, or Bluetooth LE
Platform Authenticator	Where OpenSSH is supported
Roaming Authenticator	Security key, Mobile device
Required Protocol Extensions	N/A

Use Case 9: Tap-and-Go authentication for first responders, factory employees, and others

Description: Enable FIDO2 Authentication for time-sensitive use cases such as first responders, and factory employees who may be using gloves or may not be able to use common biometrics such as fingerprints[8]. Similarity, users with disabilities may not be able to provide biometrics or manually enter a PIN. For such scenarios, an identifier-less authentication flow without UV is most suitable. As an identifier-less flow without UV, the authenticator is a bearer token. It should only be allowed in controlled environments or for use cases that do not require high assurance.

[8] https://www.mitre.org/sites/default/files/publications/pr19-1396-usability-biometrics-for-disabilities.pdf

Table 9: Use Case 9 Properties

Authentication Mechanism	**FIDO2**
Client	Web browser, Local operating system Native application
Gesture	UV required
Transport Protocols	USB, NFC, or Bluetooth LE
Platform Authenticator	Windows 10, MacOS, Chrome OS, Android, iOS, iPadOS
Roaming Authenticator	Security key, Mobile device
Required Protocol Extensions	Discoverable Credentials required May require enterprise attestation by policy

Use Case 10: Physical access using FIDO

Description: Organizations have been using RFID and smart card technologies for access control systems to secure their facilities for decades. The security concerns of RFID cards and the overhead of public-key infrastructure (PKI) to manage the life cycle of smart cards led organizations to look for alternative solutions. FIDO roaming authenticators built into smartphones, key fobs, rings, or other form factors are an ideal replacement. Users can simply tap their authenticator device on an NFC- or Bluetooth LE-equipped reader to initiate a FIDO protocol exchange for identification and authentication and unlock doors or other physical systems.

Table 10: Use Case 10 Properties

Authentication Mechanism	**FIDO2**
Client	Control panel
Gesture	UV recommended, UP optional
Transport Protocols	USB, NFC, or Bluetooth LE
Platform Authenticator	N/A
Roaming Authenticator	Security key, Mobile device
Required Protocol Extensions	Discoverable Credential Required

Appendix: Choosing Authenticators Per Industry

Different organizations have different use cases for MFA and needs for FIDO Authenticators. In the following subsections, we describe the authenticator choices organizations within the same industry have that address their unique use cases.

Banking, Financial Services, and Insurance (BFSI)

Generally, BFSI employees work in an office setting, either in corporate offices or at the branches. Employees often deal with highly sensitive information, including client private data and transactions. They are required to use company-provided for business-only use devices. At the corporate offices, employees use dedicated devices on which they can enroll platform authenticators. At the branch and call centers, employees, including clerks, reps, and managers, use shared devices. For those employees, roaming authenticators with UV protection are recommended.

Manufacturing

Depending on the type of goods being manufactured or the target markets, secure human authentication can be essential. One application is physical access to manufacturing facilities. For instance, access to factories where security-sensitive products are being made (e.g. defense, IT infrastructure) could be required to ensure that only those individuals who are authorized are allowed entry. This could take the form of FIDO-enabled smartcards (e-badges) or even personal devices with FIDO platform authenticators that have been onboarded onto the factory access system. A second critical use case in manufacturing that can benefit from the use of FIDO is access to online design systems (e.g. CAD/CAM, PCB layout). Such systems often contain proprietary information or trade secrets that can require restricted access. Moreover, FIDO Authentication can be applied in securitization of the manufacturing supply chain. For instance, there is growing support for the ISO 20800 standard for secure supply chain management, which requires verification of all suppliers involved in the manufacture of finished products.[9] For instance, a human authentication record (via a FIDO assertion) can be used to audit each stage of transport of a necessary component in order to improve traceability and reduce the likelihood of theft or counterfeiting.

Aviation, Airlines

Airline companies are some of the largest employers in the world. The number of employees per airline can range from under 1,000 employees to over 120,000. A large number of the employees are on the go, working at the airport, or on the aircraft. This includes pilots, flight attendants, aircraft mechanics, airport sales agents, lounge staff, luggage handlers, etc. In their roles, they generally access protected online resources from shared devices (tablets or airport workstations) or personal devices (bring your own device (BYOD)). For these employees, roaming authenticators such as security keys are recommended. Office-centric employees may or may not have dedicated workstations or laptops. For example, reservation agents at a call center shared workstation, while executives, marketing, and office staff have dedicated machines. Employees with dedicated corporate machines can be enabled to use platform authenticators.

[9] J. Kurowski, “Security as an Underappreciated Factor in Optimizing The Supply Chain”, Mechanics Transport Communications, Issue 3, 2011

Acknowledgments

We would like to thank all FIDO Alliance members who participated in the group discussions or took the time to review this paper and provide input, specifically:

- John Bradley, Yubico
- Tim Cappalli, Microsoft
- Karen Chang, Egis Technology
- John Fontana, Yubico
- Max Hata, NTT DOCOMO
- Karen Larson, Yubico
- Bill Leddy, LoginID
- Giri Mandyam, Qualcomm
- Dean Saxe, AWS
- Andrew Shikiar, FIDO Alliance
- Shane Weeden, IBM