Yubico Comments on update to NIST 800-63-3
10 August 2020

Executive Summary

NIST 800-63-3 greatly improved identity and authentication guidelines. The NIST team has put significant thought and dedication into ensuring the safety of government systems and private systems. We appreciate and applaud their dedication to this work.

With the 800-63-4 revisions targeted for implementation in late 2022, we must look forward in crafting guidelines that ensure strong identity assurance and authentication, provide a reasonable replacement for Token Binding, recognize modern innovations and attack vectors, and support remote employees and the services they use. Guidelines must consider remote IAL and AAL as the norm at all levels. In addition, awareness of new innovation in authentication technology since 800-63-3 must be absorbed into NIST's Digital ID guidelines.

NIST must re-classify AAL levels to recognize credential phishing resistance as a distinguishing and important advancement with modern hardware authenticators, including hardware built into devices. Current authentication options, namely SMS and OTP, that don't address this persistent phishing vulnerability need to be relegated to AAL1. This creates a legitimate security position at AAL2 and recognizes the restraints on AAL3 created by the absence of Token Binding.

With respect to FIDO2/WebAuthn, identity binding is validated by using the IETF's Token Binding RFC's and Draft RFC's. Unfortunately, except for Microsoft's support in its Edge (non-chromium) Browser, no other browser or platform provides Token Binding support or has it on the roadmap. NIST should provide guidance around support for a user agent in the absence of Token Binding to achieve Verifier Impersonation Resistance at AAL3 for FIDO-based authentication.

NIST should explore WebAuthn and Certificate Transparency for AAL3 options. Credential phishing resistance native to WebAuthn also should be evaluated for AAL3 designations by utilizing Certificate Transparency for Verifier Impersonation Resistance combined with authenticator levels that can produce the highest levels of security.

The previous revision of NIST guidelines showed an affinity for hardware-backed, web-based strong authentication as defined by FIDO. This innovation must continue with Revision 4. Other considerations include guidelines that establish remote proofing as an equal to in-person proofing, and provide combinations of AAL, IAL, and FAL assurance levels that guide government and industry to grades of protection that match their use cases. In addition, when our adversaries are exploiting well-known vulnerabilities on the web at an alarming rate, legacy solutions need to be explicitly disallowed.

We believe the following suggestions will help improve NIST guidelines to address innovations realized since the June 2017 publication of 800-63-3, and meet security demands of evolving government and industry computing.

Yubico's Major Points:

1. Require credential phishing resistance at AAL2; solutions unable to provide that protection are relegated to AAL1.
2. Explore Certificate Transparency combined with FIDO-based authentication for potential at AAL3.
3. Closely Evaluate Remote ID Proofing innovations to meet IAL3.
4. Provide guidance on IAL/FAL/AAL combinations to achieve the highest level of assurance.
5. Depreciate SMS and Push Notification / Limit to legacy solutions.

Principle Comments

- **Re-define AAL2**
  - Reclassify AAL2 by adding credential phishing resistance as a requirement. Products that don't include this feature cannot advance past AAL1. Create these categories in the absence of Token Binding to achieve AAL3. This move eliminates the confusing grouping of strong hardware-backed FIDO tokens with SMS and OTP. AAL2 is too broad and any implementation guidance will not reflect the level of protection needed to justify the investment.
- **Certificate Transparency**
  - In terms of AAL3, NIST should consider Certificate Transparency as a replacement for Token Binding. While Certificate Transparency matches up less than 100% to Token Binding, it may provide a suitable placeholder. Today, all major browsers support Certificate Transparency, and Certificate Authorities can publish to Certificate Transparency logs for monitoring and auditing.
- **Remote ID Proofing**
  - Given knowledge gained from the on-going pandemic, NIST should look to innovation within remote proofing technologies and schemes that would define as equals remote solutions and In-Person proofing. NIST may want to examine proofing models or techniques such as those adopted by eIDAS, which helped Europe maintain on-line services when the pandemic hit. In addition, NIST should provide specific guidance for combining IAL with AAL, so that after achieving a high IAL, a weak AAL should not be bound to the IAL.
- **Assurance Level Combinations**
  - NIST should include guidance for better all-around security by adding implementation guidance based on combinations of IAL/AAL/FAL Assurance

Levels. Such guidance may include how to solve for specific use cases or environments including disallowing binding a strong IAL to a weak AAL or FAL

- **Deprecate SMS and Push Notification / Limit Legacy Solutions**
    - NIST should take this revision opportunity to signal legacy solutions have a shelf life, and to set sights on improvements to authentication with modern protocols. We understand the push back from vendor and other technology associations, but lobbying for specific outcomes likely will never adequately solve security issues.
- **FIDO Alliance support**
    - We had an opportunity to contribute and review the comments submitted by the FIDO Alliance. As a Board member of the Alliance, we agree with the comments made on authentication - including adding a new AAL category - clearly differentiating authentication security features, and adding explicit references to FIDO2 if NIST adds a new AAL to group non-phishing resistant technology.

<u>Suggested 9 Points to consider for 800-63-4 revision</u>

Point 1:
Privacy enhancements and considerations for identity proofing, authentication, and federation, including new developments in techniques to limit linkability and observability for federation.

- Outcome of FIPS 201 doesn't have to be a PIV card but could be another secure authenticator and/or form factor, such as a FIDO2 authenticator. Binding should be associated with identity.
  - *yubico*

Point 2:
Continued use of short message service (SMS) and public switched telephone networks (PSTN) as restricted authentication channels for out-of-band authenticators.

- Decouple any security mechanism from something that the user does not own, such as a phone number.
  - *yubico*

- SMS in the legacy form should not be allowed above xAL1.
  - *yubico*

- SMS and PSTN SHOULD be depreciated. Move SMS to “CANNOT” status and move Push solutions to a “deprecated” status. There are options such as FIDO-based authenticators that are more secure and easy to use without mandating additional hardware.
  - *yubico*

- Update 800-63-4 in a way that signals out-dated second factors will eventually not be considered adequate under NIST security guidelines.
  - *yubico*

Point 3:
Security and performance capabilities (e.g., presentation attack detection/liveness testing) for biometric characteristic collection to support Identity Assurance Level 2 remote identity proofing in the areas of identity evidence verification (physical/biometric comparison) or binding of authenticators.

- IAL2 or above SHOULD NOT allow binding weak authenticator (AAL1).
  - *yubico*

- NIST SHOULD provide prescriptive direction on associating authenticator (AAL) to Identity (IAL). Or include it in the 800-63-3 Conformance Document.
  - *yubico*

- NIST needs to list minimum combinations for risk - Use FedRamp as a use case/example. (North star: IAL2 with AAL3 (high/high) [Best practices vs open framework].)
  - *yubico*

- Guidance on binding strong authenticator to ID-proofed events.
  - *yubico*

- Move AAL1 to depreciation or add guidance for use. AAL1 should not be involved for anything requiring proofed information/identity. No new systems should be built using an AAL1 authenticator flow. Strong ID proofing must lead to strong or stronger authentication/Authenticator. Cannot follow strong IDProofing with weaker authenticator.
  - *yubico*

- High Federated assurance level should require strong IAL and AAL - recommended path should detail minimum level for all.
  - *yubico*

Point 4:
Capabilities and innovative approaches for remote identity proofing to achieve equivalent assurance as in-person identity proofing.

- Remote identity proofing is as strong as in-person proofing when issuing a credential over a secure channel. Yubico also recommends providing clear guidance for the IAL and AAL combinations so IAL2 or above SHOULD NOT allow binding weak authenticator (AAL1).
  - *yubico*

Point 5:
Security and privacy considerations and performance metrics for the use of behavioral characteristics as an authentication factor.

- Authentication via behavioral characteristics do not allow for the user to demonstrate intent to authenticate, which can lead to accidental breaches in security and privacy.
  - *yubico*

- Behavioral biometric authentication modalities SHALL demonstrate user intent as part of the authentication flow when coupled with any authentication factor meeting AAL2 or higher requirements.
  - *yubico*

Point 6:
Use of dynamic knowledge-based information for identity verification.

- Knowledge-based identity verification cannot serve as a sole method for identity verification. It can be used as a starting data point in conjunction with other sources of identity. Keep as a legacy/grandfathered only solution (IAL1 only). New systems should be IAL2 and above, and not rely on only knowledge-based information for identity verification.
  - *yubico*

- Entire Level 1 should include all existing older systems that embrace aging KB technology. New systems should be developed at Level 2 or higher.
  - *yubico*

- IAL levels should take into account modern advances in technology and have an underlying order that loosely corresponds to Level 1- legacy system, 2- current solutions, and 3- state of the art.
  - *yubico*

Point 7:
Capabilities to meet Federation Assurance Level 3 (see SP 800-63C FAQ C03)

- FAL3 is a difficult bar to meet, even with strong authentication options such as PIV/CAC and/or FIDO2. One solution to provide reasonable identity assurance may be to combine the IAL3 level of identity proofing with the strength of an AAL2 token.
  - *yubico*

- Currently, FAL3 provides a strong probability that the identity asserted is trusted and has been properly vetted by the Federation partner. With the use of PIV/CAC credentials the identity is bound to the token via Mutual TLS, ensuring that the asserted identity is actually represented by the token (PIV/CAC) being presented. This issue severely impacts the ability to meet FAL3 requirements for tying the identity to the token for new, modern authentication mechanisms. NIST may consider putting a requirement into the new NIST SP 800-63 revision that specifically calls out Token Binding as a needed or required technology.
  - *yubico*

Point 8:
Capabilities and security considerations for Verifier Impersonation Resistance (see SP 800-63B FAQ B04).

- We encourage NIST to examine the Token Binding issue and supply guidance or consider altering the definitions of AAL grading. Currently FIDO technologies cannot achieve AAL3 without Token Binding to meet verifier impersonation.
  - *yubico*

- In terms of AAL3, NIST should consider Certificate Transparency, which is supported by all major browsers, as a replacement for Token Binding.
  - *yubico*

- Specifically note the declining availability and application of methods to implement Verifier Impersonation Resistance at AAL3, notably browser options with Token Binding, which is NOT implemented by most browsers.
  - *yubico*

- Implementation of Verifier Impersonation Resistance at AAL3 should be qualified with respect to PIV smart cards with Mutual TLS since adoption is non-existent beyond networks deemed top-secret.
  - *yubico*

Point 9:
Additional controls and mitigation to address the ongoing evolution of threats such as phishing and automated attacks.

- Passwords by themselves are no longer sufficient for securing systems, and should be depreciated as an approved authentication method.
  - *yubico*

- Reclassify AAL2 by adding phishing resistance as a requirement. Current definitions of AAL2 are not sufficient to address modern phishing attacks.
  - *yubico*

- Consider expanding terminology (MUST, SHOULD, etc.) to include description of "abilities" (i.e. credential phishing resistance) as a flexible and accurate method to refine definitions of assurance levels.
  - *yubico*

- Products that don't include phishing resistance are AAL1 only. This eliminates the confusing grouping of strong hardware-backed FIDO tokens with SMS and OTP, which do not combat phishing.
  - *yubico*

- Solutions (including FIDO protocols) providing Verifier Impersonation Resistance for meeting AAL3 are not achievable at scale today, making AAL3 unreachable for large-scale deployments with a wide user-base.
  - *yubico*

- AAL1 should require multi-factor authentication for all authentication options.
  - *yubico*

- AAL2 should provide a strong and scalable position between AAL1 and AAL3 that is achievable with solutions available today.
  - *yubico*

- Certificate Transparency is a widely supported browser technology which may be used for identifying mis-issued certificates utilized as part of a verifier impersonation attack. Explore leveraging this technology in conjunction with phishing resistant authentication solutions in order to provide a path to addressing the requirements for AAL3.
  - *yubico*

- NIST should provide guidance around support for a user agent given the absence of Token Binding for any AAL3 equation or combination. Furthermore, NIST should provide in the addendum, guidance around Certificate Transparency and if this technology combined with authenticator levels could produce the highest levels of security.
  - *yubico*

Additional Comments

Restrictions Concerning Level 1:

- Entire Level 1 should include all existing older systems that embrace aging KB technology. New systems should be developed at Level 2 or higher.

- All xAL categories should take into account modern advances in technology and have an underlying order that loosely corresponds to Level 1- legacy system, 2- recognized solution, and 3- state of the art.