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

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

| | |
|---|---|
| ***Organization:*** | *The Digital Chamber* |
| ***Name of Submitter/POC:*** | *Jonathan Rufrano and Jean-Philippe Beaudet* |
| ***Email Address of Submitter/POC:*** | [redacted] |

| Comment # | Publication (Base, 63A, 63B, 63C) | Section | Page # | Line # | Comment (Include rationale for comment) | Suggested Change |
|---|---|---|---|---|---|---|
| 1 | Base | 2.2.1 | 12 | 683-684 | We strongly support the inclusion of general purpose and subscriber-controlled wallets as a standard option in these guidelines. | |
| 2 | Base | 2.4 | 15 | 775-778 | We applaud NIST for recognizing and stating the importance of data minimization and allowing the use of pseudonymous identifiers and derived attribute values. | |
| 3 | Base | 3 | 23 | 982-984 | Would it not be appropriate to also make the DIAS available to the subscriber? | Make DIAS available to subscriber as well. |
| 4 | Base | 3.1 | 27 | 1078-1079 | We believe the addition of this disclaimer requirement for RPs is appropriate, and will help subscribers better understand how their data is being handled and what rights they have. | |
| 5 | Base | 3.4.4 | 44 | 1652 | Would it not be appropriate to also make the DIAS available to the subscriber? | Make DIAS available to subscriber as well. |
| 6 | Base | 3.6 | 49 | 1769 | We believe the inclusion of a dedicated function to handle redress issues is critical in any identity system, especially in digital identity systems that have higher levels of automation. | |
| 7 | Base | 3.6 | 49 | 1783-1784 | This provision requiring tracing and tracking of redress issue data is a threat vector for cybersecurity and privacy issues. | Recognizing that data collection and analysis is beneficial to system improvements and that collection of such data is a significant threat vector to user privacy and system cybersecurity, we suggest this data should be either anonymized, aggregated, and encrypted. |
| 8 | Base | 3.6 | 50 | 1809-1811 | We appreciate NIST's guidance to minimize data in this arena. | |
| 9 | Base | 3.8 | 51 | 1830-1834 | We applaud NIST for including this provision. It is paramount that the use of AI/ML in identity processes is fully transparent and auditable. This allows not only understanding of potential equity and privacy issues, but also allows for steps to be taken to remedy them. | We suggest adding specific methods of sharing this data, and would value seeing this data posted on a public, immutable, trusted ledger when possible so as to garner greater public trust and create a verified source of truth. This verified source of truth is especially important as AI/ML systems are creating an explosion of fake data and narratives. |
| 10 | Base | 3.8 | 51 | 1830-1834 | We strongly support the inclusion of such strong AI/ML model transparency requirements, especially as it comes to digital identity. We applaud NIST and would hope federal agencies follow this normative guidance for non-identity systems as well. | |
| 11 | 63A | 2.5.1 | 14 | 775-818 | As remote unattended identity verification use cases are growing in number, we believe it would be wise to create a discrete section for this, instead of sequestering this method to in an example in the last sentence in the Authentication and Federation Protocols bullet. | Create a discrete section for remote unattended identity verification methods. |
| 12 | 63A | 3.1.3.1 | 21 | 1008-1010 | We applaud NIST for creating normative risk assessments requirements around non-PII data risks. | |
| 13 | 63A | 3.1.3.1 | 21 | 1012-1017 | We applaud NIST for creating normative requirements on creation, mitigation, and documentation of privacy risks associated with identity proofing and enrollment. | |
| 14 | 63A | 3.1.3.1 | 22 | 1023-1025 | It is unclear why summaries of privacy risk assessments would not be available to subscribers as well. | Require privacy risk assessments to be available to subscribers as well. |
| 15 | 63A | 3.1.3.2 | 22 | 1033-1035 | We support the normative requirements of training in privacy policies for all individuals and entities that have access to PII gathered or retained by the CSPs. | |
| 16 | 63A | 3.1.3.2 | 22 | 1046-1052 | We believe this section is suited for additional user data protections. | Amend "and the details of any records retention requirement if one is in place" to "and the details of any records retention requirement if one is in place, including applicant's right to request data deletion or engage in other forms of redress." |
| 17 | 63A | 3.1.4 | 23 | 1075-1077 | We applaud NIST for including equity considerations so prominently in the ID proofing process, as intentional or unintentional bias in these processes is a present risk, and the outcomes are potentially damaging. | |
| 18 | 63A | 3.1.7 | 24 | 1116-1118 | We are concerned that not all federal agencies have Senior Agency Officials for Privacy, and are therefore unsure to whom this responsibility would be delegated if an SAOP does not exist, and are further concerned that such a delegate may not have the required cybersecurity and privacy expertise to perform this function as written. | Clarify the process and who is responsible if an agency does not have an SAOP or other qualified responsible party to take on these requirements. |
| 19 | 63A | 3.1.8 | 25 | 1126-1129 | We applaud NIST in ensuring that diverse populations are equitably and fairly served. | |
| 20 | 63A | 3.1.11 | 27-28 | 1230-1234 | We applaud NIST in ensuring that biometric data can be requested to be deleted by subscribers, and that CSPs must comply. Retention of biometric data in circumstances where it is no longer needed after the initial proofing event is a significant cybersecurity and privacy risk. | |
| 21 | 63A | 3.1.13 | 33 | 1412 | We applaud NIST for including applicant references as an option for identity proofing. In various communities and across certain industries, this is a more viable option--and sometimes the only viable option--than other methods of proofing. | |
| 22 | 63A | 3.1.13.5 | 34 | 1468-1469 | We believe that statements recorded on public blockchains could also suffice if multiple data points are referenced to demonstrate a relationship between the applicant and the applicant's reference. TDC does not seek to prescribe, however, the standards or requirements needed to create certainty in such a relationship. We merely want to keep the door open to the technology as a method of verification in this circumstance. | We suggest adding "blockchain-based verification" to the list of example verification methods in this section. |
| 23 | 63A | 4.2.6.1 | 42 | 1706 | We support the inclusion of non-biometric proofing methods. Due to personal or cultural beliefs, levels of technical literacy, or cybersecurity and privacy concerns, certain individuals or populations will refuse to go through an identity proofing process if biometrics are involved. Creating an alternative is therefore necessary. | |

| | | | | | | |
|---|---|---|---|---|---|---|
| 24 | 63A | 4.2.6.2 | 43 | 1743-1751 | TDC supports fully digital identity proofing methods, as they can provide significant improvements in speed, security, and privacy. We also would like to see digital wallets and blockchain-based communications added to this list of approved verification methods. | We suggest adding "or digital wallet/blockchain based addressor account" in section 2a. We suggest adding "or digital wallet/blockchain based address or account" in section 2b. We suggest adding "or digital wallet" in section 2c. |
| 25 | 63A | 4.3.3 | 45 | 1806-1808 | We do not believe CSPs must retain biometric data in order to support account recovery, non-repudiation, etc. | Change "Shall" to "May." Or, approve other non-biometric pathways to to achieve these requirements, and combine them with the biometric options in this section giving CSPs optionality, and keep "Shall." |
| 26 | 63A | 4.3.7 | 47 | 1874-1874 | The applicant should also have the ability to request deletion of this video after the identity proofing process has been successfully completed, as it is a privacy and cybersecurity risk if the CSPs retain the data. | Add the following provision after line 1876: "The CSP shall delete any video session(s) recorded during the identity proofing process upon the applicant's request." |
| 27 | 63A | 5.4 | 52 | 1988-1990 | We applaud NIST for including this provision. It is critical that subscribers are able to ensure their sensitive data is not being 'held captive' by a CSP after the relationship is ended. | |
| 28 | 63A | 7 | 57 | 2034 | We greatly appreciate NIST including a comprehensive section on privacy. Not only are these informative guidelines practical, but they signal NIST's commitment to privacy when setting normative requirements for digital identity practices. | |
| 29 | 63A | 8.3 | 66 | 2357 | As digital technologies continue to evolve and consumers continue to adopt them, it is critical to be forward looking toward the next communications platforms where subscribers will spend their time in the digital age. | We recommend adding in digital/blockchain based wallets and decentralized protocols or dApps as an example method of valid code transfer. |
| 30 | 63A | 9 | 69 | 2435 | We greatly appreciate NIST including a comprehensive section on equity. Not only are these informative guidelines practical, but they signal NIST's commitment to equity when setting normative requirements for digital identity practices. | |
| 31 | 63B | 2.4.3 | 9 | 640-650 | We appreciate NIST's normative guidance on minimizing and protecting retained data, and publishing overall privacy requirements in the authentication process. | |
| 32 | 63B | 3.1.6.1 | 25 | 1100 | Does NIST consider any blockchain-based digital wallets or cryptography sufficient in meeting these requirements? | Clarification is needed on whether blockchain-based digital wallets meet these requirements. We would posit that they do meet the requirements. |
| 33 | 63B | 3.1.7.1 | 26 | 1142 | Does NIST consider any blockchain-based digital wallets or cryptography sufficient in meeting these requirements? | Clarification is needed on whether blockchain-based digital wallets meet these requirements. We would posit that they do meet the requirements. |
| 34 | 63B | 3.1.7.3 | 27 | 1171 | We applaud NIST for supporting the usage of subscriber-controlled wallets. We believe this is a wise choice that will allow greater subscriber control over their identity attributes, and may foster a market for wallet creators. We are unclear however if this definition of subscriber-controlled wallets includes, or could include, blockchain-based wallets. | Clarify whether subscriber-controlled wallet definition includes blockchain-based wallets. We argue that they should and do meet the definition and requirements. |
| 35 | 63B | 3.1.7.3 | 27 | 1184 | We support NIST's decision to make a normative requirement that biometric data shall be erased immediately after authentication. Not only does this protect user privacy broadly, but it also significantly lowers the risk of collusion between authenticators that could use such biometric data for ill purposes. | |
| 36 | 63B | 3.2.3 | 30 | 1265-1266 | We strongly support the normative requirement for alternatives to biometric data during authentication. | |
| 37 | 63B | 3.2.3 | 30 | 1273-1274 | We applaud NIST for requiring normative equity standards in the authentication process. | |
| 38 | 63B | 3.2.3 | 31 | 1298-1299 | We believe that local biometric comparison should be the standard, but recognize that instances will occur where local comparison is not viable or does not meet certain authentication requirements. | We encourage NIST to make local biometric comparisons the required normative method, and allow centralized verifier comparison as an alternative method if the local method is not viable. |
| 39 | 63B | 3.2.3 | 31 | 1318-1320 | We strongly disagree with this practice of biometric data being used for training models, especially as written. | We would like to see this provision removed completely. As a second alternative, this section should be rewritten to ensure that user consent is required for both training of comparison algorithms and for research purposes. As currently written, it would only be required for research purposes. |
| 40 | 63B | 3.2.3 | 31 | 1321-1322 | While we do not agree with the broader provision on model training that this point on data erasure refers to, we do appreciate NIST's efforts to include data erasure requirements. | |
| 41 | 63B | 3.2.11 | 36 | 1499-1500 | Does this provision preclude the use of blockchain wallets and networks as viable methods to achieve these normative requirements in this section? If so, we believe that their exclusion as a viable method from this section would extend to most if not all other sections throughout the entirety of 800-63-4 draft 2. Is this the case? And is there any distinction made between "hot" and "cold" blockchain wallets, or permissioned and permissionless blockchain networks? | Clarify whether blockchain based wallets and protocols meet the normative requirements of this section, and by extension, the normative requirements of the entire publication. We argue that blockchain wallets can/do meet these requirements. |
| 42 | 63B | 4.6 | 47 | 1848-1849 | As digital technologies continue to evolve and consumers continue to adopt them, it is critical to be forward looking toward the next communications platforms where subscribers will spend their time in the digital age. | We recommend adding in digital/blockchain based wallets and decentralized protocols or dApps as an example method of receiving account notifications. |
| 43 | 63B | 7 | 61 | 2078 | We greatly appreciate NIST including a comprehensive section on privacy. Not only are these informative guidelines practical, but they signal NIST's commitment to privacy when setting normative requirements for digital identity practices. | |
| 44 | 63B | 9 | 75 | 2514 | We greatly appreciate NIST including a comprehensive section on equity. Not only are these informative guidelines practical, but they signal NIST's commitment to equity when setting normative requirements for digital identity practices. | |
| 45 | 63C | 3 | 9 | 635-636 | As digital technologies continue to evolve and consumers continue to adopt them, it is critical to be forward looking toward the next communications platforms where subscribers will spend their time in the digital age. | We recommend adding in digital/blockchain based wallets as an example in this section in addition to web browsers. |
| 46 | 63C | 3.3.1 | 15 | 826 | We greatly appreciate the inclusion of pseudonymous pairwise identifiers, as we believe this practice will minimize data retention and increase subscriber privacy and overall cybersecurity. | |
| 47 | 63C | 3.3.1.1 | 15 | 843-845 | We applaud NIST for recognizing the importance of creating privacy policies to mitigate and prevent subscriber data correlation. | |
| 48 | 63C | 3.3.1.1 | 15 | 854-856 | We applaud NIST for recognizing the importance of preventing PPI and data mapping to mitigate and prevent subscriber identity recreation. | |
| 49 | 63C | 3.3.1.3 | 16 | 871 | This section should also include subscriber right to delete PPI attribution to their account. | At the end of line 871, add "and is given clear steps on their option and right to request deletion of any shared PPIs." |
| 50 | 63C | 3.3.1.3 | 16 | 877-880 | We applaud NIST for recognizing the importance of creating privacy policies to mitigate and prevent subscriber data correlation. | |

| | | | | | | |
|---|---|---|---|---|---|---|
| 51 | 63C | 3.4 | 17 | 932 | We believe the wording in this provision, specifically in line 932, is inconsistent with how NIST has set normative requirements throughout the rest of this publication. | Change "the terms of the trust agreement need to" to "the terms of the trust agreement Shall." |
| 52 | 63C | 3.4.1 | 18 | 948 | The term "no additional requirements" is vague; what do "additional requirements" include in scope? | Clarify what "additional requirements" mean. |
| 53 | 63C | 3.4.2 | 20 | 969 | We recommend adding in a normative requirement for data deletion. | Amend line 969 to state "retention, aggregation, deletion, and disclosure to third parties." |
| 54 | 63C | 3.4.2 | 20 | 980-983 | We commend NIST for adding privacy risk assessments as a normative requirement to this section | |
| 55 | 63C | 3.4.3 | 21 | 992 | It is unclear what the scope of "redress" entails. | Define "redress" and provide examples. |
| 56 | 63C | 3.5 | 22 | 1030 | What are the specific responsibilities and requirements of these third party services? Who will be held liable if these third party services do not follow requirements? How will subscribers and other parties be notified? What are the redress options? | Clarification on "third party service" responsibilities to remain compliant, consequences if they do not meet these responsibilties, and subscriber notification and redress of violations. |
| 57 | 63C | 3.5.1 | 23 | 1051 | We appreciate NIST adding the practice of key rotation as a normative requirement in federated instances. We believe this should be a standard practice in identity systems. | |
| 58 | 63C | 3.5.1 | 23 | 1056-1057 | As digital technologies continue to evolve and consumers continue to adopt them, it is critical to be forward looking toward the next communications platforms where subscribers will spend their time in the digital age. | We recommend adding in digital/blockchain based wallets or public addresses as an example method of valid IdP key identification and verification. |
| 59 | 63C | 3.5.3 | 23 | 1073 | We applaud NIST for including software attestations as a normative requirement. This practice serves to protect subscribers from engaging with fraudulent RPs that would improperly use subscriber data. | |
| 60 | 63C | 3.6 | 23 | 1096-1097 | We applaud NIST for including this prohibition as a normative requirement. Ensuring authentication protocols must meet this requirement ostensibly means those protocols will be built with this as a technical specification, ensuring that the protocol does not have the technical capability of transferring these attributes for non-approved purposes. | |
| 61 | 63C | 3.6 | 23 | 1104-1106 | We believe this provision is a necessary privacy control and will become beneficial to user education on data sharing over time. | |
| 62 | 63C | 3.9 | 27 | 1231 | To create consistency with the normative privacy requirements throughout the rest of this document, the "Should" in line 1231 should be changed to "Shall." | Change "Should" to "Shall." |
| 63 | 63C | 3.9 | 28 | 1237 | We are concerned that not all federal agencies have Senior Agency Officials for Privacy, and are therefore unsure to whom this responsibility would be delegated if an SAOP does not exist, and are further concerned that such a delegate may not have the required cybersecurity and privacy expertise to perform this function as written. | Clarify the process and who is responsible if an agency does not have an SAOP or other qualified responsible party to take on these requirements. |
| 64 | 63C | 3.9 | 28 | 1259 | We believe this provision would be more clear if rewritten. | Change to "If the subscriber opts in, trust agreements May request that identity attributes be shared, using a runtime decision as discussed in Sec. 4.6.1.3." |
| 65 | 63C | 3.9.1 | 28 | 1270 | The term "security incident" is too broad. What does it encompass? | Define examples of "security incident" that would trigger the data transfer provision in this section. |
| 66 | 63C | 3.9.1 | 28 | 1282 | The term "security incident" is too broad. What does it encompass? | Define examples of "security incident" that would trigger the data transfer provision in this section. |
| 67 | 63C | 3.10.2 | 30 | 1344-1346 | We believe it's unnecessary and improper for device location and identity to be included in this list, and are unclear why NIST would list passing this data on as a "good idea," but not make any determinations on whether the data May, Should, or Shall be passed on. | Remove device location from this list, and clarify any normative requirements in this provision |
| 68 | 63C | 3.10.2 | 30 | 1346 | "Additional attributes" is too broad. We are unclear on what the scope of this term could entail, but are concerned that it would allow inappropriate attributes to be collected and shared. | Clarify and narrow the scope of "additional attributes" |
| 69 | 63C | 3.10.2 | 30 | 1351-1353 | We applaud NIST for including requirements on derived attribute values and recommending they be used as a primary source where possible. However, we would like to see this changed from "Shall" to "Should" in an effort to better ensure user privacy and cybersecurity. | Change "Should" to "Shall." |
| 70 | 63C | 3.10.3 | 31 | 1360 | What are is included in the scope of "appropriate controls?" It would be beneficial to include a list of examples or to link to a section of the guidelines that fully covers what these are. | Define "appropriate controls" |
| 71 | 63C | 3.11.1 | 32 | 1398 | We recommend using derived attribute bundles as a standard where and when derived attribute values meet the authentication and verification requirements of an RP. | Amend line 1398 to read "instead Shall be disclosed to the RP when selective disclosure meets the requirements of the RP." |
| 72 | 63C | 3.11.2 | 32 | 1422 | We strongly suggest adding normative requirements to ensure IdPs and CSPs create the technical capabilities to create derived attribute values, and that RPs have the capabilities to accept them. If these provisions are not added, we are concerned that the other requirements on derived attribute values throughout all parts of SP 800-63 may be moot. | Add "IDPs and CSPs Shall ensure methods of creating, authenticating, and verifying derived attribute values. RPs Shall ensure methods of authenticating, verifying, and accepting derived attribute values." |
| 73 | 63C | 3.11.3 | 32 | 1493 | We believe subscribers should be required to be notified and must give consent to share attributes. | Add provision stating "Subscriber Shall be notified and required to give consent to share the attributes, and be allowed to select each discrete attribute they consent to sharing." |
| 74 | 63C | 3.12.2 | 35 | 1513 | As digital technologies continue to evolve and consumers continue to adopt them, it is critical to be forward looking toward the next communications and data platforms where subscribers will spend their time and find trusted data in the digital age. | We recommend adding in blockchain based addressses or registries or verified entries as a normative example. |
| 75 | 63C | 3.12.3 | 35 | 1534 | As digital technologies continue to evolve and consumers continue to adopt them, it is critical to be forward looking toward the next communications and data platforms where subscribers will spend their time and find trusted data in the digital age. | We recommend adding in blockchain based addressses or registries or verified entries as a normative example. |
| 76 | 63C | 3.15 | 38 | 1607-1608 | As digital technologies continue to evolve and consumers continue to adopt them, it is critical to be forward looking toward the next communications and data platforms where subscribers will spend their time and find trusted data in the digital age. | We recommmend adding blockchain wallet added as notification/verification mechanism for subscribers. |
| 77 | 63C | 4 | 43 | 1709-1710 | It is unclear whether this provision includes blockchain-based digital wallets. | We would encourage this section to clarify and state that blockchain-based wallets are included. |
| 78 | 63C | 4.3.1 | 46 | 1780-1805 | It is critical for user privacy and data minimization that requirements on derived attribute data are included in this section and in trust agreements. | Add to this list "Agreements on using derived attribute data as the standard when non-derived attribute data is not required." |
| 79 | 63C | 4.3.1 | 47 | 1828-1829 | It is critical for user privacy and data minimization that requirements on derived attribute data are included in this section and in trust agreements. | Amend the end of line 1829 to read "function of the system, and use derived attribute data as the standard when non-derived attribute data is not required." |
| 80 | 63C | 4.3.2 | 48 | 1856-1863 | It is critical for user privacy and data minimization that using derived attribute data is standard practice where full attribute values are not needed. | Amend line 1862 to read "available for the means of deletion, whether derived attribute values can be used in place of actual attribute values, and the subscriber's right to request actual or derived attribute values be deleted." |

| | | | | | | |
|---|---|---|---|---|---|---|
| 81 | 63C | 4.4.1 | 49 | 1895-1899 | We applaud NIST for including manual registration, and including normative requirements on trust agreements pertaining to automated registration, including cybersecurity enhancing techniques such as key distribution and cache lifetimes. | |
| 82 | 63C | 4.6.1.2 | 51 | 1973-1976 | Does this mean that the IdP shall not flag the RP as a blocklisted entity? If so, how does this impact future cases of fraud or improper subscriber attribute sharing with this blocklisted RP? What are the risks to subscribers? | Clarity is needed on this provision. |
| 83 | 63C | 4.6.1.3 | 52 | 1984-1991 | Who can take on the role of an administrator? | Clarity needed on who can take the role of "administrator." |
| 84 | 63C | 4.6.1.3 | 52 | 2003-2007 | It may be an easier solution to just show the attribute fields requested, instead of the attribute values being requested, in order to solve the issue of "shoulder surfing." | Change the provision to show the requested attribute fields instead of showing the actual data being requested. |
| 85 | 63C | 4.6.1.3 | 52 | 2008-2012 | We believe the subscriber should be notified of this practice, and be presented with the option to consent. This is a standard practice in other areas, such as prompting users to give consent for websites to store their credit card data for future purchases. | Amend lines 2010 and 2011 to read "If such a mechanism is provided, the IdP shall gain consent from the subscriber. The IdP Shall allow the authorized party to revoke such remembered access at a future time." |
| 86 | 63C | 4.6.2.3 | 53 | 2040 | As digital technologies continue to evolve and consumers continue to adopt them, it is critical to be forward looking toward the next communications and data platforms where subscribers will spend their time and find trusted data in the digital age. | Add blockchain wallet address as an example in addition to email address. |
| 87 | 63C | 4.6.2.3 | 53 | 2044-2049 | We believe the subscriber should be notified of this practice, and be presented with the option to consent. This is a standard practice in other areas, such as prompting users to give consent for websites to store their credit card data for future purchases. | Amend lines 2048 and 2049 to read "If such a mechanism is provided, the RP shall gain consent from the subscriber. The RP shall also allow the authorized party to revoke such remembered options at a future time." |
| 88 | 63C | 4.6.3 | 54 | 2077-2082 | We are unclear on when or in which scenarios the pre-provisioning process would occur. This process seems to be a potentially large threat vector to both user privacy and cybersecurity, and therefore TDC would appreciate examples on when this process would be relevant. | Add examples of situations where pre-provisioning would occur. |
| 89 | 63C | 4.6.3 | 54 | 2083-2092 | We applaud NIST for categorizing and creating normative guidance around authentication processes where subscriber data is deleted after authentication, and therefore not retained. This is a significant privacy and cybersecurity enhancement that will allow subscribers to gain greater confidence in IdPs, CSPs, RPs, and in digital identity overall. | |
| 90 | 63C | 4.6.4 | 56 | 2109-2111 | We strongly suggest the specification of what "other attributes" RPs may collect, as we fear the provision as written is extremely broadly. Further, we are concerned by RPs having the ability to overwrite data asserted and verified by the IdP. This gives RPs tremendous ability to damage subscriber data attributes and prevent them from being used at other RPs. We believe this is dangerous and creates empowers RPs to act unethically. We are concerned that NIST would approve of this. | Clarify what "other attributes" entail. Remove ability for RPs to override IdP assertions. |
| 91 | 63C | 4.6.5 | 57 | 2139 | Does the RP direct query ability in line 2139 refer to the ability for RPs to "phone home?" | Clarify whether this provision allows for "phoning home." |
| 92 | 63C | 4.6.5 | 57 | 2165-2167 | Do the "external attribute providers" in this provision have the ability to provide primary identity attribute data, or only supplemental data? | Clarify whether external attribute providers have the ability to provide only primary identity data, or subblemental data as well, what is within the scope of supplemental data. |
| 93 | 63C | 4.6.6 | 58 | 2175-2176 | We believe the subscriber should be notified of this practice, and be presented with the option to consent. This is a standard practice in other areas, such as prompting users to give consent for websites to store their credit card data for future purchases. | Amend line 2176 to read "those provided by the IdP. The RP shall request and gain subscriber consent to do so." |
| 94 | 63C | 4.6.6 | 58 | 2184-2185 | We assert that these attributes should be governed by a separate trust agreement between the RP and the Subscriber, and follow the requirements of other trust agreements in 800-63. | Add a provision requiring that these attributes Shall be governed by a separate trust agreement between the RP and the Subscriber, and Shall follow the requirements of other trust agreements in 800-63. |
| 95 | 63C | 4.7 | 59 | 2233-2235 | We believe approval of RP and IdP communication in this section may result in collusion for nefarious purposes, unbeknownst to the subscriber. | If this provision remains, create privacy-oriented rules that protect the subscriber's attribute bundle usage data and prevent tracking. Otherwise, we request the removal of this provision. |
| 96 | 63C | 4.7 | 61 | 2262-2265 | We appreciate this clarification on RP authentication of identity APIs and assertions. | |
| 97 | 63C | 4.7 | 61 | 2271-2272 | We suggest that this SP should in fact cover RP access to non-identity APIs, as in many cases, these APIs contain or provide user data that, while perhaps not containing information about address, phone number, health records, or other primary attribute data covered by this SP, such data and metadata could still be considered PII broadly. Moreover, it is unclear why an RP would need to, or be provided the ability to, access these APIs on a subscriber's behalf if the subscriber is no longer associated with the RP. This seems like a large threat vector against subscriber privacy and data security. | Include normative requirements and restrictions on RP access to non-identity APIs, placing privacy and cybersecurity considerations as top priorities. |
| 98 | 63C | 4.8 | 61-62 | 2282-2314 | We are concerned that the section on shared signaling is an approval by NIST of issuer-verifier collusion. | We highly recommend holding another public comment feedback session in order for commenters to speak with the authors on this section and address concerns. |
| 99 | 63C | 4.8 | 62 | 2303 | We are unclear why this section is not required. | Change "Should" to "Shall." |
| 100 | 63C | 4.8 | 62 | 2313 | As shared signaling seems to be a method of issuer-verifier collusion, it is critical that if this practice is allowed to stand, that subscriber privacy is made paramount. | Remove this provision. If this is infeasible, change "May" to "Shall." |
| 101 | 63C | 4.9 | 62 | 2325 | We applaud NIST for including this comment stating that the guidelines do not restrict the type of protocol or data payload. We believe this will allow these guidelines to remain applicable while technologies and use cases evolve. | |
| 102 | 63C | 4.9 | 64 | 2386-2388 | We believe this is invasive to subscriber privacy and goes against the data minimization suggestions and requirements written into this publication. | Remove this provision. If not removed, add a requirement stating that "RPs must inform and gain consent from the subscriber before gathering and associating additional data through identity APIs." |
| 103 | 63C | 4.10 | 65 | 2401 | Why is this section not mandatory? | Change "Should" to "Shall." |
| 104 | 63C | 4.11 | 65 | 2406-2416 | We are unclear on this new categorization of presentation methods. Is this "back channel" method a new way to describe what has traditionally been know as "phoning home?" | Clarify if this "back channel" method is the functional equivalent of the practice of "phoning home." |
| 105 | 63C | 5.2 | 69 | 2526-2527 | As written this section is unclear as to whether the subscriber can supply their own wallet(s) that the data attribute bundle will be issued to. | We suggest clarifying that subscribers May use their own digital wallets and are not required to use those provided by the IdP. |
| 106 | 63C | 5.3 | 71 | 2543-2544 | Does this established relationship require the wallet to be provisioned by the CSP? If a subscriber elects to use a third party (not CSP provisioned) wallet to contain the CSP-provisioned credential (data attribute bundle), doesn't the fact that the CSP found the wallet to be an acceptable receptacle for the credential (data attribute bundle) mean that the RP can/should trust the third party wallet transitively? | Clarification needed. |
| 107 | 63C | 5.3 | 71 | 2557-2560 | We believe that listing derived attribute values that would satisfy RP requirements in many cases. As such, we believe that a provision should be added to address this. | Between lines 2559 and 2560, insert "The set of derived attribute values that can be used to satisfy the RP's requirements." |

| | | | | | | |
|---|---|---|---|---|---|---|
| 108 | 63C | 5.4.1 | 73 | 2591-2601 | This section describes the methods acceptable to deprovision attribute bundles, not subscriber-controlled wallets. | This section needs to be renamed to accurately reflect its content. |
| 109 | 63C | 5.5 | 73 | 2606 | As digital technologies continue to evolve and consumers continue to adopt them, it is critical to be forward looking toward the next communications platforms where subscribers will spend their time in the digital age. | We suggest adding "public blockchain address" in addition to URL. |
| 110 | 63C | 5.5 | 73 | 2614-2627 | We applaud this methodology of ensuring multi-party trust. | |
| 111 | 63C | 5.6 | 74 | 2631 | We assert that this should be a base requirement of wallets, and by extension, a base requirement of RPs. | Change "Should" to "Shall" and add a provision that would require the RP to accept selectively disclosed attributes, and to prioritize the usage of them over the usage of a full attribute bundle of non-derived attributes, if they meet the RP's requirements. |
| 112 | 63C | 5.6 | 74 | 2631 | We assert that this section should also contain a requirement for wallets, and by extension, RPs, to be able to present, verify, authenticate, and accept derived attribute values, and posit that derived attributes should be used in place of user attributes in order to maximize privacy and lower the probability of data interception, leakage, and RP collusion. | Require for usage of derived attributes as the standard when possible and create requirements for RPs to be able to utilize them. |
| 113 | 63C | 5.7 | 74 | 2642-2643 | In line with the comment on the row above. | We suggest that notification of acceptance of derived credentials should be conveyed to the subscriber and the subscriber should be allowed to choose to assert derived values/credentials in place of full identity attributes/values. |
| 114 | 63C | 5.8 | 76 | 2691-2694 | We believe that requiring attribute bundles to have the capacity to contain derived values in addition to user attribute values is key to privacy and protection of personal data. | Rewrite lines 2691 and 2692 to state "Attribute bundles shall have the capacity to contain derived attribute values, which may then be included in the attribute bundle." |
| 115 | 63C | 5.9 | 76 | 2704 | It does not seem clear to us why this would be a "should" and not a "shall." | Change "Should" to "Shall." |
| 116 | 63C | 5.11 | 77 | 2731-2732 | We suggest that if the issuer makes this list available, that it should only contain the public keys associated with each attribute bundle. | We recommend including digital trust registries or public blockchain addresses as normative examples. |
| 117 | 63C | 5.11 | 77 | 2739-2740 | Does "remove" in this section mean removal of certain attributes, or removal (deletion) of the subscriber account overall? | Clarification needed. |
| 118 | 63C | 6.1 | 78 | 2768-2770 | Is this a recommendation that this practice be used, even though it turns IdPs into centralized honeypots for attackers? | Clarification needed. |
| 119 | 63C | 7 | 81-85 | 2773-2974 | We greatly appreciate the inclusion of a full section on privacy, and applaud NIST in this regard. | |
| 120 | 63C | 8.2.1 | 88 | 3033-3038 | We greatly appreciate the inclusion of this section on privacy, data minimization, and user expectations. | |
| 121 | 63C | 8.2.1 | 89 | 3062-3063 | This is a potentially rare occurrence, but it is still necessary to cover and provide guidance on in this document. We applaud NIST for catching this. | |
| 122 | 63C | 8.2.1 | 89 | 3065-3068 | We applaud NIST for including this section on user control and authority over their data. This is especially key as more US states pass laws that require that users have paths to request and ensure the deletion of their data held by external parties. | |
| 123 | 63C | 8.2.1 | 89 | 3071-3075 | We applaud NIST for including this provision in ensuring users have sufficient privacy options, and by extension, recognizing that there are valid circumstances where user anonymity and pseudonymity are appropriate and valid. | |
| 124 | 63C | 8.2.2 | 90 | 3090-3091 | We applaud NIST for including this section on user control and authority over their data. This is especially key as more US states pass laws that require that users have paths to request and ensure the exportability and correction of their data held by external parties. | |
| 125 | 63C | 8.2.2 | 90 | 3098-3100 | We applaud NIST for including this provision on informed user experience and the role it plays in digital identity. | |
| 126 | 63C | 9 | 93 | 3173-3191 | We applaud this provision for user consent and allowance of selective disclosure of attributes. | We recommend adding to this list the capacity for users to present derived attribute values in place of full data when derived attribute values meet RP requirements. |