**Comment Template for: NIST SP 800-63-4 Suite (Initial Public Draft)**

*Please submit responses to dig-comments@nist.gov by March 24 April 14, 2023*

| | |
|---|---|
| ***Organization:*** | *Centers for Medicare and Medicaid Services -- not an official response* |
| ***Name of Submitter/POC:*** | *Elizabeth Schweinsberg* |
| ***Email Address of Submitter/POC:*** | [REMOVED] |

| Comment # | Publication (Base, 63A, 63B, 63C) | Section | Page # | Line # | Comment (Include rationale for comment) | Suggested Change |
|---|---|---|---|---|---|---|
| 1 | 63B | 6.1.2.4 | 44 | 1690 | **An exmample of "External Authenticator Binding" would make this section clearer. Is this an example of set app like gGoogle authenticator?** | |
| 2 | 63B | **6.1.4** | 46 | 1749 | "The subscriber SHOULD bind a new or updated authenticator an appropriate amount of time before an existing authenticator's expiration." This sentence could be more clear. Also, the section does not specify what an appropriate amount of time is. Is it necessary to include that phrase? | Consider "The subscriber SHOULD bind a new or updated authenticator in an appropriate amount of time before an existing authenticator's expiration." or "Before an existing authenticator's expiration, the subscriber SHOULD bind a new or updated athenticator." |
| 3 | 63B | 5.1.6.2 | 27 | 1085 | "The requirements for a single-factor cryptographic software verifier are identical to those for a single-factor cryptographic device verifier, described in Sec. 5.1.7.2." It would be clearer to write out the requirements in 5.1.6.2 and refer back to them in 5.1.7.2 rather than refer the description in the future. | Move the content of 5.1.7.2 to 5.1.6.2. |
| 4 | 63B | 5.2.2 | 32 | 1243 | "Accepting only authentication requests that come from an allowlist of IP addresses from which the subscriber has been successfully authenticated before." Do IP address allow lists really provide enough value when seeking to exclude attackers? With the proliferation of remote work and general roaming while using mobile devices there may be too many IPs to make this useful. | Add a caveat that IP addresses can be spoofed, and consider only putting enterprise IP addresses on the allow list. |
| 5 | 63B | 5.2.5.2 | 35 | 1385 | Ther Verifier Name binding section is unclear as to it's purpose. Perhaps an example of when you would need to do this would help. | |
| 6 | 63B | 5.1.3.2 | 22 | 913 | "Out-of-band verifiers that send a push notification to a subscriber device SHOULD implement a reasonable limit on the rate or total number of push notifications that will be sent since the last successful authentication." Accidental acceptance of pushes are common — are there requirements we can make here that would help stop that problem? | |
| 7 | 63B | 8.1 | 52 | Table 3 | Table 3 does not include social engineering of Out of Band verifiers that use push notifications. | Include the risk of out of band push notification abuse leading to accidental acceptance of an attacker's authentication request. |
| 8 | 63b | 11 | 74 | | The inclusion of the Equity section is thoughful and should help agencies provide better experiences around authentication | n/a |