**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:*** | *Canadian Centre for Cyber Security* |
| ***Name of Submitter/POC:*** | *Erin McAfee* |
| ***Email Address of Submitter/POC:*** | [REMOVED] |

| Comment # | Publication (Base, 63A, 63B, 63C) | Section | Page # | Line # | Comment (Include rationale for comment) | Suggested Change |
|---|---|---|---|---|---|---|
| 1 | 63B | 4 | 10 | 592 | Clarify whether this means that one of the two authenticators must satisfy both of the properties or that there must be at least one authenticator satisfying each. | |
| 2 | 63B | 5 | 14 | 685 | Clarify language. | Verifiers SHOULD permit a maximum length of memorized secrets of at least 64 characters. |
| 3 | 63B | 5 | 16 | 751-768 | Reconsider technical terminology used here. "One-way function" is not defined. | "The password hashing scheme SHALL use an approved Hash Function or MAC such as …", "The chosen output length of the password hashing scheme SHOULD be the same as the length of the underlying Hash Function or MAC output. " |
| 4 | 63B | 5 | 16 | 751-768 | PBKDF2 was a recommended password hashing scheme in the previous edition of this document. It is mentioned later in Lines 769-772, but omitted in this paragraph which says "NIST has not published guidelines on specific password hashing schemes". PBKDF2 is the only approved password hashing scheme for AAL1 and above (under the FIPS 140 requirement). Additionally, the recommendation that "A function that is both memory-hard and compute-hard SHOULD be used…" is difficult to meet since PBKDF2 is not memory-hard. | Replace "A function that is both memory-hard and compute-hard SHOULD be used because it increases the cost of an attack. While NIST has not published guidelines on specific password hashing schemes, examples of such functions include Argon2 [Argon2] and scrypt [Scrypt]." with "PBKDF2 [SP800-132] is an example of an approved password hashing scheme that can be validated for AAL1 and above. Memory-hard password hashing schemes, such as Argon2 [Argon2] and scrypt [Scrypt], may increase the cost of an attack, but configurations SHOULD avoid negative impacts on users and servers. NIST has not published guidelines on the use of such memory-hard password hashing schemes." |
| 5 | 63B | 5 | 18 | 766,811 | Reconsider use of term "arbitrarily". This does not align with the spirit of the paragraph. | Use "randomly" instead. |
| 6 | 63B | 5 | 18 | 825 | Typo: "authentiction" should be authentication | Use "authentication". |
| 7 | 63B | 5 | 26 | 1050 | Typo : "authentictor" should be authenticator | Use "authenticator". |
| 8 | 63B | 5 | 34 | 1346 | "MitM" should be replaced with "AitM" as used in other places in the document. | Use "AitM". |
| 9 | 63B | 5 | 40 | 1540 | Correct grammar, missing article. | "… authenticated pairing, pairing code …" should be "…authenticated pairing, a pairing code…" |
| 10 | 63B | 6 | 42 | 1609-1615 | Clarify any normative requirements, if any, for lifetimes of temporary secrets, as in lines 1684-1689. | Add requirements if necessary or refer to lines 1684-1689 |
| 11 | 63B | 6 | 43 | 1643 | It is unclear whether this section also outlines the requirements for a subscriber adding an additional authentication factor but remaining at AAL1. Clarify if this case is covered by line 1645. | |
| 12 | 63B | 6 | 44 | 1673 | Ambiguous grammar. Clarify what is common. | The need to replace a lost(i.e, forgotten) memorized secret is problematic because it is very common. |
| 13 | 63B | 8 | 52 | | Table 3. Inconsistent format of text in table. | Add a period to the entries in the first two rows of the table. In the "Theft" row, replace "Attacker" with "attacker". |
| 14 | 63B | Appendix A.4 | 82 | 2711-2712 | Typo: "the requirements… is different" should be "the requirements… are different" | |