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

SP 800-63-4 Digital Identity Guidelines (Draft)

April 2023

The Fast Identity Online (FIDO) Alliance welcomes the opportunity to comment on NIST's Draft of SP 800-63-4 Digital Identity Guidelines.

The FIDO Alliance is a multi-stakeholder, public-private, industry standards development organization comprised of more than 300 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 we were pleased to see that many of the issues we raised in our August 2020 comments to NIST (in response to NIST's pre-draft call for comments) were addressed in the new draft. We understand that NIST faces a notable challenge in trying to address inputs from dozens of different stakeholders, and appreciate NIST's willingness to consider our inputs.

We are submitting comments regarding specific sections and wording in the formal Excel comment template you published.

Additionally, we have a number of higher level comments that respond to some of the questions NIST asked in its December 16th announcement. Those follow below.

Note that NIST's questions are italicized; our responses are not:

Authentication and Life Cycle Management

- *Are emerging authentication models and techniques – such as FIDO passkey, Verifiable Credentials, and mobile driver's licenses – sufficiently addressed and accommodated, as appropriate, by the guidelines? What are the potential associated security, privacy, and usability benefits and risks?*

  We believe support for multi-device (i.e., syncable) FIDO passkeys are appropriately addressed in the new draft of SP 800-63B; the changes to 5.1.8.1 (Multi-Factor Cryptographic Software Authenticators) are helpful. There are two areas where we believe the guidance could be further improved:

1) It would be helpful for NIST to include additional language to discuss how to secure the "sync fabric" associated with passkeys - perhaps with language that ensures that authenticators facilitating the synchronization of private keys among different devices do so in an end-to-end-encrypted fashion protected by an appropriate key strength, and the authentication to the sync fabric meets appropriate requirements. There are a number of ideas from members on this point and we would welcome the opportunity to discuss pros and cons of different ideas.

2) It would also be helpful for NIST to include reference to FIDO and other authentication standards on a consistent basis in the body of SP 800-63B. As we noted in our 2020 comments, we continue to hear from implementers who are confused about whether use of FIDO standards is supported in SP 800-63B. While we ourselves know that it is supported, many implementers consult SP 800-63B and see reference to standards like TOTP 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, and also point to references in NIST’s SP 800-63-3 Implementation Resources. However, the confusion is notable.

   We note that NIST does reference other authentication standards in SP 800-63B such as Time-based OTPs (TOTP) in Sections 5.1.4.2 and 5.1.5.2, and the TOTP standard [RFC 6238) is listed in the references Section. Given NIST’s willingness to make reference to this standard, FIDO standards should also be referenced.

   In general, NIST can make the document much easier for implementers to comprehend and implement by incorporating key references like this into the body of the document, rather than include them in separate implementation resources. In practice we have found most people do not know the Implementation Resources exist or how they should use them, and for key questions like “is FIDO supported” it would make things much easier for implementers for the guidance to answer this question in a straightforward fashion.

- *Are the controls for phishing resistance as defined in the guidelines for AAL2 and AAL3 authentication clear and sufficient?*

  We believe the new approach, which focused on use of either Channel Binding or Verifier Name Binding, hits the mark. However, to our point above, it would be good to note what standards can be used to address the two approaches to phishing resistance in the body of the document, to make this clear to implementers.

  The draft appropriately calls out the use of Client-authenticated TLS as an example of way an implementer can achieve Channel Binding in 5.2.5.1, but does not provide any example for Verifier Name Binding in 5.2.5.2.

  For clarity's sake - and to make it easier for implementers who do not share NIST's expertise in understanding how the FIDO approach to phishing resistance aligns with NIST guidance - it would be VERY helpful to note in 5.2.5.2 that WebAuthN/FIDO2 is one example of an approach to Verifier Name Binding (as NIST did in slide 35 of its January 12th webinar slides).

  We do remain concerned that, given that attackers have caught up with AAL2 authenticators that are not phishing resistant, 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. Anything NIST can do to more clearly differentiate between legacy and phishing-resistant authenticators in AAL2 will help to address this issue – we had previously suggested the idea of calling phishing-resistant AAL2 authenticators “AAL2+” as one example of how this could be done. Additionally, we believe NIST should consider calling for any new deployments of AAL2 solutions to use phishing-resistant authentication.

- *What impacts would the proposed biometric performance requirements for this volume have on real-world implementations of biometric technologies?*

  In general we believe that what NIST has proposed here is in line with where industry is capable of delivering.

  Comments 18-30 in the Excel comments sheet we submitted address different aspects of biometric requirements.

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.

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