Phishing-Resistant MFA: Fact vs. Fiction

Guidelines for meeting phishing-resistant MFA requirements in OMB M-22-09

Jeremy A. Grant
Managing Director of Technology Business Strategy

Zachary P. Martin
Senior Policy Advisor

Ross B. Nodurft
Senior Director of Cybersecurity Services

August 2022

VENABLE LLP

Introduction

Imagine an employee at a federally funded research and development center (FFRDC) that directly supports a service branch in the Department of Defense (DoD). The DoD issues them a credential that uses the modern FIDO2 Web Authentication (WebAuthn) specification to access secure resources. The employee receives an email asking them to review a document from a coworker – but the email is actually a well-crafted phishing attack from a hostile nation. Just a few years ago, the employee's account might have been protected with legacy multifactor authentications (MFAs) like a one-time password (OTP) – and if they unwittingly clicked on the link and typed in both their password and OTP code, their account would be compromised. But with FIDO2/WebAuthn, this attack fails because there are no credentials to phish: the FIDO2 credential thwarts the attack.

Not all MFA is created equal. As the security technology has become ubiquitous, attackers have innovated as well, finding ways to circumvent some types of legacy MFA, such as those relying on text messages (SMS), one-time passwords, and push notifications. In February 2022 the White House flagged the concerns with legacy MFA in its recent Zero Trust Strategy (OMB M-22-09), noting:

> MFA will generally protect against some common methods of gaining unauthorized account access, such as guessing weak passwords or reusing passwords obtained from a data breach. However, many approaches to multi-factor authentication will not protect against sophisticated phishing attacks, which can convincingly spoof official applications and involve dynamic interaction with users. Users can be fooled into providing a one-time code or responding to a security prompt that grants the attacker account access. These attacks can be fully automated and operate cheaply at significant scale.

Modern successful cyberattacks — such as those seen in the 2020 Twitter attack, the SolarWinds attacks, and the 2021 Colonial Pipeline attack — are the reason why President Biden's Executive Order 14028 on Protecting the Nation's Cybersecurity mandated MFA, and why the White House Office of Management and Budget's Zero Trust Strategy — M-22-09 — called specifically for the use of phishing-resistant MFA throughout the federal government, as well as for access to citizen-facing digital services.

While the federal government has standardized around smart cards paired with PKI — the PIV and CAC platforms, both of which are phishing-resistant — smart cards do not integrate easily with all devices and applications, especially those that are cloud-hosted or mobile-based. For this reason, the federal government is prioritizing extending phishing-resistant MFA to every device and application to address gaps that smart cards cannot fill.

Here, M-22-09 highlights the ways that agencies should look to the FIDO2 standards to fill these gaps. Per the memo:

> Fortunately, there are phishing-resistant approaches to MFA that can defend against these attacks. The Federal Government's Personal Identity Verification (PIV) standard is one such approach. The World Wide Web Consortium (W3C)'s open "Web Authentication" standard (developed as part of the FIDO Alliance's FIDO2 standards), another effective approach, is supported today by nearly every major consumer device and an increasing number of popular cloud services.

FIDO2[1] is the overarching term for FIDO Alliance's set of specifications, of which Web Authentication (WebAuthn) is the most relevant. WebAuthn can be used in combination with a FIDO2 hardware security key for phishing-resistant MFA as the federal government moves authentication from the network level to the application level. In Appendix A, we look at the specific language from the various government policies that govern the use of multifactor authentication to better understand the federal government's evolving policy perspective.

[1] https://fidoalliance.org/fido2-2/fido2-web-authentication-webauthn/

According to the National Institute of Standards and Technology (NIST), “verifier impersonation-resistant" MFA[2] — as defined in the Digital Identity Guidelines (Special Publication 800-63-3) — uses public/private key cryptography and stresses the criticality of protecting the key material.[3] In this paper we look at the different MFA modalities in the market and discuss the different levels of MFA as public and private sector entities weigh their decisions about the type of MFA to enable for enterprise and mission use cases.

Phishing-resistant MFA defined

Phishing resistance is referred to by NIST in Special Publication 800-63-3 as “verifier impersonation-resistant” authentication, or more specifically:

> Verifier impersonation resistance places requirements on authenticators to reasonably thwart a phishing attack. Phishing attacks attempt to fool an individual into providing valid credentials to an attacker or a rogue site. At AAL3, SP 800-63B requires authenticators that use a verifier impersonation-resistant authentication protocol to prevent possible phishing attacks.[4] There are a number of ways to do this, including various encryption protocols and digital signature technologies that bind the authenticator output to a specific protected channel.

As part of efforts to update SP 800-63, NIST has indicated its intention to move away from the use of “verifier impersonation-resistant” authentication to “phishing-resistant” authentication. A draft of SP800-63-4 is expected later in 2022.

Phishing-resistant MFA is an authentication modality that is immune from attempts to compromise or subvert the authentication process, commonly achieved through phishing attacks, which includes but is not limited to spear phishing, brute force attacks, man-in-the-middle attacks, replay attacks, and credential stuffing. It is based on public/private key cryptography and reduces the attacker’s ability to intercept and replay access codes, as there are no shared codes, and sharing occurs only between the user’s device and the site they are visiting. For all practical purposes, this means the use of either PKI or FIDO2.

Phishing resistance within an authentication mechanism is achieved by requiring that each party provide not only proof of their identity, but also intent through deliberate action. Passwords, SMS and other one-time passwords (OTPs), security questions, and even push notifications are not considered phishing-resistant mechanisms, as they are all susceptible to some or all of the attacks previously listed. Nonetheless, MFA can be phishing-resistant via a FIDO2 authenticator, for example, and provide a smooth user experience.

[2] According to NIST, the phrase “verifier impersonation resistance” will be updated to “phishing resistance” in the next revision of SP 800-63, which will be published in draft form in 2022.

[3] https://pages.nist.gov/800-63-3/sp800-63-3.html

[4] https://pages.nist.gov/800-63-3/sp800-63b.html

MFA modalities

There are many MFA modalities available to consumers, companies, and the federal government. The table below offers a sampling of the different types of MFA available on the market today and whether they are phishing-resistant and why.

Table 1: MFA modalities

MFA Type	Authentication Strength	Reason
PIV/CAC smart cards	High assurance and phishing resistant	Uses PKI with public/private key pairs that have previously been registered with the relying party. No shared secrets and authentication are between the device – in this case the smart card – and the site or application being accessed. Requires a specialized smart card reader and may require middleware (depending on the application or device, which creates some integration challenges).
FIDO2 security key (i.e., YubiKey)	High assurance and phishing resistant	Similar to the PIV and CAC, FIDO2 security keys such as the FIPS 140-2 validated YubiKey from Yubico use asymmetric public key cryptography that has previously been registered with the relying party, implemented using the FIDO2 standards. There are no shared secrets or codes. Security keys can interact with other devices over USB or Bluetooth. The FIDO2 standard is supported by nearly every major consumer device and an increasing number of popular cloud services. Some YubiKeys are unique in their ability to support both PIV and FIDO2, along with OTP and OpenPGP on a single key – enabling a single device to be used to support multiple authentication protocols. The added benefit of a FIDO2 security key is portability, which enables a user to use a single key across a variety of applications and devices.
FIDO2 platform authenticator	High assurance and phishing resistant	Similar to security keys in function, FIDO platform authenticators are embedded in devices like smartphones and laptops. Platform authenticators can be a good option for someone who has only one device, but unlike security keys, they cannot easily be used across multiple devices, as the cryptographic material is embedded in the device.
Push-based mobile app	Medium assurance and not phishing-resistant	Push-based authenticators have gained popularity in recent years because of their ease of use: rather than enter a one-time code, a user simply has to push "approve" in response to a prompt that is pushed by a service provider to a user's smartphone authentication app. They are very effective at blocking most attacks based on credential stuffing and password reuse.
One-time passcode (OTP) – both token-based and app-based	Medium assurance and not phishing resistant	This has the individual enter an OTP that is generated either in a stand-alone hardware token or by an app from a mobile device. They are very effective at blocking most attacks based on credential stuffing and password reuse. They are not phishing resistant, however, in that users can be tricked into typing in an OTP in the same way that they can be tricked into entering the password into a phishing site – and these attacks have become more common and scalable.
SMS OTP	Weak and not phishing resistant	The granddaddy of MFA for consumers is susceptible to many forms of attack, including phishing, man-in-the-middle attacks, and SIM swapping. Additionally, SMS messages can often be rerouted to other devices, which essentially nullifies their use as a "proof of possession" authentication factor. SMS OTP was deprecated in NIST's 800-63-3 because of these vulnerabilities but remains one of the most widely used forms of MFA because of its ease of use.

Considerations for deployment of phishing-resistant MFA

Implementing phishing-resistant MFA is not as simple as clicking a few boxes, and agencies will have to prepare accordingly to implement the new modalities. As with most IT projects, agencies will want to have a discovery and planning phase where they learn about the technology, identify use cases, evaluate vendors, and ask about FIDO2 solutions.

Many agencies will start deployment in strategic areas, missions, and components, leveraging risk management practices to determine where to roll out phishing-resistant MFA across the enterprise. In some instances, agencies will want to consider the mission needs of various components while other agencies will want to look for access of enterprise employees and leadership.

After the identification of initial customers, the pilot phase would begin by building the user experience, piloting the use cases, and then improving the user experience. Once the pilots are running smoothly, it's time to roll out the new MFA modality with an education campaign for employees and contractors.

How to fund the move to phishing-resistant MFA

Between SolarWinds remediation and the mandate to move to a zero-trust architecture, funding is available for agencies wanting to deploy phishing-resistant MFA. Agencies need to make sure all new funding requests are tied to OMB M-22-09. There are funding pathways that agencies can consider as they look to implement phishing-resistant MFA. Below we highlight the four pathways for MFA that agencies can pursue.

Funding through shared services

For both the military departments (MILDEPS) and the federal civilian executive branch (FCEB) agencies, there are shared services that provide backbone for the governments' root of trust. These shared services underpin the current PIV/CAC cards and some other authentication services. For the MILDEPS, the Defense Information Systems Agency (DISA) plays a key role in driving the proofing and authentication requirements across the agencies. It also provides funding for certain DoD elements and department-wide contract vehicles

FCEB agencies have traditionally been issued their PIV cards through the General Services Administration's USAccess program.[5] While USAccess does not offer security keys at this time, this is an area that the government is actively exploring. FCEB agencies can access YubiKeys through the Continuous Diagnostics and Mitigation (CDM) program at CISA, although the agency will need to leverage agency funds to pay for the keys.

Funding through working capital funds

As part of the Modernizing Government Act, agencies have working capital funds that they can leverage when money is made available through appropriations.[6] Through the FY 2022 appropriation process, several agencies had funds made available through their working capital funds for enterprise information technology investments.[7] Agencies also have an opportunity to advocate for a percentage of unused resources to be reallocated to their working capital funds to fund modernization and cybersecurity projects. These funding streams provide potential pathways for funding and maintaining YubiKey or other security key purchases.

Funding through reimbursable funds

FCEB agencies and MILDEPS can also work with GSA to apply for funding for FIDO security keys or other phishing-resistant authentication solutions through two specific funds — the Technology Modernization Fund (TMF) and the Federal Citizen Services Fund (FCSF).

The TMF is an alternative funding model for technology modernization projects that allows agencies to propose projects that advance security or modernize environments. Through those modernization efforts, agencies should achieve efficiencies that can be paid back into the fund. For certain security projects, there are minimal repayment requirements. The TMF board, which oversees the fund, currently has over $2 billion in proposed projects and less than $1 billion in available funding. Additionally, the TMF is continuously analyzing and awarding new projects. That said, agencies can identify specific project proposals and potentially amend or update those proposals to include purchases of security keys to assist with modernization and move to secure, phishing-resistant, zero-trust architectures. Agencies can also work with the TMF board to submit new proposals to fund projects that can include security keys.

The FCSF is a fund managed by GSA that supports government-wide shared services meant to bolster additional digital interactions and transformations. According to GSA's budget justification document, "the FCSF initiatives help individuals, businesses, other governments, and the media to easily interact with Federal information, services, benefits, and business opportunities."[8] The FCSF supports agency-facing programs that drive

[5] https://www.gsa.gov/technology/technology-purchasing-programs/usaccess-identity-credentials-and-access-management
[6] https://www.congress.gov/bill/115th-congress/house-bill/2227
[7] https://www.congress.gov/bill/117th-congress/house-bill/2471/text
[8] https://www.gsa.gov/cdnstatic/05_FY_2022_CJ_FCSF_Narrative_Final_1.pdf

government-wide transformation through shared services, platforms, and solutions. The programs funded by the FCSF also provide technical expertise to agencies to improve their operations and the public's experience with government in support of the administration’s priorities and cross-agency priority goals. One of the programs that the FCSF supports is Login.gov.[9] This program provides single sign-on services to federal agencies and eventually state governments. Agencies that want to provide stronger authentication services can work with GSA to talk about inclusion of security keys as part of Login.gov or another one of the programs funded and supported by the FCSF.

Funding through annual budgeting processes

The final, slowest, but most direct way of funding the purchases of security keys is through the annual budgeting and appropriations processes. Typically, FCEB agencies work on budgets two years ahead of their current cycle. For example, in FY 2022, an agency will be developing its budget request for FY 2024. As part of that process, an agency can develop a plan for purchase and the roll-out of phishing-resistant security keys across an enterprise or for use by a specific team or mission within an agency. To do this, the agency budget office would work with the program or mission area owner or CIO to build out the funding requirement information and submit it to OMB. OMB then reviews the agency budget requests and prepares the annual budget submission. After the budget is submitted, agencies work with the appropriations committee staff members to defend and adjust budget requests for each program and line item. This total process takes between 18 and 24 months to complete.

MILDEPS work slightly differently and tend to build out five-year budget plans through the programming phase of the program and the planning, budget, and execution process. Military departments start by developing a program objective memorandum, which describes how defense agencies want to allot future funding for programs to align with the service program guidance (SPG) and the defense planning guidance (DPG). Elements within each MILDEP must work through their specific organization’s processes to submit their budget request. While these plans are updated annually during the budget process, they are still being developed two years in advance of appropriations. End-of-year unobligated appropriations can also be a funding source for security keys, and elements should work with their budget officers to understand the various options.

[9] https://login.gov/

Appendix A

Organization	Policy	Phishing-Resistant/MFA Language
White House - Executive Office of the President (EOP)	President Biden's Executive Order 14028 on Improving the Nation's Cybersecurity	(d) Within 180 days of the date of this order, agencies shall adopt multi-factor authentication and encryption for data at rest and in transit, to the maximum extent consistent with Federal records laws and other applicable laws. To that end: (i) Heads of FCEB Agencies shall provide reports to the Secretary of Homeland Security through the Director of CISA, the Director of OMB, and the APNSA on their respective agency's progress in adopting multifactor authentication and encryption of data at rest and in transit. Such agencies shall provide such reports every 60 days after the date of this order until the agency has fully adopted, agency-wide, multi-factor authentication and data encryption. (ii) Based on identified gaps in agency implementation, CISA shall take all appropriate steps to maximize adoption by FCEB Agencies of technologies and processes to implement multifactor authentication and encryption for data at rest and in transit. (iii) Heads of FCEB Agencies that are unable to fully adopt multi-factor authentication and data encryption within 180 days of the date of this order shall, at the end of the 180-day period, provide a written rationale to the Secretary of Homeland Security through the Director of CISA, the Director of OMB, and the APNSA.
Office of Management and Budget (OMB)	M-22-09, Moving the US Government Toward Zero Trust Cybersecurity Principles	Agencies must use strong MFA throughout their enterprise. • MFA must be enforced at the application layer, instead of the network layer. • For agency staff, contractors, and partners, phishing-resistant MFA is required. • For public users, phishing-resistant MFA must be an option. In this document, "phishing-resistant" authentication refers to authentication processes designed to detect and prevent disclosure of authentication secrets and outputs to a website or application masquerading as a legitimate system
White House - National Security Council	National Security Memorandum-8, Memorandum on Improving the Cybersecurity of National Security, Department of Defense, and Intelligence Community Systems	This memorandum sets requirements for National Security Systems that are equivalent to or exceed the cybersecurity requirements for Federal Information Systems set forth within Executive Order 14028 and establishes methods to secure exceptions for circumstances necessitated by unique mission needs.
Cybersecurity and Infrastructure Security Agency (CISA)	Cloud security Technical Reference Architecture	Agencies should implement the strongest security features wherever possible such as implementing phishing-resistant multi-factor authentication (MFA), and they should consider when to use convenience features like single sign-on. Best practices such as enabling phishing-resistant MFA and setting more granular levels of access and permissions for privileged accounts can limit unauthorized access and privilege escalation within the network, directory services, and applications. Agencies should take precautions regarding network access and network security settings, for example encrypting connections, using phishing-resistant multi-factor authentication, etc. However, while many authentication providers may offer MFA, the MFA may not meet requirements for government systems, like PIV-enabled- or phishing-resistant-MFA. In some instances, third party MFA applications can be added to an authentication service, but they will come with additional fees, and some may require the purchase of physical hardware tokens or the use of virtual hardware tokens. Phishing-resistant multi-factor authentication can be integrated into federated identity management solutions.
National Institute of Standards and Technology (NIST)	NIST Update: Multi-Factor Authentication and SP 800-63 Digital Identity Guidelines	6/17 NIST SP 800-63-3 Digital Identity Guidelines: MFA required for AAL2/3 and access to any personal information. AAL2 recommends and AAL3 requires MFA to support verifier impersonation (phishing) resistance. SP 800-63-3 uses the term "verifier impersonation resistance." The term "phishing resistance" is planned for SP 800-63-4. Verifier impersonation resistance is required for AAL3 and recommended for AAL2. Phishing-resistant authentication requires PW or biometric + asymmetric key cryptographic processes (PIV, CAC, FIDO2). Key Update Consideration: 63B: AAL2 differentiation of non-phishing-resistant MFA and strong (phishing-resistant) MFA.

VENABLE LLP

Attorney advertising. This document is published by the law firm Venable LLP. It is not intended to provide legal advice or opinion. Such advice may be given only when it is related to specific fact situations that Venable has accepted an engagement as counsel to address.