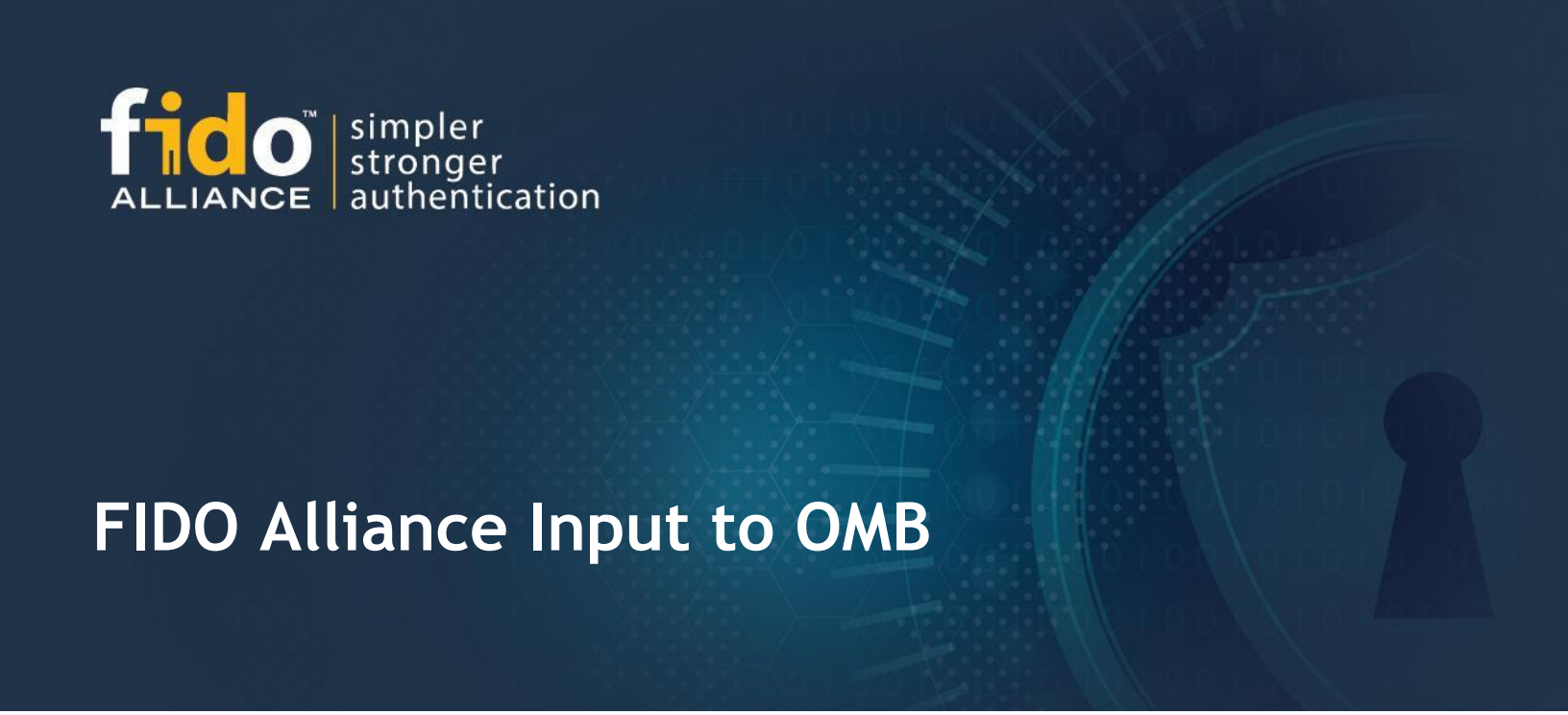

FIDO Alliance Input to OMB

Draft Federal Zero Trust Strategy

September 2021

The Fast Identity Online (FIDO) Alliance welcomes the opportunity to comment on the Draft Federal Zero Trust Strategy published by the White House Office of Management and Budget (OMB).

The FIDO Alliance is a multi-stakeholder, public-private, industry standards development organization comprised of more than 250 companies and government agencies from around the world dedicated to the creation of standards and certification programs for Multi-Factor Authentication (MFA) and passwordless authentication, as well as remote identity verification.

Our 40+ board members, whose logos are included below, demonstrate the strength of the FIDO Alliance's leadership, as well as the diversity of its membership. Our members include leading firms in banking, payments, and fintech, as well as those in security, health care, and information technology.

The launch of the FIDO Alliance in 2012 – and the subsequent creation and mass adoption of FIDO authentication standards over the eight years that have followed – has helped to transform the authentication market, addressing concerns about the problems with passwords, as well as the increasing phishability of legacy, first-generation MFA tools like One Time Passwords (OTPs) while also enabling significant improvements in the usability of MFA.

Today, the FIDO2 suite of standards – Web Authentication (WebAuthn) and Client to Authenticator Protocol (CTAP) – have emerged as the de-facto best choice for implementers seeking to deploy phishing-resistant authentication that is both more secure and also easier to use than legacy MFA tools.

As the draft OMB strategy notes, WebAuthn *"is supported today by nearly every major consumer device and an increasing number of popular cloud services."* Apple, Google, and Microsoft have all embedded support for FIDO2 at the device, operating system, and browser level, enabling new models for deployment phishing-resistant MFA to be "built in" rather than "bolted on."

The increasing ubiquity of FIDO support in commercially available smartphones and other computing devices has created new options for consumer authentication that improve security, privacy, and usability.

FIDO Alliance commends OMB for its focus here on phishing-resistant MFA. Whether it is in authentication or other layers of cybersecurity, one truism is that adversaries never stop innovating and are always coming up with new ways to attack legacy tools; what was secure yesterday may not be secure tomorrow. This has been a particularly large challenge when it comes to MFA over the last six years, as attackers have become increasingly proficient in phishing SMS and OTP codes, as well as tricking users into approving login requests sent by push notification.

Amidst this new wave of attacks, many governments across the globe have simply relied on advising implementers to "use MFA" and then treated all MFA tools as being equal in security. But while use of any MFA is better than none at all, all MFA is not the same. OMB's focus on differentiating between different approaches to MFA and requiring phishing-resistant MFA will ensure that government Zero Trust systems cannot be compromised with phishing attacks.

We offer three suggestions on ways to improve the draft guidance – with our rationale outlined below and then followed by suggested redline edits that incorporate these points:

1. WebAuthn is one of two standards in the FIDO2 suite, the other being Client to Authenticator Protocol (CTAP). The two standards work seamlessly together to enable phishing-resistant authentication, and FIDO Alliance runs an open certification program to validate that servers and authenticators conform to both specifications and can interoperate with other FIDO2 solutions.

   As background, both WebAuthn and CTAP originated through standards work done in FIDO Alliance; FIDO and its members then partnered with W3C to formally develop the WebAuthn standard, given the vital and unique role W3C plays in browser and web security standards and the focus of WebAuthn on browsers and web applications.

   If a security key is used to support authentication with WebAuthn, it is the CTAP standard that enables the security key to interact with the computing device running the web application. Likewise, if someone is using their smartphone as a security key – something that is increasingly an option today given that Apple and Google now both support this capability in iOS and Android – CTAP enables the interaction.

   For this reason, we believe it would be helpful for implementers to understand that CTAP also plays a role when implementing WebAuthn. In general, "FIDO Authentication" or "FIDO2" is the term that most enterprise decision-makers and consumers will be familiar with (Google trends shows 2x the number of searches for "FIDO2" over "WebAuthn") and we encourage OMB to consider using either FIDO term to help avoid confusion.

2. WebAuthn and CTAP are not just about security keys; we expect most of the public will first use these technologies via "on device authenticators" that are built into their computer or smartphone – and that many already use on a frequent basis to unlock their devices or to consummate login flows in mobile apps.

   Also referred to as "platform authenticators," given that support for FIDO2 is being built directly into the platform by Apple (via FaceID / TouchID), Google (Android biometrics), and Microsoft (Windows Hello), these types of embedded authenticators enable consumers to enjoy the security benefits of a FIDO2 authenticator without needing an external security key. Notably, the GSA's Login.gov platform supports these on-device FIDO2 authenticators as a second factor today.

   We believe it is worth noting that these on-device FIDO2 authenticators are also a good option for public users.

3. Other governments such as Australia and the United Kingdom (U.K.) have not only referenced FIDO standards in their guidance but FIDO certification as well. In 2020, both the Australian and U.K. governments specifically called out FIDO standards and certification programs by name in their MFA guidance.

- The Australian Cyber Security Centre (ACSC) – via its "Essential Eight" guidance on "Implementing Multi-Factor Authentication" – specifically recommends that implementers only use security keys have been certified by the FIDO Alliance.[1]

- The U.K. – as part of its "Using authenticators to protect an online service" guidance (Good Practice Guide 44) published jointly by the Government Digital Service and Cabinet Office– notes that an authenticator token "is high quality if it has been independently tested to prove it meets industry standards, such as the Common Criteria guidelines, FIDO or NIST FIPS 140-2."[2]

FIDO Alliance's certification program has gained this recognition thanks to the robustness and rigor of its program. Moe than 850 products have been FIDO® Certified – demonstrating a mature, competitive, interoperable B2B ecosystem of authentication and identity solutions.[3] Indeed some governments have also pursued their own FIDO certifications – for example, Germany's Federal Office for Information Security (BSI).[4]

We believe it will be helpful for agency officials looking to implement WebAuthn and CTAP in accordance with this guidance to know that they should look for those authentication solutions that have been certified by FIDO Alliance, in line with similar UK and Australia guidance. It may not be essential for this recommendation to be in the Zero Trust Strategy itself; this recommendation could also be included in complementary guidance around its implementation.

Given the points above, we believe the following edits (in red) might make the final Zero Trust Strategy a bit clearer to agency implementers:

In paragraph #5 of the" Multi-factor authentication and resisting phishing" section:

> 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, and so will help many agency systems meet this baseline. The World Wide Web Consortium (W3C)'s open "Web Authentication" standard, another effective approach, is supported today by nearly every major consumer device and an increasing number of popular cloud services; WebAuthn is part of FIDO Alliance's open FIDO2 standard, working in concert with FIDO's "Client to Authenticator Protocol (CTAP)" to enable phishing-resistant MFA. Any other authentication protocol that meets NIST SP 800-63B's definition of "verifier impersonation-resistant" will also resist the kind of phishing described above.

In paragraph #7 of the "Multi-factor authentication and resisting phishing" section:

> However, agencies' highest priority should be to rapidly implement a requirement for phishing-resistant verifiers, whether this is PIV or an alternative method, such as FIDO2 standards (e.g., WebAuthn) with CTAP.

[1] See page 5 of https://www.cyber.gov.au/sites/default/files/2020-06/PROTECT%20-%20Implementing%20Multi-Factor%20Authentication%20%28June%202020%29.pdf. Note that this guidance currently references FIDO U2F certification, calling for implementers to *"use U2F security keys that have been certified to the latest U2F specification version."* It is expected that the next revision will shift the focus to FIDO2.

[2] https://www.gov.uk/government/publications/authentication-credentials-for-online-government-services/giving-users-access-to-online-services

[3] See https://fidoalliance.org/certification/ for more details on FIDO's certification programs

[4] See https://fidoalliance.org/authenticator-certification-hits-a-new-milestone-with-first-l3/

In paragraph #5 of the "Public-facing authentication" section:

> To that end, **public-facing agency systems that support MFA must give users the option of using phishing-resistant authentication. Because most of the general public will not have a PIV or CAC card, agencies will have to meet this requirement by providing support for WebAuthn and FIDO-based approaches, such as FIDO security keys or on-device FIDO authenticators built into consumer devices.**

We greatly appreciate OMB's consideration of our comments. We look forward to further discussion with OMB on this topic and would welcome the opportunity to answer any questions or collaborate on approaches to address some of the issues we raised in this response. Additionally, we are available to present an overview of FIDO standards and the FIDO Alliance, should OMB staff or other Executive branch officials desire to learn more about how FIDO authentication and how its certification programs work.

Please contact our Executive Director, Andrew Shikiar, at andrew@fidoalliance.org, or our government engagement advisor, Jeremy Grant, at jeremy.grant@venable.com.