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

*Please submit responses to dig-comments@nist.gov by October 7, 2024.*

| | |
|---|---|
| ***Organization:*** | *individual* |
| ***Name of Submitter/POC:*** | *KATSUHARA Tatsuya(Amazon Web Services Japan) , HAYASHI Tatsuya(Digital Agency), MAEKAWA Sami(Digital Agency)* |
| ***Email Address of Submitter/POC:*** | [redacted] |

| Comment # | Publication (Base, 63A, 63B, 63C) | Section | Page # | Line # | Comment (Include rationale for comment) | Suggested Change |
|---|---|---|---|---|---|---|
| 1 | 63-Base | 2.1 | 10 | 644-646 | The document should not define its own unique meaning for the general term "Service Provider" Since the term "service provider" is used infrequently, it would be best not to introduce it with a different meaning than the important technical term used in SAML. While there may be unfortunate collisions with other words, there is no need to intentionally create new confusion by defining it differently. | |
| 2 | 63-Base | 2.2 | 11 | Fig.1 | “ID Proofing” in fig 1 should be "Identity Proofing" | |
| 3 | 63-Base | 2.2.1 | 12 | 683 | “general-purpose or subscriber-controlled wallets” should be “general-purpose **IdP** or subscriber-controlled wallets”. | |
| 4 | 63-Base | 2.3.1 | 12-13 | 690-739 | It would be good to provide additional information regarding the same authentication element (to 63B) >For example, a user-generated PIN and a password do not constitute two factors as they are both "something you know." Mentioning that the reuse of the same element is a practical reality and including NIST's perspective on this would help broaden the coverage of this document, which is widely referenced.<br><br>Example:<br>The document recognizes that there are real-world cases where the same authentication element, such as a primary password and a secondary password, are used, which are not truly distinct. However, the document does not provide any evaluation criteria or guidelines regarding the assessment of such practices. | |
| 5 | 63-Base | - | - | | The document uses terms like "identity systems" and "digital identity systems" but there are no definitions provided, making their scope and role ambiguous. It would be beneficial to supplement an explanation of these terms in the context that this document intends to convey. | |

| | | | | | | |
|---|---|---|---|---|---|---|
| 6 | 63-Base | 3 | 22 | 937-945 | As an example of the risks to be considered in DIRM (Digital Identity Risk Management), instead of just using "impersonates someone," it may be beneficial to divide it into "impersonates someone who exists" and "impersonates someone who does not exist in reality."<br><br>This document is referenced across various industries, and it should also consider services that utilize IAL0, where the risk of a malicious user impersonating a non-existent person and becoming a subscriber is meaningful to include. | |
| 7 | 63-Base | 3 | 22 | 943-945 | Expanding the concept of "linking/associating" in the Federation model could be useful for the diverse industries that reference this document.<br><br>The Federation model does not explicitly address common commercial use cases where the RP (Relying Party) already has existing accounts. While it touches on the linking aspect from the perspective of correlating identities across RPs, it may be beneficial to introduce the concept of linking existing RP users. In business practice, it is common for the identities of the RP and IdP (Identity Provider) to be tied to different individuals, and such use cases likely exist. If NIST's intent is to completely prohibit this for the U.S. government, then a significant change in the description may not be necessary. However, at the very least, acknowledging the existence of such real-world use cases and the need for additional considerations in those situations could be valuable. (This is not a specific critique of the 63-4 content, but is also related to the content in 63-4C as well.) | |
| 8 | 63-Base | 3.3.3.1 | 37 | 1419-1420 | Strengthening the description on the existence of services that do not require Identity Proofing.<br><br>It is possible that IAL0 does not exist for U.S. government agencies, but given that this document is intended for widespread reference, this description may be too simplistic, risking confusion for the reader. It would be better to explicitly acknowledge that IAL0 does exist in the real world, and in such cases, the appropriate expression would be "data minimization & not validate/verify" rather than "not require any personal information."<br><br>Additionally, it would be beneficial to explicitly state in Section 3.3.2.1 IAL that the IAL0 use case, which no longer exists, is widely prevalent. | |
| 9 | 63-Base | 3.4.2 | 43 | 1603-1631 | We would like to clarify the positioning of Compensating Controls. Compensating Controls is an important concept, as we understand it to be about risk recognition, compensating controls, and residual risk acknowledgement in cases where it is absolutely impossible to comply with a requirement.<br><br>However, it is unclear whether Compensating Controls can also compensate for SHALL requirements in the Normative sections, and the positioning remains ambiguous. We would like to see a clear declaration of the approach regarding Compensating Controls. | |

| | | | | | | |
|---|---|---|---|---|---|---|
| 10 | 63A | 2.1.3 | 8 | 591-608 | Can the reflection of Supervised Remote in the Identity Proofing Types be improved?<br>Originally, Supervised Remote required the "participation of an operator" regardless of whether the claimants are at remote/local(Kiosk). However, the current Onsite Unattended allows for the absence of an operator.<br><br>Additionally, Onsite Attended now includes both the case where there is an operator at the counter and the case where there is a remote operator connected to the Kiosk terminal, which is confusing.<br><br>It would be better to separate them as follows.<br>- Remote Unattended<br>- Remote Attended(omit: 100% remotely)<br>- Onsite Unattended<br>- Onsite Attended locally(at the counter)<br>- Onsite Attended remotely(connected from kiosk) | |
| 11 | 63A | 2.4 | 10 | 649 | While the use of the term "valid" instead of "expired" is an improvement, the resulting criteria have become ambiguous, so further clarification would be beneficial.<br><br>It would be better to explicitly add here that it is the responsibility of the CSP to allow each organisation to define its own criteria of 'valid'. (Similar to some of the wording in 2.4.2.) | |
| 12 | 63A | 2.4.1.1 | 11 | 677-678 | "a facial portrait" should be "a facial portrait or other biometrics". | |
| 13 | 63A | 2.5.1 | 14 | 784-786 | The description of the verifiable scope and purpose of Confirmation Code Verification should be clarified.<br><br>It should be explicitly stated whether the verification is limited to demonstrating control over the address to which the confirmation code is sent, or if it can also be used as a means to validate the address, or if it binds the person who can control both the identity evidence and the address.<br><br>NIST has positioned the confirmation code as an effective means to verify the address in various places, but it would be helpful if NIST could clearly state how NIST is considering the risks of address takeover or interception during delivery. | |
| 14 | 63A | 3.1.2.1 | 18 | 910-913 | Regarding how to detect SIM Swap, since it involves a new concept, the organization may want to avoid providing specific details on the implementation methods.<br><br>On the other hand, if they are envisioning somewhat realistic means, including example(s) after stating "this is not limited to" could help facilitate the reader's understanding. | |
| 15 | 63A | 4.2.6.1 | 42 | 1716-1734 | Regarding the ambiguous use of "And/Or", it is important to clarify it with more plain language. | |
| 16 | 63A | 4.4 | 49 | Table 1. | There are places where the "And/or" description is missing, making it ambiguous. It should be stated explicitly. | |

| | | | | | | |
|---|---|---|---|---|---|---|
| 17 | 63A | 4.4 | 49 | Table 1. | Shouldn't the physical evidence "tactile inspection" included in IAL2 be required in IAL1 as well? (May be Error in the table). | |
| 18 | 63B | 3.1.1 | 12-13 | 711, 727 | It is desirable to provide additional supplementary information on the periodic change and complexity of Password Authenticators.<br><br>While it was "SHOULD NOT" in the previous 3rd revision, changing it to "SHALL NOT" this time may exacerbate the tendency to interpret it conveniently in isolation, which is not the intent of this document.<br><br>Indeed, I have heard about implementations that have decided on the basis of this/previous document not to change the password periodicity, but have ignored other SHALL/MUST requirements. As passwords are a concept of particular interest, it may be useful to document that the stated requirements are a comprehensive package of measures that are intended to be met simultaneously. | |
| 19 | 63B | 2.5 | 10 | Fig. 1 | Explicit hardware requirements in the Summary of Requirements.<br><br>To avoid ambiguity, following content(Sec. 3.2.5. line 1480-1483) should be explicitly reflected in the table in 2.5.<br><br>---<br><br>For authenticators that are usable at AAL3, verification of activation secrets SHALL be performed in a hardware-protected environment (e.g., a secure element, TPM, or TEE). At AAL2, if a hardware-protected environment is not used, the authenticator SHALL use the activation secret to derive a key used to decrypt the authentication key. | |
| 20 | 63B | 4.1.2 | 40-41 | 1618, 1621, 162 | Vague as there is no definition of ‘authenticated endpoint’.<br><br>Describe the Authenticated endpoint, either in the definition or in the description in the text. | |
| 21 | 63B | 4.1.2.2 | 40-41 | 1616-1662 | Diagram added to facilitate understanding of the newly detailed External Authenticator Binding concept.<br><br>Add a diagram describing "Authenticator Binding concept" | |