FIDO Alliance Guidance for U.S. Government Agency Deployment of FIDO Authentication

1. Executive Summary

At the request of the White House Office of Management and Budget (OMB) and the Department of Homeland Security's Cybersecurity and Infrastructure Security Agency (CISA), the Board of Directors of the FIDO Alliance established a Committee to help improve and accelerate adoption of FIDO technology within federal agencies.

The FIDO Alliance applauds the U.S. Government's prioritization of phishing-resistant authentication tied to enterprise identities as a part of cybersecurity modernization. Narrowing the types of multi-factor authentication (MFA) used in government workforce Identity Credential and Access Management (ICAM) to those resistant to phishing is critical to countering widely available phishing as a service platform. Denying bad actors the means to systematically exploit U.S. Government information systems by compromising authentication credentials is the most fundamental requirement of the Federal Zero Trust Strategy—offering immediate mitigation of a rampant threat and providing fundamental capabilities that enable the remainder of the strategy.

This Committee finds normative and permissive guidance from OMB, the National Institute of Standards and Technology (NIST) and CISA that can support agency-led modernization of identity to counter threats and improve mission outcomes. *Federal agencies* ***must*** *begin their Zero Trust Architecture (ZTA) journeys by implementing an inclusive user identity capability that supports both FIDO and PKI-based phishing-resistant MFA*. M-22-09 went beyond this to state that agency staff, contractors, and partners must use phishing-resistant MFA. Such a capability is required to integrate the lifecycle of identity management across all person types with the lifecycle of access management across the agency's digital resources, regardless of the authentication methods being used. Phishing-resistant authentication is necessary for others in the federal workforce, for example, those individuals who are not PIV eligible, or to quickly enable access for new employees who are waiting for their PIV to be issued, or those individuals who work remotely and don't need access to federal facilities.

This paper outlines ways that U.S. Government Departments and Agencies can more readily adopt FIDO authentication capabilities in order to meet immediate priorities defined in OMB 22-09, Federal Zero Trust Strategy, and, in conjunction with other normative and informative Federal guidance, advance cybersecurity outcomes by enabling future phases of Federal Zero Trust Architecture efforts.[1]

The Presidential Executive Order on Improving the Nation's Cybersecurity (EO14028) mandated agency use of MFA for all data at rest and in transit; OMB M-22-09 made clear that agencies should only be using MFA that is resistant to phishing attacks. The FIDO2 standards (FIDO), which include both the Web Authentication (WebAuthn) standard and also the Client To Authenticator Protocol (CTAP), together offer capabilities that complement existing Federal Public Key Infrastructure (FPKI), Personal Identity Verification (PIV), and Common Access Card (CAC) capabilities to bring phishing resistance to use cases where agencies rely upon username-password or other authentication methods that are vulnerable to phishing.

This paper will identify lines of effort the Federal Departments and Agencies ("D/A") are undertaking to implement normative guidance and identify key technical recommendations that must be considered in order to integrate FIDO authentication and enable immediate and longer-term outcomes.

Although broader U.S. Government adoption of FIDO authentication is consistent with Government-wide priorities within its Zero Trust Strategy, FIDO deployment is proceeding slowly, in large part because agencies do not yet have a good grasp on how to integrate FIDO authenticators into a PIV-centric ecosystem.

This document is intended to highlight areas where FIDO offers the best value to address U.S. Government use cases as an enhancement of existing infrastructure, while minimizing rework as U.S. Government Agencies advance their zero trust strategies with phishing-resistant authentication tied to enterprise identity as the foundation.

While FIDO has plenty of representative use cases in the commercial market, leveraging FIDO in enterprise government use cases presents different challenges because the lifecycle and services models are different.

FIDO implementations should consider lifecycle management and user journeys that:

- Extend agency authentication capabilities to persons who may not be authorized to receive a PIV or Derived PIV (DPIV), or for whom smart cards or PKI are not feasible for technology or mission reasons.
- Support applications' needs to select and enforce authentication assurance requirements; for example, applications and devices that cannot easily make use of PIV or PKI.
- Minimize the need for reconfiguring relying party systems to advance additional Zero Trust-driven modernization once FIDO capabilities are in place.

2. Scope Statement

This document will provide information on FIDO Alliance technology standards and why they are cited in OMB as well as in other guidance. In addition, this paper provides guidance on implementation of FIDO credentials within the federal digital identity ecosystem, and other deployment considerations and recommendations.

This document will not discuss multilateral federation, citizen-facing digital identity, or general PIV/CAC replacement.

2.1 Audience

The audience for this document is Chief Technology Officers, Chief Information Officers, Chief Information Security Officers, human resource officials, cybersecurity officials, digital services officials, privacy officials, including senior federal identity officials and architects with procurement authority that want to add another phishing-resistant authenticator to complement PIV or CAC.

3. Background

3.1 What is FIDO?

FIDO (Fast Identity Online) Authentication is based on public key cryptography. Developed by the FIDO Alliance, FIDO is a global authentication standard that provides a simpler user experience with phishing-resistant security.[3] The FIDO2 specifications are the World Wide Web Consortium's (W3C) Web Authentication (WebAuthn) specification and FIDO Alliance's corresponding Client-to-Authenticator Protocol (CTAP).

3.2 What are Passkeys?

A passkey is a consumer-friendly term for a discoverable FIDO credential. The term "passkey" -- and plural form "passkeys" -- is a cross-platform general-use term, not a feature tied to any specific platform. In general, it could refer to the following:

- Synced passkeys - passkeys that are synced between a user's devices.
- Device-bound passkeys - passkeys that never leave a single device (including those on security keys, as well as applications implementing the older FIDO UAF standard). Device-bound passkeys can be used on FIDO Certified authenticators and security keys, including those that have achieved various levels of security level certification in order to meet specific requirements.[4]

The majority of content in this paper refers to use of device-bound passkeys, as guidance around synced passkeys is still emerging; we expect that agencies will initially want to focus on device-bound passkeys for enterprise FIDO authentication deployments, at least until additional guidance on the protection of synced passkeys is published. Note that device-bound passkeys may support both AAL3 and AAL2; synced passkeys are limited to use at AAL2.

As the passkey terminology is new, and the federal government's references FIDO authentication in various documents rather than passkeys, this paper will refer to the credentials as "FIDO authenticators" or "FIDO credentials." However, note that the term "passkey" can also be used interchangeably in practice.

3.3 Federal Government Policy and Guidance

Over the course of more than a decade, U.S. Federal cybersecurity and identity guidance has driven agencies toward a more risk-aware approach, targeting architectural weaknesses that require urgent action based on malicious activity and demonstrated capability.

In the 2015 Cyber Sprint, a response to the breach at the Office of Personnel Management caused by a compromised password, there was an urgent drive to get all agencies to start using MFA. Around that same time, "hacking as a service" tools emerged that enabled scaled credential theft through phishing and that could also phish some legacy MFA tools such as One-Time Passwords (OTPs), therefore security professionals across the globe started to focus on replacing these phishable authenticators with phishing-resistant authentication.

In 2019, OMB Memorandum M-19-17,[5] "Enabling Mission Delivery through Improved Identity, Credential, and Access Management," directed agencies to implement NIST SP 800-63-3 and calls for adapting the Government's approach to HSPD-12 and PIV and shifting focus to managing the lifecycle of credentials to the lifecycle of identities. This includes piloting additional authenticators, implementing processes to enhance management of access control, revocation of the credential, and established the Digital Identity Risk Assessment (DIRA) process[6] as a repeatable means to determine assurance requirements for different resources and contexts. Additionally, the directive calls for cross-agency federation and interoperability, and further directs:

- Agencies shall leverage federated solutions to accept identity and authentication assertions made by mission and business partners.
- Agencies shall accept assertions by partners based on digital identity risk and associated assurance levels in accordance with NIST guidelines and Governmentwide ICAM requirements.
- Agencies shall confirm that these assertions use open commercially available standards to the extent available.

OMB M-22-09 serves as the Federal Zero Trust Strategy and provides direction across "pillars" that initiate a change in thinking in federal cybersecurity. In this document, OMB specified initial requirements for digital identity, including implementation of enterprise identity and access management, phishing-resistant MFA, and implementation of authorization to use resources.

In 2017, NIST SP 800-63-3, *Digital Identity Guidelines*[7], focused further on concern about phishable MFA. In addition to modernizing the treatment of identity assurance into identity assurance levels, authentication assurance levels, and federation assurance levels, NIST also coined the term "verifier impersonation resistance" to capture the quality of "phishing resistance" as core to meeting Authentication Assurance Level 3 (AAL3), though optional at AAL2. This paper will use "phishing resistance" as the preferred term and use references to NIST SP 800-63-3 unless specified. By decomposing identity assurance into three orthogonal values that can be expressed as a "Vector of Trust," NIST provided a means to tailor solutions to different use cases and capabilities. The means of conveying identity assurance requirements is defined in Section 5, Digital Identity Risk Management.[8]

NIST SP 800-63B[9] requires the use of approved cryptography for cryptographic authenticators and verifiers:

> *"Cryptographic authenticators used at AAL2 SHALL use approved cryptography. Authenticators procured by government agencies SHALL be validated to meet the requirements of FIPS 140 Level 1.*

"Multi-factor authenticators used at AAL3 SHALL be hardware cryptographic modules validated at FIPS 140 Level 2 or higher overall with at least FIPS 140 Level 3 physical security. Single-factor cryptographic devices used at AAL3 SHALL be validated at FIPS 140 Level 1 or higher overall with at least FIPS 140 Level 3 physical security."FIPS-201-3[10] updated HSPD-12 standards to introduce Derived PIV requirements that could be met by non-authenticators by pointing to requirements for AAL2 and AAL3 authenticators from NIST SP 800-63B. This further expanded options for agencies to use FIDO authenticators. The enduring role of FIDO authenticators in PIV is clear in drafts of SP 800-157-1 and SP 800-217. NIST 800-217 will further elaborate on the Federation Considerations for PIV included in FIPS-201-3, which is critical for enterprise FIDO deployments.

The informative FICAM architecture, coordinated across agencies using the ICAM Subcommittee of the Federal CIO Council and CISO Council, has delivered FICAM Playbooks to address the patterns essential for implementing Federal direction from OMB. The essential patterns detailed in FICAM Playbooks include Enterprise Single Sign-On (SSO),[11] Cloud Identity, and Identity Lifecycle Management.[13]

CISA's Hybrid Identity Solutions Architecture guidance document[14] helps "agencies understand potential options for identity management interoperability between on-premises and cloud-based solutions, the challenges involved in each, and how to address those challenges."[15]

The FIDO Alliance supports the informative guidance produced by the ICAMSC and CISA to support agency efforts to meet the needs for centralization of enterprise identity services and making those available to applications. The informative FICAM architecture, coordinated across agencies using the ICAM Subcommittee of the Federal CIO Council and CISO Council, has delivered FICAM Playbooks to address the patterns essential for implementing Federal direction from OMB. The essential patterns detailed in FICAM Playbooks include Enterprise Single Sign-On (SSO),[16] Cloud Identity,[17] and Identity Lifecycle Management.[18]

A marquee capability of FIDO authentication is that it is intended to meet the phishing-resistant requirements laid out by OMB. It also gives agencies options for alternative authenticators that had not been previously available.

3.4 "Phishing Resistance" in the U.S. Government

Phishing-resistant MFA is mandated for federal staff, contractors, and partners in M-22-09. That same memo defines "phishing-resistant" authentication as "authentication processes designed to detect and prevent disclosure of authentication secrets and detect outputs to a website or application masquerading as a legitimate system." NIST 800-63B defined phishing resistance as "verifier impersonation resistance." Not all MFA is phishing resistant, but all FIDO and PKI authenticators fit into this category.

The draft of 800-63B-4 recognizes two methods of phishing resistance: channel binding and verifier name binding.[19] FIDO authenticators use verifier name binding by establishing an authenticated protected channel with the verifier, then generating an authenticator output that is cryptographically bound to a verifier identifier authenticated as part of the protocol the domain name of the verifier.

PKI uses the channel binding method in the Mutual Transport Security Layer (MTLS) by establishing an authenticated, protected channel with the verifier and strongly and irreversibly binds a channel identifier that was negotiated in establishing the authenticated protected channel to the authenticator output.

Not all MFA is created equal. Even AAL2 technology can be compromised. Devices that provide rotating codes are a simple example of a "phishable authenticator." The user is tricked into visiting a site impersonating a legitimate site. The phony site prompts the user to log in, and the user reveals the valid code needed to log into the real site. Once the malicious actor has the code, they use it at the destination site to impersonate the user. CISA has clarified that MFA solutions that use push notifications are not phishing resistant, even when those capabilities implement number-match[20].

Like PKI-based credentials, FIDO authenticators and credentials have differing assurance levels and characteristics, which will be described later in more detail. As in Federal PKIs, the most important distinction is the inclusion or absence of hardware protection of private keys, which is further differentiated by the use of FIPS-140 validated cryptographic modules.

However, FIDO technology is not a complete replacement for PIV. PIV provides critical capabilities that are outside of logical identity authentication that FIDO cannot provide. PIV is a badge for physical access control and includes technologies for using certificate-based authentication for physical access. PIV includes certificates for FIPS-140 certified encryption and digital signatures. This paper describes how U.S. Federal agencies can advance mission and security outcomes by deploying FIDO solutions as a complement to PIV and other ICAM capabilities in their enterprises.

4. Agency Actions

Implementing support for phishing resistant FIDO authentication is best integrated with other directed efforts that advance agency Zero Trust strategies. Agencies should integrate FIDO deployments into their requirements and plans for these capabilities. These efforts are urgently needed within agency ecosystems, even if some agencies are currently meeting their phishing resistant-authentication requirements exclusively with PKI-based credentials. The three efforts, **single sign-on**, **lifecycle management**, and **digital identity risk assessments**, are table stakes for federal Zero Trust implementations and prerequisites for U.S. Government FIDO deployments. The Enduring Security Framework Identity and Access Management Recommended Best Practices for Administrators[21] describes how phishing resistant MFA should be integrated with SSO and Identity Governance of the identity and access lifecycle.

The following are recommended pre-requisites that can be implemented concurrently with FIDO rollouts.

1. **Adopt Single Sign-on** – Implementing PIV and FIDO-based solutions concurrently requires capabilities to support complementary usage and management. Single Sign-On or Identity as a Service (IdaaS) facilitates consistent usage by managing different verifier roles while providing protected resources with consistent authentication context.
2. **Implement Digital Identity Risk Assessment Process** - Agencies must establish a Digital Identity Risk Assessment (DIRA) process to assist applications and mission owners in determining the authenticator assurance level that is needed to protect specific agency resources.
3. **Adopt Integrated Identity Lifecycle Management** - Continuous Diagnostics and Mitigation (CDM) brought identity governance and administration (IGA) capabilities to agencies. IGA solutions can help manage identity and access lifecycles. Integrated identity lifecycle management supports consistent management of credentials issued to users across the different authenticator types.

4.1 Adopt Single Sign-On (SSO)

Why SSO? Adopting federated authentication services reduces implementation complexity and allows integration of FIDO solutions alongside existing PIV and DPIV solutions. By leveraging federated services, the user registers their FIDO credential once to the enterprise service and can authenticate to any of the applications they require access to without additional setup.[22] Federation also simplifies credential lifecycle management by providing a single point of disenrollment for each FIDO credential.

Agencies may identify specific services that require phishing-resistant authentication in the absence of SSO. For example, cloud services, non-Government services/accounts, and denied, degraded, intermittent and limited bandwidth (DDIL) environments where personnel may be accessing systems. Agencies would apply both the SSO steps and the application steps to the application or service in those instances. ILM should be considered during analysis and planning DDIL authentication solutions.

As another example, an agency may depend upon a software-as-a-service (SaaS) business application that does not offer SSO integration but allows for registration of passkeys. In such cases, it may be useful to establish a mechanism for users to register such services and cue users to report their exclusive use of phishing-resistant authentication to support cybersecurity monitoring and awareness.

4.2 Implement Digital Identity Risk Assessment (DIRA) Process

Why DIRA? Some organizations have gravitated to “PIV- or CAC-only” access policies, which has driven a waiver culture rather than meeting risk-appropriate protection requirements with alternate, permissible technologies that support agency missions. Others have entrenched username-password capabilities that facilitate some mission scenarios but expose sensitive mission resources to exceptional risk. Either of these “extreme” cultures, if present, can drive up risk to agency missions. Agencies need a repeatable process to consistently determine per-resource protection requirements within a much more diverse and more capable authentication ecosystem.

The resource’s impact sensitivity and information assurance needs will dictate what authenticator assurance level (AAL) is needed. NIST SP 800-63-3 introduced the idea of risk assessments for digital identity proofing, authenticators, and federation.

The DIRA[23] process identifies the required IAL/AAL/FAL for a specific resource. The DIRA Process will determine that AAL3 is required if the assessor's answer to any of the following questions is "yes":

- *Did you assess at "high" for any of the impact categories?*
- *Did you assess "moderate" for personal safety?*

If the DIRA process did not determine AAL3 is required, it will determine AAL2 if the assessor's answer to any of these questions is "yes:"

- *Did you assess "moderate" for any of the remaining impact categories?*
- *Did you assess "low" for harm to agency programs or public interests, unauthorized release of sensitive information, personal safety, or civil or criminal violations?*
- *Are you making personal data accessible?*

The DIRA tool can help agencies address cultural extremes by more thoughtfully aligning protection requirements to potential mission risk.

The complete DIRA process will result in an IAL/AAL/FAL combination for a specific resource, using similar question flows from most restrictive to least restrictive impact sensitivity. The resulting identity assurance requirements, based on impact sensitivity factors, is different from an authorization policy.

Although DIRA provides agencies with a target authenticator assurance level for protection of each resource, M-22-09 limits selection to phishing-resistant options.

4.3 Adopt Integrated Identity Lifecycle Management

Why ILM? Identity Lifecycle Management is the mechanism for leveraging centralized enterprise identity by integrating the FICAM lifecycles of identity management, credential management, and access management with services.

> *"To the greatest extent possible, agencies should centrally implement support for non-PIV authenticators in their enterprise identity management systems, so that these authenticators are centrally managed and connected to enterprise identities." – OMB M-22-09*

The FICAM ILM Playbook[24] describes how agencies can implement ILM through establishment of a Master User Record (MUR) and lifecycle processes.

Agencies that have already invested in MFA solutions that are not phishing resistant may have already implemented more flexible user journeys to complement their PIV and NIST SP 800-157 PKI credential lifecycle management capabilities. In these cases, the agency has already adapted typical FIPS-201 Identity Management System (IDMS) technology, and the ID or badging office processes for PIV to support broader enrollment, issuance, activation, renewal, and revocation in order to support additional credential or person types in conformance with NIST SP 800-63-3.

Agencies should extend core identity lifecycle capabilities to support additional use cases, rather than establishing independent or loosely connected processes and technologies for additional person types or authenticators. To the extent possible, agencies should retain and enhance the level of automation and flow across lifecycle management and avoid introducing manual process connections across systems.

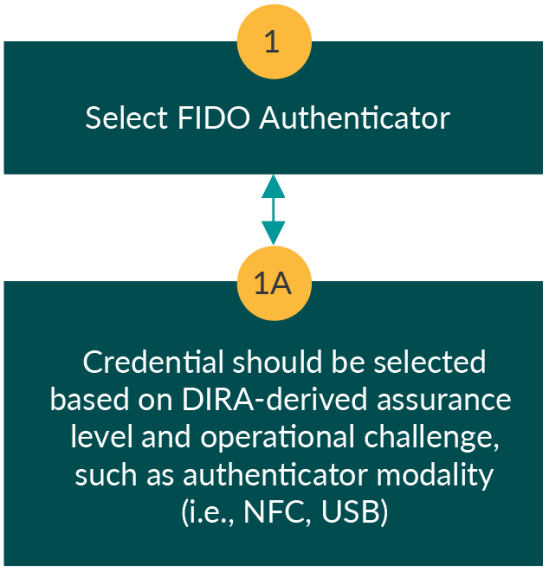
Leveraging automation tools and workflows enables agencies to implement credential lifecycle management for users who aren't eligible for PIV or who haven't yet received their PIV. It also enables automation of access lifecycle management across enterprise applications for the purpose of implementing least privilege and analytics.

5. FIDO-specific Architectural Considerations and Recommended Agency Actions

5.1 Agency Action #1: Select FIDO Authenticator(s)

Agencies are seeking one of the following capabilities to mitigate gaps in mission user authentication:

- Providing high-assurance authentication to users who either are not eligible for a PIV or need high-assurance access while completing PIV issuance requirements.
- Replacing phishable credentials, or even username-password, with authentication solutions that offer phishing resistance, but not PIV-equivalent high-assurance.



All FIDO Authenticators produce phishing-resistant credentials. Agencies must validate attestations from the authenticator to ensure they meet the AAL3 requirements. Alternatively, agencies may use non-attestable authenticators with other attestation sources (e.g., direct supervision, mobile device management) to ensure the authenticator meets the AAL3 requirements.

The FIDO White Paper *Choosing FIDO Authenticators for Enterprise Use Cases* helps identify available security and operational features that map Federal and Agency requirements that enable selection of suitable authenticators for Agency use cases.[25]

5.1.1 Selecting FIDO Authenticators below AAL3

Agencies selecting FIDO authenticators at lower assurance levels may have determined, via the DIRA process, that protection at AAL2 or AAL1 is appropriate for specific resources. Or there may be technical or operational challenges in implementing authentication solutions at AAL3 which is driving a risk decision to adopt a lower-assurance authenticator to support the mission.

Regardless, M-22-09 does not specify AAL in its direction to implement phishing resistant multifactor authentication. Agencies are strongly encouraged to implement FIDO authentication for non-AAL3 scenarios and maximize support for remote registration of additional FIDO credentials based on possession of higher-assurance credentials.

A FIDO discoverable credential, which is FIPS 140 Level 1 validated, protected with an activation secret, and provided from an attested authenticator, can be treated as an AAL2 phishing-resistant credential.

5.1.2 Selecting AAL3 FIDO Authenticators

Agencies implementing FIDO authentication capabilities alongside PIV and CAC can implement PKI-FIDO parity by leveraging security features that meet the requirements of NIST SP 800-63-3 and FIPS-201-3. These agencies are seeking authenticators that can be used in contexts where a smart card cannot, and which will focus on roaming or platform types; authenticator sourcing, ownership, and control; transport; and gesture types.

Required:

- Device-bound passkey-capable (DBK), such as security keys
- User verification (UV) or user presence (UP) gesture
- Enterprise Attestation (EA): either Vendor Facilitated (VC) or Platform Managed
- FIDO Certification L2 or higher
- If government-procured, the following additional requirements apply:
  - Trade Agreements Act (TAA) of 1979 Country of Origin[26], FAR and agency-specific regulations
  - FIPS-140 certified Level 2
  - FIPS-140 physical certified Level 3
  - Verifier FIPS-140 Level 1

Permitted:

- Government Furnished Equipment (GFE) Roaming and platform authenticators, such as security keys.
- USB, Near-Field Communication (NFC), or Bluetooth Low-Energy (BLE) CTAP transport, such as security keys.
- Discoverable FIDO credential capable.

What's the story with synced passkeys?

Agencies may want to consider leveraging synced passkeys, which can be used across platforms and browsers they may already own, to address AAL2 requirements. However, as guidance around synced passkeys is still emerging; we expect that agencies will initially want to focus on device-bound passkeys such as security keys for enterprise FIDO authentication deployments.

Synced passkeys may be suitable for some AAL2 use cases, depending on the security or regulatory requirements of the enterprise. Synced passkeys are attractive due to their recoverability and ease of use; however, they also change where credentials are stored (they can move) and who controls them. Any use of synced passkeys should look very closely at the security of the sync fabric, data at rest, and recovery options. Additional controls can be put in place through attended registration, trusted platform modules, and mobile device managers.

At the time of writing this document, NIST has indicated it intends to provide guidance for synced capabilities within upcoming issuances; we expect that until this emerges, agencies will focus on device-bound passkeys.

5.2 Distinguishability at Registration: Attestations

FIDO authenticator attestation offers agencies flexibility in lifecycle management by providing security and functional characteristics and inventory data remotely through attestation. This distinguishability reduces the need for other controls, such as in-person supervision of authenticator issuance and registration, or device management, to determine assurance characteristics of the authenticator and bindings of the credentials.

In most federal enterprise scenarios, the agency will provide the authenticator. There are few scenarios where an agency will allow an individual to use their own authenticator for access to federal resources. However, if that is the case, there are steps agencies can take to increase the security of that authenticator.

Some FIDO authenticators include an authenticator attestation statement during credential registration. This data can be used to lookup authenticator security characteristics (e.g., from FIDO Metadata Service, MDS). However, users may block attestations in unmanaged browsers. In the absence of attestable authenticator data, the authenticator security characteristics are unknown, but may be obtained through alternative means such as supervised registration and mobile device management (MDM). If authenticator attestation is unavailable during registration or if the attestation is insufficient to the needs of the verifier, registration of that credential may be denied. Implementers should consider how to make registration denial understandable from a user experience perspective.

As Federal Agencies deploy FIDO authentication in their environments to implement M-22-09 requirements, this also introduces important context for the selection of authenticators, the use of attestation as a part of registration, and the passing of authentication context within ICAM services. It is also critical that the IAM system store the necessary information about the FIDO credential so in the future its use can be logged, as with PIV, and eventually revoked/offboarded.

For systems that do not require distinguishability between AAL2 and AAL3 solutions, any FIPS 140 Level 1 validated passkey solution protected with an activation secret can be treated as an AAL2 phishing-resistant credential without further attestation. While the “any passkey” approach may seem to offer simplicity in single-system and SSO deployments it is not recommended.

5.3 Agency Action #2: Plan FIDO Authenticators Lifecycle

There are points agencies need to consider before issuing FIDO authenticators. Agencies may have already created a Master User Record (MUR) to impose management of the lifecycle of identities, credentials, accounts, and access through integrations across platforms, SSO, and credential management capabilities.

Planning effective identity lifecycle people, processes, and technologies is critical to consistent outcomes and auditability across the integrated ICAM capabilities the agency needs to accomplish its mission.

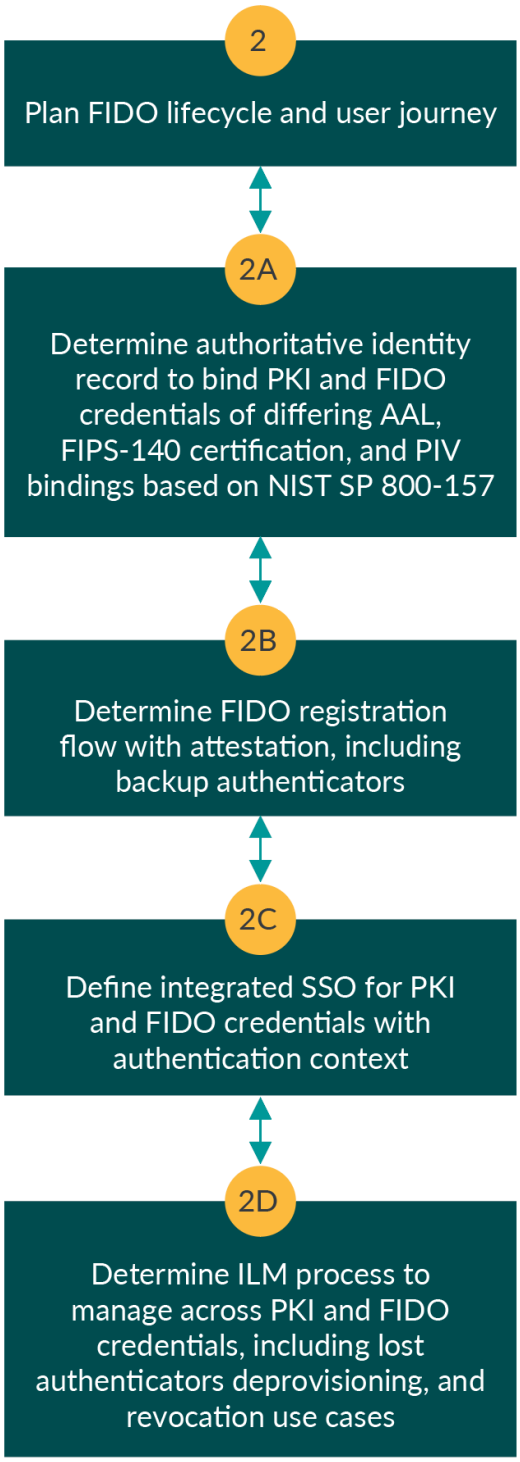
Upon registration of an authenticator, attestation data will need to be collected – it's the only time this step can be performed.[27] If an agency is using unmanaged browsers, that attestation may be blocked therefore blocking registration of the authenticator.

It is also important to consider a way for this authenticator attestation "metadata" to be stored and made available to verifiers after the registration is completed. For example, if a future weakness or vulnerability is discovered for a given authenticator type, this metadata registry will be critical to revoking the at-risk authenticators. FIDO does offer an official FIDO Metadata Service.[28] A depiction of all available MDS data for the universe of authenticators registered with the FIDO Alliance is also available.[29]

Agencies may determine that other relevant data not available from FIDO Alliance or vendor MDS must be maintained as an extension for lookup at the registering service or via an extended metadata service to be centrally operated. Some Agencies, or a USG shared service provider, may determine the need to establish a hosted metadata service for U.S. Government purposes. Providing validated vendor claims of FIPS-140 certification or a reviewed/confirmed country of origin may be examples of data that may require authoritative government data.

One relevant distinction between the lifecycle management of PKI credentials and FIDO credentials is the impact of specific FIDO authenticator attributes established during registration. While PKI credentials are revoked by a centralized PK infrastructure, FIDO credentials must be de-registered from the individual relying party. This means the authenticator must be identifiable (such as with a user-assigned ID or "nickname") to facilitate proper identification for later de-registration in case the device must be deactivated due to loss or other reasons.

It is a best practice to allow users to assign a nickname to the credential.[30] FIDO supports the concept of Enterprise Attestation. This enables the relying party to track the inventory of security keys from the moment of handing them over to the user: first, registering FIDO credentials, then de-registering. EA can provide the serial number of the security key, but that data element is up to the agency to decide. The EA also includes the agency domain to indicate that this is a key that was minted for that agency. The EA cert can only be added at manufacturing and not afterward. EA is a future capability that is just being rolled out across the security keys, browsers, and IDPs so agencies should plan for this capability as it's not widely available yet. Lastly, there are not yet any FIPS validated security keys that support EA. Some platforms are also scheduled to support EA via platform authenticators by the end of 2023.



5.3.1 Distinguishability at the Verifier: Authentication Context

The claims required to express authentication context that meets FIPS-201-3 and NIST 800-63-3 requirements (IAL/AAL/FAL) do not need to include all of the data attested during registration to enable policy administration and enforcement in a way that preserves relevant privacy equities. However, end verifiers will require more than the IAL, AAL, and FAL from the provider to implement M-22-09 and FIPS-201-3. Context is a challenge without specific standards.

In practice, federal verifiers have under-implemented existing distinguishability among authenticators. Federal Information Systems have enjoyed distinguishability among PKI credentials for some time, and Federal PKI policy and management have carefully delivered distinguishability to support nuanced requirements. FPKI PKI certificate profiles require the use of Object Identifiers (OIDs) to allow relying parties to distinguish higher-assurance hardware-protected PKI certificates from those with lower assurance security characteristics. However, many systems do not check OIDs or Extended Key Usage (EKU) attributes and may not sufficiently validate PKI credentials using Online Certificate Status Protocol (OSCP) or a certificate revocation list (CRL). As the verifier role is implemented more centrally for FIDO authentication, the verifier can take on much of the complexity of distinguishability, making it more accessible to a broader set of resources at lower aggregate cost.

As the Federal Government prioritizes the urgent elimination of MFA solutions that are vulnerable to phishing, AAL2, as a policy claim consistent with NIST SP 800-63-3, does not always convey phishing resistance. The importance of phishing resistance in M-22-09 and FISMA reporting requires phishing resistance be an expectation of RP authentication requests to a provider, and confirmation received in the federated authentication token (or assertion).

The RP may also be expected to distinguish between authentication using credentials that deliver Personal Identity Verification consistent with HSPD-12 and FIPS-201-3, which is not included in xAL claims. In this way, “PIVness” is another characteristic that must be separately supported in RP requests to and responses from agency SSO or IdaaS solutions.

5.3.2 Authentication Context claim values

The Internet Assigned Numbers Authority (IANA) Registry specifies Authentication Method Reference values[31] and provides available expressiveness for authenticator assurance level using SAML and OIDC. The federal identity ecosystem with PKI, FIDO, non-phishing resistant MFA, and username-password as potential options for any given user session, needs to be communicated consistently among service providers and relying parties to enable strategic policy enforcement and management. However, these claim values are inconsistently implemented across vendor products, vendor IdaaS services, and government service instances. Below are sample authentication method reference claim strings that agency service providers might adopt to convey authentication context:

Typical non-phishing resistant MFA: “amr” : [“pwd” , “otp” , “mfa”]

Password, only “amr” : [“pwd”]

PIV/CAC “amr” : [“sc” , “hwk” , “pop” , “mfa” , “user” , “pin”]

PKI-based DPIV “amr” : [“swk” , “pop” , “mfa” , “user”]

FIDO synced passkey “amr” : [“swk” , “pop” , “mfa” , “user”]

FIDO device-bound passkey “amr” : [“hwk” , “pop” , “mfa” , “user”]

Using these standardized claims, it may seem ambiguous whether PKI or FIDO was used in a particular authentication event. However, the priority in M-22-09 clearly distinguishes phishing-resistant methods from non-phishing resistant methods.

Policy context is better conveyed using authentication context class reference values, which may be used to convey xAL, phishing resistance, and PIVness in requests and responses.

5.3.3 Step-up Authentication

In order to support a positive user experience while enabling a single provider to support multiple credential assurance levels, it’s necessary to support step-up authentication.

During a session if a user attempts to conduct a transaction for which the assurance requirement is higher than the authenticator assurance level of the authenticated session, the user should be redirected to the SSO provider to authenticate using a sufficiently assured method.[32]

5.3.4 Selecting SSO Solutions

Agencies should consider their credential ecosystem when selecting a product or service to support PKI and FIDO, and the need for support across the lifecycle of the credential, including configurability for registration, attestation, and authentication context.

Traditionally, U.S. Government Agencies have tied a single PKI credential to a single human identity. This approach makes it difficult to separate a single human identity, their potential multiple accounts, and potential multiple credentials attached to one or more of those accounts.

While the ability to tie multiple credentials to an account and to tie multiple accounts to an identity, Draft NIST 800-157 Rev. 1 derived PIV guidance requires the FIDO server (derived PIV credential issuer) to enforce PKI-AUTH authentication before binding the new credential to an identity account. SP 800-157 is undergoing an update and this guidance could change in future iterations. Additionally, if the derived credential is to be used at AAL3, the application must also identify themselves with a biometric sample. This is something that is rare amongst existing issuers or must be integrated into existing tools. Additionally, the FIDO server must also support the full lifecycle of the PIV card credential allowing for revocation of any managed derived credential based on defined events such as PIV card revocation, suspected credential compromise or PIV card replacement.

In addition to credential support, FIDO servers and SSO solutions should also support interoperability and security profiles that continuously improve mitigations to evolving threats. Agencies should adopt interoperability and security profiles that are actively maintained, such as the Financial Grade API profiles for OIDC and OAuth 2.0[33], the iGov profiles[34], or the MITRE Enterprise Tailored profiles for OIDC and OAuth 2.1[35].

As the U.S. Government implements FIDO authentication to mitigate credential compromise threats, adversaries can be expected to develop approaches to exploit weaknesses in other segments of the trust chain. Implementing phishing resistance is a major step toward mitigating evolving threats.

5.3.5 Supply Chain Concerns and Secure Procurement

Agencies may determine that other relevant data not available from FIDO Alliance or vendor MDS must be maintained as an extension for lookup at the registering service or via an extended metadata service to be centrally operated. Some Agencies, or a USG shared service provider, may determine the need to establish a hosted metadata service for US Government purposes.

Providing validated vendor claims of FIPS-140 certification or a reviewed/confirmed country of origin may be examples of data that may require authoritative government data. Currently, this data is maintained as part of the NIST Cryptographic Metadata Validation Program (CMVP) and not included in the FIDO Metadata Service. Over time, vulnerabilities may be found forcing the revocation and recertification of approved modules. There is additional confusion, because the FIPS validated hardware Authenticator Attestation Globally Unique Identifier (AAGUID) is not included within the NIST CMVP certificate. This may leave issuers to guess at the appropriate hardware AAGUID from each vendor or trust data posted on vendor websites or in emails from vendor representatives. It would be helpful to get additional guidance and clarification from NIST on how to best approach this.

In terms of secure procurement, documents 800-63-3 mentions that FIPS-140 validation is required for government procured authenticators. This validation ensures that cryptographic modules meet well-defined security standards and can provide a level of assurance for the U.S. Government.

Additionally, just because the chip in the authenticator for the hardware module is trusted, not all chips (i.e., in band wireless ones) are certified the same way and some may be vulnerable to side channel attacks at registration time.

5.4 Agency Action #3: Deploy

Once the target User Journey with ILM is defined, agencies must select one or more methods to onboard agency verifiers to the FIDO-enabled SSO service. Agencies must then deploy existing identities with their credentials, or phishing-resistant replacement credentials with sufficient enterprise identity bindings into the new lifecycle.

Agencies will have verifiers that have been issuing their own credentials to subscribers that do not yet have PIVs or are PIV ineligible. These need to be onboarded to the SSO and ILM, which will require syncing locally managed subscriber accounts and any locally issued credentials with their enterprise identities. Any users with PIV can be migrated using a self-service mechanism, but existing users without sufficient IAL/AAL will need to restart the journey.

Once the SSO and ILM services are in place, new users can be onboarded using the new user journey for new users.

6.0 User Journey

The user journey toward obtaining a FIDO credential is similar to the PIV journey with a few differences, as displayed in the graphic below.

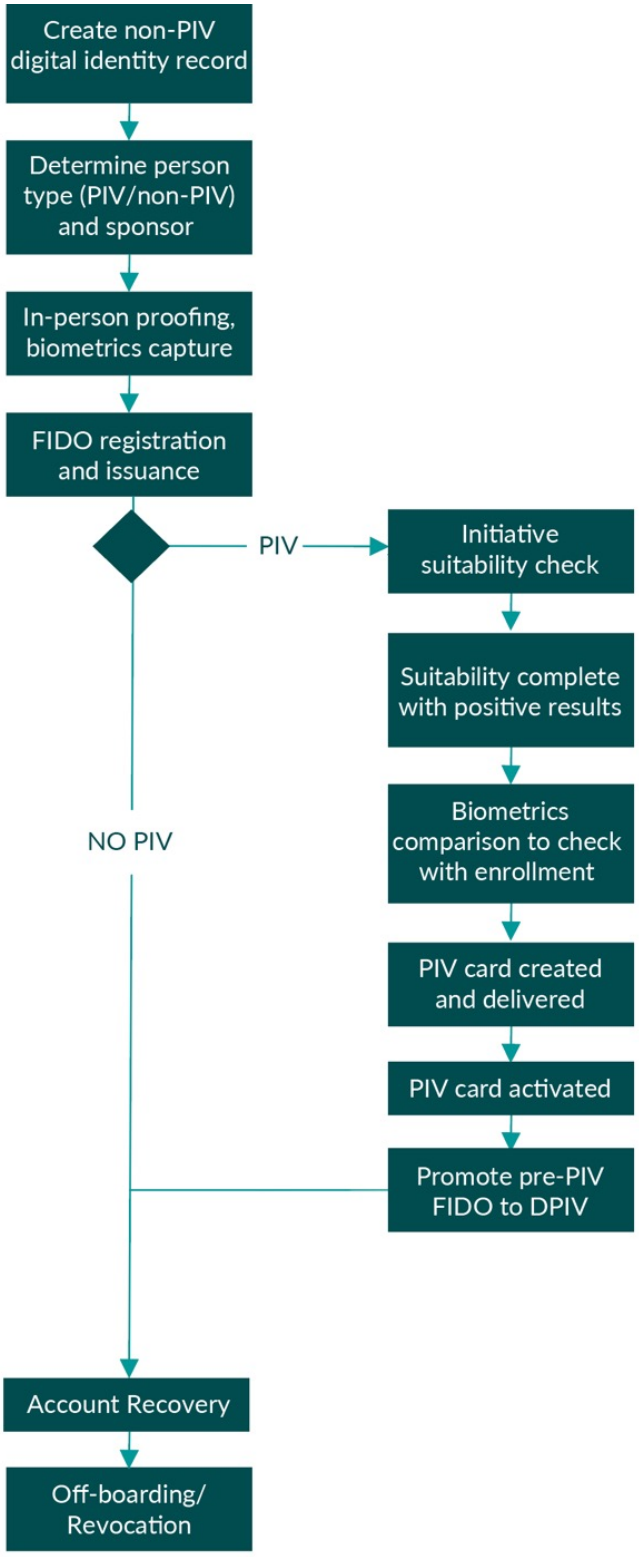


Figure 1: FIDO User Journey

Task	Description
Create non-PIV record	Create non-PIV digital identity record and identifier(s) agnostic of person-type in directory used for authentication.
Determine PIV/non-PIV	Determine person type or types based on legal status and organizational sponsorship(s).
In-person proofing, biometrics, FIDO registration and issuance	In-person proofing, biometric capture and registration [pre-PIV/no-PIV] • Attestations, UX, considerations
Account recovery	What happens when a credential is lost/stolen/expired.
Off-boarding/Revocation	Removing the token from the IAM when an individual leaves an agency.

Table 1: FIDO User Journey Sequence

7.0 FIDO Considerations and Lessons Learned

The PIV and CAC have been around for almost 20 years and have a very mature set of standards and guidance. FIDO authentication uses a different model that separates authentication and account management. Additionally, FIDO's approach focuses on a self-service privacy preserving model that is different from a centrally managed PKI-based credential.

However, since many details around FIDO implementations for federal agencies are new, there are specific considerations that agencies need to keep in mind. These include everything from making sure USB ports can be used to read the FIDO credentials, locking a device if the FIDO security key is removed, and others.

Because of the differences between the two technologies, we identified the following considerations that government FIDO credential issuers and relying parties will want to consider.

7.1 USB Resistance and Enablement

Federal agencies have shown a reluctance to enable employees to use USB drives on their government equipment due to concerns around malware on USB drives and data exfiltration. But there is a way to enable USB-based FIDO security keys for authentication without opening the ports up to other drives. The system settings can be limited via Product ID (PID) setting to enable selected authenticators to be used while still locking out other USB technologies.[36]

7.2 Device Lock

When A PIV or CAC is removed from a computer the device is locked. That same functionality isn't inherent to FIDO standards and will need to be managed separately. This is managed at the operating system level, but automation of this additional support would be necessary. Third-party scripts can also be written to achieve this functionality. Additionally, this can be achieved by adjusting the inactivity timeout appropriately and using the PIV for desktop login and the FIDO token for other applications.

7.3 Near Field Communication (NFC)

NFC is a wireless protocol used by mobile devices to authenticate and transfer small amounts of information to other systems. Many agencies do not enable this functionality on devices so to use NFC, other steps or credentials will need to be used or exceptions will have to be made to policy.

7.4 Forgotten PIN

One use case explores using the FIDO authenticator to reset a PIN on the PIV/CAC or on another FIDO credential. There is no centralized way to reset a PIN for a FIDO authenticator. One approach that FIDO Alliance has advocated for in the past is issuing multiple security keys so that the PIN could be reset via another previously registered key. It could also be possible to use the PIV or CAC to reset a PIN.

8.0 Conclusion

This document details how U.S. Government agencies can implement an inclusive user identity capability that supports both FIDO- and PKI-based phishing-resistant MFA to integrate the lifecycle of identity management across all person types with the lifecycle of access management across the agency's digital resources, regardless of the authorization methods being used.

The document also provides technical considerations for deploying FIDO authentication to meet current and future Zero Trust strategic objectives.

By taking these defined agency actions to implement the target lifecycle, FIDO-based solutions can provide phishing-resistant authentication for users who are not PIV eligible, those individuals who work remotely and don't need access to federal facilities, or users who are new employees or contractors waiting for their PIV to be issued. Innovative FIDO authenticators also provide strong authentication where agencies are using username-password or phishable MFA because traditional PKI technologies don't work.

PIV and CAC offer tremendous capability for physical and logical access that will endure, but FIDO authentication and the supporting enterprise identity and access lifecycle capabilities that can support FIDO standards are urgently needed to elevate certificate-based authentication as a foundation of Zero Trust.

Appendix A: Use Cases

Use Cases

The focus on this document is filling the gaps in FIDO lifecycle management that are not documented today. Below are the specific use cases including sequence diagrams and steps to complete the use case.

1. Pre-PIV: Issuance of a FIDO credential

A popular use case for FIDO in the federal space has been issuing credentials during onboarding so a new employee/contractors can access necessary resources while waiting for their PIV/CAC. Below we document the steps that need to be taken to initially issue the FIDO credential. The agency must work with authenticator vendors to include the enterprise attestation on the FIDO credential.

Table 2: Sequence for remote Interim PIV FIDO credential issuance

#	Description
1	Individual undergoes remote identity proofing.
2	If individual passes proofing, the source of truth within the agency registers them into the Identity Governance & Administration (IGA).
3	Individual is sent an email with a link to apply for FIDO credential.
4	Individual navigates to the registration page and enters requested information.
5	IAM checks with Identity Governance & Administration (IGA) to validate information presented.
6	Account is created with limited access based on the Pre-PIV status. User is monitored to make sure access is not elevated.
7	FIDO credential is generated. Device attributes information will be captured. Device attestation can be used to identify authenticator attributes include FIPS certification, FIDO certification and CTAP versions. Enterprise attestation can be used to identify the unique authenticator that can also hold a PIV credential. Ensuring the same device is holding the FIDO and PIV credentials provides a higher level of assurance that the FIDO credential is bound to the PIV credential.
8	FIDO credential information stored in identity directory.
9	IGA and/or IAM will identify accounts as having a FIDO pre-PIV credential. This attribute can be used for authorization policies and used for binding operations when a PIV credential is issued.
10	FIDO credential is mailed to address on record.
11	Once PIV is issued agency binds FIDO credential to the PIV record.

Table 3: Sequence for in-person Pre-PIV FIDO credential issuance

#	Description
1	Individual undergoes in-person identity proofing.
2	If individual passes proofing, agency registers them into the Identity Governance & Administration (IGA).
3	Account is created with limited access based on the Pre-PIV status.
4	FIDO credential is generated. Device attributes will be captured. Device attestation can be used to identify authenticator attributes include FIPS certification, FIDO certification and CTAP versions. Enterprise attestation can be used to identify the unique authenticator that can also hold a PIV credential. Ensuring the same device is holding the FIDO and PIV credentials provides a higher level of assurance that the FIDO credential is bound to the PIV credential.
5	FIDO credential information stored in identity directory.
6	IGA and/or IAM will identify accounts as having a FIDO pre-PIV credential. This attribute can be used for authorization policies and used for binding operations when a PIV credential is issued.
7	FIDO credential is given to the individual.
8	Once PIV is issued agency binds FIDO credential to the PIV record.

Use Case Considerations:

- Might require special claims that flow with this level of verification.
- Might not need claims but action on the absence of PIV attributes.
- Given this use case does not bind to a PIV credential, at a minimum the scenario should encourage device attestation and plan for future use of enterprise attestation to capture the most signals of the FIDO authenticator.
- Use case should reference Binding existing FIDO token to new PIV use case as this specific use case has the assumption that a PIV card will be issued in the future.

2. Bind new FIDO credential to existing PIV credential

There are many scenarios where a backup credential might be necessary to enable access. A FIDO credential can readily fill that role and below are the proposed steps to bind a new FIDO credential to an existing PIV/CAC.

Table 4: Sequence for binding new FIDO credential to existing PIV

#	Description
1	Individual navigates to registration page on IDP/IAM.
2	User enters necessary information and is authenticated via PIV/CAC.
3	IGA Checks with CMS and directory for validity.
4	IAM checks with Identity Governance & Administration (IGA) to see if individual is authorized to have PIV/CAC.
5	IGA and directory send approval of deny for credential request.
6	Approve/Deny.
7	Not approved, error out and go back to registration page.
8	Approved IGA authorized creation of the FIDO credential.
9	User is allowed to register a FIDO credential on the registration page.
10	FIDO public key and attestation certificate are stored in directory and bound to PIV/CAC.
11	The associated PIV/CAC CRL is linked to the specific FIDO public key so that future authentication with the FIDO credential can check against a valid PIV/CAC credential.

3. Lost FIDO credential

The below detail the steps that need to be taken to unbind a FIDO credential from a PIV in case it is lost or damaged and issue another FIDO credential.

Table 5: Sequence for lost FIDO credential

#	Description
1	FIDO credential is reported lost, stolen, damaged.
2	IT security runs script to remove the public key from the user's account.
3	User navigates to registration page on IAM with an established PIV/CAC.
4	IGA removes the FIDO public key from the user account.
5	The user can register a new FIDO credential at this time by following the process previously defined. The FIDO credential is generated, and updated information is stored in the directory and bound to the PIV/CAC.

4. Binding existing FIDO token to new PIV

The below steps detail the steps to binding an existing FIDO credential to a new PIV.

Table 6: Sequence for binding existing FIDO credential to new PIV

#	Description
1	User navigates to registration page on IDP/IAM with new PIV/CAC.
2	PIV/CAC attributes are associated with existing account, including FIDO credential.
3	PIV/CAC validity and FIDO token are both verified in the IGA and directory.
4	IGA binds the PIV/CAC to the FIDO credential in the directory.
5	Binding is complete.

5. Recovery scenarios for FIDO and PIV

The below detail various recovery scenarios for FIDO and PIV, including forgotten PIN.

Table 7: Non-PIV Eligible Issuance and Use

This use case will describe how to issue and use a FIDO credential in a non-PIV eligible use case.

#	Description
1	Individual undergoes necessary background check for non-PIV eligible role and is approved.
2	Agency registers them into the Identity Governance & Administration (IGA).
3	Individual is sent an email with a link to apply for FIDO credential.
4	Individual navigates to the registration page and enters requested information.
5	IAM checks with Identity Governance & Administration (IGA) to validate information presented.
6	Account is created with limited access based on the Pre-PIV status.
7	FIDO credential is generated. Device attributes will be captured. Device attestation can be used to identify authenticator attributes include FIPS certification, FIDO certification and CTAP versions. Enterprise attestation can be used to identify the unique authenticator that can also hold a PIV credential. Ensuring the same device is holding the FIDO and PIV credentials provides a higher level of assurance that the FIDO credential is bound to the PIV credential.
8	FIDO credential information stored in identity directory.
9	IGA and/or IAM will identify accounts as having a FIDO non-PIV credential.
10	FIDO credential is mailed to address on record.

Acknowledgements

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

- Tim Baldridge, Department of Defense
- Tim Cappalli, Microsoft
- Tom Clancy, Mitre
- Arynn Crow, Amazon
- Ross Foard, Cybersecurity Infrastructure & Security Agency
- Ryan Galluzzo, National Institute of Standards and Technology
- Kevin Goldman, Trusona
- Chris Grant, U.S. Army
- Jeremy Grant, Venable LLP
- Ehud Itshaki, Microsoft
- John Jacob, Idemia
- Babur Kohy, General Service Administration
- Karen Larson, Axiad
- Rolf Lindemann, Nok Labs
- Zack Martin, Venable LLP
- Michael Magrath, Easy Dynamics
- Sean Miller, RSA
- Ken Myers, General Service Administration
- Lisa Palma, LC&J Security Solutions
- Andrew Regenscheid, National Institute of Standards and Technology
- Bryan Rosensteel, Ping Identity
- Dean H. Saxe, Amazon
- Joe Scalone, Yubico
- Matt Topper, UberEther Inc.
- David Treece, Yubico
- Steve Venema, ForgeRock
- Andrew Webb, Idemia
- Teresa Wu, Idemia

1. https://www.whitehouse.gov/wp-content/uploads/2022/01/M-22-09.pdf
2. https://www.whitehouse.gov/briefing-room/presidential-actions/2021/05/12/executive-order-on-improving-the-nations-cybersecurity/
3. https://fidoalliance.org/overview/
4. https://fidoalliance.org/passkeys/
5. https://www.whitehouse.gov/wp-content/uploads/2019/05/M-19-17.pdf
6. https://playbooks.idmanagement.gov/playbooks/dira/
7. https://pages.nist.gov/800-63-3/sp800-63-3.html
8. https://pages.nist.gov/800-63-3/sp800-63-3.html#sec5
9. https://pages.nist.gov/800-63-3/sp800-63b.html
10. https://doi.org/10.6028/NIST.FIPS.201-3
11. https://playbooks.idmanagement.gov/playbooks/sso/
12. https://playbooks.idmanagement.gov/playbooks/cloud/
13. https://playbooks.idmanagement.gov/playbooks/ilm/
14. https://www.cisa.gov/sites/default/files/2023-03/csso-scuba-guidance_document-hybrid_identity_solutions_architecture-2023.03.22-final.pdf
15. https://www.cisa.gov/resources-tools/services/secure-cloud-business-applications-scuba-project
16. https://playbooks.idmanagement.gov/playbooks/sso/
17. https://playbooks.idmanagement.gov/playbooks/cloud/
18. https://playbooks.idmanagement.gov/playbooks/ilm/
19. https://pages.nist.gov/800-63-4/sp800-63b.html#verifimpers
20. https://www.cisa.gov/news-events/alerts/2022/10/31/cisa-releases-guidance-phishing-resistant-and-numbers-matching
21. https://media.defense.gov/2023/Mar/21/2003183448/-1/-1/0/ESF%20IDENTITY%20AND%20ACCESS%20MANAGEMENT%20RECOMMENDED%20BEST%20PRACTICES%20FOR%20ADMINISTRATORS%20PP-23-0248_508C.PDF
22. https://playbooks.idmanagement.gov/playbooks/sso/
23. https://playbooks.idmanagement.gov/playbooks/dira/
24. https://playbooks.idmanagement.gov/playbooks/ilm/
25. https://media.fidoalliance.org/wp-content/uploads/2022/03/FIDO-White-Paper-Choosing-FIDO-Authenticators-for-Enterprise-Use-Cases-RD10-2022.03.01.pdf