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

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

| | |
|---|---|
| ***Organization:*** | *National Institutes of Health* |
| ***Name of Submitter/POC:*** | *Jeff Erickson* |
| ***Email Address of Submitter/POC:*** | [REMOVED] |

| Comment # | Publication (Base, 63A, 63B, 63C) | Section | Page # | Line # | Comment (Include rationale for comment) | Suggested Change |
|---|---|---|---|---|---|---|
| | 63-Base | 5.2.2.1 | 31 | 1198-1199 | As written, the IAL1 criteria do not seem practically different from IAL2 in actual implementation. If one cannot accept attestation of something like name and birthday from the evidence itself, and one has to have an external source, this prevents the implementation of an in-person process where one can show an ID card and the registrar can accept it based on visual inspection. This was the 'industry' standard of a Low (or even Medium outside NIST) level of assurance prior to this draft. IAL1 is supposed to be low assurance, and one should not have to implement as much as IAL2 to achieve IAL1. | Remove requirement from IAL1 for external validation of core attributes. It's LOW assurance, and need to be able to implement without putting an IAL2-level burden of implementation on CSPs whose users need to access LOW Impact systems. Core attributes for IAL1 should be considered validated by the evidence itself. |
| | 63-Base | 5.2.3.1 | 50 | 1252-1254 | The text asserts that if no PII is required, then identity proofing is not required. This appears to be a false statement. There are other sensitive data that drives a system to higher FISMA baselines, which would, in turn, require stronger assurance in identity on who is accessing the sensitive data, PII or not. | Clarify/correct the statement to not suggest that "no PII = no ID proofing required". |
| | | | | | | |
| | 63A | 2.2 | 4 | 412-415 | As written, the IAL1 criteria do not seem practically different from IAL2 in actual implementation. If one cannot accept attestation of something like name and birthday from the evidence itself, and one has to have an external source, this prevents the implementation of an in-person process where one can show an ID card and the registrar can accept it based on visual inspection. This was the 'industry' standard of a Low (or even Medium outside NIST) level of assurance prior to this draft. IAL1 is supposed to be low assurance, and one should not have to implement as much as IAL2 to achieve IAL1. | Remove requirement from IAL1 for external validation of core attributes. It's LOW assurance, and need to be able to implement without putting an IAL2-level burden of implementation on CSPs whose users need to access LOW Impact systems. Core attributes for IAL1 should be considered validated by the evidence itself. |
| | 63A | Section 4.3.4.2 | 13 | 617-619 | Should not be required for IAL1 as long as lines 624-626 are in force. IAL1 should allow the visual and tactile inspection by trained personnel, but be able to accept 'evidence-asserted attributes' such as name and date of birth given that the evidence is 'validated' (at IAL1) for risk of forgery by the visual inspection including anti-tamper techniques such as watermarks and holograms. | Remove requirement from IAL1 for external validation of core attributes. It's LOW assurance, and need to be able to implement without putting an IAL2-level burden of implementation on CSPs whose users need to access LOW Impact systems. Core attributes for IAL1 should be considered validated by the evidence itself. |
| | 63A | Section 4.3.4.3 | 13 | 625-626 | Should not be required for IAL1 | Remove requirement from IAL1 for external validation of core attributes. It's LOW assurance, and need to be able to implement without putting an IAL2-level burden of implementation on CSPs whose users need to access LOW Impact systems. Core attributes for IAL1 should be considered validated by the evidence itself. |
| | 63A | Section 4.3.4.4 | 13 | 629+ | Should not be required for IAL1, or add the evidence itself as a validation source of the core attributes for IAL1 only. | Remove requirement from IAL1 for external validation of core attributes. It's LOW assurance, and need to be able to implement without putting an IAL2-level burden of implementation on CSPs whose users need to access LOW Impact systems. Core attributes for IAL1 should be considered validated by the evidence itself. |
| | 63A | 5.4.2.1 | 26 | 1056 | IAL1 IS LOW assurance. "One Strong + 1 Fair" is too much at IAL1, particularly in-person proofing. One strong (presenting a govt-issued photo ID for visual inspection) should be sufficient for an IAL1 in-person proofing process. Maybe consider requiring the +1 Fair for remote unsupervised proofing, but IAL1 should allow an implementation (in person) that allows the presentation of a single piece of evidence without needing the cryptographic features of SUPERIOR. | IAL1 accepts a single STRONG piece of evidence; delete "and one piece of FAIR" for IAL1. |
| | 63A | 5.3.3 | 27 | 1070-1075 | Should not be required for IAL1. IAL1 should allow the visual and tactile inspection by trained personnel, but be able to accept 'evidence-asserted attributes' such as name and date of birth given that the evidence is 'validated' (at IAL1) for risk of forgery by the visual inspection including anti-tamper techniques such as watermarks and holograms. | Delete lines. |
| | 63A | 5.1.9 | 24 | 960 | mandate for trusted agents should be clarified to be govt | Change "CSP" to "federal government CSP" |
| | 63B | 9.1 - 9.2 | 59 | 1998-2003 | Statements about Privacy Controls and NIST 800-53 seem out of scope for this document on authentication strength and assurance. NIST 800-53 is already required for US Federal Information Systems, and addresses Privacy. NIST 800-63B, however, is also encouraged for use in the private/non-govt sector. The guidance should not require non-govt entities to implement NIST 800-53 in order to be able to declare (and signal in federated logins) an xAL level. | Remove explicit requirement to implement 800-53 privacy controls from this document, or explicitly scope it to federal agencies; Federal agencies will be implementing 800-53 anyway. |
| | | | | | | |
| | 63C | 2 | 16 | 347 & 364 | Not all assertions need identify the subscriber. Incoming user attributes exist on a spectrum:<br>Affiliation—no user identifier, just a successful login from that institution<br>Entitlements—no user identifier, just user rights assignments/licenses<br>Pseudonymous—unique ID for each person, but real ID unknown<br>Personal—includes real world identity and contact information (name, email)<br>Your affiliation might be used to give a student discount. Your entitlements could let you access a journal subscription. In those cases, the SP/RP doesn't need to know your identity. No need to know => Don't send them an ID. | Revise text to not be prescriptive in sending an identifier. Change to "An assertion MAY include…" |
| | 63C | 4 | 20 | 459 | Seeking clarification… the text states that all FAL levels require at least FISMA Moderate control baselines. Is it intended that any use of federation requires a LOW impact system to be upgraded to MODERATE as far as the applied controls? | Clarification. |
| | 63C | 4.4 | 10 | 550-555 | At this location and other associated locations in this document: what's the code for attribute values? Should an attribute tagged "IAL" return "1", "IAL1" or "IAL-1"? Same question for other xALs. If someone is IAL-3 should they also signal IAL1 and IAL2 (I recommend they should, so RPs can configure their service provider to look for the code they require; internationally, REFEDS Assurance Framework requires the same thing, that an IAP-HIGH assertion also needs to independently include IAP-LOW and IAP-MEDIUM in the SAML assertion… because, if an RP requires IAP-Medium but the CSP only signals IAP-HIGH, the user won't get in). | Request clarity on all required xAL tagging in federated assertions. Recommend NOT leaving it up to each individual CSP and RP to negotiate this for themselves; that will not scale over real-world organizational relationships with many parties. RPs (the risk accepters in federation) need to be able to know what to look for to validate their required xAL level from the CSPs, and not worry that there will be variable permutations for NIST assurances between different govt agencies. |
| | | | | | | |
| | 63C | All Section 4 | | | To confirm: there is no more requirement to encrypt federated assertions/responses at any FAL level? | Request clarification. |

| | | | | |
|---|---|---|---|---|
| 63C | All Section 4 | | IdP authenticating the subscriber via MFA  - It would be great if NIST would provide clear guidance around IdP ability to signal to RPs on strength of MFA session like Phishing resistant vs Text vs TOTP | Suggest NIST to include guidance around signal strength of AAL assurance level |