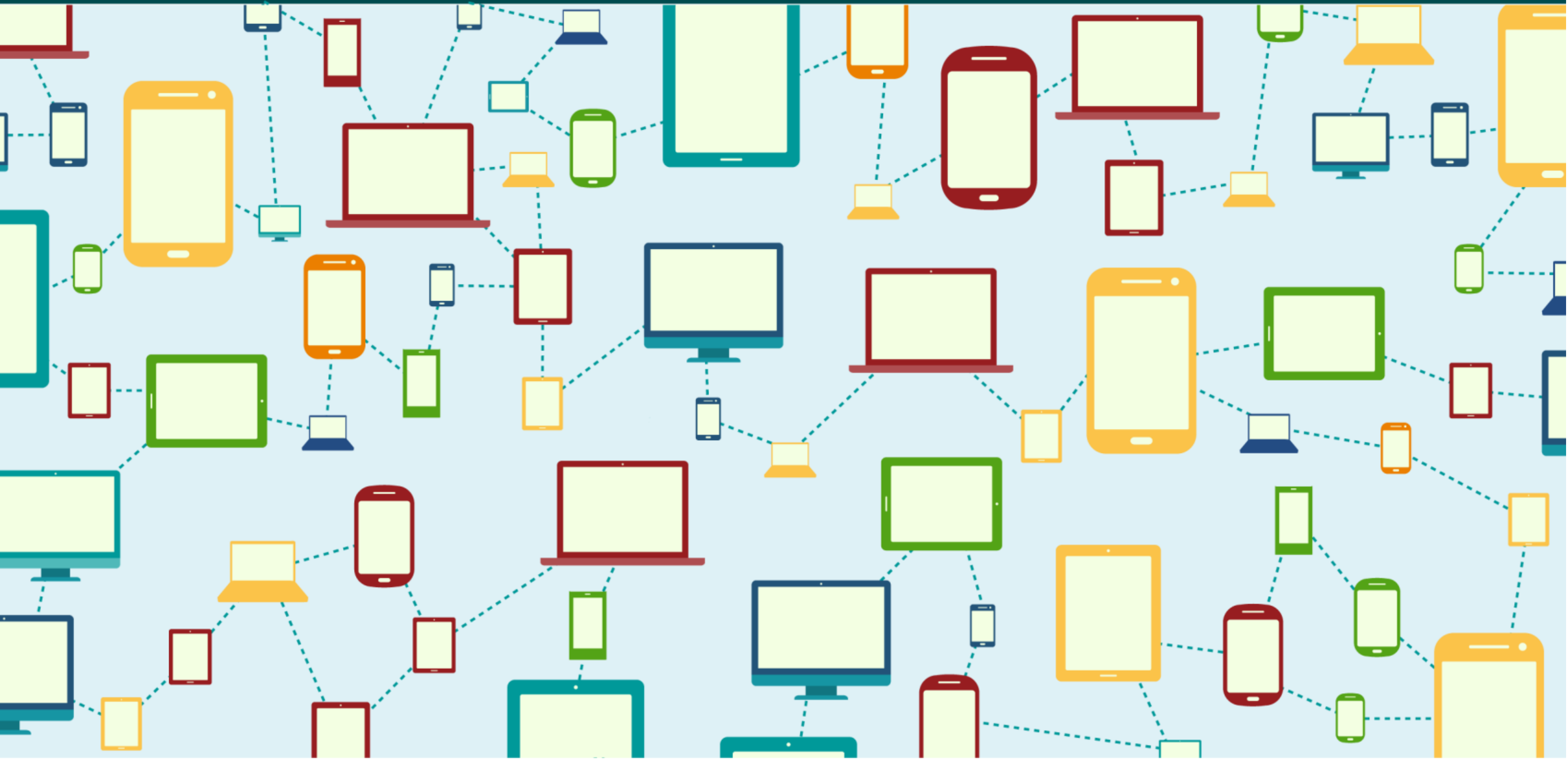
fido ALLIANCE simpler stronger authentication



# Enterprise Adoption Best Practices

## Managing FIDO Credential Lifecycle for Enterprises

April 2018

# 1 Audience

This white paper is aimed at enterprises deploying FIDO for strong authentication. It is intended to provide guidance to IT and Security professionals on how to manage FIDO authentication credentials throughout their full lifecycle.  It should be noted that the descriptions and the guidance of this paper may not apply to other use cases such as those of consumers.

It is assumed that the reader has understanding of FIDO architecture and protocols.

# Contents

# 2 Scope of Document

Life cycle management of FIDO credentials is a critical element of deploying FIDO Authentication in the enterprise. This document provides guidance and proposes best practices on how to manage FIDO credentials throughout their full lifecycle for enterprises. (The term "FIDO credentials" refers to the public and private key pair that is used in FIDO protocol for user authentication). More specifically, the document addresses the problem of registering FIDO credentials as part of the employee on-boarding process and account creation, registering and binding new FIDO credentials to existing user corporate accounts, revoking FIDO credentials when they are compromised or employees leave the company, renewing FIDO credentials, and recovering access to corporate accounts when FIDO credentials are lost.

Additionally the document describes the different types of FIDO authenticators enterprises can choose from. Although some aspects of FIDO credentials life cycle management in the enterprise apply to consumer applications, the document does not address consumer use cases.

# 3 Introduction

FIDO is the next generation in authentication technologies, designed to standardize the use of the authenticators that are carried around every day. Authenticators can be included in users' phones, computers or attached to their key ring. The goal of the FIDO model is to provide high quality cryptographic assurance that the user authenticating is indeed the user assigned to that account.

There are two established FIDO authentication protocols and one emerging standard. The Universal Authentication Framework (UAF) protocol is a model of authentication which enables the authenticators in phones and other devices to be trusted for use in authentication. Solutions built on UAF are utilizing authenticators to create a strong password-less and multi-factor experience for users.

The Universal Second Factor (U2F) protocol is a model of authentication which enables users to use a credential stored on a second-factor authenticator in addition to a password. Solutions built with U2F are utilizing authenticators to create a simpler second-factor authentication (2FA) experience.

The FIDO2 protocol (comprised of W3C's Web Authentication specification and FIDO's corresponding Client-to-Authenticator Protocol or CTAP) is a merger of UAF and U2F use cases to address both FIDO's password-less and second-factor experiences and provides users with the ability to utilize bound authenticators and roaming authenticators. Enterprises deploying FIDO2 authentication solutions should consider using credentials in bound authenticators and/or in roaming authenticators to offer the correct authentication experience for their users.

## 3.1 How does FIDO work?

While each protocol (UAF, U2F, and FIDO2) has its differences, the primary premise of each protocol is that key material is generated on a local authenticator that is then used for user verification the next time the user attempts to access the system. The FIDO protocols are fundamentally challenge/response protocols that use public-key cryptography to remove many of today's common attacks against passwords. Phishing and Man-in-the-Middle (MITM) attacks can be eliminated with the implementation of full FIDO authentication specifications.

## 3.2 Is FIDO multi-factor authentication?

To comply with the NIST SP800-63 definition of multi-factor authentication (MFA), an authentication system must be built requiring two of the three categories of authentication; something you are, something you know and something you have. Proper utilization of the FIDO protocols allows a system design to meet NIST SP800-63. Authenticators can include biometric sensors or PIN verification capabilities, which may enable use cases that meet the requirements for MFA. However, that evaluation is implementation and device specific, which is outside the scope of this document. This document provides architects and engineers with the understanding required to develop a system that meets MFA requirements.

# 4 FIDO Authenticators

There are two major classes of authenticators, bound and roaming. Each authenticator class has different properties that enable different use cases. Both classes of authenticators should be evaluated when designing a FIDO authentication solution. This evaluation ensures adopters get the benefits of both security as well as the desired user experience.

Whether bound or roaming, FIDO Authenticators from different vendors have different security characteristics. Enterprises may define different access policies for different types of resources that require authenticators to meet a specific security requirement.  For example, access to privileged accounts may require an authenticator with a higher security characteristic, while normal user accounts may require authenticators with a medium security characteristic. Enterprises need to ensure that users have the authenticators with the right assurance levels to access highly sensitive resources.

## 4.1 Bound Authenticators

Bound authenticators are built directly into access devices such as laptops and smartphones. They are generally more prevalent since they are built into devices that users already carry and use. They include fingerprint scanners, iris scanners, facial recognition, and voice recognition. These authenticators are typically used to replace password-based authentication solutions and provide a greater user experience.

When designing applications that rely on bound authenticators, it is important to understand that the application runs on the same device as the bound authenticator. When a user generates a credential on that bound authenticator this credential resides in that authenticator only and cannot be exported. In order for the user to run and access the application from another device, they will have to generate and register a new credential on the new device.

Typically FIDO UAF authenticators are bound authenticators while they can be used as roaming authenticators.  Platform vendor-provided FIDO2 authenticators can also be bound authenticators.

## 4.2 Roaming Authenticators

Roaming authenticators are physically separated from the access devices, connected via such media like USB, Bluetooth or NFC, and are able to roam between different devices with the FIDO credentials. FIDO roaming authenticators can support both password-less and 2FA authentication models.

FIDO U2F authenticators are generally roaming authenticators.  They are used to enable 2FA where password and a second factor is required.  FIDO2 authenticators may be roaming authenticators, but would communicate with the FIDO client via the FIDO standardized Client-to-Authenticator Protocol (CTAP).  FIDO UAF authenticators may also be used as roaming authenticators.  Generally, a device containing a bound authenticator, such as a FIDO UAF authenticator in a smartphone or a tablet can be used with another device as a roaming authenticator in addition to its function as a bound authenticator for local applications.

## 4.3 Authenticator Types

A bound or a roaming FIDO authenticator is a set of hardware and software components that implement the authenticator portion of the FIDO stack.  In addition to FIDO authenticators that are typically embedded in access devices such as laptops and smartphones, organizations can choose from a wide range of form factors from different vendors, offering different usability, availability and security features. Price points range from free to higher cost.

While FIDO protocol is secure by design and can prevent phishing and man-in-the-middle attacks, FIDO authenticators from different vendors have different security characteristics and offer different defense mechanisms against various types of software and hardware attacks. Security-aware enterprises should validate the security of the authenticators they choose or allow their employees to use for network or applications access.

For a successful FIDO deployment, enterprises should select the authenticator type that meets their business and technical requirements. Typically, a FIDO Authenticator Application combines critical services from the underlying operating system and device environment (hardware and firmware) to provide the full functionality of a FIDO authenticator. Such services may include the cryptographic functions, key storage, biometric matching and device attestation. The operating environment might be a high-level operating system (HLOS) such as rich mobile operating systems or a restricted operating environment (ROE) that is separated from the HLOS, such as a trusted platform module (TPM), a trusted execution environment (TEE) or a secure element (SE). ROEs might be used to provide security services to the HLOS or be completely isolated and used to run secure applications such as a FIDO Authenticator Application. The security strength of the authenticator depends predominantly on where the Authenticator Application runs, how it is protected and where FIDO cryptographic keys and sensitive data are stored and operated on, inside a ROE or on a HLOS that may or may not leverage some services from the ROE.

It is important that organizations vet FIDO authenticators that employees bring in before they can register them to access company resources. They should also ensure that Authenticator Application developers have implemented best practices and security controls that meet the minimum requirements for the protection FIDO credentials.

Realizing the importance and complexity for enterprises to evaluate and assess the security of FIDO authenticators from different vendors and select the right authenticator type, FIDO Alliance designed a security certification program in addition to the functional certification program for authenticators. While the functional certification program is designed to ensure interoperability of the authenticators with other components in the FIDO solution from different vendors, the security certification program is designed to evaluate the security features of the authenticators based on FIDO authenticator security requirements covering multiple types and levels of attacks ranging from remote software attacks to physical hardware attacks. This program is still evolving and it is expected that new certifications and new requirements will be added.

# 5 FIDO Credential Lifecycle Management in the Enterprise

FIDO authentication presents many benefits when designing authentication solutions, but it is important to understand the lifecycle of FIDO credentials. Designing environments anchored on the FIDO authentication protocols is very different when compared to traditional smart card, one-time password, and password-based systems. In the existing solutions, most systems use the fewest number of credentials possible. However, in a FIDO-based system, many users are likely to possess a handful of different authenticators at the same time (for instance, one for a mobile device and another for a laptop).

The FIDO credential lifecycle has two primary phases, registration and authentication; and two conditional phases, renewal and revocation. Designing an enterprise authentication solution using FIDO credentials requires an understanding of how to integrate the FIDO credentials into the processes for credential revocation and deletion, credential renewal, and account recovery.

## 5.1 Registration

Registration is the process of binding a FIDO credential on a given authenticator to a specific account. These accounts may either already exist or may be created as part of the registration flow. Understanding the FIDO credential registration process requires knowledge of the registration models for user account credentials. FIDO credentials are used for authentication and not for identification. Systems utilizing FIDO credentials must be able to properly support many credentials per user and each credential must be registered using one of the following models:

- Trust on First Use (TOFU) model
- Invitation model
- Federation model
- Identity Proofing model

- Anchor model

Proper combination of these models will enable a FIDO-enabled ecosystem that is not only secure but unintimidating to users. When examining the registration models for a FIDO credential, it is important to examine how the credential registration process fits in the bigger identity management process for user accounts. The model chosen for registration will impact the overall identity assurance of the account, which in turn affects the processes that can be allowed for account recovery.

The following state transition diagrams illustrate different approaches for registering FIDO credentials in relation to accounts. As introduced below, Figure 1(a) represents the models for registering FIDO credentials directly. Since there are no existing accounts for the FIDO credential, it requires creating a new account at the same time. Figure 1(b) represents the model where FIDO credentials are registered based on an existing account that has been established previously by a conventional way.

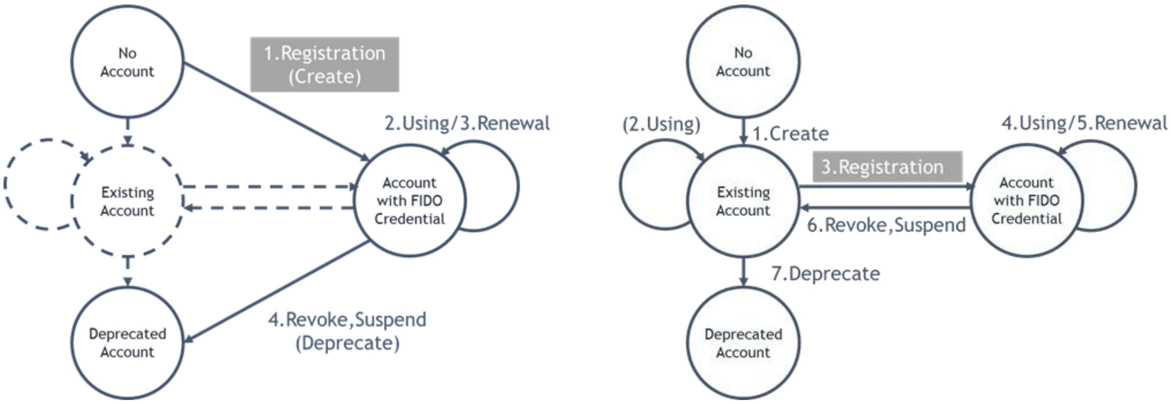


Figure 1 State Transition: (a) Registering FIDO credential directly, (b) Registering FIDO credential based on an existing account.

### 5.1.1 FIDO Credential Registration Models for the Creation of New[1] Accounts

The process for registering the first FIDO credential as part of the creation of a new account is simple and straight-forward, which enables users to immediately and securely access the application. The first credential registered is the trust anchor for the account. The following models detail the process for how a user registers the first FIDO credential for their account.

#### 5.1.1.1 Trust on First Use Model

As the name suggests, Trust on First Use (TOFU) is a model for registration where the credentials that the user provides during initial registration is trusted for the account. This model is typically applied to services that do not require identity verification or proofing and where the goal of the authentication is to ensure that only the person who registered the account has access to the account.

It is important to note that when building a system using the TOFU model, FIDO credential registration and account recovery processes must be carefully considered due to the lack of a verified identity to fall back on. The TOFU model is only applicable during registration of the account.

[1] Creating a new account refers to the process of setting up an account for the first time with a relying party.

### 5.1.1.2 Invitation Model

In many cases, the TOFU model does not provide sufficient identity assurance for the application and resources that a user is attempting to access. The first option in enabling a tighter process for binding people to user accounts relies on an invitation process. The invitation model improves on the TOFU model by utilizing an attribute that was registered through a separate process for enrolling the user. This allows a previously registered email or phone number to be a mechanism for sending an invite to the user to begin the registration process.

This model is commonly used in vendor identity management systems where a trusted user such as an administrator sends a registration invite with a one-time registration code to a new user. This process enables an audit trail which shows who registered the credentials and who invited them to register. Ultimately, this provides assurance that the person registering FIDO credentials on a given system is authorized and who they claim to be.

Delivering an invitation through the physical mail is another method that provides assurance that the account holder at a given address is the person registering. This method, however, introduces a significant latency to the registration process.

### 5.1.1.3 Federation Model

The federation registration model enables users to utilize an existing identity to authenticate and provide initial user attributes during registration. The federated registration is used as either a process for simplifying registration by obtaining user attributes from the federation provider or for providing authentication capabilities. In either scenario, users can register a FIDO credential with their accounts during the registration process.

Registering a separate set of FIDO credentials on the user account allows the account to be de-coupled from the federated identity provider and enables the user to use FIDO for authentication and have a high assurance authentication for subsequent sessions. FIDO credentials provide a high assurance authentication solution that pairs with registration processes that need identity proofing.

## 5.1.2 FIDO Credential Registration Models for Existing Accounts

Users may register and bind new FIDO credentials with existing accounts by going through the FIDO registration process that provides at a minimum the same level assurance than the process used to logon to the account.

Any of the Invitation, Federation and Identity proofing models can be used for registering a new FIDO credential for existing accounts.

The TOFU model must *not* be used for registering FIDO credentials for existing accounts. If TOFU is used for any subsequent FIDO credential registration, there are insufficient controls in place to protect the account from a hijack. The attack on the account would be to register a new authenticator and claim that the attacker is the target account.

In addition to the three models above that enable users to bind new FIDO credentials to existing accounts, there is one additional model to register FIDO credentials on an existing account.

### 5.1.2.1 Anchor Model

The Anchor model allows for the use of existing trusted authentication credentials on an account to be used for the registration of FIDO credentials on the account. Depending on the existing enterprise environment and authentication solution, different types of authentication credentials could qualify and be used for the registration of FIDO credentials and preserve the identity assurance on the accounts.  These may include smart card PKI credentials or other types of authentication credentials.

#### 5.1.2.1.1 Other Existing Authentication Credentials

Many organizations have strong authentication solutions deployed. If the existing solution such as MFA has sufficient assurance levels to meet the need for the applications being accessed, then the existing MFA requirements of the enterprise can serve as anchor for the FIDO ecosystem. This model enables organizations to utilize their MFA solutions to either bootstrap FIDO authentication or as a system that works in conjunction with FIDO until the migration to the new authentication services is completed. For example, a user can register and bind a new FIDO credential to an existing account after the user has logged in to their account by providing existing credentials such as a password and an additional factor, and selecting a registration option from account management settings to invoke FIDO registration process.

#### 5.1.2.1.2 Existing Smart Card Credentials

Systems designed to implement FIDO on top of an existing smart card authentication solution have additional options during registration to maintain the identity assurance on the account. The smart card solutions include such US government standards as personal identity verification (PIV), commercial identity verification (CIV) or common access card (CAC). The existing smart card credential is used during the FIDO registration process to bootstrap the FIDO credential registration process. This bootstrapping process creates an audit trail showing the primary credential used to authenticate to the registration process. In addition to actively authenticating the user before the FIDO credential is registered, existing credentials can be used in a workflow process before allowing the use of a newly registered credential.

This capability enables the design of a self-service registration model that maintains the assurance level of the existing credential that was issued to the user. The result is a large reduction in costly processes required to deploy and manage new traditional authenticators.

### 5.1.3 FIDO Credential Registration Models for Subsequent Credentials

The registration process used to register the initial FIDO credentials for an account sets the minimum identity assurance level for that specific account. To maintain the assurance level on that account, all subsequent FIDO credentials must either be registered using the same registration process or be anchored to an existing FIDO credential. Anchoring a new FIDO credential to an existing FIDO credential ensures the account’s assurance level is not degraded. The assurance for any given account is only as strong as the weakest credential or account management process.

The following models may be used to register subsequent credentials.

#### 5.1.3.1 Invitation Model

For the invitation model to work for registering a FIDO credential on a new authenticator, the invitation must be delivered to a registered device on a user account. There are many processes that could be designed to enable the invitation model to work for registering specific accounts on specific devices. These processes could range from an expiring code manually entered on the device to a message delivered to the existing or new device over a secure channel. This model creates a multi-step registration process for users attempting to register another authenticator.

#### 5.1.3.2 Identity Proofing Model

For the identity proofing model to work for registering a new FIDO credential in an authenticator, the same identity proofing process must be completed on the new device with the authenticator before the new FIDO credential can be created. This model maintains the assurance level for the user, but may have high transactional costs and be time consuming for that user.

This model is not as efficient as the other models due to the operational overhead of identity proofing additional authenticators. However, if a user is completing an in-person proofing[2] process, and to avoid having the user complete another tedious and costly in-person proofing process, it is recommended that the user registers multiple authenticators so that in the future the FIDO-anchored model can be used to address any other registrations.

#### 5.1.3.3 Anchor Model

The process for registering FIDO credentials anchored to an existing credential can be implemented using both in-band and out-of-band mechanisms. The in-band model enables a user to register a new FIDO credential by forcing the user to re-authenticate with the existing FIDO credential during the registration process. However, there are many scenarios where existing FIDO credentials cannot not be used in-band with another device attempting to register a new FIDO credential. This is where the out-of-band process would resolve potential issues.

For example, if a user registered a FIDO credential utilizing a laptop's bound authenticator and the user desired to register another FIDO credential on their mobile device, the user would need an out-of-band registration process for enabling secure authentication on their mobile device. The out-of-band model would require the user wanting to register a new FIDO credential to verify the registration request. Given the previous example, a user would attempt to register a FIDO credential on their mobile phone, but before that credential could be activated the user would have to sign into the application on their laptop and authorize the credential on their mobile device for use on their account. Alternatively, the user would first sign into the application on their laptop using the FIDO credential in the bound authenticator and then initiate the registration process for an additional FIDO credential on their mobile device by using a QR code or an SMS code. Enterprises need to evaluate the threats associated with each one of these methods and implement additional controls accordingly to ensure the security of the registration process. To provide the best user experience enterprises may consider implementing more than one method.

### 5.1.4 Other Considerations

There are many considerations for account lifecycle that registration and authentication of FIDO credentials do not cover.

#### 5.1.4.1 Enable Multiple FIDO Credentials

According to a 2015 Gallup Survey, 44% of Americans upgrade their phone every two years. This means that every two years, nearly half of America would need to re-register their FIDO authenticators on a new device. This begs the question of how can this user behavior be supported without creating undue risk or cost?

The recommended method for managing this use case is to allow or require the user to register multiple FIDO credentials. The FIDO credential is not portable like a password, so the user must either have a roaming FIDO authenticator or the ability to securely register multiple bound authenticators on a single account.

#### 5.1.4.2 Personalize FIDO Credentials

During the registration process, prompting the user to provide a personalized name for the authenticator that they just registered a credential on or displaying an image of the authenticator obtained from the attestation metadata will enable a more customized experience for the user. This will help users understand which authenticators are being used to access their accounts.

[2] In-person proofing is a method of verifying the identity of an individual that requires live interactions with an authorized operator either face-to-face by appearing physically at an identity verification office or remotely through a continuous high-resolution video transmission session. Please refer to NIST 800-63a for in-person proofing requirements.

### 5.1.4.3 FIDO Authenticator Registration Metadata

During the registration process the authenticator provides the FIDO server with attestation information that is critical for enterprises to understand the properties of the authenticator. Parsing and recording the attestation information during the registration process enables enterprises to have additional capabilities.

Enterprises should subscribe to the FIDO Alliance Metadata Service (MDS), which is a web-based tool where FIDO UAF, U2F and FIDO2 authenticator vendors can publish Metadata Statements for servers to download. The FIDO MDS provides organizations deploying FIDO UAF, U2F and FIDO2 servers with a centralized and trusted source of information about authenticators. FIDO authenticators may have many different form factors, characteristics and capabilities. A Metadata Statement specified by the FIDO Alliance defines a standard means for authenticator vendors to describe the relevant pieces of information about an authenticator in order to interoperate with it, or to make risk-based policy decisions about transactions involving a particular authenticator.

The attestation certificate along with Metadata Statements from the MDS allows organizations to create a whitelist of authenticator types or models that can be used in their enterprise. This allows enterprises to create policies regarding authenticators that meet their specific requirements. Policies can be defined based on authenticator properties or specific authenticator models. Additionally, an attestation certificate can be compared to a blacklist of authenticators, which would allow an organization to only reject certain authenticators.

Organizations may also choose to blacklist authenticators that use self-signed attestations, provide attestations with trusted roots that may not meet the enterprise’s security requirements or for which a security flaw has been reported.  This would be the case, for example, when additional tools such as MDM (Mobile Device Management) or device and application integrity verification and reputation services are not available to them to verify the authenticity, integrity and legitimacy of the authenticators.

## 5.2 Authentication

With an existing FIDO credential, the user has a very straightforward use case. The user will provide user intent verification to the FIDO authenticator, allowing a properly configured authenticator to complete the authentication process with the FIDO authentication server. For a user, authenticating with a FIDO authenticator should become something transparent and simple to complete.

The process of authenticating with FIDO credentials is slightly different when dealing with shared devices. A shared device presents additional challenges when compared to a device used only by a single user.

### 5.2.1.1 Individual Device(s)

When dealing with an individual device, a user will authenticate by simply using an authenticator available to them. In this scenario, the user account is stored as the default account, which simplifies the authentication process for the user. For individual devices, the user behavior that is most common for logout will be that the user locks the workstation when idle or when they leave.

### 5.2.1.2 Shared Device(s)

When dealing with a shared device, the authentication process must have a method for prompting users to provide their username as a hint as to who they are. The simpler it is for a user to be recognized by the system, the less friction the user experiences when authenticating. In environments where multiple workstations are shared, the use of roaming authenticators and portable bound authenticators that can act as roaming authenticators are recommended – whereas in environments where a single workstation that is shared amongst a few users the bound authenticators could be used. It is important to note that in the shared device use case, the workstation must log off when idle or when the user leaves.

### 5.2.2 Additional Recommendations for Enterprises

Learning from existing deployments is important. The following sections highlight best-of-breed design patterns that enable a good user experience by simplifying the process and providing quality audit data for enterprises.

#### 5.2.2.1 Simple Authentication Process

When users are accessing an application without an existing session, the authentication process should utilize pre-defined industry patterns for providing an account chooser. The ability to use an account chooser simplifies the process for end users to authenticate. For a shared workstation, it might be preferable to disable the account chooser.

#### 5.2.2.2 Collect Authenticator Usage Metadata

Collecting audit data about authenticator usage will enable both users and administrators to understand how accounts are being accessed. For a user it is helpful to know the last time they used a specific authenticator as this will enable them to determine if a lost device has been used to compromise their accounts. Additionally, the audit data will enable organizations to understand which authenticators their users prefer.

## 5.3 FIDO Credential Revocation and Deletion

Users and administrators must have methods to revoke or suspend specific FIDO credentials on an account. Since FIDO credentials are registered on devices, a lost or tampered device will give users or administrators reason to either revoke or suspend a FIDO credential from being used for authentication.

In the event a security flaw is discovered in an authenticator model or a single or batch of registered authenticators were compromised, it should be possible for the administrators to revoke them from user accounts without user intervention. Users will have to be informed that their FIDO credentials on compromised authenticators can no longer be used for authentication and should be given instructions on how to enrol new credentials.

There are some other situations where user FIDO credentials will be deleted from the enterprise backend system and can no longer be used. Examples include when a user account is deleted, a user credential is inactive after a certain period of time defined by policy or when the user deletes the credential from the device. For a user to suspend a FIDO credential without negatively impacting access to enterprise systems, the user must have alternate credentials (whether FIDO or not) already registered on their account.

## 5.4 FIDO Credential Renewal

FIDO credentials do not have an expiration date, however there are use cases where an enterprise may want to force a FIDO credential to be renewed on some authenticators. These use cases may include the deprecation of devices with specific cryptographic algorithms as well as complying with corporate policy on duration of credentials. FIDO credential renewal is not a concept that is natively supported in the FIDO protocol; therefore any renewal process must be designed into the system supporting FIDO authentication. Implementers of the renewal capability should be careful to ensure that the renewal process has the same level of security as was enforced in the registration process. It is important to verify that a user will not be forced into an account recovery flow through a credential registration. If a user maintains the ability authenticate during the renewal process, then any of the existing credential registration flows should be supported.

# 6 Additional FIDO Credential Management Scenarios

FIDO was designed to create a world where users are empowered to manage their own credentials using the devices that they already carry or devices that they are issued. The enablement of self-service processes for the user also requires that the enterprise elevate the traditional credential management capabilities for both the user and their helpdesk.

## 6.1 Self-Service Credential Management Portals

A user must be able to sign into a system with a FIDO authenticator or a credential with an equivalent authenticator assurance in order to manage the credentials on their account.

This enables a user to perform the following actions:

- Revoke a credential on a lost device
- Suspend a credential on a lost device
- Register new authenticators
- Renew FIDO credentials on an authenticator

## 6.2 Centralized Credential Management Portals

Many of the use cases for enterprises involve centralized management. This use case covers everything from administrative policy through help desk support. Any enterprise deploying such a system needs to consider the following capabilities in an enterprise credential management portal:

- Allow Help Desk staff to revoke/suspend a credential
- Allow Help Desk staff to mark credentials for renewal
- Allow Help Desk staff a method to support account recovery
- Allow Administrators to manage approved attestation certificates

## 6.3 Account Recovery for Enterprises

When you enable FIDO authentication, all other methods for authenticating or recovering an account must be considered. FIDO authentication provides a big step forward for user experience and system security. However, existing processes for self-service account recovery as well as help desk-supported account management must be carefully examined. Each of these processes is vulnerable to exploit as they bypass the security benefits of FIDO.

Account recovery processes are often the weakest link in account security, therefore the recommended solution provides the user with enough FIDO authentication options that the account recovery process is only required in extremely rare circumstances. If a system is built in such a way that it minimizes the usage of account recovery processes, then the rigor of the account recovery system can be increased.

Due to the inherent risks in account recovery, it is important that account recovery processes are run as rarely as possible. To achieve that, organizations should allow users to enroll and use multiple authenticators on the same account. In the event one authenticator is lost, they will have another registered authenticator to access their account or to enroll a replacement authenticator. Additionally or alternatively, organizations should promote user access to a centralized credential management portal using a dedicated FIDO authenticator that is different from the lost authenticator or an equivalent non-FIDO authenticator before they use the account recovery processes, revoke their lost FIDO authenticators and register new authenticators. When using multiple FIDO authenticators, users should assign unique friendly names to their authenticators.

There are two primary architectures that will need to be considered for designing the account recovery processes: FIDO-only and Multi-Access models.

Typically, the account recovery function is part of the company's centralized credential management portal. However, some organizations may consider delegating account recovery function to a trusted account recovery service provider with whom the user has an account. In this scenario, users authenticate to the trusted account recovery service using a variety of methods, including FIDO[3] and non-FIDO based methods, and request an account recovery token that they can present to their organization's centralized credential management portal or applications portal and enroll new FIDO authenticators. Organizations should ensure that the authentication method used by the account recovery service provider is adequate and offers the same or higher level of assurance about the identity of the user than that of the lost authenticator.

[3] Users may be required to enroll and use a FIDO authenticator with the account recovery service provider that is different from the lost authenticators used to access their organization's account.

### 6.3.1 Account Recovery for FIDO-only Accounts

Account recovery in a FIDO-only world assumes a user is not in possession of any registered FIDO authenticators on their account.

Account recovery options in this scenario include:

- An administrator or similarly authorized user is able to run an application that is designed to register a FIDO credential on behalf of another user. The administrator executing this process would need to authenticate with their own FIDO credential and would need to revoke the user's lost authenticator and register an authenticator for the user, then give the authenticator to the user.
- An administrator or similarly authorized user is able to revoke the user's lost authenticator, set the account into a registration-only state and send an invite to the user enabling them to register an authenticator. This method works well for external users.

### 6.3.2 Account Recovery for Multi-Access Accounts

Account recovery in a multi-access authentication system assumes the user is not in possession of any registered FIDO authenticators on their account but may be in possession of other non-FIDO authenticators on the same account.

Possible account recovery options in this scenario include:

- Relying on the Existing Multi-Factor Authentication Credential Anchor Model, the user revokes the lost authenticator and registers a new FIDO credential by authenticating to a purpose-built registration application using an existing MFA system.
- Relying on the Existing Smart Card Credential Anchor Model, the user revokes the lost authenticator and registers a new FIDO credential by authenticating to a purpose-built registration application using existing PIV/CIV/CAC or other similar smart card solution.
- Relying on the Identity Proofing Model, the user revokes the lost authenticator and registers a new FIDO credential by completing an identity proofing process.

## 6.4 MDM\EMM and FIDO

If an enterprise has a Mobile Device Management (MDM) solution, also known as enterprise mobile management (EMM), there are additional options that may be advantageous for the enterprise to consider.

Integrating Device Lost scenarios in the MDM system with the credential management solution will provide users a single place to report a device as lost and will reduce the amount of time that lost authenticators are active.

# 7 Additional Topics for Enterprises

There are many items worth considering when developing an enterprise authentication strategy for FIDO authentication. The following sections include suggestions on how to not only design a successful FIDO-based system, but also how to deploy it in a global enterprise scenario.

## 7.1 FIDO Deployment Techniques

Integrating FIDO credential registration into the on-boarding process for most enterprises is a simpler task than determining how to deploy FIDO to an existing user population. The following suggestions enable the construction of processes to simplify the deployment processes.

### 7.1.1 Authenticators with Pre-Loaded Credentials

Pre-loading credentials on authenticators enables a traditional deployment model where an enterprise can ensure that the correct user has the correct authenticator. By preloading credentials on an authenticator, administrators can link a specific authenticator to a specific user (or group). That way, only the designated user is able to use the registration system to prove they hold the right credential assigned and bound to their specific account.

### 7.1.2 Trusted Devices and Authenticators

One of the challenges organizations face in enabling FIDO-based authentication is how to on-board employees quickly and securely. The core challenge is how an authorized employee in the organization can enables a user to register their credentials. In many cases a solution is built using a set of dedicated authenticators issued to new employees and users during the initial registration process. For example, a payroll clerk may register a FIDO credential on behalf of an employee that is being on-boarded. The FIDO credential is only good for a specific user and is only able to authenticate to the registration application. This model enables a user to complete the self-service registration processes and have them anchored to an internal identity process.

## 7.2 Enterprise FIDO Credentials vs External RP FIDO Credentials

It is important to understand the differences between the FIDO credentials managed by an enterprise versus credentials that enterprise employees have registered at relying parties for personal use. As FIDO becomes more prevalent, there will be FIDO credentials managed by enterprises but also credentials that reside with relying parties in the same authenticator. Due to the nature of the FIDO's registration process, if a user registers a FIDO credential on a relying party's site, the data cannot be tracked or maintained by the enterprise authentication solution. This data will be associated with the user's personal account at the replying party only. The user is required to manage these credentials independently of enterprise-managed FIDO credentials. For example, if a FIDO authenticator is lost, a user must revoke the authenticator with the enterprise and everywhere else the authenticator was used to register FIDO credentials. Likewise, if the user leaves the enterprise, the enterprise-managed FIDO credentials will be revoked by the enterprise, but the user's personal account credentials at replying parties remain intact.

# 8 Editors

- Salah Machani, RSA
- Derek Hanson, Yubico

# 9 Acknowledgements

The editors would like to thank all FIDO members who reviewed or contributed to this paper, namely

- Paul Madsen, Ping Identity
- Mingliang Pei, Symantec
- Max Hata, NTTDOCOMO
- John Fontana, Yubico
- Giridhar Mandyam, QUALCOMM
- Hidehito Gomi, Yahoo! Japan