

Overall themes for feedback


| | |
|---|--|
| Scope and narrative nature of document | The focus on the mission fulfillment and equity concerns are much appreciated and the OpenID Foundation wholly supports that. The scope of the 800-63-4 document set is quite clearly defined yet there are quite a number of areas that it deviates from that scope. Both readers and authors would be better served if the scope were stuck to more rigorously and the resulting set of documents was shorter overall. There should also be focus on whether the document is intended to be guidance in a general sense or if it is intended to contain a large amount of direct and measurable requirements that implementers must use. In this draft there are conversational narrative sections, normative sections and normative language that in several cases lack specifics about what must be done in order to comply, this interweaving of normative sections and flexible use of normative language will make it a lot harder than necessary for implementers to meet the requirements. |
| Scope of communities, use cases and solutions covered | With the increasing digitalisation of services the communities of applicants and subscribers that need to be taken account of has significantly grown since previous iterations of this document set. It seems that some of the normative requirements are only considering "Single-Sign-On" use cases. Federation has wider utility than that so the requirements should be reviewed in the context of a much wider set of subscribers (including citizens and foreign nationals) and a much wider set of use cases than it appears have been considered. |
| Privacy | In this set of documents privacy is mentioned in a number of sections. Unfortunately the topic of privacy is highly complex and the current draft falls short of addressing that complexity fully and does not highlight for implementers that there are difficult trade-offs to be made around privacy. One important step to take is to enhance the threat modelling to directly include threats to individuals privacy across the full range of communities served, this would then naturally lead to those threats being more directly addressed. We would propose one of two options be taken to resolve this issue: 1. Strengthen the coverage of privacy related matters to the extent that privacy concerns are much more thoroughly addressed for all communities of subscribers than seem to have been addressed so far OR 2. Address privacy concerns in a separate set of documentation that addresses the full range of privacy concerns and refer to that from these documents, minimising as far as possible privacy issues dealt with within the digital identity guidelines We believe that option 2 is the better option to take |
| Interoperability | When federation is used in between larger groups of IDPs and RPs the challenges of interoperability become more significant. This concern does not seem to have been covered in much detail in this document set and we believe it to be an important consideration that deserves some additional guidance in order to avoid scalability issues. With the increase in digitalization of systems the number of parties involved has dramatically increased and if services are to remain available, cost effective interoperability needs to be made easier to deliver. The following list are suggested requirements that should be integrated into the guidance somehow: 1. Requirements to implement standardised and interoperele interfaces 2. Conformance testing of the technical interfaces of IDPs and RPs 3. Monitoring of services to be alert to any standards conformance issues that cause failures in order that those issues can be identified and resolved quickly |
| Risk based approach | A risk based approach to Digital Identity is a good starting point, unfortunately there are significant portions of the document that define requirements without linking those requirements to the wide variety of risks that should be mitigated. An expression of the key goals for the Digital Identity Guidelines followed by a thorough expression of the risks to the delivery of those goals which then is directly referenced by each section where normative requirements are defined would provide a much richer understanding of why certain normative requirements are there. This would then enable implementers to better meet the intent of the guidelines rather than blindly following the requirements as they are currently defined. The 800-63-base-4 document describes a risk based approach to xALs and tailoring of same and there are two issues with that directly: 1. It is unclear whether the tailoring involves stepping the xAL in question to a different xAL in some circumstances or that tailoring relates to flexibility of some specific component requirement of the Initial Assurance Level selected 2. If it is the latter then the consequence would be that additional details of how the xAL was achieved would need to be taken into account by the RP when making access decisions necessitating communication of the underlying xAL metadata from IDP to RP in context with the transaction. |
| Decentralised architectures | There seems to be some work to address decentralised federation architectures as part of this draft. It is not clear whether the intent is to include decentralised digital identity architectures within the definition of federation provided. The current entry in the "definitions and abbreviations" appendix actually includes all decentralised architectures yet the 800-63C-4 does not obviously address these approaches. The OIGF is of the view that all decentralized models are forms of federation. Suggestion would be to leave "federation" as a term that covers all architectures and then use a description that more clearly describes the features of decentralised architectures to define the different requirements. As part of that expand 800-63C-4 to cover other relatively mature digital identity models (perhaps mDL, ID3.1.5) and define requirements for each of the models. |
| Consent | There is no clear definition of consent in the document and it would be helpful to define that. In some other contexts it has proved useful to separate "consent" (to process data) from "authorization" (to share data). Whatever terms are used by NIST, the separation is a real one for end users and not having clarity on that separation risks mis-communication and lack of clarity with all of the attendant issues for consumer confidence that arise. |

Questions from "Notes to reviewers"

| Question | Comment (include rationale for comment) |
|--|---|
| Identity Proofing and Enrollment | |
| NIST sees a need for inclusion of an unattended, fully remote Identity Assurance Level (IAL) 2 identity proofing workflow that provides security and convenience, but does not require face recognition. Accordingly, NIST seeks input on the following questions: | no response |
| What technologies or methods can be applied to | no response |
| Are these technologies supported by existing or | no response |
| Do these technologies have established metrics | no response |
| What methods exist for integrating digital evidence | no response |
| What are the impacts, benefits, and risks of | The processes that are used in identity proofing could readily integrate digital evidence. Assuming an mDL or VC was available in the end-user's wallet then it could be impacts: |
| Are there existing fraud checks (e.g., date of death) | There are some standardised events defined in the the "Shared Signals Framework" produced by the "Shared Signals" Working Group at the OpenID Foundation. |
| How might emerging methods such as fraud | no response |
| What accompanying privacy and equity | The OpenID Foundation has commissioned and published a draft that relates to this question: https://openid.net/2023/04/05/open-for-comment-privacy-landscape . |
| Are current testing programs for liveness detection | no response |
| What impacts would the proposed biometric | no response |
| Risk Management | |
| What additional guidance or direction can be | The objective of risk management is to drive a set of outcomes and reduce the likelihood and impact of things that detract from meeting those outcomes. |
| How might equity, privacy, and usability impacts be | Clear measurable definition of outcomes relating to equity, privacy and usability should be included in the digital identity risk management framework described in the |
| How might risk analytics and fraud mitigation | no response |
| Authentication and Life Cycle Management | |
| Are emerging authentication models and | no response |
| Are the controls for phishing resistance as defined | Phishing resistance as a term is not defined in the guidelance so it is somewhat difficult to address this question. Based on assumptions we have made about the intent |
| How are session management thresholds and | Focus should be on adequate mitigation of risk in support of delivering defined outcomes rather than specific technical thresholds. It may be more valuable to discuss |
| What impacts would the proposed biometric | no response |
| Federation and Assertions | |
| What additional privacy considerations (e.g., | Management of data lifecycle - i.e. requirement that data is not retained for any longer than necessary to fulfil the agreed purpose for holding or processing the data |
| Is the updated text and introduction of "bound | No - it has led to confusion and a lack of understanding about what is meant among the reviewers. It seems very likely that implementers would need to make |
| General | |
| Is there an element of this guidance that you think | We are providing feedback on many of the sections in the documents where we think specific improvements can be made. Aside from those there are the following |
| is any language in the guidance confusing or hard | yes - tried to highlight that in the specific document feedback. |
| Does the guidance sufficiently address privacy? | In a US federal government agency context when relating to federal staff or contractors this is assumed to be covered by contractual terms and therefore privacy is not a |
| Does the guidance sufficiently address equity? | While equity is mentioned in the base document there seems to be little in the normative guidance that reflects that stated intent. |
| What equity assessment methods, impact | no response |
| What specific implementation guidance, reference | We would recommend the use of mature Open Standard interfaces as a critical component - this has been covered in the guidance to some degree. The reasons for this |

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

| | |
|--|-------------------|
| Organization: | OpenID Foundation |
| Name of Submitter/POC: | Gail Hodges |
| Email Address of Submitter/POC: | [REMOVED] |

| Comment # | Publication (Base, 63A, 63B, 63C) | Section | Page # | Line # | Comment (Include rationale for comment) | Suggested Change | |
|-----------|-----------------------------------|--------------|---------|------------|---|---|--|
| NS1 | 63-Base | All | 0 | 0 | Currently, there are multiple SHALL, SHOULD, MAY etc. in one paragraph and is hard to refer to. Being able to refer to | Change all the sentence that include SHALL, SHOULD, MAY an independent numbered bullet as in Base 5.3. | |
| NS5 | 63-Base | 4 | 0 | 0 | Identity lifecycle needs to be managed at various level. Currently, it is mentioned in 63C as part of the RP responsibility | Insert General Identity Lifecycle Management aspect as a subsection of section 4. Consider using ISO/IEC 24760-1 | |
| NS7 | 63-Base | | 0 | 0 | Credential (data that binds authenticator to the account at CSP) and Authenticator lifecycle needs to be managed at | It is required in both 63B and 63C, and potentially in 63A as well when considering credential first flow. | |
| NS8 | 63-Base | ii | 149 | | misspelling for identify (should be identity)??? | change to 'identity' | |
| NS9 | 63-Base | 4.1 | 11 | 633 | In modern identity systems (including OpenID Connect that is 10 years old), there is another important actor: "Claims | add following: | |
| NS10 | 63-Base | | | | | | |
| NS11 | 63-Base | 4.3.3 | | 19 | 814 | Is there a protocol that runs like Figure 4? | If not, replacing with a real protocol flow may be preferable. |
| NS12 | 63-Base | | | | 1100 | Missing section header "Loss of Sensitive Information" | Add sect |
| NS13 | 63-Base | Appendix A. | 43 | 1588 | While the section is marked "informative", requirements are referring to these terms and thus in effect they are | Consider  mative. | |
| NS14 | 63-Base | Appendix A. | 43 | 1589 | What is in A.1 is the combination of terms and definitions. | Change t | |
| NS15 | 63-Base | Appendix A. | 43 | 1592 | As pointed out in line 1592, some of the terms defined here are used inconsistently within the four documents. | Commer | |
| NS16 | 63-Base | Appendix A. | 43 | 1594 | Defining such a generic single word term like "Access" make the writing of consistent document hard. Examining the | Remove | |
| NS17 | 63-Base | Appendix A. | 43 | 1596 | Same with the comment on line 1594. | Remove claimant | |
| NS18 | 63-Base | Appendix A. | 43 | 1601 | Is this statement "Since all multi-factor authenticators are physical authenticators" correct? Is a software authenticators | Remove | |
| NS19 | 63-Base | Appendix A. | 44 | 1624 | Assertion reference by itself may not identify the verifier. It may be through other parameters in the protocol or through | Amend t | |
| NS20 | 63-Base | Appendix A. | 45 | 1667 | This entry is unnecessary. The definition just says "See Authentication" | Remove the entry. | |
| NS21 | 63-Base | Appendix A. | 47 | 1731 | Defining a verb generally is not a good idea. Moreover, the definition text is a noun. Define Authorization instead. | Change "Authorize" to "Authorization" | |
| NS22 | 63-Base | Appendix A. | 50 | 1838 | Interestingly, Digital identity is not defined in this document. | Define digital identity as: | |
| NS23 | 63-Base | Appendix A.I | 52 | 1904 | "uniquely describes" is a little limiting. Identity of a person, at its root, is how a person recognises themselves and it may | Define Identity and identifier as belows: | |
| NS24 | 63-Base | | | | | | |
| NS25 | 63-Base | | 45 | 1673-1675 | The 2nd sentence onwards are not part of the definition. It is just a note and examples. The commenter is just taking this | Authenticated Protected Channel | |
| NS26 | 63-Base | Appendix A. | 46 | 1699-1700 | Why are we defining Authentication Secrets through the attacker's capability? | Define directly rather than indirectly. | |
| NS27 | 63-Base | Appendix A. | 46 | 1708 | (Something the claimant possesses) - What about a password? Is it considered to be possessed even though it is | Delete "possesses and" | |
| NS28 | 63-Base | Appendix A.C | 49 | 1790-1791 | Make the phrase (via an identifier or identifiers -and (optionally) additional attributes) into a note or make it a new | An object or data structure that authoritatively binds an identity to at least one authenticator possessed and controlled by | |
| NS29 | 63-Base | Appendix A.V | 61 | 2201 - 221 | The definition of Validation and Verification does not go well with the signature processing in this document. | Instead of defining Validation and Verification, define more specific terms like "identity verification", "signature | |
| MH01 | 63-Base | 2.2 | 5 | 456 | It seems that the statement "While many systems could have the same numerical level for | Interoperability across systems should be given greater prominence in the thinking behind these guidelines. We see | |
| MH02 | 63-Base | 2.3.2 | 7 | 534 | "When designing, engineering, and managing digital identity systems, it is imperative to | Suggest adding statement to say "It is also important to consider managing the lifecycle of the digital identity data | |
| MH03 | 63-Base | 2.3.4 | 9 | 587 | perhaps make a stronger point about the delivery of a usable solution to all the communities referred to in the | Suggest adding "... for all communities served" | |
| MH04 | 63-Base | 4.1 | 11 | 626 | although this is the same as previous version use of this term has some risk of additional confusion as it has an | Suggest changing the term "Verifier" | |
| MH05 | 63-Base | 4.1 | 11 | 630 | "An entity in a federated model" - what is a federated model defined as? Could a Wallet be part of a federation? | As suggested elsewhere in this feedback, find a better way of describing the entities in different models - by definition | |
| MH06 | 63-Base | 4.1 | 11 | 635 | "a non-federated model" - what is a non-federated model defined as? It is not defined in Appendix A and on | As suggested elsewhere in this feedback, find a better way of describing the entities in different models - by definition | |
| MH07 | 63-Base | 4.1 | 14 | 677 | "Step 5: All communication, including assertions, between the RP and the IDP happens through federation | Suggest making this step optional and briefly mention one or two cases where it is not needed | |
| MH08 | 63-Base | 4.1 | 11 - 14 | 635 - 692 | "Non-federated" and "federated" are so similar that there is little architectural difference - why does there | As suggested elsewhere in this feedback, find a better way of describing the entities in different models - by definition | |
| MH10 | 63-Base | 5.2.2.3 | 32 | 1229 | "additional authenticator" - this is mixing federation concerns with authentication concerns - so if FAL3 a requirement f | Suggest moving the authentication requirement to the AAL space and stating that FAL3 also requires AALx | |
| MH11 | 63-Base | 5.2.2.3 | 32 | 1230 | it is really not clear what is meant by "bound authenticator" | Suggest adding definition of "bound authenticator" to Appendix A | |
| MH12 | 63-Base | 5.2.2.3 | 32 | 1232 | "The trust agreement and registration cannot be dynamic." what if there is a strong dynamic mechanism | Develop more detail in these guidelines about dynamic registration. The definition is weak and therefore open to | |
| | | | | | "Organizations SHALL use a risk-based approach to select the most appropriate identity proofing requirements for their RP application." - so RPs will need details of identity proofing communicated beyond IAL? In that case what is | that risk based tailoring will result in additional data and metadata being passed from IDP to RP. This risk based tailoring should be done in a way that recognises the trade-offs involved in simplicity:complexity and security:data proliferation that arise from this. | |
| MH13 | 63-Base | 5.2.3.1 | 32 | 1245 | the use of the IAL? | Suggestion would be to be very specific and standardised about xALs but allow RPs to make risk based decisions based | |
| MH14 | 63-Base | 5.2.3.1 | 33 | 1252 | "Not all RP applications will require identity proofing. If the RP application does not require any personal | suggest reword to "Not all RP applications will require identity proofing. If the RP application does not require identity | |
| MH15 | 63-Base | 5.2.3.1 | 33 | 1278 | "The overall impact level assessed by the organization leads to a preliminary selection of the IAL from which further | see comment and suggestion MH13 | |
| MH16 | 63-Base | 5.2.3.2 | 34 | 1293 | Basically the same comments about authentication and AAL as above WRT tailoring and the consequence for | see comment and suggestion MH13 | |
| MH17 | 63-Base | 5.2.3.3 | 35 | 1336 | Basically the same comments about Federation and FAL as above WRT tailoring and the consequence for | see comment and suggestion MH13 | |
| MH18 | 63-Base | 5.3 | 36 | 1375 | TAILORING - trust issues | see comment and suggestion MH13 | |
| MH19 | 63-Base | 5.3.2 | 37 | 1421 | "Countermeasures" seems to be a better term than "Controls" to me. Controls imply something absolute which | Suggest changing the term to "Countermeasures" | |
| MH20 | 63-Base | 5.4 | 39 | 1476 | need to be able to represent when the xALs were assessed. it is likely that IAL, AAL and FAL are all assessed at | Suggest adding something about maintaining a version controlled and time stamped history of the tailoring of the xALs. | |
| MH21 | 63-Base | Appendix A. | 45 | 1652 | "OpenID Connect scopes [OIDC] are an implementation of attribute bundles." that is not quite the case | I would suggest "Scopes can be used in some OpenID Connect [OIDC] implementations to request attribute bundles." | |
| MH22 | 63-Base | Appendix A. | 60 | 2179 | Token definition | suggest offering some disambiguation with other forms of token like id token or access token | |
| MH23 | 63-Base | Whole docur | 0 | 0 | Data minimization not really well addressed at all and there is a risk that when communicating digital identity attributes | Suggest adding a small section stating that data minimisation should be a key design principle for all implementers as it | |

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

Organization: OpenID Foundation

Name of Submitter: Gail Hodges

Email Address of S: [REMOVED]

| Comment # | Rationale (Base) | Section | Page # | Line # | Comment (Include rationale for comment) | Suggested Change |
|-----------|------------------|----------|---------|--------|---|--|
| NS/A01 | 63A | All | | | Currently, there are multiple SHALL, SHOULD, MAY etc. in one paragraph and is hard to refer to. Being able to refer to | Change all the sentence that include SHALL, SHOULD, MAY an independent numbered bullet as in Base 5.3. |
| NS/A02 | 63A | | 4 | 6 | This section provides "and" (spelling) overview | Change to 'an' |
| NS/A03 | 63A | | 9.3 | 48 | 1620 "per 4.2 requirement (5)" points to wrong/non-existent requirement | fix reference |
| NS/A04 | 63A | | 8.3 | 41 | 1390 Is NISTIR8062 a requirement? | Clarify requirement |
| NS/A05 | 63A | | 4.2 | 9 | 492 The phrase "to include the initial detection of potential fraud" doesn't seem to fit in/make sense. | Clarify |
| NS/A06 | 63A | | 4.3.2 | 10 | Does the acceptable digital evidence require a digital signature? | Clarify requirement |
| NS/A07 | 63A | | 4.3.3.X | | This whole section seems to have some confusion regarding requirements for physical and digital evidence | For each of the evidence strength levels, it might be better organized as a) requirements common for both physical and |
| NS/A09 | 63A | | 4.3.3.3 | 12 | 594 Does this apply to physical evidence? | Clarify requirement |
| NS/A10 | 63A | | 4.3.3.3 | 12 | 595 Does this apply to digital evidence? | Clarify requirement |
| NS/A11 | 63A | | 5.1.8 | 23 | 933 List specific ISO/IEC standards | List required standards - Provide it in the annex. |
| NS/A12 | 63A | | 5.4.3 | 28 | 1117 missing statement about the validation of FAIR evidence that is present in 5.3.3 (1068) | Add missing requirements if any |
| NS/A14 | 63A | | 6.3.2 | 35 | 1280 Requiring account termination without a course for redress seems too excessive. Maybe reference a standard for identity | Expand on account lifecycle management or refer to standard on account lifecycle management, e.e., ISO/IEC 24760-1 |
| NS/A20 | 63A | | 2.1 | 4 | 399 The term "core attributes" appears here for the first time in this document without significant explanation though there | Please explain the concept of "core attributes" before the first use. |
| NS/A21 | 63A | | 4 | 6 | 438 It states "SHOULD enable optionality" in spite of conditioning with "To the extent practical". This has impact on the | Change the combination to "SHALL" and "SHALL" or at least "SHOULD" and "SHALL". |
| NS/A22 | 63A | | 4.1 | 6 | 446 The word "common" in "describes the common pattern" should be avoided as it can be interpreted in two ways, i.e., | Rewrite to be more exact. |
| NS/A23 | 63A | | 4.1 | 6 | 449 When printed, [SP800-63] in "See [SP800-63] for details on how to choose the most appropriate IAL" cannot be clicked so | Change to "See the main document [SP800-63] ..." |
| NS/A24 | 63A | | 4.1 | 6 | 451 Since "Identity Proofing" is defined to be the process for a CSP, the statement "The objective of identity proofing is to | Replace "The objective" with "Since it is a process for a CSP, the objective". |
| NS/A25 | 63A | | 4.1 | 6 | 452 While it is easy to read, "who they claim to be" may have connotation like it needs to include name, which is not true. | Replace "the applicant is who they claim to be" with "the attributes about the applicant claimed by the applicant is |
| NS/A26 | 63A | | 4.1 | 6 | 454 The following probably is explaining how to determine "core attributes" but it is not referencing the term. There can be | If it is the case, make it clear to the reader that it is talking about core attributes. If it is not, then make it clear as well. |
| NS/A27 | 63A | | 4.1 | 6 | 458 Although this is an example, the commenter still believes that it is inappropriate to include all of three attributes cite | Remove "to the extent they are the minimum necessary" |
| NS/A28 | 63A | | 4.1 | 7 | 462-463 To facilitate the reader's understanding, it is nicer to provide some examples for "CSPs collecting additional information | Provide at least one example. |
| NS/A29 | 63A | | 2 - b) | 8 | 477 This should come before a) as if b) is false, a) is unnecessary. | Change the order of a) and b) |
| NS/A30 | 63A | | 4.3.1 | 10 | 517 Depending on the kind of the physical evidence, "printed name of the applicant" may not be necessary. For example, a | Either drop the requirement or spell out the reasons. |
| NS/A31 | 63A | | 4.3.2 | 10 | 526 The term digital evidence is not defined. Apparently, a photo of a document seem to work as a digital evidence but it is a | Define/clarify what is digital evidence and digitized evidence. Make a distinction between them especially on the |
| NS/A32 | 63A | | 4.3.2 | 10 | 528-531 It requires "The presented digital evidence contains the name of the applicant as the subject of the digital information or | Either drop the requirement or spell out the reasons. |
| NS/A33 | 63A | | 4.3.2 | 10 | 534 It is requiring the "name" of the issuer but that may not be unique enough. We are talking about the digital evidence | Change to "issuer identifier". |
| NS/A34 | 63A | | 4.3.2 | 10 | 541 "commensurate with the assessed IAL" sounds a bit unusual. | Change "commensurate with" to "proportionate to". |
| NS/A35 | 63A | | 4.3.3 | 10 | 544-546 Format the list as bullets for better readability | Insert line breaks before 1), 2), and 3). |
| NS/A36 | 63A | | 4.3.3.1 | 11 | 555 reference number should be defined better. e.g. whether it can be validated at the source, etc. Also, it probably does not | Define what is meant by reference identifier perhaps in the parenthesis. |
| NS/A37 | 63A | | 4.3.3.2 | 11 | 576 Does "physical security features" apply to digital evidence? Or does it mean that only a non-extractable digital evidence | Please clarify. |
| NS/A38 | 63A | | 4.3.3.3 | 12 | 586 What is exactly meant by "visually identified the applicant" is unclear. With an unclear definition, it cannot be tested for | Define what is meant by it. |
| NS/A39 | 63A | | 4.3.4.1 | 12 | 604-607 The list should be numbered for easier reference. | change to numbered list. |
| NS/A40 | 63A | | 4.3.4.1 | 12 | 612 It states "validated through verification of the digital signature" but "verification" in this document is defined as "The | Remove "verification" from defined terms. Define "identity verification" which is mentioned in the current definition as |
| NS/A41 | 63A | | 4.3.4.1 | 13 | 613-614 Wouldn't "the public key of the issuing authority" be too constrained? The issuing authority and the CSP may have a | Change to accommodate the use of shared keys and other verification method. Put a requirement on the finding of the |
| NS/A42 | 63A | | 4.3.4.2 | 13 | 618 Is the "must" a "SHALL"? | Change to "SHALL" |
| NS/A43 | 63A | | 4.3.4.3 | 13 | 623 How is "Visual inspection by trained personnel for remote identity proofing" performed? | Clarify |
| NS/A44 | 63A | | 4.3.4.3 | 13 | 628 Wouldn't "the public key of the issuing authority" be too constrained? The issuing authority and the CSP may have a | Change to accommodate the use of shared keys and other verification method. Put a requirement on the finding of the |
| NS/A45 | 63A | | 4.3.4.4 | 13 | 633 An authoritative source is an important concept and is worth making it to a headline element so that it can easily be | Insert a header "4.3.4.4.1 Authoritative Source". |
| NS/A46 | 63A | | 4.3.4.4 | 13 | 647 An credible source is an important concept and is worth making it to a headline element so that it can easily be found. | Insert a header "4.3.4.4.2 Credible Source". |
| UK/A01 | 63A | | 5.1.9 | 24 | 969 "Trusted referees are agents of the CSP" may be problematic. It may block the registration of the individuals for the | Make it sure that it serves the interest of the individuals. |
| MH/A01 | 63A | Abstract | | 119 | "This guideline focuses on the enrollment and verification of an identity for use in digital authentication." - it is unclear w | Suggest: "This guideline focuses on the enrollment and verification of an identity and the binding to a natural person for |
| MH/A02 | 63A | | 2 | 3 | 366 The first two sentences are mis-leading. "One of the challenges of providing online services is being able to associate a set | of activities with a single, specific individual. While there are situations where this is not necessary - such as when anon |
| MH/A03 | 63A | | 1 | 2 | 357 "individuals" This term is not defined. It could mean individuals of many different types, companies, machines, butterflies | suggest "individual natural persons" |
| MH/A04 | 63A | | 1 | 2 | 352 This section does not define a purpose for the document, it does describe what the document does but not what it is for. | suggest adding the purpose of the document and then re-considering whether the rest of the document delivers on that |
| MH/A05 | 63A | | 2.1 | 4 | 397 "Evidence validation: confirm that all supplied evidence is genuine, authentic, and unexpired" - maybe not "all" in every us | suggest change "all" to "sufficient" |
| MH/A06 | 63A | | 2.1 | 4 | 393 It seems that there should either be undesirable outcomes that are to be avoided that would usefully be mentioned here | Suggest adding sub-section about outcomes that SHOULD be avoided, including "un-necessary invasion of privacy" and |
| MH/A07 | 63A | | 2.2 | 4 | 419 The direct requirement for direct interaction seems to be a mitigation rather than something driven by a threat or risk. It | Suggest changing the focus from solutions to requirements that are about risk mitigation |
| MH/A08 | 63A | | 4 | 6 | 434 "Collectively, the elements of the identity proofing process are designed to ensure that attacks against a CSP's identity ser | change "require greater time and cost than the value of the data being protected" to "cost sufficiently much that the |
| MH/A09 | 63A | | 4.1.1 | 9 | 485 The CSP sends an enrollment code to the validated phone number of the applicant, the applicant provides the enrollment c | change the wording to: "reducing the risk that the applicant is not in possession and control |
| MH/A10 | 63A | | 4.3 | 9 | 495 "Identity Validation and Identity Evidence Collection" is not in the correct logical order | change to "Identity Evidence Collection and Identity Validation" |
| MH/A11 | 63A | | 4.3 | 9 | 500 "and related to a real-life subject." is verification and therefore not appropriate in this sub-section | remove "and related to a real-life subject." |
| MH/A12 | 63A | | 4.3.1 | 10 | 522 In reality there may well be useful evidence where the issuer did not perform identity proofing and it should be reflected | perhaps change point 4 to say: "Where the issuer of the document performed identity proofing of the applicant prior |
| MH/A13 | 63A | | 4.3.2 | 10 | 536 same as commentary for MH/A12 | "perhaps change point 4 to say: ""Where the issuer of the document performed identity proofing of the applicant prior to |
| MH/A14 | 63A | | 4.3.2 | 10 | 541 "digital evidence can be verified through authentication at an AAL or FAL commensurate with the assessed IAL" - what do | provide definition of "commensurate" or define explicitly which AALs and FALs are required in which circumstances. |
| MH/A15 | 63A | | 4.3.3 | 10 | 544 "Strength of identity evidence is determined by three aspects: 1) the issuing rigor..." The issuing rigor requirement is du | Remove "identity proofing" requirements from sections 4.3.1 and 4.3.2 or from section 4.3.3 |
| MH/A16 | 63A | | 4.3.3.1 | 11 | 549 "confirmed the claimed identity through an identity proofing process" - this doesn't appear to allow for things like utility b | either create a "WEAK" evidence class or relax the requirements for FAIR such that it permits things like utility bills or |
| MH/A17 | 63A | | 4.3.3.1 | 11 | 557 This is a very specific requirement that although it may be a useful starting point does not have a clear link to mitigation | describe risks to be mitigated and that a risk based approach should be taken |
| MH/A18 | 63A | | 4.3.3.2 | 11 | 570 "There is a high likelihood that the evidence issuing process would result in the delivery of the evidence to the person to w | please be specific and include a measurable threshold of "high likelihood" |
| MH/A19 | 63A | | 4.3.3.3 | 12 | 594 What is "digital information" defined as? just a few 1's and zeros? | please be more specific as to what "digital information" is defined as |
| MH/A20 | 63A | | 4.3.3.3 | 12 | 594 "that is cryptographically signed" should be much more specific as to the types of entity that may sign this and that the cry | perhaps: "The evidence includes digital information that contains at least one reference number that uniquely |
| MH/A21 | 63A | | 4.3.3.3 | 12 | 595 "The evidence includes physical security features" - this means that Superior evidence can not be digital is that what is m | If that is what is meant then that feels like something to be very explicit about and nearer the top of the list |

| | | | | | | |
|--------|-----|---------|----|----------|---|---|
| MH/A22 | 63A | 4.3.4.1 | 12 | 612 | "The authenticity and accuracy of identity evidence or attribute information that is cryptographically protected can be validated" | suggest: "...that is |
| MH/A23 | 63A | 4.1.3.4 | 13 | 613 | "The CSP SHALL use the public key of the issuing authority of the evidence to verify digitally signed evidence or attribute data" | suggest "Where a digital signature is used and the public key has been provided in a trustable manner the CSP SHALL use |
| MH/A24 | 63A | 4.3.4.2 | 13 | 617 | "All core attributes, whether obtained from identity evidence or applicant self-assertion, must be validated." - even at IAL2 | suggest "All core attributes, whether obtained from identity evidence or applicant self-assertion, |
| MH/A25 | 63A | 4.4.1 | 14 | 668 | "Remote (attended and unattended) physical facial image comparison" word physical is not required and is confusing | Remove word "physical" |
| MH/A26 | 63A | 4.4.1 | 14 | 669 | "CSP operator" does not seem to be defined anywhere - what is required for this role? IAL, AAL, FAL, training pre-employment | add definition for "CSP operator" |
| MH/A27 | 63A | 4.4.1 | 15 | 686 | "Control of a digital account. An individual is able to demonstrate control of a digital account (e.g., online bank account) or | Suggest splitting this bullet into two "control of digital account" and "control of signed digital assertion" |
| MH/A28 | 63A | 5.1 | 16 | 697 | "The requirements in this section apply to all CSPs performing identity proofing at any IAL." - does this include IAL0? | Suggest IAL 1 or above |
| MH/A29 | 63A | 5.1.2.1 | 18 | 770 | "The CSP SHALL make a summary of its privacy risk assessment available to any organizations that use its services. The summary | Add similar provision for applicants and subscribers? |
| MH/A30 | 63A | 5.1.2.2 | 18 | 776 | "The CSP MAY collect the Social Security Number (SSN) as an attribute when necessary for identity resolution, in accordance | Change this section to be about persistent identifiers like SSN (or NI number in the UK case) |
| MH/A31 | 63A | 5.1.4 | 20 | 824 | "SHALL occur over an authenticated protected channel." - no clear definition of what the requirements for "authenticated | be more specific about what risks need to be mitigated and how they might be mitigated as a secondary matter |
| MH/A32 | 63A | 5.1.4 | 20 | 826 | "All PII, in the form of identity attributes, collected as part of the identity proofing process SHALL be protected to ensure the | adjust the wording to be about "mitigating risks to confidentiality and integrity of the information" |
| MH/A33 | 63A | 5.1.6 | 21 | 868 | "The following requirements apply to all CSPs that employ enrollment codes at any IAL" - does this include IAL0? | Suggest IAL 1 or above |
| MH/A34 | 63A | 5.1.7 | 22 | 890 | "Notifications of proofing are sent to the applicant's validated address notifying them that they have been successfully identified | reword to reflect that it "reduces the risk of a fraudulently proofed digital identity persisting for a significant period of |
| MH/A35 | 63A | 5.1.8 | 23 | 948 | "CSPs SHALL make all performance and operational test results publicly available." - that is a very broad requirement that | Clarify scope of the "performance and operational" test results that need to be made publically available |
| MH/A36 | 63A | 5.1.8 | 23 | 951 | "CSP SHALL collect biometrics in such a way that ensures that the biometric is collected from the applicant, and not another | Suggest re-wording to say "significantly reduce risk that the biometric is not collected from a person other than the |
| MH/A37 | 63A | 5.1.9 | 24 | 977 | No definition of "applicant reference" | Add definition |
| MH/A38 | 63A | 5.1.9 | 24 | 988 | "The role of applicant reference is limited to facilitating the identity proofing process and applicant references are not used | Reword to make it clearer that the identity proofing process does not authorise the applicant reference |
| MH/A39 | 63A | 5.1.9.1 | 25 | 997 | Add requirement that the trusted referee should be assured to at least the same xAL as the applicant will be | |
| MH/A40 | 63A | 5.1.9.1 | 25 | 997 | Add requirement that the trusted referee should act in the best interests of the applicant | |
| MH/A41 | 63A | 5.1.9.1 | 25 | 1002 | Add requirement that the trusted referee should be trained in avoidance of conflicts of interest and ethics | |
| MH/A42 | 63A | 5.1.9.2 | 25 | 1004 | "CSPs SHOULD allow the use of applicant references." - in order to avoid exclusion of communities enhance this to "MUST" | |
| MH/A43 | 63A | 5.1.10 | 25 | 1019 | "When interacting with persons under the age of 13, the CSP SHALL ensure compliance with the Children's Online Privacy Protection | Extend this section to allow for other applicable laws |
| MH/A44 | 63A | 5.3.1 | 26 | 1049 | "The CSP SHALL implement a means to prevent automated attacks on the identity proofing process. Acceptable means include | reword to describe specific risks that need to be mitigated and probably the means from this document |
| MH/A45 | 63A | 5.4.1 | 28 | 1099 | same as comment MH/A44 | |
| MH/A46 | 63A | 5.4.2.1 | 28 | 1106 | "One piece of STRONG evidence and one piece of FAIR evidence" - this precludes two pieces of STRONG | reword to allow for both "One piece of STRONG evidence and one piece of FAIR evidence" and "Two pieces of STRONG |
| MH/A47 | 63A | 5.5.1 | 29 | 1151 | same as comment MH/A44 | |
| MH/A48 | 63A | 5.5.8 | 32 | 1232 | same comment as MH/A31 | |
| MH/A49 | 63A | 5.6 | 33 | Table 1B | For IAL1 and IAL2 columns "1 piece of SUPERIOR or 1 piece of STRONG plus 1 piece of FAIR" | change to |
| MH/A50 | 63A | 6.1 | 34 | 1238 | This paragraph structure should be inverted to state that subscriber accounts should only be created when... | suggest: |
| MH/A51 | 63A | 6.1 | 34 | 1254 | "All attributes that were validated during the identity proofing process or in subsequent transactions to support RP access" | Reword this to reflect that the subscriber should have the opportunity to choose to maintain fewer attributes in their |
| MH/A52 | 63A | 6.2 | 35 | 1270 | "The CSP SHALL provide the capability for subscribers to change or update the personal information contained in their subscriptions" | suggest: "The CSP SHALL provide the capability for subscribers to change or update or delete the personal |
| MH/A53 | 63A | 7 | 37 | Table 2S | "Opening a credit cards in a fake name to create a credit file." - what is the definition of a fake name? in the UK it is entirely | Suggest re-word from "Opening a credit cards in a fake name to create a credit file." to "Opening a credit card in a |
| MH/A54 | 63A | 7.2 | 39 | 1331 | "Where the CSP is external, this may be complicated, but should be considered in contractual and legal mechanisms" - add | suggest: "Where the CSP is external, this may be complicated, but should be considered in contractual and legal |
| MH/A55 | 63A | 8 | 40 | 1338 | Add a paragraph that states clearly up front that the risks and considerations in this section relate to risks to individual applicants | suggest add paragraph "These privacy considerations cover topics that are largely about risk to applicant and |
| MH/A56 | 63A | 8.1 | 40 | 1340 | "collection of only the PII necessary to validate the existence of the claimed identity and associate the claimed identity to the | resolve contradiction |
| MH/A57 | 63A | 8.1.1 | 40 | 1349 | essentially the same feedback as MH/A30 | |
| MH/A58 | 63A | 8.1.1 | 40 | 1357 | "limit the proliferation and exposure of SSNs during the identity proofing process" - really good to see this expressed but | move that phrase into section 8.1 "limit the proliferation |
| MH/A59 | 63A | 6.3.2 | 35 | 1293 | "in accordance with the record retention and disposal requirements" - are these defined somewhere, can they be referenced | clarify where these requirements are defined ideally with a link to some clearly defined requirements or to a document |

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

| | |
|------------------------------------|-------------------|
| Organization: | OpenID Foundation |
| Name of Submitter/POC: | Gail Hodges |
| Email Address of Submitter: | (REMOVED) |

| Comment # | Publication (Base, 63A, 63B, 63C) | Section | Page # | Line # | Comment (Include rationale for comment) | Suggested Change | |
|-----------|-----------------------------------|---------------------------------|--------|---------|---|---|---|
| NS/B01 | 63B | All | | | Currently, there are multiple SHALL, SHOULD, MAY etc. in one paragraph and is hard to refer to. Being able to refer to | Change all the sentence that include SHALL, SHOULD, MAY an independent numbered bullet as in Base 5.3. | |
| NS/B02 | 63B | 4.2.3.4.3.3 | | 9 | 552 Should the verifier be involved with timeout activity? | clarify role that holds such responsibility | |
| NS/B03 | 63B | 5.1.1.2 | | 14 | 684 Should "verifier" be the one requiring secret lengths since they only do verifying and not enrolling/binding of | Clarify entity responsible | |
| NS/B04 | 63B | 5.1.1.2 | | 14 | 684 Shouldn't CSP be responsible for enrolling authenticators and thus requirements for secret lengths, checking blocklists... | Clarify | |
| NS/B05 | 63B | | iii | 173 | phishing resistance is not defined | add definition for "Phishing resistant" | |
| NS/B07 | 63B | | 2 | 367-369 | "A successful authentication results in the assertion of a pseudonymous or non-pseudonymous identifier and optionally | A successful authentication results in the assertion of a pseudonymous or non-pseudonymous identifier to the relying | |
| NS/B08 | 63B | | 4 | 425 | "be authenticated" is passive form. Use active form. | A claimant SHALL authenticate with.... | |
| NS/B09 | 63B | | 4 | 426 | "The result of an authentication process is an identifier" - The result of an authentication process is an authenticated | | |
| NS/B10 | 63B | | 4 | 427 | "be used" is passive form. Use active form. | | |
| NS/B11 | 63B | | 4 | 428 | change "SHOULD NOT" | change "SHOULD NOT" to "SHALL NOT" otherwise, it will cause impersonation attack. | |
| NS/B12 | 63B | | 4 | 438 | "requires" | this should be edited to be a normative requirement | |
| NS/B13 | 63B | | 4.1 | 6 | 441 Authentication Assurance Level 1 - In what follows, it lists permitted authenticator terms as requirements. Instead, it | reword to describe threats that need to be mitigated | |
| NS/B14 | 63B | 4.1.2 | | 7 | 460 SHALL use approved cryptography | add a definition of what "approved cryptography" is | |
| NS/B15 | 63B | 4.1.2 | | 7 | 461 MAY - This is not specific enough to use normative terms | re-phrase to be more specific or remove normative wording | |
| NS/B16 | 63B | 4.1.2 | | 7 | 465 claimant and verifier SHALL be via an authenticated protected channel - Is that mutual authentication? P.45 of 63-4. It | clarify | |
| NS/B17 | 63B | 4.1.2 | | 7 | 467 adversary-in-the-middle (AiTM) attacks - these attacks are not necessarily mitigated by an "authenticated protected | Re-word to be more specific about countermeasures that can and SHOULD be implemented to mitigate AiTM attack | |
| NS/B18 | 63B | 4.1.3 | | 7 | 472 The text says, "SHOULD be repeated at least once per 30 days" and in 7.2 it presents the purpose of it as "(i.e., that the | Improve the consistency by modifying the text here or in 7.2 | |
| NS/B19 | 63B | 4.2.1 | | 8 | 507 "physical authenticator" is undefined. In -3, it used to be "possession-based" | change back to possession based or just use the expression "something you have" | |
| NS/B20 | 63B | 4.2.2 | | 9 | 540 one phishing-resistant authenticator option to public users at AAL2 - this wording should be improved to make it clearer | improve clarity of wording | |
| NS/B21 | 63B | 4.2.3 | | 9 | 547 Is there an evidence that "12 hours" is a good time period? | If so, please provide references. If not, then provide the justification behind it. | |
| NS/B22 | 63B | 4.2.3 | | 9 | 548 Is there an evidence that "30 minutes" is a good time period? | If so, please provide references. If not, then provide the justification behind it. | |
| NS/B23 | 63B | | 4.3 | 10 | 575 are required - Should that be a SHALL? SHALL IS specified later. | Reword to use "SHALL" | |
| NS/B24 | 63B | 4.3.2 | | 10 | 592 (related to 5.2.5). The text says phishing in this document used to be called "verifier impersonation." There is a question | If the text here is intended to discuss verifier impersonation, stick to it. | |
| NS/B25 | 63B | 4.3.2 | | 11 | 594 authentication intent - that is unclear and undefined | Define "authentication intent" or re-word to make the intent of this normative requirement | |
| NS/B26 | 63B | 4.4 | | 12 | 636-638 maintain predictability and manageability commensurate with the privacy risk arising from the additional processing. - | reword to make normative requirement clear and measurable | |
| NS/B27 | 63B | | 4.4 | 12 | 638 Why is "clear notice" MAY be included? | reword to help implementers decide when they should implement "clear notice" | |
| NS/B28 | 63B | | 4.4 | 12 | 653 Privacy Impact Assessment (PIA) - Should that be PIA Report? | reword to say "The agency SHALL publish a Privacy Impact Assessment (PIA) report...." | |
| NS/B29 | 63B | 4.5 Table 1. | | 13 | The last two rows, "Records Retention Policy" and "Privacy Controls" were removed in this version. | please note their removal and explain where those topics are covered or re-instate | |
| NS/B30 | 63B | 4.5 Table 1. | | 13 | Permitted authenticator types - Instead of listing the authenticator types, which may become vulnerable to a newly | reword to describe threats that need to be mitigated | |
| NS/B31 | 63B | 4.5 Table 1. Row1Col2 | | 13 | Make them comparable! - this table format in row on is very difficult to read and understand, a row per authenticator | Break out authenticator requirements into a separate table for readability reasons | |
| NS/B33 | 63B | 5.1.1.1 | | 14 | 684 It states "8 characters in length". Depending on what character sets are allowed, this could be extremely weak (e.g., 8 | Add the minimum requirements on the assumed character set. | |
| NS/B34 | 63B | 5.1.3.4 | | 23 | 933 A new type of authenticator, "Multi-Factor Out-of-Band Authenticators" is now introduced. However, this could be | Create a paragraph or Note on 5.1.3.1 explaining if the Out-of-Band Authenticator requires memorised or biometrics for | |
| NS/B35 | 63B | 5.1.6.1 | | 27 | 1080 The text around "External cryptographic authenticators" is new. Supposedly, it is talking about Passkeys. Then, it would | Change | |
| NCW/B01 | 63B | 5.1.6.2 | | 27 | 1086 Software verifiers should have more considerations by nature that software is more susceptible to attacks than | Suggest clarifying or providing a rationale for why security remains whether the verifier is software or hardware based | |
| NS/B36 | 63B | 5.1.7.1 | | 28 | 1109 Cryptographic device authenticators seems to be a new text compared to SP800-63-3. Here, "device" seems to mean | In the base document, define as follows. | |
| | | 5.1.8.1 | | 29 | 1154 External cryptographic authenticators does not seem to be defined. To explain a concept such as passkeys as the complement of an undefined set is not very readable. | Rewrite based on key-extraction resistance etc. | |
| | | | | | At the very least, saying in essence "a hardware authenticator form which secret key can be extracted is called software authenticator" is a stretch. It is much better to explain based on the capability, i.e., in this case, key-extraction resistant. | | |
| NS/B37 | 63B | | | | | | |
| | | 5.1.8.1 | | 29 | 1160 This paragraph talks about biometrics as an activation factor of which various requirements are set forth in 5.2.3. | When a biometric factor is made mandatory, then the system | |
| NS/B38 | 63B | | | | However, those requirements just covers the security and does not cover equity. Perhaps this is a good place to insert those requirements as they are not going to be purely biometric. | * SHALL allow multiple modes (e.g., fingerprint and facial) as forcing a single mode may alienate some population; and * SHOULD allow the use of combination of other mechanism that addresses the threats that the system seeks to | |
| NS/B39 | 63B | 5.1.9.1 | | 30 | 1198 Cryptographic device authenticators differ from cryptographic software authenticators etc. feels repetitive. It has already been discussed. Reduce the repetition. | Consider combining the text with 5.1.6.1 and point to it to reduce the repetition. | |
| NCW/B02 | 63B | 5.2.2 | | 31 | 1235 Is there quantitative data for why the number attempts may go to 100? Or perhaps better guidance is to provide a | also express the risk(s) that should be mitigated and how that risk should be quantified | |
| NS/B40 | 63B | 5.2.3 | | 33 | 1281 It changed in -4 to 1 in 10000 from 1 in 1000 in -3. If there is a specific evidence to support it, providing it will help the | Please make available the evidence as a NOTE: | |
| | | 5.2.3 | | | 1316-13 | "An authenticated protected channel between sensor (or an endpoint containing a sensor that resists sensor replacement) and verifier SHALL be established and the sensor or endpoint SHALL be authenticated prior to capturing the biometric sample from the claimant." <- This is a new text and looks good in theory. However, from a technology buyer's point of view, it may be difficult to test. It might be helpful to state some examples of certification. | Please add an example of the certification. |
| NS/B41 | 63B | | | | | | |
| NS/B42 | 63B | 5.2.5 | | 34 | 1342 Phishing (Verifier Impersonation) Resistance - Phishing is larger than verifier impersonation | reword to express that this section covers both topics fully and have sub-sections to cover any particular requirements | |
| NS/B43 | 63B | 5.2.5 | | 34 | The text is a hanging paragraph | | |
| NS/B44 | 63B | 5.2.5 | | 34 | 1348-13 Add definition of "Phishing resistance" | phishing resistance is the ability of the authentication protocol to detect and prevent disclosure of authentication secrets | |
| NS/B45 | 63B | 5.2.5 | | 35 | 1351 "relying party" - Our understanding is that the verifier interacts with the IDP (AND RP in the case of FAL3) - Is this an | Please re-word this section to make it clear what is meant by "relying party" or replace that term | |
| NS/B46 | 63B | 5.2.9 | | 37 | 1437 Authentication Intent - Refer to 63-4 definition. | Add reference to 800-63-4 base definition | |
| NS/B47 | 63B | 5.2.10 | | 38 | 1461-14 The use of a restricted authenticator requires that the implementing organization assess, understand, and accept the | Rework and potentially update definition of "restricted (authenticator)" | |
| NS/B48 | 63B | 5.2.11 | | 38 | 1480 The first sentence of 5.2.11 is a definition of a term "Activation Secrets" which is not in the Base document. | In the base document, define Activation Secret as "Memorized secrets that are used as an activation factor for a multi- | |
| NS/B49 | 63B | 5.2.12 | | 39 | 1508 Connected Authenticators is a new term. | Please define in the Base document. | |
| NS/B50 | 63B | | 6.1 | 41 | 1568 What does "These guidelines" refer to? | clarify please | |
| NS/B51 | 63B | 6.1.1 | | 42 | 1598 It looks like a CSP is required to bind at least one physical authenticator, ruling out the possibility of just having | Please change either of them and make the document consistent. | |
| NS/B54 | 63B | | 7.1 | 49 | 1850-18 SHOULD be erased on the subscriber | Make into numbered list (text seems to have only 2 items) | |
| NS/B55 | 63B | | 8 | 52 | 1916 Threats and Security Considerations | The attacker model should be specified. | |
| NS/B56 | 63B | | 8.1 | 52 | 1936 This document assumes that the subscriber is not colluding with an attacker - This assumption is false in many cases. | remove that whole document assumption and express threats that exist in that case | |
| NS/B57 | 63B | 8.1 Table 3 | | 52 | 1940 Authenticator Threats - Authentication Fatigue attack is missing. Authenticator Download attack. Where are threats to | Add to threat model consideration of threats to all potential constituencies or stakeholders in a digital identity | |
| NS/B58 | 63B | 8.1 Table 3 row 1 col 1 | | 52 | Assertion Manufacture or Modification - Is it related to Authenticator? | This should be expressed in the threat and security considerations section of 800-63C-4 | |
| NS/B59 | 63B | 8.1 Table 3 page 54 row 2 col 1 | | 54 | "Phishing" - Verifier impersonation probably is a better term. Phishing may take a form of credential duplication e.g., | reword to change "phishing" to "verifier impersonation" | |
| NS/B60 | 63B | 8.1 Table 3 page 54 row 5 col 2 | | 54 | subscriber - What about Mitnik Attack? | Add row to table to describe "mitnik attack" or generalised version of | |
| NS/B61 | 63B | 8.1 Table 3 page 54 row 8 col 1 | | 54 | Online Guessing - Is that an authentication threat? | Review and improve threat modelling | |

| | | | | | | |
|--------|-----|----------------------------------|----|------|---|--|
| NS/B62 | 63B | 8.1 Table 3 page 55 row 2 col 1 | 55 | | Endpoint Compromise - Is that an authentication threat | Review and improve threat modelling |
| NS/B63 | 63B | 8.1 Table 3 page 55 row 6 col 1 | 55 | | Unauthorized Binding - It may be included in this, but perhaps it is probably talking about binding without the | Review and improve threat modelling |
| NS/B64 | 63B | 8.2 Table 4 page 55 row 10 col 2 | 56 | | Use authenticators that provide phishing resistance. | clarify phishing resistance as per comment NS/B44 |
| NS/B66 | 63B | 8.1 | 57 | 1945 | Several other strategies may be applied to mitigate the threats described in Table 3 - why not include in Table 3? | Review and improve threat mitigation strategies |
| | | | | | | |
| MH/B01 | 63B | | 4 | 6 | 426 "The result of an authentication process is an identifier that SHALL be used each time that subscriber authenticates to | Reword this section to reflect that it is not a direct requirement that the identifier arising from authentication is passed |
| MH/B02 | 63B | 4.2.2 | 9 | 542 | "While phishing resistance as described in Sec. 5.2.5 is not generally required for authentication at AAL2, verifiers | Suggest "While phishing resistance as described in Sec. 5.2.5 is not generally required for authentication at AAL2, |

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

| | |
|--------------------------------------|-------------------|
| Organization: | OpenID Foundation |
| Name of Submitter/POC: | Gail Hodges |
| Email Address of Submitter/PC | [REMOVED] |

| Comment # | Publication (Base, 63A, 63B, 63C) | Section | Page # | Line # | Comment (Include rationale for comment) | Suggested Change | | |
|-----------|--------------------------------------|-------------|-------------|--------|--|--|--|---|
| NS/C01 | 63C | All | | | Currently, there are multiple SHALL, SHOULD, MAY etc. in one paragraph and is hard to refer to. Being able to refer to | Change all the sentence that include SHALL, SHOULD, MAY an independent numbered bullet as in Base 5.3. | | |
| NS/C02 | 63C | | | | The term "approved cryptography shall be used" is not very specific. | Reference approved cryptography standards | | |
| NS/C03 | 63C | | | 1897 | AccountChooser is no longer in use | Remove reference or describe similar example | | |
| NS/C04 | 63C | 4 - Table 1 | | 453 | Shouldn't injection protection be required even in FAL1? | Double check if it is appropriate. | | |
| NS/C05 | 63C | | 2 | 3 | Issued by the CSP - Not necessarily "issued". It may have been issued by somebody else including the subscriber and | Change to "registered to" | | |
| NS/C06 | 63C | | 2 | 4 | "Additional attributes collected..." - It should also mention the references to external sources. Also, consider introducing | in the fourth bullet, insert "by itself or through Attribute Providers" after "collected". | | |
| NS/C07 | 63C | | 2 | 4 | RP subscriber account is not defined. Also, RP not only often but most of the time maintains an account. | Change "often" to "usually". Define RP Subscriber Account in the base document. | | |
| NS/C08 | 63C | | 2 | 4 | disclosed to the RP by the IDP - clarify that RP could obtain attributes from other sources. | Rewrite to clarify. | | |
| NS/C09 | 63C | | 2 | 4 | 393-394 | "Authentication between the subscriber and the IDP will be based on the | Rewrite | |
| NS/C10 | 63C | | 2 | 4 | 403 | Assertion Presentation - It is a bit weird that we only have presentation. Presentation should be tightly coupled with the | Change it to Assertion Request and Presentation. Add new 7.1. Back-Channel Request, 7.2. Front-Channel Request. | |
| NS/C11 | 63C | | 4 | 6 | 439 | Would "Trust Agreement" include Web PKI? | Please clarify | |
| NS/C12 | 63C | | 4 | 6 | 440 | "The IDP and RP have agreed" sounds like Trust Agreement is always bilateral. This probably is not true and multi-lateral | Amend to read as "Agreement among IDPs and RPs to participate ..." | |
| NS/C13 | 63C | | 4 | 7 | 448 | a bound authenticator - Does it really have to be bound to authenticator? e.g., (while not available today) if the assertion | Consider the possibility and if it is appropriate, make a room for it. | |
| NS/C14 | 63C | | 4 | 7 | 448 | It is weird that it only talks about Presentation. A cryptographic authentication protocol can only be assessed as one set | Add them to the list, or consider creating a security model with different attacker capability to define the levels. | |
| NS/C15 | 63C | 4 Table 1 | | 7 | 453 | Where did cryptographic ... and Audience restriction gone? | It probably is omitted because they are always required. However, it is better to include them for the completeness. | |
| NS/C16 | 63C | 4 Table 1 | | 7 | 453 | Dynamic or Static - Dynamic and Static needs clarification. Would statically registered IDP to one of the Italian | Clarify. | |
| NS/C17 | 63C | | 4 | 7 | 468 | audience-restricted to a specific RP or set of RPs - This pretty much excludes VCs unless they were dynamically minted - | Clarify. | |
| NS/C18 | 63C | | 4 | 7 | 471 | a signature and key using approved cryptography - Does not parse well. "signatures using approved cryptography and | Change to "signatures using approved cryptography and appropriately managed keys" | |
| NS/C19 | 63C | | 4 | 1 | 8 | 485-487 | It states "OpenID Connect Implicit Client profile [OIDC-Implicit], the OpenID Connect Hybrid Client profile in [OIDC]" This | Include code flow as well. |
| NS/C20 | 63C | | 4 | 1 | 8 | 487 | SAML Web SSO - Why not differentiate Artifact and Post binding? | Differentiate them to be in parallel with OIDC. |
| NS/C21 | 63C | | 4 | 2 | 8 | 493 | "strongly protected" is undefined unless an attacker capability assumptions are stated and thus is not testable although | Defined "strongly protected" so that the compliance to the requirement become testable. It probably include some |
| NS/C22 | 63C | | 4 | 2 | 8 | 495-496 | It specifies OpenID Connect Basic Client profile [OIDC-Basic] and disallows Hybrid. Actually, Hybrid Client Profile which is | Add hybrid. And for that matter, FAPI 1.0 Advanced profile might also be considered. |
| NS/C23 | 63C | | 4 | 2 | 8 | 497 | using a single-use assertion reference - The effect of a single-use assertion reference being injected is more-or-less the | Add those requirements. Note that OIDC Hybrid, FAPI 1.0 Advanced are the profile of OpenID Connect that are formally |
| NS/C24 | 63C | | 4 | 2 | 8 | 499 | additional injection protections - Check if "exp" is discussed. | suggest a definition of "injection protections" and addition of "expiry" as one of the possible mitigations |
| NS/C25 | 63C | | 4 | 2 | 8 | 502 | requiring that the federation transaction start at the RP - It actually should always be the case. Otherwise, it would be | Consider re-wording this to preclude IDP initiated flows |
| NS/C26 | 63C | | 4 | 2 | 8 | 505 | established statically - Looks like dynamic client registration at an IDP where they belong to a same federation operator | suggest wording more clearly about what is within scope of a "trust agreement" and what is "registration" |
| NS/C27 | 63C | | 4 | 3 | 9 | 519 | presenting an authenticator - Subscriber does not present authenticator. It may present the data generated by | suggest definition of an "established trust agreement" |
| NS/C28 | 63C | | 4 | 3 | 9 | 521 | bound authenticator - This probably comes from UAF but is not a generally accepted term and is confusing readers. The | Reward to more accurately reflect what is happening where subscriber is a natural person who is acting through a "user- |
| NS/C29 | 63C | | 4 | 3 | 9 | 534 | MAY - change to SHOULD from the PoV of data minimization | Consider re-wording using a different term that is more widely accepted and understood |
| NS/C30 | 63C | | 4 | 4 | 9 | 540 | Requesting and Processing XALS: The concept of telling each XAL in the response looks good on surface, however, if FAL is | change "MAY" to "SHOULD" |
| NS/C31 | 63C | | 5 | 12 | 590 | In a federation protocol, a three-party relationship is formed - What about four parties? | Consider rewording the requirement that IAL AAL and FAL are required for each federated transaction. They might not | |
| NS/C32 | 63C | 5 Fig 1 | | 12 | | Schematics of arrows unclear. UA is an important actor but it is replaced with users, which is not good. | Explain the diagram scheme, e.g., what does solid arrow means, what does dotted arrow mean, what are the meaning | |
| NS/C33 | 63C | | 5.1 | 13 | 630 | How is the population of subscriber accounts defined? | Clarify this bullet point | |
| NS/C34 | 63C | | 5.1 | 14 | 633-634 | The authorized party responsible for decisions regarding the release of subscriber attributes. Consumer protection in this | | |
| NS/C37 | 63C | | 5.1.3 | 17 | 735-739 | Common configurations include: ... - Add Wallets to the list as an example as well | If "federation" includes "decentralised" or "wallet" based solutions add one or more configurations. If not then clarify | |
| NS/C38 | 63C | | 5.2.2 | 20 | 790 | Dynamic Registration - Now that we are using "Static and Dynamic", perhaps "Dynamic Registration" need to be | Propose change the name of "Dynamic Registration" in order to avoid confusion with "RFC 7591 - Dynamic Client | |
| NS/C39 | 63C | | 5.3 | 21 | 829-83- | identity federation transactions - define the term | propose addition of definition of "identity federation transactions" as it is unclear at present | |
| NS/C40 | 63C | | 5.3 | 21 | 831-832 | A subscriber's attributes are not to be transmitted for any other purposes, even when parties are allowlisted. - Why is it | Consider explaining what risk is being mitigated by this requirement | |
| NS/C41 | 63C | | 5.3.3 | 22 | 874 | an authorized party identified by the trust agreement - check the definition of "authorized party" | propose adding a definition of "authorized party" | |
| NS/C42 | 63C | | 5.4.1 | 27 | 995-996 | allowing the RP to be more simplified with less internal state - A bigger use-case is the attribute-based authorization to | Propose adding an additional use case under "Ephemeral" where a persistent identifier is not needed by the RP and is | |
| NS/C43 | 63C | | 5.4.2 | 27 | 1012-1013 | From the RP's perspective, the IDP is the authoritative source for any attributes that the IDP asserts as being associated | re-word the paragraph to state that the RP may or may not, at its own discretion, consider attributes provided by the | |
| NS/C44 | 63C | | 5.4.2 | 28 | 1018-1019 | The IDP SHOULD signal downstream RPs when the attributes of a subscriber account available to the RP have been | | |
| NS/C45 | 63C | | | | 1026 | Requiring RP account termination is too intrusive. Account may be linked to multiple IDPs. It may as well go against | Expand on account lifecycle management or refer to standard on account lifecycle management | |
| NS/C46 | 63C | | | | 1062 | Requiring RP account termination is too intrusive. Account may be linked to multiple IDPs. It may as well go against | Expand on account lifecycle management or refer to standard on account lifecycle management | |
| NS/C47 | 63C | | | | 1127 | Requiring RP account termination is too intrusive. Account may be linked to multiple IDPs. It may as well go against | Expand on account lifecycle management or refer to standard on account lifecycle management | |
| NS/C49 | 63C | | 5.6 | 31 | 1161 | MAY - This sentence seems to be a best practice though it has not been implemented widely due to technical difficulty. | Propose change to "IDP SHOULD communicate ... if possible" | |
| NS/C50 | 63C | | 6 | 35 | 1259-1262 | Key binding was dropped. In -3, there was Key binding. | Please provide the reasons. | |
| NS/C51 | 63C | | 6 | 45 | 1269 | Signature validation - verification and validation should be defined. | More specific requirements should be defined particularly around signature validation, either in this document or v | |
| NS/C52 | 63C | | 6.1 | 36 | 1301 | Assertion Binding - This probably caused a new title "Bound Authenticators" which used to be HoK Assertions. The title of | | |
| NS/C53 | 63C | | 6.2.2 | 43 | 1449 | MAC - Is a MAC a signature? | propose an edit to make explicit what is meant here | |
| NS/C54 | 63C | | 6.2.5.2 | 45 | 1512 | identifying information - This is not well defined. From one point of view, a PPID is an identifying information of a sort. | propose re-word to clarify this question and consider reference to ISO spec | |
| NS/C55 | 63C | | 6.2.5.2 | 45 | 1518 | one pair of endpoints(e.g. IDP-RP) - IDP and RP are not endpoints. "One pair of entities" may be more accurate. Also, it is | Propose re-word to address issues described | |
| NS/C56 | 63C | | 6.3 | 46 | 1561 | Access to the identity API SHALL be time limited. - Are you sure? | Reward to permit persistent access if there is agreement from the authorizing party and it is necessary | |
| NS/C57 | 63C | | 6.3.1 | 46 | 1575 | A model including Attribute Providers as actors should be introduced perhaps near the beginning of the document. It forms | Instead of adding Attribute provider here, present the generalized model early on. | |
| NS/C59 | 63C | | 7.1 | 49 | 1646 | The commenter, who happens to be an author of RFC7636, is not quite sure if using RFC7636 only would really protect | Use the provided examples instead. | |
| NS/C60 | 63C | | 7.2 | 52 | 1672 | Cross-site script protection and CSRF protection is always needed. At the same time, they do not necessarily protect | Those set of known safe combinations probably should be given at least as an example. | |
| NS/C58 | 63C | | 8.1 Table 2 | 53 | | This is quite incomplete. A protocol used for federation should be formally verified instead of being tested against ad-hoc | Propose creating a separate document that is focussed on a thorough description of how threat modelling should be | |
| NS/C61 | 63C | | | 67 | 2112 | "Normative requirements have been established..." - Where are normative requirements specified for Equity? | Please define normative requirements in this section or provide links to other parts of this document set where | |
| MH/C01 | 63C | Abstract | | 112 | | Note that this document "focuses on the use of federated identity and the use of assertions to implement identity | Clarify whether the intent is to include "decentralised", "ssi" or "wallet" based solutions in the scope of "federation, and | |
| MH/C02 | 63C | | 1 | 2 | 330 | "This document, SP 800-63C, provides requirements to identity providers (IDPs) and | Re-word "purpose" and/or change content of document to match | |
| MH/C03 | 63C | | 2 | 3 | 241 | "The RP receives the assertion provided by the IDP | suggest ""The RP receives the assertion provided by the IDP | |
| MH/C04 | 63C | | 2 | 3 | 347 | "The RP uses the information | Suggest "The RP cause the information in the assertion to identify the subscriber and make decisions about their | |
| MH/C05 | 63C | | 2 | 3 | 364 | "An assertion includes a federated identifier for the subscriber, allowing association of | "An assertion includes a federated identifier for the subscriber. When using a non-ephemeral identifier this allows | |
| MH/C06 | 63C | | 2 | 4 | 374 | "When evaluating a particular federation structure, it may be instructive to break it down into its component | suggest: "When evaluating a particular federation structure, it may be instructive to break it down into its component | |
| MH/C07 | 63C | | 2 | 4 | 395 | it is not a table | suggest converting it to a table or modifying text to say "list" | |
| MH/C08 | 63C | | 4 | 6 | 414 | "This section defines allowable federation assurance levels (FALS)." - wording is not terribly clear | suggest "This section defines the set of NIST 800-63 federation assurance levels (FALS)." | |
| MH/C09 | 63C | | 4 | 7 | 458 | "Examples of assertions used in federated protocols include the ID Token in OpenID Connect | suggest: "Examples of assertions used in federated protocols include the ID Token in OpenID Connect | |

| | | | | | | | |
|--------|-----|---------|-----|-------------|---|--|---|
| MH/C10 | 63C | | 4.2 | 8 | 499 | "If front channel presentation is | Specify the additional protections needed |
| MH/C11 | 63C | | 4.2 | 8 | 501 | "Regardless of the presentation method used, injection attacks can be further mitigated by | suggest replacement of "can" with "SHALL" to read: Regardless of the presentation method used, injection attacks SHALL |
| MH/C12 | 63C | | 4.2 | 9 | 513 | this paragraph could be made more widely applicable | suggest "IDPs asserting FAL2 SHALL protect keys used |
| MH/C13 | 63C | | 4.3 | 9 | 532 | "At FAL3, the trust agreement and registration between the IdP and RP SHALL be | Reword to allow for dynamic and automated key rotation "with appropriate supporting controls |
| MH/C14 | 63C | | 4.4 | 9 | 540 | "Requesting and Processing xALs" - paragraph about requesting xALs is important and buried deep within this section | suggest move the paragraph about requesting xALs to the top of this section to improve readability |
| MH/C15 | 63C | | 4.4 | 9 | 544 | "The RP SHALL be informed of the following information for each federated transaction" - this is highly likely to be un- | Suggest moderation of this language to use "MAY" |
| MH/C16 | 63C | | 4.4 | 10 | 569 | "In a federation process, only the IdP has direct access to the details of the subscriber | suggest adding a clause to moderate this that says "... unless the IDP has passed metadata about IAL or AAL to the RP to |
| MH/C17 | 63C | | 4.4 | 10 | 574 | "The RP SHALL ensure that the federation transaction meets the requirements of the FAL | suggest reword to say: "The RP SHALL ensure that it meets all of its obligations described in the requirements of the FAL |
| MH/C18 | 63C | | 5 | 12 | 590 | "In a federation protocol, a three-party relationship is formed between the subscriber, the | permit a wider range of federation architectures and describe each of them and the corresponding requirements that are |
| MH/C19 | 63C | | 5 | 13 | 599 | "Next, the IdP and RP perform registration to establish their trust at a protocol level." - this is mixing trust, registration | suggest reword to "Next, the IdP and RP perform registration to integrate at a protocol level," |
| MH/C20 | 63C | | 5 | 13 | 607 | "Next, the IdP and RP determine that they want to engage in a federated | suggest "Next, the IdP and RP determine that they want to engage in a federated |
| MH/C21 | 63C | | 5 | 13 | 611 | "The decision made in this step builds on the | suggest "The decision made in this step builds on the |
| MH/C22 | 63C | | 5 | 13 | 612 | "Finally, the subscriber authenticates to the IdP and the result of that authentication | suggest splitting this list item: |
| MH/C23 | 63C | | 5.1 | 14 | 659 | "Disclosure of attributes in dynamic trust agreements SHALL be subject to a | clarify the intent behind this requirement or remove it |
| MH/C24 | 63C | 5.1.1 | 15 | 698 | "The RP SHALL disclose its list of required attributes to the IdP, including its purpose for | suggest "The RP SHALL disclose its list of required attributes across all cases to the IdP" | |
| MH/C25 | 63C | 5.1.3 | 17 | 747 | "Proxies can also mitigate some of the privacy risks described in Sec. 5.5 below." - this implies there are no downsides to | suggest: "Proxies can mitigate some of the privacy risks described in Sec. 5.5 below to other risks arise due to there | |
| MH/C26 | 63C | 5.1.3 | 18 | 754 | "Likewise if a federation takes in an assertion at FAL1 but presents a | suggest: "Likewise if a federation takes in an assertion at FAL1 IT SHOULD NOT be presented downstream at a higher | |
| MH/C27 | 63C | 5.2.1 | 19 | 773 | "In the manual registration model, the operators of the IdP and RP manually provision | suggest "In the manual registration model, the operators of the IdP and RP each provision | |
| MH/C28 | 63C | 5.2.1 | 19 | 781 | "The IdP and RP then communicate using a standard federation protocol" - "standard" is not defined and is an un- | suggest "The IdP and RP then communicate using a federation protocol" | |
| MH/C29 | 63C | 5.2.2 | 20 | 803 | "Register RP attributes. The RP sends its attributes to the IdP, and the IdP associates | suggest: "Register RP attributes. The RP makes its attributes available to the IdP, and the IdP associates | |
| MH/C30 | 63C | 5.2.2 | 21 | 811 | "IDPs SHOULD issue pairwise pseudonymous subject identifiers to dynamically registered | suggest: "IDPs SHOULD consider the risks of issuing assertions to dynamically registered | |
| MH/C31 | 63C | 5.2.2 | 21 | 815 | "Software statements are lists of attributes describing the | suggest: "Software statements are lists of attributes describing a federation participant's software (IDP, RP, etc), | |
| MH/C32 | 63C | 5.3.3 | 24 | 952 | "An authenticated session SHALL be created by the RP only when the RP has processed | suggest: "An authenticated session SHALL only be created by the RP once the RP has processed | |
| MH/C33 | 63C | 5.4.1 | 27 | 1004 | "All organizations SHALL document their provisioning model as part of their trust | suggest: "All organizations SHALL document their provisioning models as part of their trust | |
| MH/C34 | 63C | 5.4.2 | 28 | 1018 | "The IdP SHOULD signal downstream RPs when the attributes of a subscriber account | suggest: "The IdP SHOULD signal downstream RPs when the attributes of a subscriber account | |
| MH/C35 | 63C | 5.4.2 | 28 | 1026 | "Upon receiving such a signal, the RP SHALL terminate the RP subscriber | suggest: "Upon receiving such a signal, the RP MAY choose to terminate the RP subscriber | |
| MH/C36 | 63C | 5.4.3 | 28 | 1039 | "The attributes in the provisioning API available to a given RP SHALL be limited to | suggest: "The attributes in the provisioning API available to a given RP SHALL be limited to | |
| MH/C37 | 63C | 5.4.3 | 28 | 1049 | "A provisioning API SHALL NOT be made available under a dynamic or implicit trust | suggest: "A provisioning API SHALL NOT be made available under a dynamic or implicit trust | |
| MH/C38 | 63C | 5.4.3 | 29 | 1058 | "External attribute providers MAY be used as information sources" - external attribute providers should e defined. Also | Add definition for "External Attribute Providers" | |
| MH/C39 | 63C | 5.4.3 | 29 | 1061 | "When a provisioning API is in use, the IdP SHALL signal to the RP when a subscriber | suggest: "When receiving such a signal, the RP MAY choose to terminate the | |
| MH/C40 | 63C | 5.4.4 | 29 | 1067 | "All attributes associated with an | suggest better definition of "associated with" | |
| MH/C41 | 63C | 5.4.4 | 29 | 1070 - 1077 | These two paragraphs have clearly stepped into data protection domain and that is not in scope of this document. These | Delete these paragraphs | |
| MH/C42 | 63C | 5.5 | 30 | 1091 | This section on privacy overlaps with section 9 - Also this covers matters that are already governed in certain jurisdictions | Avoid defining privacy requirements in this document as they are likely to be incomplete and my also conflict with other | |
| MH/C43 | 63C | 5.5 | 30 | 1114 | Comment MH/C42 notwithstanding, there are Normative requirements (SHALL) without a closed list of specific technical | Either remove the normative language or define a specific list of "technical measures" | |
| MH/C44 | 63C | 5.5 | 30 | 1126 | Comment MH/C42 notwithstanding, "RPs that receive such a signal from the IdP SHALL | suggest: "RPs that receive such a signal from the IdP MAY | |
| MH/C45 | 63C | 5.5 | 31 | 1146 | "As a consequence, when a provisioning API is | suggest that: | |
| MH/C46 | 63C | 5.6 | 31 | 1162 | "The RP and | suggest: "The RP and | |
| MH/C47 | 63C | 5.7 | 32 | 1194 | "Signaling from the IdP to the RP SHALL require a static trust agreement." - this seems an un-necessary requirement- the | suggest: "Signaling from the IdP to the RP SHALL require a static trust agreement or countermeasures that mitigate risk | |
| MH/C48 | 63C | 6 | 34 | 1217 | "An assertion used for authentication is a packaged set of attribute values or derived attribute values about or associated | suggest: "An assertion is a packaged set of attribute values or derived attribute values about or associated with an | |
| MH/C49 | 63C | 6 | 34 | 1223 | "While the assertion's primary function is to authenticate the user to an RP, the information conveyed in the assertion | suggest delete "While the assertion's primary function is to authenticate the user to an RP," leaving "The information | |
| MH/C50 | 63C | 6 | 34 | 1234 | "Audience identifier: An identifier for the party intended to consume the assertion | suggest: "Audience: An identifier or list of identifiers for the parties intended to consume the assertion | |
| MH/C51 | 63C | 6 | 34 | 1249 | It is possible that an RP does not have any need of the IAL for their use case so in the spirit of data minimisation this | suggest move item 9 and 10 to the list of additional items at line1260 | |
| MH/C52 | 63C | 6 | 35 | 1251 | "FAL: An indicator of the IdP's intended FAL of the federation process represented by the assertion" - This is not an | In OpenID Connect for Identity Assurance there is a structure that helps with issues such as this and permits identity | |
| MH/C53 | 63C | 6 | 35 | 1253 | "If the assertion is used at FAL3 with a bound authenticator..." - wording could be improved | suggest "If the Federation Assurance Level is FAL3 then a bound authenticator is required as described in Sec. 6.1.2. | |
| MH/C54 | 63C | 6 | 35 | 1263 | "Assertions SHOULD specify the AAL when an authentication event is being asserted and | resolve contradiction | |
| MH/C55 | 63C | 6 | 35 | 1266 | "All metadata within the assertion SHALL be validated by the RP upon receipt" - this is not sufficiently constrained. | Suggest changing this to: "All the following metadata attributes within the assertion SHALL be validated by the RP upon | |
| MH/C56 | 63C | 6 | 35 | 1283 | "Although details vary based on the exact federation protocol in use, an assertion | suggest: "Although details vary based on the exact federation protocol in use, the validity time window of an assertion is | |
| MH/C57 | 63C | 6 | 36 | 1282 - 1300 | these paragraphs are very duplicative of content in section 5.6 and should be truncated or deleted al together | suggest truncate or delete these paragraphs | |
| MH/C58 | 63C | 6.1.2 | 36 | 1319 | "A bound authenticator is an authenticator presented to the RP by the subscriber alongside the assertion." - in reality it is | suggest: "Evidence of a bound authenticator is presented to the RP alongside the assertion."" | |
| MH/C59 | 63C | 6.1.2.1 | 37 | 1350 | This mechanism for bound authenticator would e great for tracking the user but really quite bad from an end-user privacy | consider highlighting this draw back | |
| MH/C60 | 63C | 6.1.2.1 | 38 | Figure 9 | This is a niev diagram of the interactions and the Subscriber does not usually interact directly and almost always will | Modify diagram to represent user agent as key participant | |
| MH/C61 | 63C | 6.1.2.2 | 40 | 1394 | "Upon successful authentication, the RP SHALL immediately prompt the | suggest: "Upon successful authentication, the RP SHALL immediately prompt the | |
| MH/C62 | 63C | 6.1.2.2 | 44 | 1494 | "they could still determine that the subscriber is the same person by comparing the name, email address, physical | suggest: "they could still determine | |
| MH/C63 | 63C | 7.3 | 52 | 1678 | While it is good that it is mentioned it is disappointing that "Protecting information" is not mentioned much earlier in the | Suggest introducing the topic of protecting information much earlier in the document | |
| MH/C64 | 63C | 7.3 | 52 | 1692 | "The RP SHALL, where feasible, request derived attribute values rather than full attribute | | |
| MH/C65 | 63C | 9.2 | 57 | 1779 | This paragraph is worded in such a way as to be very difficult tin understand | Reword to make the point more clearly | |
| MH/C66 | 63C | 9.3 | 58 | 1804 | For information - The OpenID Foundation has an early draft underway that allows for expression of data minimisation | | |
| MH/C67 | 63C | 9.5 | 59 | 1841 | "A proxy-based system has three parties" - depending which types you count a classic non-proxy federation has 4 parties | Define what parties are meant and why others are not counted | |