**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:*** | *Salesforce* |
| ***Name of Submitter/POC:*** | *Frank Csech* |
| ***Email Address of Submitter/POC:*** | [REMOVED] |

| Comment # | Publication (Base, 63A, 63B, 63C) | Section | Page # | Line # | Comment (Include rationale for comment) | Suggested Change |
|---|---|---|---|---|---|---|
| | 63-Base | 4.1 Overview | 11 | 614-616 | It would make more sense to sort role by degree of assurance i.e. applicant, claimant, subscriber. Also, it's unclear whether a subscriber's identity has been proofed. | Change to applicant, claimant, subscriber or update the description to clearly indicate subscriber comes first (given it's the result of proofing and is done before attempting authentication) |
| | 63-Base | 4.2 | | | Note to reviewers Qn 1 under Identity Proofing and Enrollment | Note to reviewers Qn 1- FIDO2 With Verifiable credentials provides remote, fully unattended IAL2 compliant identity proofing.This is supported by existing technical standards and here are some of the papers published on its usage https://kar.kent.ac.uk/80304/1/IEEE_CHADWICK_LAYOUT_FINAL.pdf. The following is a preprint paper outlining the same approach- https://kar.kent.ac.uk/81365/2/submit-ccnc2020DCedited.pdf . The entire set of supported use cases are outlined here - https://www.w3.org/TR/vc-use-cases/ |
| | 63-Base | 5.3.1 | | | Where the impact assessment in 5.1.4 examines the impact to the organization, it feels like there is an opportunity to guide the reader through a similar impact assessment from the indiviudal's perspective for at least Privacy, Equity, and Usability | |
| | 63-Base | 5.3.2 | | | Make it clearer that compensation controls should be applied to concerns raised in 5.3.1 | |
| | 63-Base | 4.2 | 16 | | Figure 3 - Suggest first step be "Request Enrollment" | |
| | 63A | 5.1.2.2 | 18 | 776 | There is an opportunity in this section to explicitly call out that CSPs must not use social security number as the unique identifier for the applicant in the CSP's internal systems | |
| | 63A | 5.1.3 | 19 | | Is there referenceable material on that would provide CSPs guidance for performing equity-related risk assessments? If not, what guidance can be offered to CSPs. | |
| | 63-Base | 4.4 Federation and Assertions | 20 | 834-839 | The use of the word protocol rather than standard (OpenID protocol, SAML protocol) | Would it be more accurate to use standard? |
| | 63-Base | 4.1 | 25 | 655 | Text reads "RP requests" - in a non-federated model, the behavior may be better left open as "obtains" or "interacts with the CSP". | |
| | 63-Base | 4.1 | 26 | 677-679 | Steps 5 and 6 text do not match with Steps 5 and 6 in diagram on Page 25 - Figure 2. First part of Step 6 seems to belong in Step 5. | |
| | 63-Base | 5.2.3.1, 5.2.3.2, 5.2.3.3 | 32-35 | 1243; 1293; 1336 | It would be nicer to spell out the acronyms IAL, AAL, and FAL in the headings | |
| | 63-Base | 4.4.2 | 34 | 902, 906 | Examples are listed as supporting optional signing, but all FAL levels require signing by IDP (per SP800-63C) - a callout that while the technology supports it, FALs do not would be a good proactive measure. | |
| | 63A | 6.1.1 | 34 | 1246 | There is an opportunity here to explicitly state that social security number or any other evidence reference SHALL NOT be used as the unique identifier for a subscriber | |
| | 63-Base | 5.1.3 | 40 | 1100 | "Loss of sensitive information:" header appears to be missing | |
| | 63-Base | Reference | 42 | 1571 | The text reads "800-63B-4" but the URL and the subheading references 800-64A | |
| | 63-Base | 5.2.1 | 43 | 1180 | By "organization RP", is this referring to each "relying party" and their application owner must select initial assurance levels? This sounds like it could refer to a "responsible person". | |
| | 63-Base | Abbreviations | 66 | 2340 | Although XACML is given as an example (like SAML), its abbreviation is not defined | Add XACML to the list |
| | 63A | 5.1.6 | 869 | | Given 5.1.6.5 is it safe to even use telephone number in 5.1.6.1? | |
| | 63A | 5.4 | | | There is an opportunity to inform the reader that Table 1 exists earlier in the document | |