FIDO Alliance Input to the National Institute of Standards and Technology (NIST)

Pre-Draft Call for Comments: Digital Identity Guidelines

August 2020

The Fast Identity Online (FIDO) Alliance welcomes the opportunity to comment on NIST's Pre-Draft Call for Comments on Digital Identity Guidelines.

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.

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.

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 MFA market, addressing concerns about 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 FIDO standards are being used across banking, health care, government, enterprises, and e-commerce to deliver authentication that is both more secure and also easier to use.

Up front, we note that SP 800-63-3 represented a significant improvement in NIST's Digital Identity Guidelines, taking a more modern approach to identity proofing, authentication, and federation. That said, technology and threat are both never static, and we are encouraged to see that NIST is embarking on another revision of the document.

We offer comments in three areas for NIST's consideration:

1. **Recognize changes in both threat and technology since the publication of SP 800-63-3.**

   MFA adoption has been steadily increasing over the last 10 years – and with it, so have attacks seeking to defeat or circumvent MFA.

   NIST rightly flagged the security limitations of SMS in its last revision of SP 800-63, starting with drafts in 2016 that highlighted the ways in which attackers had caught up with SMS. NIST's work here helped to prompt organizations across the globe to move away from SMS and embrace more secure authentication tools.

   In 2020, it's time for NIST to sound the alarm again. Attackers have moved on to compromises of other authentication tools that are also based on shared secrets, including both OTP and Push-based solutions. Here, we've seen a sharp increase in the number of phishing attacks looking to trick users into either handing over their OTP codes or pushing "approve" on a Push-based solution that has been activated as part of a phishing attack.

Google (a FIDO Alliance member) was one of the first to flag the problem, noting in 2015 that, a *"phisher can pretty successfully phish for an OTP just about as easily as they can a password"* and noted their shift to FIDO hardware-based solutions as the way to stop these targeted phishing attacks.[1] Note that Google had previously tried to drive two-factor login by offering OTP through both SMS and a free OTP app based on the OATH protocol; these comments reflected their experience with this technology.

2016 also saw what was perhaps the most visible and impactful phish of an OTP code, when Clinton campaign chair John Podesta's OTP-protected account was phished by the Russian government.

Since that time, the ability of adversaries to successfully phish OTP has only increased. Free, open source tools like Evilginx are easily available to anyone looking to phish a shared-secret-based authentication factor.[2] Per the release notes for Evilginx 2: *"Evilginx, being the man-in-the-middle, captures not only usernames and passwords, but also captures authentication tokens sent as cookies. Captured authentication tokens allow the attacker to bypass any form of 2FA enabled on user's account (except for U2F)."*[3]

OTP is routinely phishable, as attackers have figured out ways to phish OTP codes from users. Attackers have also found ways to phish authentication based on push notifications. If attackers can trick users into typing in a password, they can also trick them into sharing a six digit code or clicking "approve" on a push-based authentication app.

As a result, leaders in the security community have begun to move away from OTP and other authentication tools based on "shared secrets." Industry is shifting toward "high assurance" MFA where at least one factor is based on public key cryptography, and thus cannot be phished. Authentication using the FIDO standards is one such example.

This is an area where we believe the current version of SP 800-63-3 needs some updates. Today, a variety of authenticators based on shared secrets – including Look-Up Secrets, Out-of-Band Devices (i.e., Push), and OTP apps and tokens – are given the same weight in AAL2 as authenticators based on asymmetric public key cryptography. Given how attackers have caught up with the former, it no longer makes sense to list these two types of authenticators alongside each other.

Doing so misleads implementers into thinking that these two categories of authenticators are still equivalent in strength or resiliency.

Going forward, NIST should adjust its approach to AALs to help implementers clearly differentiate between tools that are phishing resistant and those that are not. Ideas here include:

- Expanding the number of AALs to four – leaving the weaker shared secrets-based tools at AAL2, elevating those tools that are based on asymmetric public key cryptography to a new AAL3, and then creating a new AAL4 that reflects the current AAL3. We realize that doing this might create other issues, given the uniformity of three levels in IAL, AAL, and FAL, but we think it is worthy of consideration.
- Creating an AAL called "2+" which would encompass the idea of a new AAL3 in the previous bullet. This would allow NIST to keep the three levels of AALs while effectively differentiating between authentication tools based on shared secrets and those based on asymmetric public key cryptography.
- Calling for any new deployments of AAL2 solutions to use phishing-resistant authentication based on based on asymmetric public key cryptography.

Note that while we would like to suggest recognizing FIDO at AAL3, we understand that AAL3 currently imposes other ancillary requirements around the deployment of an authenticator that FIDO, in and of itself, typically does not meet. Also, per our next comment below, the withdrawal of support for token binding by major browser vendors has created some challenges.

[1] See https://www.youtube.com/watch?v=UBjEfpfZ8w0

[2] See https://github.com/kgretzky/evilginx2

[3] See https://breakdev.org/evilginx-2-next-generation-of-phishing-2fa-tokens/. Note that while Evilginx is formally published as a tool for researchers, it and many other similar tools can be used for nefarious purposes.

2. AAL3 – explore new paths.

When SP 800-63-3 was first published, it created a path for some FIPS 140 validated FIDO authenticators to meet AAL3 – if those authenticators were deployed in concert with token binding to deliver Verifier Impersonation Resistance.

Since that time, most major browser vendors have withdrawn support for token binding. Per discussions with NIST, we understand that this means that FIDO authenticators can no longer meet AAL3 without implementing other approaches to mitigate the loss of token binding.

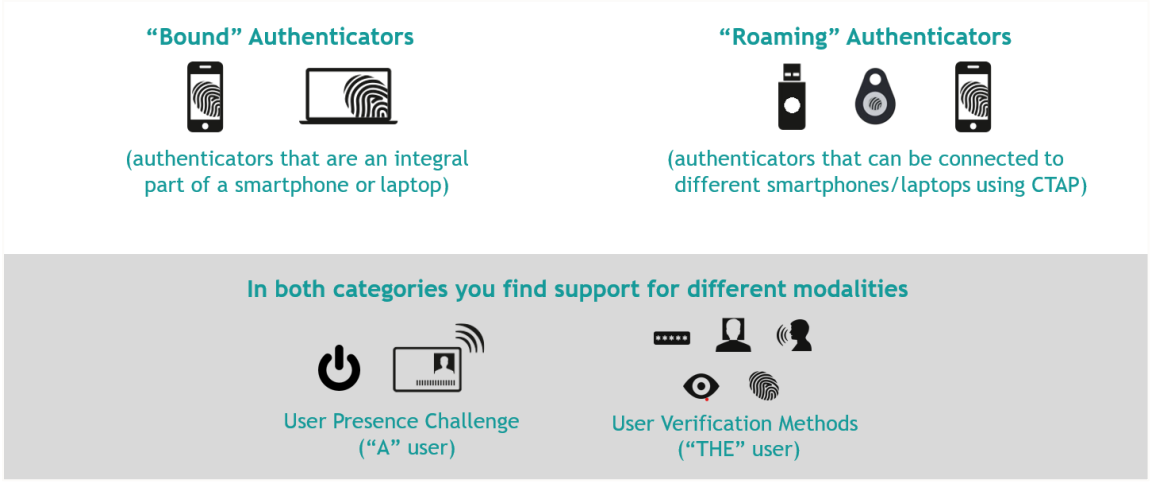
As NIST embarks on the next revision of SP 800-63, we urge NIST to engage with FIDO Alliance to explore other alternatives to enable FIDO authenticators to meet AAL3 requirements. FIDO Alliance and its members have delivered a significant innovation with the FIDO standards; the fact that support for FIDO is now embedded in most operating systems, platforms, and browsers gives the government and other implementers a valuable tool that they can use to deliver high-assurance authentication outside of the classic PIV/CAC model, leveraging authentication capabilities that are built into devices and browsers rather than ones that need to be bolted on. Government and industry would both benefit from finding ways to enable use of these capabilities at AAL3.

One idea is to look to explore the ways that the embrace by major browsers of Certificate Transparency might be able to achieve the same goals as token binding, with regard to enabling protection against mis-issued certificates.

We encourage NIST to work with FIDO Alliance to examine this issue – and supply guidance or help remove blockers that limit AAL3 options, impact needed innovation, and leave implementers of web-based technology with less than ideal choices.

3. Reference to FIDO standards.

As NIST is aware, FIDO authentication is not "one thing" in terms of how it can be implemented. As detailed below, FIDO standards support a variety of different form factors and use cases including both "roaming" and "bound" authenticators, as well as models where a multi-purpose device like a smartphone can serve as both, depending on the authentication use case. The one theme that unites all FIDO implementations is their reliance on asymmetric public key cryptography paired with a user gesture to verify either presence or the user himself.



SP 800-63B describes *Requirements by Authenticator Type* but is inconsistent in how it points to standards that support that type. This has created some confusion in the marketplace when implementers consult SP 800-63B and see reference to standards like OTP and PKI but do not see any specific reference to FIDO. That has led to the Alliance receiving a number of questions from organizations looking to implement MFA asking "Why is FIDO not supported in SP 800-63B?" We have in most cases been able to walk implementers through the document and point to where FIDO is in fact supported, however, the confusion is notable.

We note that NIST does reference other authentication standards in SP 800-63B as part of section 11.2 Standards, including those for Time-based OTPs [RFC 6238] and Internet X.509 Public Key Infrastructure Certificate and CRL Profile [RFC 5280]. Given NIST's willingness to make reference to these standards, FIDO standards should also be referenced.[4]

NIST's recently published Implementation Guidance is helpful in this regard, in that it points out how use of FIDO standards may be aligned with different Authenticator Types. We do note, however, that the Guidance only refers to U2F and UAF and makes no mention of the FIDO2 standards, which is likely to create some further confusion. Moreover, the fact that an implementer would have to first read SP 800-63-3 and then consult the implementation guidance to understand where FIDO fits creates a bit of a convoluted path for an implementer to get up to speed on the topic.

Going forward, we offer three suggestions:

1. Include a reference to FIDO standards in the body of SP 800-63B, alongside other authentication standards that are currently referenced in both 11.2 and the body of the document.
2. Embed the Implementation Guidance directly in the body of SP 800-63-4. This will ensure that the next version of SP 800-63 is much more user friendly, covering both normative and informative guidance in a single document. Implementers can read just one document, rather than going back and forth between two.
3. Within this guidance, outline how FIDO2 fits into Authenticator Types, in addition to U2F and UAF.

We greatly appreciate NIST's consideration of our comments. We look forward to further discussion with NIST 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.

[4] Note that FIDO UAF is now ITU-T X.1277, FIDO CTAP is now ITU-T X.1278, and Web Authentication is now a W3C standard.