FIDO Alliance Guidance for U.S. Government Agency Deployment of FIDO Authentication (Version 1.1, March 2025)[1]

March 2025

[1] Version 1.1 implements updated references and policy changes, and addresses select errata from Version 1.0.

1 Executive Summary

The FIDO Alliance Board of Directors established the US Government Deployment Working Group (USGDWG) to improve and accelerate adoption of FIDO technology within federal agencies.

The FIDO Alliance applauds the U.S. government for prioritizing phishing-resistant authentication of enterprise identities within the cybersecurity modernization process. The government is taking a critical step in countering widely available Phishing as a Service platforms by limiting the types of multi-factor authentication (MFA) that the government workforce Identity Credential and Access Management (ICAM) uses to only allow phishing resistant methods. The most fundamental requirement of the Federal Zero Trust Strategy is denying bad actors the means to systematically exploit U.S. government information systems by compromising authentication credentials. This offers immediate and complete mitigation of a rampant attack and provides fundamental capabilities that enable the remainder of the strategy.

> **"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, *Moving the U.S. Government Toward Zero Trust Cybersecurity Principles)*

To counter threats and improve mission outcomes, the USGDWG collects normative and permissive guidance from the Office of Management and Budget (OMB), the National Institute of Standards and Technology (NIST), and the Cybersecurity and Infrastructure Security Agency (CISA) to support agency-led modernization of identity. *Having reviewed this guidance, the USGDWG has determined that federal agencies **must** begin their Zero Trust Architecture (ZTA) journey by implementing user identity solutions that support both FIDO and PKI-based phishing-resistant authentication methods.*

To integrate enterprise identity management for all person types with access management for all the agency's digital resources, agencies need Identity Management Systems (IdMS) that support both Public Key Infrastructure (PKI) and FIDO authentication methods. To quickly enable access for new employees who are waiting for their PIV to be issued, and for those users who are not eligible for the credential, agencies need alternative phishing-resistant authentication capabilities for the federal workforce.

This paper outlines how U.S. government departments and agencies can more readily adopt FIDO authentication capabilities to meet immediate priorities as defined in OMB Memorandum M-22-09, Moving the U.S. Government Toward Zero Trust Cybersecurity Principles2, and help advance the cybersecurity outcomes outlined in the federal Zero Trust Maturity Model published by CISA.[3]

The presidential Executive Order on Improving the Nation's Cybersecurity (EO 14028) mandated agency use of MFA for all data at rest and in transit. OMB M-22-09 made clear that agencies should only use multifactor authentication (MFA) that is resistant to phishing attacks[4]. FIDO2 standards (FIDO) include both the Web Authentication (WebAuthn) protocol and the Client to Authenticator Protocol (CTAP). FIDO2-compliant capabilities are resistant to credential phishing attacks and complement existing Federal Public Key Infrastructure (FPKI), PIV, and Common Access Card (CAC) capabilities. FIDO2-compliant authentication can replace username and password, or other authentication methods, that are vulnerable to credential phishing.

The presidential Executive Order on Strengthening and Promoting Innovation in the Nation's Cybersecurity (EO 14144)[5] further urged agency FIDO deployments of commercial phishing resistant standards and clarified the enduring role of those standards in Federal ICAM.

> *"To prioritize investments in the innovative identity technologies and processes of the future and phishing-resistant authentication options, FCEB agencies shall begin using, in pilot deployments or in larger deployments as appropriate, commercial phishing-resistant standards such as WebAuthn, building on the deployments that OMB and CISA have developed and established since the issuance of Executive Order 14028. These pilot deployments shall be used to inform future directions for Federal identity, credentialing, and access management strategies."*

CISA and the U.S. Department of Agriculture jointly published **Phishing-Resistant Multi-Factor Authentication (MFA) Success Story: USDA's Fast IDentity Online (FIDO) Implementation**[6]**,** a case study that illustrates the need for agencies to support

2 https://zerotrust.cyber.gov/downloads/M-22-09%20Federal%20Zero%20Trust%20Strategy.pdf
3 https://www.cisa.gov/zero-trust-maturity-model
4 https://www.federalregister.gov/documents/2021/05/17/2021-10460/improving-the-nations-cybersecurity
5 https://www.federalregister.gov/documents/2025/01/17/2025-01470/strengthening-and-promoting-innovation-in-the-nations-cybersecurity
6 https://www.cisa.gov/resources-tools/resources/phishing-resistant-multi-factor-authentication-mfa-success-story-usdas-fast-identity-online-fido

authentication for users that are not eligible for or cannot use PIV solutions and how FIDO solutions can be deployed to complement PIV architectures.

This publication identifies lines of effort (LOEs) that departments and agencies are undertaking to implement normative guidance and provides key technical recommendations that must be considered in order to integrate FIDO authentication and enable immediate and long-term outcomes.

Although broader U.S. government adoption of FIDO authentication is consistent with priorities in the Zero Trust Strategy, deployment of FIDO authentication is proceeding slowly. This is due in large part, to agencies not yet having a firm understanding of how to integrate FIDO authenticators into a Personal Identity Verification (PIV) centered ecosystem.

This document highlights areas where FIDO offers the best value to address U.S. government use cases. To advance zero trust strategies with phishing-resistant authentication tied to enterprise identity as the foundation, this document recommends enhancing existing infrastructure and minimizing rework. FIDO has developed use cases for the commercial market but recognizes that leveraging FIDO authentication in enterprise government use cases presents different challenges due to differences in the lifecycle and service models.

FIDO implementations should account for 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 due to technology or mission reasons.
- Support the need for applications 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 of access management once FIDO capabilities are in place.

2 Scope Statement

This document provides information regarding FIDO Alliance technology standards and why they are cited in OMB documentation. It also provides guidance on implementation of FIDO credentials within the federal digital identity ecosystem, as well as other deployment considerations and recommendations.

This document does not discuss citizen-facing digital identity or general PIV or Common Access Card (CAC) replacement.

2.1 Audience

The audience for this document includes chief technology officers, chief information officers, chief information security officers, human resource officials, cybersecurity officials, digital services officials, privacy officials, and senior federal identity officials and architects with procurement authority who want to add another phishing-resistant authenticator to complement PIV or CAC.

3 Background

This section explains FIDO and passkeys, then discusses guidance and policy of the Federal Government and the need for phishing resistance.

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.[7] The FIDO2 specification consists of the World Wide Web Consortium (W3C) Web Authentication (WebAuthn) specification and the FIDO Alliance's Client-to-Authenticator Protocol (CTAP).

3.2 What are Passkeys?

A "passkey" is a FIDO authentication credential based on FIDO standards, that allows a user to sign in to apps and websites with the same steps that they use to unlock their device (biometrics, PIN, or pattern). With passkeys, users no longer need to enter usernames and passwords or additional factors.

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

- **Synced passkeys**: passkeys that are stored securely in a credential manager and accessed across devices (mobile phones, tablets, and computers).
- **Device-bound passkeys**: passkeys that are bound to and used only on a single device, such as a security key or a laptop with a secure element or trusted platform module (TPM). Device-bound passkeys can be created on FIDO Certified authenticators and security keys, including some that have been certified to meet specific security and functional requirements.[8]

This paper focuses on device-bound passkeys. Agencies can refer to recent guidance from NIST for more information around the use of synced passkeys.

[7] https://fidoalliance.org/overview/
[8] https://www.passkeycentral.org/introduction-to-passkeys/passkey-types

Note: While device-bound passkeys may satisfy both AAL3 and AAL2 requirements within **NIST SP 800-63B**, synced passkeys are limited to AAL2 use only.

Because passkey terminology is new, and the federal government references FIDO authentication or WebAuthn in various documents rather than the term “passkey”, this paper will refer to the credentials as “FIDO authenticators” or “FIDO credentials.” However, note that in practice, the term “passkey” can also be used interchangeably. The first FIDO protocol, FIDO Universal Authentication Framework (UAF), also provides users with a passwordless experience and FIDO UAF credentials are also called passkeys. “Passwordless” is a collective name given to the authentication methods and user experiences that allow users to verify their identity without using a traditional password.

Refer to Passkey Central[9] to learn more about passkey types.

3.3 Federal Government Policy and Guidance

For more than a decade, U.S. Federal cybersecurity and identity guidance has been driving agencies toward a more risk-aware approach by targeting architectural weaknesses that require urgent action based on malicious activity and demonstrated capability.

During the federal government’s response to the breach at the Office of Personnel Management caused by a compromised password in 2015, the OMB urged all agencies to begin using MFA. Around that same time, “hacking as a service” tools emerged that enabled scaled credential theft through phishing by bad actors. These malicious tools could also phish some legacy MFA tools such as One-Time Passwords (OTPs). Security professionals across the globe began to focus on replacing these phishable authenticators with phishing-resistant authentication.

In 2019, **OMB Memorandum M-19-17 Enabling Mission Delivery through Improved Identity, Credential, and Access Management**[10] directed agencies to implement NIST SP 800-63-3. This publication called for adapting the government’s approach to HSPD-12 and PIV and shifted focus from managing the lifecycle of credentials to managing the lifecycle of identities. This directive encouraged piloting additional authenticators, implementing processes to enhance management of access control, improving timeliness in revocation of access privileges and credentials, and incorporating Digital Identity Risk Management (DIRM) into agency processes. The General Services Administration (GSA) led development of a Digital Identity Risk Assessment (DIRA)

[9] https://www.passkeycentral.org/home
[10] https://bidenwhitehouse.archives.gov/wp-content/uploads/2019/05/M-19-17.pdf

playbook to assist agencies with DIRM by providing a repeatable process to determine assurance requirements for different resources and contexts.[11]

Additionally, OMB M-19-17 called for agencies to use cross-agency identity federation to promote interoperability:

- 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 specified initial requirements for digital identity to advance Zero Trust, including implementation of enterprise Identity and Access Management, exclusive use of phishing-resistant MFA, and implementation of authorization to use resources. **OMB M-22-09** serves as the federal Zero Trust strategy, provides direction that aligns with CISA's five pillars, and initiates a change in thinking in federal cybersecurity.

NIST SP 800-63-3 Digital Identity Guidelines,[12] focused further on phishable MFA concerns. 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), but optional at AAL2. This paper uses the preferred term, "phishing resistance" and uses references to **NIST SP 800-63-3** unless otherwise 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."[13]

In April 2024, NIST released **NIST SP 800-63B supplement 1, Incorporating Syncable Authenticators into NIST SP 800-63B: Digital Identity Guidelines – Authentication and Lifecycle Management**.[14] While previous guidance required that private keys must not be cloneable or exportable, this supplement enabled government agencies to synchronize, or duplicate, a private key between different devices. This

[11] https://www.idmanagement.gov/playbooks/dira/
[12] https://pages.nist.gov/800-63-3/sp800-63-3.html
[13] https://pages.nist.gov/800-63-3/sp800-63-3.html#sec5
[14] https://csrc.nist.gov/pubs/sp/800/63/b/sup/final

supplement also included considerations that agencies should consider when deploying the technology.

The supplement states:

> *"Agencies determine which authenticators they will accept for their applications based on the specific risks, threats, and usability considerations they face. Syncable authenticators may be offered as a new option for applications seeking to implement up to AAL2, and, like any authenticator, the trade-offs of this technology should be well balanced based on their expected outcomes for security, privacy, equity, and usability."*

In 2022, NIST published **FIPS-201-3**,[15] which updated **HSPD-12** standards to introduce Derived PIV requirements that could be met by non-PKI authenticators by pointing to requirements for AAL2 and AAL3 authenticators from **NIST SP 800-63B**. This 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**. **SP 800-217** elaborates on federated PIV considerations introduced in **FIPS-201-3**.

The informative Federal Identity, Credential, and Access Management (FICAM) architecture, which is coordinated across agencies using the Identity, Credential, and Access Management (ICAM) Subcommittee of the Federal Chief Information Officer (CIO) Council and Chief Information Security Officer (CISO) Council, has delivered Federal Identity, Credential, and Access Management (FICAM) Playbooks to address the patterns that are essential for implementing federal direction from the Office of Management and Budget (OMB). These essential patterns include Enterprise Single Sign-On (SSO),[16] Cloud Identity,[17] and Identity Lifecycle Management.[18] In February 2024, the General Services Administration (GSA) released a FICAM Phishing Resistant Authenticator Playbook[19] to assist agencies with deploying their own pilots by providing extensive information and lessons learned from FIDO pilots deployed by other agencies.

To help "agencies understand potential options for identity management interoperability between on-premises and cloud-based solutions, the challenges involved in each, and

[15] https://doi.org/10.6028/NIST.FIPS.201-3
[16] https://www.idmanagement.gov/playbooks/sso/
[17] https://www.idmanagement.gov/playbooks/cloud/
[18] https://www.idmanagement.gov/playbooks/ilm/
[19] https://www.idmanagement.gov/playbooks/altauthn/

how to address those challenges,"[20] CISA published an updated document, *Secure Cloud Business Applications Hybrid Identity Solutions Guidance.*[21]

The FIDO Alliance supports the informative guidance produced by the Identity, Credential, and Access Management Subcommittee (ICAMSC) and CISA that supports agency efforts to meet the needs for centralization of enterprise identity services and make them available for applications.

A leading capability of FIDO authentication is that it is intended to meet the phishing-resistant requirements laid out by OMB. FIDO provides agencies with options for alternative authenticators that are widely supported by the commercial hardware and software used in government deployments.

3.4 Phishing Resistance in the U.S. Government

The **M-22-09** memorandum mandates phishing-resistant MFA for federal staff, contractors, and partners. It also refers to "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** refers to phishing resistance as "verifier impersonation resistance." While not all MFA is phishing resistant, all FIDO and PKI authenticators fit into this category.

The final draft of NIST SP 800-63B-4 recognizes two methods of phishing resistance: verifier name binding and channel binding.[22] FIDO authenticators use verifier name binding. During the registration flow of WebAuthn, which creates the FIDO credential, the name of the relying party is captured as the "relying party identifier (RPID)".[23] The RPID is cryptographically bound to the FIDO credential. The RPID must match the online service before the associated FIDO credential can be discovered or used, delivering phishing resistance.

PKI credentials, such as PIV or CAC, use channel binding. Clients and servers leverage the Transport Layer Security (TLS) protocol to mutually authenticate. During the basic TLS handshake, which modern web browsers use by default, the server's certificate is validated by the client against a list of trusted certificate issuers. Mutual TLS (mTLS) authentication leverages that initial secure TLS session to allow the client to securely present its own public key to the server. Once the server validates that the client's certificate is from a trusted provider, the server and client collaboratively create a

[20] https://www.cisa.gov/resources-tools/services/secure-cloud-business-applications-scuba-project
[21] https://www.cisa.gov/sites/default/files/2024-05/CISA%20SCuBA%20Hybrid%20Identity%20Solutions%20Guidance_0.pdf
[22] https://pages.nist.gov/800-63-4/sp800-63b.html - verifimpers
[23] https://www.w3.org/TR/webauthn/ - relying-party-identifier

symmetric key that is used to secure a new channel bound to both the server and client identities.

Both phishing resistant authentication methods, FIDO and mTLS using PKI, defeat credential phishing attacks.

Not all types of MFA are equally secure and some AAL2 technology can be compromised. A simple example of a "phishable authenticator" is a device that provides rotating codes. In a credential phishing attack, the user is tricked into visiting a site that is impersonating a legitimate site. The phony site prompts the user to log in, and the user enters the valid code needed to log in to the legitimate site. The malicious actor then uses the code to impersonate the user. CISA has clarified that MFA solutions that leverage push notifications are not phishing resistant, even when those capabilities implement number-match.[24]

As described in more detail in Section 5, FIDO-Specific Architectural Considerations and Recommended Agency Actions, FIDO authenticators and credentials, like PKI-based credentials, can have differing assurance levels and characteristics. Similar to the security value of credentials from various federal PKIs, the most important distinction is the inclusion, or absence, of hardware protection for private keys. Hardware protection is further differentiated by the use of Federal Information Processing Standard (FIPS) 140 validated cryptographic modules.

FIDO technology is not a complete replacement for PIV. PIV provides critical capabilities that FIDO's logical identity authentication cannot provide. PIV is a badge for physical access control that includes technologies for using certificate-based authentication for physical access and 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 within their enterprises.

4 Agency Actions

Implementation of 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.

[24] https://www.cisa.gov/news-events/alerts/2022/10/31/cisa-releases-guidance-phishing-resistant-and-numbers-matching

Single sign-on, **lifecycle management**, and **digital identity risk assessments**, are three efforts included in the minimum requirements for federal Zero Trust implementations and are prerequisites for U.S. government FIDO deployments. The Enduring Security Framework published **Identity and Access Management: Recommended Best Practices for Administrators**,[25] which describes how phishing resistant MFA should be integrated with SSO and Identity Governance of the identity and access lifecycle.

The following are recommended prerequisites that can be implemented concurrently with FIDO rollouts:

1) **Adopt single sign-on (SSO)** – Concurrent implementation of PIV and FIDO-based solutions requires capabilities to support complementary usage and management. Identity as a Service (IdaaS), which includes single sign-on, facilitates consistent usage by managing different verifier roles while providing protected resources with consistent authentication context.
2) **Implement the Digital Identity Risk Assessment process** - Agencies must establish a Digital Identity Risk Assessment (DIRA) process to assist application owners 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 for integration of FIDO solutions alongside existing PIV and DPIV solutions. By leveraging federated services, the user registers their FIDO credential to the enterprise service once and can authenticate to any of the applications they require access to without additional setup.[26] Federation also simplifies credential lifecycle management by providing a single point of disenrollment for each FIDO credential.

Federal guidance includes SSO functionality in descriptions of agency Identity Management Systems (IdMS). **FIPS-201-3** explicitly includes the Identity Provider (IdP)

[25] https://www.cisa.gov/sites/default/files/2023-12/ESF%20IDENTITY%20AND%20ACCESS%20MANAGEMENT%20RECOMMENDED%20BEST%20PRACTICES%20FOR%20ADMINISTRATORS%20PP-23-0248_508C.pdf
[26] https://www.idmanagement.gov/playbooks/sso/

capability as an expected IdMS system. **OMB M-22-09** recommends agencies "consolidate the means of authenticating to as few agency-managed identity authentication systems as practicable" as a precursor to effectively gaining a holistic view of users and the ability to verify their identities when they access systems.

Agencies may identify specific services that require phishing-resistant authentication in the absence of SSO, for example, cloud services, non-Government services/accounts, and Disrupted, Degraded, Intermittent, and Low-Bandwidth (DDIL) environments where personnel may be accessing systems. Agencies would apply both the SSO steps and the application steps to be used with the application or service in those instances. Identity Lifecycle Management (ILM) should be considered during analysis and planning for DDIL authentication solutions.

In 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 these cases, it may be useful to establish a mechanism for users to register those services, then cue users to report their exclusive use of phishing-resistant authentication in support of 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. Other organizations rely on 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.

Impact sensitivity and information assurance needs of a resource will dictate the Authenticator Assurance Level (AAL) needed. **NIST SP 800-63-3** introduced the idea of risk assessments for digital identity proofing, authenticators, and federation.

The DIRA[27] process identifies the required Identity Assurance Level (IAL) / Authenticator Assurance Level (AAL) / Federation Assurance Level (FAL) for a specific resource. AAL3 is required if the assessor's answer to any of the following questions is "yes":

- Did you assess a "high" impact level for any of the impact categories?

[27] https://www.idmanagement.gov/playbooks/dira/

- Did you assess a “moderate” impact level for personal safety?

When AAL3 is not required, AAL2 is required if the assessor’s answer to any of the following questions is “yes”:

- Did you assess a “moderate” impact level for any of the remaining impact categories?
- Did you assess a “low” impact level 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 Digital Identity Risk Assessment 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 by using similar question flows, from most restrictive impact sensitivity to least restrictive. The resulting identity assurance requirements, based on impact sensitivity factors, is different from an authorization policy.

Although DIRA provides agencies with a target AAL for protection of each resource, **M-22-09** limits selections to phishing-resistant options for access to enterprise resources. M-22-09 tailors AAL2 by narrowing permitted MFA methods based on the pervasive threat of credential phishing attacks. Although NIST SP 800-63B includes AAL2 options that are not phishing resistant, M-22-09 tailors AAL2 for federal enterprises to permit phishing resistant authentication, exclusively.

4.3 Adopt Integrated Identity Lifecycle Management

Why ILM? ILM is a critical capability of agency enterprise IdMS and is fundamental to 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

M-22-09 directs that “Agencies must employ centralized identity management systems for agency users that can be integrated into applications and common platforms.” The FICAM Identity Lifecycle Management (ILM) Playbook[28] describes how agencies can

[28] https://www.idmanagement.gov/playbooks/ilm/

implement ILM through establishment of a centralized IdMS and lifecycle processes. The authoritative user directory component of these systems may also be called a Master User Record (MUR), indicating authoritative orchestration and control over identity data synchronization and event handling by the IdMS across the agency's ICAM services.

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 to support additional credential or person types in conformance with **NIST SP 800-63-3**.

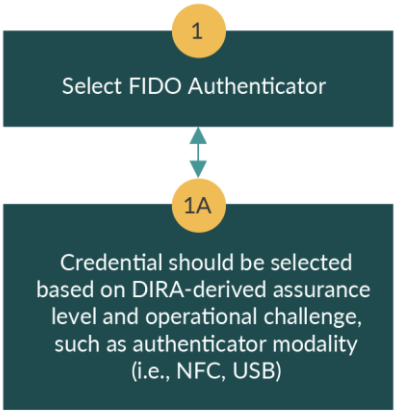
Agencies should extend core identity lifecycle capabilities to support additional use cases, rather than establishing independent or loosely connected processes and technologies for additional person types or authenticators. To the extent possible, agencies should retain and enhance the level of automation 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 are not eligible for PIV or who have not yet received their PIV. It also enables automation of access lifecycle management across enterprise applications for the purpose of implementing least privilege and analytics features.

5 FIDO-Specific Architectural Considerations and Recommended Agency Actions

5.1 Agency Action #1: Select FIDO Authenticators

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 AAL3 requirements. Alternatively, agencies may use non-attestable authenticators with other attestation sources (for example, direct supervision and mobile device management) to ensure the authenticator meets the AAL3 requirements.

The FIDO White Paper “Choosing FIDO Authenticators for Enterprise Use Cases” helps to identify available security and operational features that map to federal and agency requirements allowing selection of suitable authenticators for Agency use cases.[29]

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. In some cases, agencies may encounter technical or operational

[29] https://fidoalliance.org/wp-content/uploads/2022/03/FIDO-White-Paper-Choosing-FIDO-Authenticators-for-Enterprise-Use-Cases-RD10-2022.03.01.pdf

challenges in implementing authentication solutions at AAL3 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.

NIST SP 800-63B [Supplement 1] provides guidance on the federal use of synced passkeys. 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, compared to device-bound passkeys, they are not as secure in terms of storage and access. Agencies using synced passkeys should very closely examine the security of the sync fabric, data at rest, and recovery options.

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 situations where a smart card cannot, and which will focus on:

- Roaming or platform types
- Authenticator sourcing, ownership, and control
- Transport
- Gesture types

The following is a list of authenticator attributes and features that are required by or permitted under this standard:

Required:

- Device-bound passkey-capable, such as security keys or certain platforms
- 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[30], Federal Acquisition Regulation (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

5.2 Distinguishability at Registration: Attestations

FIDO authenticator attestation offers agencies lifecycle management flexibility by providing security characteristics, functional characteristics, and inventory data remotely. This 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 a few scenarios where an agency allows individuals to use their own authenticator for access to federal resources. In such cases, there are steps agencies can take to increase the authenticator security.

Some FIDO authenticators include an authenticator attestation statement during credential registration. This data can be used to look up authenticator security characteristics. For example, from the FIDO Metadata Service or other metadata service (MDS). In some cases, 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 not sufficient for the needs of the verifier, registration of that credential may be denied. In these cases, implementers should consider ways to make registration denial understandable for users.

Important context for the selection of authenticators has been introduced as federal agencies deploy FIDO authentication in their environments to implement **M-22-09** requirements. These include the use of attestation as a part of registration and the

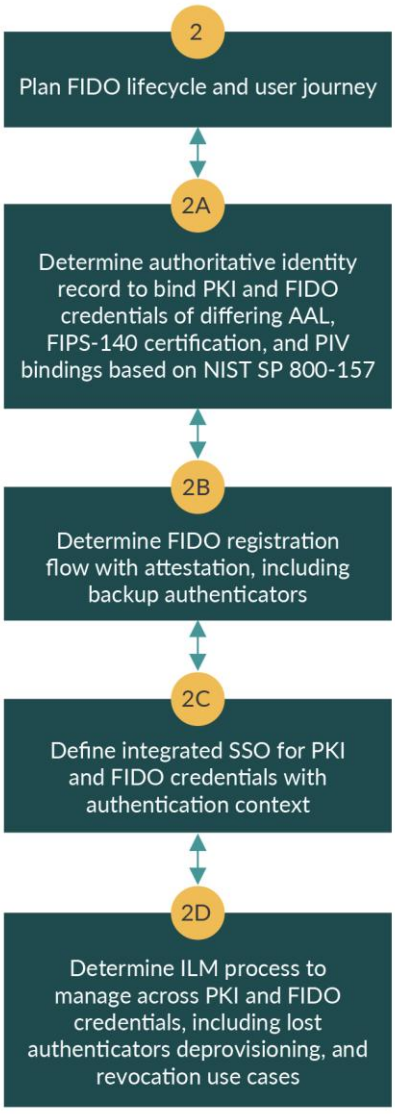
[30] https://www.acquisition.gov/far/subpart-25.4

passing of authentication context within ICAM services. It is critical that the IdMS store the necessary information about the FIDO credential so that, 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 that is protected with an activation secret can be treated as an AAL2 phishing-resistant credential without further attestation. Note that 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 implemented enterprise IdMS to impose management on the lifecycle of identities, credentials, accounts, and access through integrations across platforms, SSO, and credential management capabilities.



To produce consistent outcomes and auditability across integrated ICAM capabilities, it is crucial to plan an effective identity lifecycle capability, consisting of people, processes, and technologies.

When an authenticator is registered, attestation data needs to be collected because this is the only time this step can be performed.[31] If an agency is using unmanaged browsers, the attestation may be blocked, therefore blocking registration of the authenticator.

It is also important to consider a way to store this authenticator attestation metadata and make it available to verifiers after the registration is complete. 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. One solution is for agencies to use the official FIDO Metadata Service.[32] A list of registered authenticators and related metadata is also available.[33]

[31] https://www.w3.org/TR/webauthn-2/ - sctn-authenticator-credential-properties-extension
[32] https://fidoalliance.org/metadata/
[33] https://opotonniee.github.io/fido-mds-explorer/

Agencies may determine a need to maintain other relevant data that is not available from the FIDO Alliance or vendor MDS, as an extension for lookup at the registering service or via an extended metadata service, to be centrally operated. Some agencies or U.S. government (USG) shared service providers 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 are 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.[34]

FIDO supports Enterprise Attestation (EA), which enables agencies to track the inventory of security keys in their supply chain and throughout the credential lifecycle. EA can provide the serial number of a security key, as well as other agency-defined data. To allow authorized RPs to cryptographically verify the key was minted for a particular agency, EA also includes the agency domain. An EA certificate can only be added at the time of manufacturing. EA is being rolled out for security keys, browsers, and RP software, so agencies should plan to leverage EA even though it is not currently widely available. Currently no FIPS validated security keys support EA.

5.3.1 Distinguishability at the Verifier: Authentication Context

As agencies implement federated authentication with SSO, verifiers of user authentication need to be able to determine the authenticator type and security properties and communicate the assurance levels met to the applications that rely upon federated authentication services. To enforce phishing resistant authentication, applications need more information about user authentication events than “base AAL” from service providers. Service providers, serving as authentication verifiers, need “distinguishability” as a property of authenticators they support.

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

[34] https://fidoalliance.org/ux-guidelines/security-key-ux-guidelines/

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 (OCSP) services or a certificate revocation list (CRL). Centralizing authentication to support FIDO authentication offers an opportunity to improve complementary distinguishability outcomes for both PKI and FIDO while reducing the complexity of individual applications.

As the Federal Government prioritizes the urgent elimination of MFA solutions that are vulnerable to phishing, applications need to be able to specify phishing resistant authentication as a requirement in authentication service requests to a provider. Communicating assurance levels in federation protocols is done using metadata claims that convey distinguishable attributes that can be used for access policy enforcement. AAL2 alone as an authenticator assurance level value, is insufficient to express phishing resistance in the protocol's language of service requests and responses. More detail is required by the application. In addition to "AAL2 plus phishing resistance", applications may require the ability to distinguish PIV credentials from non-PIV or DPIV credentials.

5.3.2 Authentication Context Claim Values

Agencies should configure their SSO capabilities and SSO clients to use authentication context in federation protocols, such as OpenID Connect (OIDC) or Security Assertion Markup Language (SAML). Authentication context enriches client authentication requests and server responses to enable distinguishability of authentication methods and assurance levels. Authentication context helps clients to request authentication that meets their authentication policy enforcement objectives, such as those defined by 2025 Federal Information Security Modernization Act (FISMA) CIO Metrics.[35]

"AuthenticationContext" in SAML and "Authentication Context Class Reference (ACR)" in OpenID Connect are claims with a string value that corresponds to an authentication policy to be met. As an example of currently implemented authentication policy strings, GSA's Login.gov SSO offers three different policy string values for client applications that may be used to request user authentication.[36] Each of Login.gov's policy string corresponds to a reportable authentication policy question in FISMA CIO metrics.

[35] https://www.cisa.gov/sites/default/files/2025-01/FY25-FISMA-CIO-Metrics-v1.1.pdf
[36] https://developers.login.gov/oidc/authorization/

- **http://idmanagement.gov/ns/assurance/aal/2** - This string specifies that the user must authenticate or have been authenticated using a separate second factor (for example, not a remembered device).
- **http://idmanagement.gov/ns/assurance/aal/2?phishing_resistant=true** - This string specifies that a user must authenticate or have been authenticated using WebAuthn or a PIV/CAC.
- **http://idmanagement.gov/ns/assurance/aal/2?hspd12=true** - This string specifies that a user must authenticate or have been authenticated with an HSPD12 credential (PIV/CAC).

Standardized federal policy strings have not been defined. Each string value is a uniform resource identifier (URI) and not intended to be a navigable Uniform Resource Locator (URL).

Agencies should leverage authentication context in their federation protocols to convey tailored assurance level information in requests and responses.

5.3.3 Step-up Authentication

To support a positive user experience, while enabling a single provider to support multiple credential assurance level policies for a specific application, it is necessary to support step-up authentication.

A single application may have functionalities of differing impact sensitivity available to users that each have a different access policy. If a user initially authenticates at a lower authenticator assurance level, and later in the session needs to perform a more sensitive function, the application may prompt the authentication service provider to re-authenticate the user using a higher-assurance authentication method. This capability is called “Step-up” authentication. Configuring Step-up flows requires configuration at the authentication service and each client that leverages it. Step-up can be implemented using open standards.[37]

5.3.4 Selecting SSO Solutions

When selecting a product or service to support PIV and FIDO in a complementary architecture, agencies should consider their entire credential ecosystem and consider the need to support PIV and FIDO throughout the credential lifecycle.

With traditional PIV credentials, U.S. government agencies have tied a single PKI credential to a single human identity. The addition of “derived” credentials to the federal

[37] https://datatracker.ietf.org/doc/rfc9470/

credential ecosystem increases the number of PKI credentials bound to a single identity account, which introduces a degree of complexity to orchestrating derived credentials lifecycle.

The addition of non-PKI phishing-resistant credentials to the ecosystem adds permitted derived PIV options, including FIDO. It also adds the need to orchestrate SSO accounts. FIDO credentials should be bound to the SSO subscriber account, as alluded to in FIPS-201-3. For lifecycle management, derived PIV requires the FIDO server to enforce PKI-AUTH before binding a new credential to an identity account, per 800-157. Note that **SP 800-157** is undergoing an update, and this guidance could change in future iterations.

If the derived credential is to be used at AAL3, the application must also identify themselves with a biometric sample. Use of biometric samples is somewhat rare among existing issuers and must be integrated into existing tools. The FIDO server must also support the full lifecycle of the PIV card credential and allow 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 support interoperability and security profiles that mitigate evolving threats. Agencies should adopt interoperability and security profiles that are actively maintained, such as the Financial-grade API profiles for OpenID Connect and OAuth 2.0,[38] the International Government Assurance (iGov) profiles,[39] or MITRE's profiles for OIDC and OAuth 2.1 that are tailored for enterprise missions[40]. The SAML V2.0 Deployment Profile for Federation Interoperability (saml2int)[41] from the Kantara Initiative may be helpful to agencies leveraging SAML for SSO.

Agencies should refer to the final version of NIST SP 800-217, once published, for additional requirements and considerations that should inform their SSO deployments.

As the U.S. government implements FIDO authentication to mitigate credential phishing 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 in mitigating evolving threats.

[38] https://openid.net/wg/fapi/specifications/
[39] https://openid.net/wg/igov/specifications/
[40] https://www.mitre.org/news-insights/publication/enterprise-mission-tailored-oauth-21-and-openid-connect-profiles
[41] https://kantarainitiative.github.io/SAMLprofiles/saml2int.html

5.3.5 Supply Chain Concerns and Secure Procurement

Agencies may determine a need to maintain relevant data, in addition to the data available from the FIDO Alliance or vendor MDS, for lookup at the registering service or from a centrally operated extended metadata service. Some agencies or USG shared service providers 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 are examples of data that may require authoritative government sources. Currently, this data is maintained as part of the NIST Cryptographic Metadata Validation Program (CMVP) and is not included in the FIDO Metadata Service. Over time, circumstances may prompt agencies to sunset currently approved cryptographic modules. This may be more complex if the effected modules cannot be determined using the hardware Authenticator Attestation Globally Unique Identifier (AAGUID) or NIST CMVP certificate. This can leave issuers guessing the appropriate hardware AAGUID from each vendor, or trusting data posted on vendor websites or in emails from vendor representatives. In such cases, it is helpful to seek additional guidance and clarification from NIST on how to best approach obtaining the correct AAGUID.

In terms of secure procurement, **NIST SP 800-63-3** states 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.

5.4 Agency Action #3: Deploy

Once the target user journey for the ILM process is defined, agencies must select one or more methods to onboard agency applications to the FIDO-enabled SSO service.

For users that have PIV or other phishing resistant credentials of the appropriate assurance level, agencies can leverage those existing credentials to facilitate registration of new FIDO authenticators. For users that don't have either PIV, PKI, or FIDO credentials, a new proofing and registration ceremony will be required.

Agencies often have applications or platforms that have been issuing their own credentials to subscribers who do not yet have PIVs or are PIV ineligible. These applications and platforms need to be onboarded to SSO and ILM services. Doing so will require syncing locally managed subscriber accounts and any locally issued credentials with their enterprise identities. Any users with PIV credentials can migrate

using a self-service mechanism, but existing users without credentials of a sufficient IAL/AAL will need to restart the journey with proofing.

Once SSO and ILM services are in place, new users are onboarded through the new user journey.

6 User Journey

The user journey to obtain a FIDO credential is similar to the PIV journey, with a few differences. The following figure and table outline the steps in the user journey.

Figure 1: FIDO User Journey

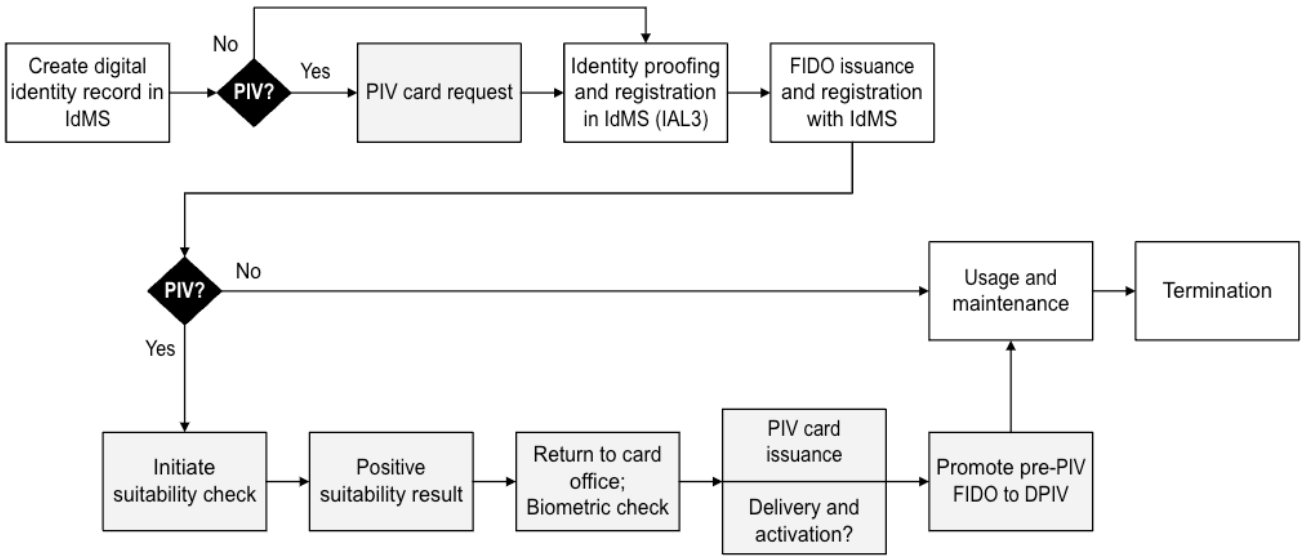


Table 1: FIDO User Journey Sequence

Task	Description
Create a digital identity record in IdMS	Create a non-PIV digital identity record and identifiers that are agnostic of person-type in the directory used for authentication.
Determine PIV/non-PIV	Determine person type or types based on legal status and organizational sponsorships.
(If applicable) PIV card request	Request PIV card, if applicable.
Identity proofing and registration in IdMS (IAL3)	In-person proofing, biometric capture, and registration for all users, including pre-PIV and no-PIV.
Initiate suitability check	For PIV, only, per **FIPS-201-3.**
Positive suitability result	For PIV, only, per **FIPS-201-3.**
PIV card issuance	For PIV, only, per **FIPS-201-3**. The person returns to the card office. Biometric check.
Delivery and activation	For PIV, only, per **FIPS-201-3**. This step only occurs if the card is not issued and activated on the spot. This step includes secure delivery of the card to the user and activation of the card by the user.
Promote pre-PIV FIDO to DPIV	For PIV only. Once the PIV card is issued, the initial FIDO credential can be bound to the PIV identity record along with the PIV authentication key in the IdMS.
Usage and maintenance	Usage, account recovery, lifecycle replacement. For PIV/DPIV, per **FIPS-201-3** and **NIST SP 800-157**.
Termination	Remove credentials from IdMS when the user is no longer eligible.

7 FIDO Considerations and Lessons Learned

PIV cards 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 from PIV cards and CAC, that separates authentication and account management. FIDO's approach focuses on a self-service privacy preserving model that is different from a centrally managed PKI-based credential. Many details around FIDO implementations for federal agencies are new and are different from PIV and CAC implementations. Therefore, there are specific considerations that agencies need to keep in mind including making sure USB ports can be used to read FIDO credentials and locking a device if the FIDO

security key is removed. The following are considerations that government FIDO credential issuers and relying parties will want to consider.

7.1 USB Resistance and Enablement

Federal agencies have shown reluctance to enabling employees to use security keys that connect using USB ports on government equipment due to concerns about malware and data exfiltration. However, agencies can leverage the USB Product ID (PID) capability to permit specific USB-based FIDO security keys for authentication while excluding unknown USB devices.[42]

7.2 Device Lock

Agency endpoints are commonly configured to go to a lock screen when the user's PIV card or CAC is removed. This operating system mechanism will not function the same way using devices that leverage FIDO standards. To achieve a similar effect, agencies need to implement a different mechanism within the operating system, which might be done using third-party scripts. Another way to implement device lock controls are to adjust the inactivity timeout or use PIV for desktop login and FIDO credentials for other applications.

7.3 Near Field Communication

Near Field Communication (NFC) is a wireless protocol used by mobile devices to authenticate and transfer tiny amounts of information to other devices in proximity. Since many agencies do not enable NFC functionality on devices, agencies will need to use other steps or credentials or make exceptions to policy to use NFC.

7.4 Forgotten PIN

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

8 Conclusion

In response to credential phishing threats, agencies must take urgent action to protect federal information systems by implementing authentication capabilities resistant to credential phishing attacks and eliminating authentication methods that are vulnerable to credential phishing.

[42] https://support.yubico.com/hc/en-us/articles/360016614920-YubiKey-USB-ID-Values

This document has detailed how U.S. government agencies can implement an inclusive user identity capability that supports both FIDO and PKI-based phishing-resistant MFA. Within agencies, this approach advances integration of the lifecycle of identity management across all person types with the lifecycle of access management across the agency's digital resources.

In addition, technical considerations for deploying FIDO authentication to meet current and future Zero Trust strategic objectives have been provided.

Agencies should examine use cases where traditional PKI technologies do not work, groups of users who do not have PIV credentials, or users who do not need access to government facilities. Included in these groups are new employees who have not yet received a PIV credential but need access to information resources to do their jobs. Employing innovative FIDO authenticators provides strong authentication where agencies might currently use username-password or phishable MFA to enable mission critical access use cases, exposing those missions to significant risk.

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

9 Appendix A: Use Cases

9.1 Use Cases

This document focuses on expanding available FIDO lifecycle management documentation. Specific use cases, including sequence diagrams and steps to complete the use case, are listed in the following tables.

9.1.1 Pre-PIV: Issuance of a FIDO credential

A popular use case for FIDO in the federal space is issuing credentials during onboarding so a new employee/contractor can access necessary resources while waiting for their PIV card/CAC. In Tables 2 and 3, we document the steps that need to be taken to initially issue the FIDO credential. Agencies must work with authenticator vendors to include the enterprise attestation on the FIDO credential.

Table 2: Sequence for remote Interim PIV FIDO credential issuance

Step	Description
1	Individual undergoes remote identity proofing.
2	If the individual passes proofing, the source of truth within the agency registers them into the Identity Governance and 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 and 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, verify 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.

Step	Description
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, the agency binds FIDO credential to the PIV record.

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

Step	Description
1	Individual undergoes in-person identity proofing.
2	If the individual passes proofing, the agency registers them into the Identity Governance and 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, the 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.

9.1.2 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 Table 4 lists proposed steps to bind a new FIDO credential to an existing PIV/CAC.

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

Step	Description
1	Individual navigates to the 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 and Administration (IGA) to see if the 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 the 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.

9.2 Lost FIDO credential

Table 5 details 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

Step	Description
1	FIDO credential is reported lost, stolen, damaged.
2	IT security runs a script to remove the public key from the user's account.
3	User navigates to the 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.

9.2.1 Binding existing FIDO token to new PIV

Table 6 details the steps for binding an existing FIDO credential to a new PIV.

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

Step	Description
1	User navigates to the registration page on IDP/IAM with the new PIV/CAC.
2	PIV/CAC attributes are associated with the 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.

9.2.2 Recovery scenarios for FIDO and PIV

Table 7 lists various recovery scenarios for FIDO and PIV, including forgotten PIN.

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

Table 7: Non-PIV Eligible Issuance and Use

Step	Description
1	Individual undergoes necessary background check for non-PIV eligible role and is approved.
2	Agency registers them into the Identity Governance and 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 and 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.

10 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 and 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