## 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:                   | AWS                           |  |  |  |  |  |
|------------------------|---------------------------------|-------------------------------|--|--|--|--|--|
| Name of Submitter/POC: |                                 | Jean-Francois "Jeff" Lombardo |  |  |  |  |  |
|                        | Email Address of Submitter/POC: |                               |  |  |  |  |  |

| March   Marc   |           |                       |         |        |          |   |                  |
|--|-----------|-----------------------|---------|--------|----------|---|------------------|
| The lettle prevented SML Is a SQL 10 Comparison, and solving or worth User right for comments. The universal comments of the square of the squ |           | Publication           |         |        |          | Comment   |                  |
| The lettle prevented SML Is a SQL 10 Comparison, and solving or worth User right for comments. The universal comments of the square of the squ | Comment # | (Base, 63A, 63B, 63C) | Section | Page   | # Line # | (Include rationale for comment)   | Suggested Change |
| Section 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1  |           |                       |         |        |          | "The entire password SHALL be subject to comparison, not substrings or words that might be contained        |                  |
| 1.6   1.6   2.7   1.6   2.8   2.8   1.6   2.8    |           |                       |         |        |          | therein." Stil we should look at "Context-specific words, such as the name of the service, the username,    | 1                |
| 1.6   1.6   2.7   1.6   2.8   2.8   1.6   2.8    | 01        | 63B                   | 3.1.1.2 | 14     | 746      | and derivatives thereof" that means we should look at substrings.   | 1                |
| this bacter does not have a recommendation pointer for asymmetric flex jet for symmetric flex jet flex jet for symmetric flex jet  |           |                       |         |        |          |   |                  |
| 1  |           |                       |         |        |          | 8-8   |                  |
| 1  |           |                       |         |        |          | why is this section does not have a recommendation pointer for asymmetric keys ike for symmetric            |                  |
| A Significant Process of Significant Process  | 03        | 63B                   | 3162    | 21     | 112/     |   | 1                |
| OK   Sign  | - 03      | 030                   | 5.1.0.2 |        | 7 112-   |   |                  |
| 9 6 18   | 04        | 620                   | 2171    | 24     | 115/     |   | 1                |
| We see in 503, should we not focus on the EPP feer instance of come not the identity of 150 miles above value to be considered in the EPP in this case does not the identified to 150 miles and the production of the instance of the EPP in this case does not not the identified to 150 miles and 150 miles are seen as a second of the EPP in this case does not the identified to 150 miles are placed in the EPP and the Individual on the product and a second of immediate the Individual of Individual on Individual of Individual on Individu |           |                       |         |        |          |   |                  |
| Oct   15   15   15   15   15   15   15   1   | 05        | 038                   | 4.2.2.2 | 4:     | 5 1//8   |   |                  |
| Section   Sect   | 0.0       | can                   |         |        | 404      |   | 1                |
| No requirement at an investor for ordation associated large related to trust establishment in between 10 and 16 an |           |                       |         |        |          | 0   |                  |
| Obe SC Global Program Fast part \$3.1. This sounds strange for FAS also one force rotation an immissiman period of time in through the user good multiple lety with or fast part of the SC Global Program Fast part of the SC Fast part of the SC Global Program Fast part of the SC Fast part of the SC Global Program Fast part of the SC Fast part part part part part part part par  | 07        | 63B                   | 8.2.6   | /(     | ) 2402   |   |                  |
| on 85  |           |                       |         |        |          |   | 1                |
| Sections used in Education protocols include the 10 Taken in OpenID Connect meant as a proof of authentication in the 8P and should not be sent to the 8P because meant as a proof of authentication in the 8P and should not be sent to the 8P because meant as a proof of authentication in the 8P and should not be sent to the 8P because meant as a proof of authentication in the 8P beta of the should not be sent to the 8P because the document membros two times notice of 8P3 risk while the rest of the document in more aligned a level of assurance proofs 8P3 risk while the rest of the document in more aligned a level of assurance proofs 8P3 risk while the rest of the document in more aligned a level of assurance proofs 8P3 risk while the rest of the document in more aligned a level of assurance proofs 8P3 risk while the rest of the should be placed in the 8P but for supporting a sensitive operation at the 8P requiring a high assurance. Risk here has a level of assurance proof through FA3 risk while the rest of the should be placed in the 8P but for supporting a sensitive operation at the 8P requiring a high assurance. Risk here has a level of assurance proof through FA3 risk while the rest of the should be placed in the 8P but for supporting as sensitive operation at the 8P requiring a high assurance. Risk here has a level of assurance proof through FA3 risk while the rest of the should be a substance operation of the 8P but for supporting as sensitive operation at the 8P but for supporting the place of the 8P but for supporting the 8 |           |                       |         |        |          |   | 1                |
| means as a proof of subterfaction for the IP and should not be sent to the IP. How the IP could establish as separate destablish as separate definition.    Part   | 08        | 63C                   | Global  |        |          |   | <u> </u>         |
| description of the comment mentions two times notion of RP's risk white the rest of the document is more aligned a well of assurance appeting RP' or level of protection required by RP. The FA Is and the text or bringing in AI.  10 GC 21 5 54 Evelowy to converge toward multicolouses of the RP, which is not the year.  11 GC 2, 3 5 54 Evelowy to converge toward multicolouses of the RP, which is not the popular.  12 GC 2, 3 5 55 Every converge toward multicolouses of the RP, which is not the popular.  13 GC 2, 3 5 55 Every converge toward multicolouses of the RP, which is not the popular.  14 GC 2, 3 5 55 Every converge toward multicolouses of the RP, which is not the popular.  15 GC 2, 3 5 55 Every converge toward multicolouses of the RP, which is not the popular.  16 GC 2, 3 5 55 Every converge toward multicolouses of the RP, which is not the popular.  17 GC 2, 3 12 17, 2 75 Department of the Propriet of the Propri |           |                       |         |        |          |   | 1                |
| Book   Company   |           |                       |         |        |          | meant as a prood of authentication for the IdP and should not be sent to the RP. How the RP could           | 1                |
| the document mentions two times notion of RPs risk while the rest of the document is more aligned a level of a surrance experting RP, or level of protection required by RP. The PAL is not here be mitigate risk of the RP but for supporting a sensitive operation at the RP requiring a light assurance. Risk here has a sensitive supportion at the RP requiring a light assurance. Risk here has a sensitive operation at the RP requiring a light assurance. Risk here has a sensitive operation at the RP requiring a light assurance. Risk here has a sensitive operation at the RP requiring a light assurance. Risk here has a sensitive operation at the RP requiring a light assurance. Risk here has a sensitive operation at the RP requiring a light assurance. Risk here has a sensitive operation at the RP requiring a light assurance. Risk here has a sensitive operation at the RP with a sin of the point.  1 of SC 12.1 5.5 52 purpower of the region of the RPS requires and the potential impact or not on the RST guidance document.  1 of SC 2.3 3.1.1 1.2 720 boold mention that this is do know as a Stroker.  1 of SC 3.3.1.1 1.5 850 middle RPS as it provipely policy and consent burst of the policy of the second policy of the RPS represent the same subscriber at different RPS requires and the policy of the SPS represent the same subscriber at different RPS requires and advantage of the RPS requirement and the RPS requ |           |                       |         |        |          | establish a session based on it then? Pretty sure you mean "the Access Token in OpenID Connect              | 1                |
| level of assurance expecting 8P, or level of assurance expecting 8P, or level of protection required by high assurance. Bits here to mitigate risk of the 8P but for supporting a sensitive operation at the 8P required in the point.  1 5 5 1  | 09        | 63C                   |         | 2.1    | 499      | [OIDC]"   |                  |
| level of assurance expecting 8P, or level of assurance expecting 8P, or level of protection required by high assurance. Bits here to mitigate risk of the 8P but for supporting a sensitive operation at the 8P required in the point.  1 5 5 1  |           |                       |         |        |          |   |                  |
| of the RP but for supporting a sensitive operation at the RP requiring high plas surrous. Risk here has a  1 1 SC 2.1 5 151 telemony for converge towards maliciousness of the RP, which is not the point.  1 1 SC 2.1 5 151 telemony for the RP but for supporting a sensitive operation at the RP requiring high plas surrous for the RP, which is not the point.  1 1 SC 2.1 5 151 telemony for the RP but for surrous for the RP, which is not the point.  1 1 SC 2.1 5 151 telemony for the RP but for surrous f |           |                       |         |        |          | the document mentions two times notion of RP's risk while the rest of the document is more aligned a        | 1                |
| of the RP but for supporting a sensitive operation at the RP requiring high plas surrous. Risk here has a  1 1 SC 2.1 5 151 telemony for converge towards maliciousness of the RP, which is not the point.  1 1 SC 2.1 5 151 telemony for the RP but for supporting a sensitive operation at the RP requiring high plas surrous for the RP, which is not the point.  1 1 SC 2.1 5 151 telemony for the RP but for surrous for the RP, which is not the point.  1 1 SC 2.1 5 151 telemony for the RP but for surrous f |           |                       |         |        |          | level of assurance expeting RP, or level of protection required by RP. The FAL is not here to mitigate risk |                  |
| 10 SGC 2.1 5 5 1.4 tendency to converge towards mail/colourses of the RP, which is not the point.  1 SGC 2.1 5 5 1.5 tendency to converge towards mail/colourses of the RP, which is not the point.  1 SGC 2.1 5 5 5.5 substitute through RFAL3*?  1 SGC 3.1.2 11 939 first time liker* this is also known as the offering party (Pp)**.  1 SGC 3.2.3 12 12 725 Should mention that this also known as the offering party (Pp)**.  1 SGC 3.3.1 15  |           |                       |         |        |          |   | 1                |
| the succriber to reauthenticate through FALS* is this not AAL3 instead here? Of "presenting a higher 12 pick of the provided property of the provided property of the provided | 10        | 63C                   |         | 2.1    | 5 514    |   | 1                |
| 1  |           |                       |         |        |          |   |                  |
| 13 65C 3.12 1 393 Extra ten lear "this is also known as the offering party (PI)."  14 65C 3.23 1 1 728 Should mention that thisis also known as forcker  15 65C 3.23 1 1 728 Should mention that thisis also known as forcker  16 65C 3.3.1 1 1 584 this mention of the proxy and the potential impact or not on the FAL  17 65C 3.3.1 1 584 this may play a see the rest on mitigate risk on non PPI attribute, they should set a separate definition  18 65C 3.3.1 1 584 this may play as can define griving policies even if we don't use detecting the suscriber at different RPs' even if the Proxy can generate a PPI upstream it an eight of the proxy policy and consent bound AAL at the IPD which is a specific object  18 65C 3.6 2 1 1078 Should mention that this way, exist  19 65C 3.7 2 1 1079 sees not requiring each policy and consent bound AAL at the IPD which is a specific object  19 65C 3.7 2 1 1070 sees not requiring each policy and consent bound AAL at the IPD which is a specific object  19 65C 3.7 2 1 1070 sees not requiring each policy and consent bound AAL at the IPD which is a specific object  19 65C 3.7 2 1 1070 sees not requiring each policy and consent bound AAL at the IPD which is a specific object  19 65C 3.7 2 1 1070 sees not requiring each policy and consent bound AAL at the IPD which is a specific object  19 65C 3.7 2 1 1070 sees not requiring each policy and consent bound AAL at the IPD which is a specific object  20 65C 3.9 1 1070 sees not requiring each policy and consent bound AAL at the IPD which is a specific object  21 65C 3.10 2 30 1346 formation of subscriber nerve manifested previous policies and policies in considerable policies and policies and policies in considerable policies and policies in considerable policies and polici | 11        | 630                   |         | 2.1    | 5 515    |   | 1                |
| 14 63C 3.23 12 72 Should mention that this is ab now nas the offering party (OP)."  15 63C 3.23 12 72 Should mention that this is ab now nas roker  16 63C 3.3.11 15 15 Should mention that this is ab now nay as roker  17 63C 3.3.11 15 15 Should mention that this is ab now now as roker  18 63C 3.3.11 15 Should mention that this is ab now now as roker  19 63C 3.3.11 15 Should mention that this is ab now now as roker  19 63C 3.3.11 15 Should mention that this is ab now now is a compared to the other than PB as we can define privacy policies even if we don't use PB in the don't use PB in the other is a compared to the other in the other in the other in the property will be able to roke in the other one that espect "shall not use scriber alogs in the other one that espect "shall not use attribute outside" again it is not possible outside of privacy policy and consent bound AAL at the IDP which is a specific object this section is to most compared to the other one that espect "shall not use attribute outside" again it is called to to privacy policy especiation, right to be forgetten, and other privacy notions. Maximum it is called out to privacy policy especiation, right to be forgetten, and other privacy notions. Maximum it is called out to privacy policy especiation, for which the subscriber even manifested again should be included. Exemple of exemption of such deanning should mention other regulation like SOX and general use case for use case for use case not required mention of the subscriber even manifested again should be included. Exemple of exemption of exemption of such deanning should mention other regulation like SOX and general use case for use case for use case not required to extend the such as the such as a support of exemption of exemption of such deanning should mention other regulation like SOX and general use case for use case not required to the whole section. Cause if not disclosed by the trust agreement when the such as described in the properti |           |                       |         |        |          |   |                  |
| 14 63C 3.3 12 728 Should mention that thisis also known as Broker 15 63C 3.3 12 72 728 Should mention of that thisis also known as Broker 16 63C 3.3.1 12 728 Should mention of translation of format by the proxy and the potential impact or not on the FAL 17 63C 3.3.1 15 844 In apply as we can define privacy policies even if we don't use PPI 17 63C 3.3.1 1 15 Stamp PI as we can define privacy policies even if we don't use PPI 18 63C 3.5 1 1 15 Stamp PI as we can define privacy policies even if we don't use PPI 18 63C 3.5 23 1098 thing thing the Risk as it proxy ship all be to track and determine which PPIs represent the same subscriber at different RPs* even if the Proxy can generate a PPI upstream it can redeenlify the suscriber alogn 18 63C 3.5 23 1098 thing thing the Risk as the proxy will be able to track and determine which PPIs represent the same subscriber at different RPs* even if the Proxy can generate a PPI upstream it can redemity the suscriber alogn 18 63C 3.5 23 1098 thing thing the Risk as the proxy will be able to track and determine which PPIs represent the same subscriber at different RPs* even if the Proxy can generate a PPI upstream it can redemity the suscriber alogn 18 63C 3.5 23 1098 thing thing the Risk as the proxy will be able to track and determine which PPIs represent the same subscriber at different RPs* even if the IPP which is a specific object 18 63C 3.5 23 1098 thing thing the Risk as the RPs* is a specific object 18 63C 3.5 23 1098 thing thing the Risk as the RPs* is a specific object 18 63C 3.5 23 1098 thing thing thing the RPs* is a specific object 19 63C 3.7 24 1107 cases not requiring explicit consent 20 63C 3.1 2 2 163C 3.1 2 2 163C 1000 cases not requiring explicit consent 21 63C 3.1 2 2 163C 1000 cases not requiring explicit consent 22 63C 3.1 2 4 107 cases not requiring explicit consent 23 63C 3.1 2 4 107 cases not requiring explicit consent 24 63C 4.5 5 5 7 1356 (b and as a Mary reference to 17 stipulated and disclosed by the terrus as a specific object or the RPs* is a s |           |                       | 212     |        |          |   |                  |
| 15 63C 3.2.3 12 7.28 No mention of translation of format by the proxy and the potential impact or not on the FAL for how provided in the proxy are here to mitigate risk on non PPI attribute, they should seek a separate definition for the proxy are here to mitigate risk on non PPI attribute, they should seek a separate definition for the proxy are here to mitigate risk on non PPI attribute, they should seek as separate definition for the don't use PPI seek and the proxy are an experiment of the don't use PPI seek and the proxy are an experiment of the proxy and the proxy |           |                       |         |        |          |   |                  |
| If privacy policy are here to mitigate risk on non PPI attribute, het synbuld exist a separate definition  3.3.1.1 15 84 than PPI as we can define privacy policies even five don't use PPI  4.5.4 cases, the proxy will be able to track and determine which PPIs represent the same subscriber at different terbs. "even if the Proxy can generate a PPI upstream it can reidentify the suscriber alogn multiple RP as it proxyfying all this is not possible outside of privacy policy and consent bound AAL at the IDP which is a specific object.  18 63C 3.6 23 108 this is not possible outside of privacy policy and consent bound AAL at the IDP which is a specific object.  18 63C 3.6 25 108 this is not possible outside of privacy policy and consent bound AAL at the IDP which is a specific object.  18 63C 3.7 24 107 cases not requiring explicit on the other one that expect "shall not use attributes outside" again it calls out to railways exist.  19 63C 3.7 24 1107 cases not requiring explicit consent.  19 63C 3.7 24 1107 cases not requiring explicit consent.  19 63C 3.7 24 1107 cases not requiring explicit consent.  19 63C 3.9 1 28 126 for processing of such cleaning should mention of such cleaning should mention of or such depanding should mention of or such depanding of such deaning of such deaning of such deaning and provided by the trust agreement, the notion of Trust Agreement by the order of such cleaning of the system". While line 1267 makes a MAY reference to "if stipulated and disclosed by the trust agreement," the notion of Trust Agreement, the notion of Trust Agreement then it is not needed for processing therefore it shall not be transmitted.  20 63C 3.9.1 28 126 for processing, therefore it shall not be transmitted.  21 63C 3.10.2 30 134 (brantated as a MAY  22 63C 4.5.5 57 2156 by the variety of the system of the provided by the RP." is a SHALL but is optional as the RP is  |           |                       |         |        |          |   |                  |
| 16 63C 33.1.1 15 844 than PPI as we can define privacy policies even if we don't use PPI  18 63C 3.3.1.1 15 852 multiple RP as it proxy will be able to track and determine which PPIs represent the same subscriber at different RPs" even if the Proxy can generate a PPI upstream it can reidentify the suscriber alogn  18 63C 3.3.1 15 852 multiple RP as it proxylying all  18 63C 3.6 23 1098 that might not always exist  19 63C 3.7 24 1009 that might not always exist  19 63C 3.7 24 1009 that might not always exist  19 63C 3.7 24 1007 cases not reven mainfested again it calls out to privacy policy expectation, right to be forgotten, and other privacy notions. Maximum lifetime of information, for which the subscriber mainfested again it calls out to privacy policy expectation, right to be forgotten, and other privacy notions. Maximum lifetime of information, for which the subscriber remainfested again should be included. Exemple of exemption of such cleanning should mention other regulation like SOX and general use case for use remained to the privacy policy expectation of the subscriber information to only that which is necessary for functioning of the system." While Line 1267 makes a MAY reference to "if stipulated and disclosed by the trust agreement", the notion of Trust Agreement shall be est as a governing and mandatory requirement for the whole section. Cause if not disclosed on the trust agreement then it is not needed requirement for the whole section. Cause if not disclosed on the trust agreement then it is not needed requirement for the whole section. Cause if not disclosed on the trust agreement then it is not needed requirement for the value as a MAY  22 63C 4.3.1 46 1779 (configuration management. If so, it may be a good idea to pass this information along to": May is not forgotted the privace of the consent mechanism for value is consistently good to have an example with SCM for this section.  33.8 10 2 2 3 3 2 3 3 3 3 3 3 3 3 3 3 3 3 3 3   | 15        | 63C                   | 3.2.3   | 1,     | / /28    |   |                  |
| such cases, the proxy will be able to track and determine which PPIs represent the same subscriber at different RPS* even if the Proxy can generate a PPI upstream it can reidentify the suscriber alogn  3.3.1.1 15 852 multiple RP as it proxyfying all this is not possible outside of privacy policy and consent bound AAL at the IDP which is a specific object 198 but any thin to always exist to the other one that expect "shall not use attribute outside" again it calls out to privacy policy expectation, right to be forgotten, and other privacy notions. Maximum lifetime of information, for which the subscriber never manifested again should be included. Exemple of exemption of such cleaming should mention other regulation like SOX and general use case for use of exemption of such cleaming should mention other regulation like SOX and general use case for use of exemption of such cleaming should mention other regulation like SOX and general use case for use of exemption of such cleaming should mention other regulation like SOX and general use case for use of exemption of such cleaming should mention other regulation like SOX and general use case for use of exemption of such cleaming should mention other regulation like SOX and general use case for use of exemption of exemption of such cleaming should mention other regulation like SOX and general use case for use of exemption of exemption of exemption of such cleaming should mention other regulation like SOX and general use case for use of use of use of exemption of exemptio | 4.5       |                       | 2244    |        |          |   | 1                |
| different R9s* even if the Proxy can generate a PPI upstream it can reidentify the suscriber alogn    17   63C   33.1.1   15   85Z   Millipstream it can reidentify the suscriber alogn  | 16        | 630                   | 3.3.1.1 | 13     | 844      | 1 71  |                  |
| 17 63C 3 3.1 1 5 85.2 multiple RP as it proxyfying all this is not possible outside of privacy policy and consent bound AAL at the IDP which is a specific object this is not possible outside of privacy policy and consent bound AAL at the IDP which is a specific object this is not possible outside of privacy policy and consent bound AAL at the IDP which is a specific object this is not possible outside of privacy policy and consent bound AAL at the IDP which is a specific object this is not possible outside of privacy policy and consent bound AAL at the IDP which is a specific object this is not possible outside of privacy policy and consent bound AAL at the IDP which is a specific object this is not possible outside of privacy policy and consent bound AAL at the IDP which is a specific object this is not possible outside of privacy policy and consent bound AAL at the IDP which is a specific object this is not be read to the other one that expect "shall not use attributes outside" again it calls out to privacy policy expectation, right to be forgotten, and other privacy notions. Maximum lifetime of information for the requiring explicit consent "The IdP SHALL limit transmission of observation of the requiring explicit consent "The IdP SHALL limit transmission of observation of the requiring explicit consent "The IdP SHALL limit transmission of of trust Agreement shall be set as a governing and mandatory requirement for the whole section. Cause of the trust agreement then it is not needed to the observation of trust Agreement shall be set as a governing and mandatory requirement for the whole section. Cause of the trust agreement then it is not needed to pass this information along to": May is not configuration management. If so, it may be a good idea to pass this information along to": May is not configuration management. If so, it may be a good idea to pass this information along to": May is not configuration management. If so, it may be a good idea to pass this information along to": May is not configuration m |           |                       |         |        |          |   | 1                |
| this is not possible outside of privacy policy and consent bound AAL at the IDP which is a specific object that might not always exist This section is too moont compared to the other one that expect "shall not use attributes outside" again it calls out to privacy policy expectation, right to be forgotten, and other privacy notions. Maximum lifetime of information, for which the subscriber never manifested again should be included. Exemple of exemption of such cleanning should mention other regulation like SOX and general use case for use 19 63C 3.7 24 1107 cases not requiring explicit consent  "This Section is too moont compared to the other one that expect "shall not use attributes outside" again it calls out to privacy policy expectation, right to be forgotten, and other privacy notions. Maximum lifetime of information, for which the subscriber application is to subscribe again it calls out to privacy policy expectation, right to be forgotten, and tother privacy notions. Maximum lifetime of information for such that privacy notions. Maximum lifetime of information, for which the subscriber alterious page in the subscriber and privacy notions. Maximum lifetime of information for subscriber and privacy notions. Maximum lifetime of information for subscriber and privacy notions. Maximum lifetime of information of subscriber and privacy notions. Maximum lifetime of such privacy notions. Maximum lifetime of such privacy notions. Maximum lifetime for firetime for subscriber and privacy notions. Maximum lifetime of such privacy notions. Maximum lifetime of such privacy notions. Maximum lifetime of such privacy notions. Maximum lifetime for firetime for subscriber and privacy notions. Maximum lifetime of such privacy notions. Maximum lifetime for subscriber and privacy notions. Maximum lifetime for firetime for subscriber and privacy notions. Maximum lifetime o |           |                       |         |        |          |   | 1                |
| 18 63C 3.6 23 1098 that might not always exist This section is too moot compared to the other one that expect "shall not use attributes outside" again it calls out to privacy policy expectation, right to be forgotten, and other privacy notions. Maximum lifetime of information, for which the subscriber never manifested again should be included. Exemple of exemption of such cleanning should mention other regulation like SOX and general use case for use case for use and the subscriber information to only that which is necessary for functioning of the system". While Line 1267 makes a MAY reference to "if stipulated and disclosed by the trust agreement", the notion of Trust Agreement shall be set as a governing and mandatory requirement for the whole section. Suse if not disclosed on the trust agreement here it is not needed for processing, therefore it shall not be transmitted.  20 63C 3.9.1 28 1262 for processing, therefore it shall not be transmitted.  21 63C 3.10.2 30 1344 formatted as a MAY  22 63C 4.3.1 45 1779 requirement for the IdP as it will have to provide the consent mechanism for while the it is not needed ones in management. If so, it may be a good idea to pass this information along to": May is not formatted as a MAY  This section does not re-emphase the importance of Data Processing per susbcriber attribute  This section does not re-emphase the importance of Data Processing per susbcriber attribute  24 63C 4.3.1 46 1779 requirements, this will be important for the IdP as it will have to provide the consent mechanism for while the internation of the section.  While the identity information API definition had an example from OIDC, it would be consistently good  25 63C 4.6.5 57 2156 to have an example with SCM for this section.  | 17        | 63C                   | 3.3.1.1 | 15     | 852      |   | <u> </u>         |
| This section is too moot compared to the other one that expect "shall not use attributes outside" again it calls out to privacy policy expectation, right to be forgotten, and other privacy notions. Maximum lifetime of information, for which the subscriber never manifested again should be included. Exemple of exemption of such cleanning should mention other regulation like SOX and general use case for use as some requiring explicit consent.  The IdP SHALL limit transmission of subscriber information to only that which is necessary for functioning of the system". While Line 1267 makes a MAY reference to "if stipulated and disclosed by the trust agreement", the notion shall be set as a governing and mandatory requirement for the whole section. Cause if not disclosed on the trust agreement then it is not needed for processing, therefore it shall not be transmitted.  "configuration management. If so, it may be a good idea to pass this information along to": May is not 21 63C 3.10.2 30 1344 formatted as a MAY  If formatted as a MAY  This section does not re-emphase the importance of Data Processing per subscriber attribute  This section does not re-emphase the importance of Data Processing per subscriber attribute  While the Identity information API definition had an example from OIDC, it would be consistently good to have an example with SCMI for this section.  |           |                       |         |        |          |   | 1                |
| It calls out to privacy policy expectation, right to be forgotten, and other privacy notions. Maximum lifetime of information, for which the subscriber never manifested again should be included. Exemple of exemption of such cleaning should mention other regulation like SOX and general use case for use of exemption of such cleaning explicit consent  The IdP SHALL limit transmission of subscriber information to only that which is necessary for functioning of the system. While Line 1267 makes a MAY reference to "if stipulated and disclosed by the trust agreement," the notion of Trust Agreement shall be set as a governing and mandatory requirement for the whole secition. Cause if not disclosed on the trust agreement then it is not needed for processing, therefore it shall not be transmitted.  20 63C  3.9.1  28 1262 for processing, therefore it shall not be transmitted.  "configuration management. If so, it may be a good idea to pass this information along to": May is not formatted as a MAY of sit will have to provide the consent mechanism for While the Identity information API definition had an example from OIDC, it would be consistently good to have an example with SCIM for this section.  "This section does not re-emphase the importance of Data Processing per susbcriber attribute which is necessary to the consent mechanism for While the Identity information API definition had an example from OIDC, it would be consistently good to have an example with SCIM for this section.  "So None: A cryptographic nonce, if one is provided by the RP." is a SHALL but is optional as the RP is  | 18        | 63C                   | 1       | 3.6 2  | 1098     |   |                  |
| lifetime of information, for which the subscriber never manifested again should be included. Exemple of exemption of such cleaning should mention other regulation like SOX and general use case for use as a governing and mandatory requirement for the whole section. Cause if not disclosed on the trust agreement shall be set as a governing and mandatory requirement for the whole section. Cause if not disclosed on the trust agreement then it is not needed for processing, therefore it shall not be transmitted.  20 63C  3.9.1  28 1262 for processing, therefore it shall not be transmitted.  "Configuration management. If so, it may be a good idea to pass this information along to": May is not configuration management. If so, it may be a good idea to pass this information along to": May is not for mention of the standard of the shall not be transmitted.  This section does not re-emphase the importance of Data Processing per subscriber attribute  33 63C  4.3.1  46 1779 requirements, this will be important for the lide as it will have to provide the consent mechanism for While the Identity information API definition had an example from OIDC, it would be consistently good to have an example with SCIM for this section.  "Kind the Identity information API definition had an example from OIDC, it would be consistently good to have an example with SCIM for this section.  "Revenue API and the information and the subscriber and the information as the RP is as SHALL but is optional as the RP is  |           |                       |         |        |          |   | 1                |
| of exemption of such cleanning should mention other regulation like SOX and general use case for use  3.7 24 1107 cases not requiring explicit consent.  "The IdP SHALL limit transmission of subscriber information to only that which is necessary for functioning of the system". While Line 1267 makes a MAY reference to "if stipulated and disclosed by the trust agreement", the notion of Trust Agreement shall be set as a governing and mandatory requirement for the wholescetion. Cause if not disclosed on the trust agreement then it is not needed for processing, therefore it shall not be transmitted.  3. 10.2 30 1344 formatted as a MAY  "configuration management. If so, it may be a good idea to pass this information along to": May is not disclosed by the strain and th |           |                       |         |        |          | it calls out to privacy policy expectation, right to be forgotten, and other privacy notions. Maximum       | 1                |
| 19 63C 3.7 24 1107 cases not requiring explicit consent  19 63C 3.9 24 1107 cases not requiring explicit consent  19 63C 3.9 1   |           |                       |         |        |          | lifetime of information, for which the subscriber never manifested again should be included. Exemple        |                  |
| "The IdP SHALL limit transmission of subscriber information to only that which is necessary for functioning of the system". While Line 1267 makes a MAY reference to "if stipulated and disclosed by the trust agreement", the notion of Trust Agreement shall be set as a governing and mandatory requirement for the whole seciton. Cause if not disclosed on the trust agreement then it is not needed for processing, therefore it shall not be transmitted.  20 63C 3.9.1 28 1262 for processing, therefore it shall not be transmitted.  21 63C 3.10.2 30 1344 formatted as a MAY  22 63C 3.11.1 32 1389 No mentionning W3C DID sounds like an opiniated omission  23 63C 4.3.1 46 1779 requirements, this will be important for the IdP as it will have to provide the consent mechanism for While the Identity information API definition had an example with SUM for this section.  4 63C 4.6.5 57 2156 to have an example with SUM for this section.  5 8. Nonce: A cryptographic nonce, if one is provided by the RP." is a SHALL but is optional as the RP is  |           |                       |         |        |          | of exemption of such cleanning should mention other regulation like SOX and general use case for use        | 1                |
| "The IdP SHALL limit transmission of subscriber information to only that which is necessary for functioning of the system". While Line 1267 makes a MAY reference to "if stipulated and disclosed by the trust agreement", the notion of Trust Agreement shall be set as a governing and mandatory requirement for the whole seciton. Cause if not disclosed on the trust agreement then it is not needed for processing, therefore it shall not be transmitted.  20 63C 3.9.1 28 1262 for processing, therefore it shall not be transmitted.  21 63C 3.10.2 30 1344 formatted as a MAY  22 63C 3.11.1 32 1389 No mentionning W3C DID sounds like an opiniated omission  23 63C 4.3.1 46 1779 requirements, this will be important for the IdP as it will have to provide the consent mechanism for While the Identity information API definition had an example from OIDC, it would be consistently good to a consistently good to a sex and the provided by the RP." is a SHALL but is optional as the RP is   | 19        | 63C                   |         | 3.7 24 | 1107     | cases not requiring explicit consent  | 1                |
| the trust agreement", the notion of Trust Agreement shall be set as a governing and mandatory requirement for the whole section. Cause if not disclosed on the trust agreement then it is not needed for processing, therefore it shall not be transmitted.    1   |           |                       |         |        |          |   |                  |
| the trust agreement", the notion of Trust Agreement shall be set as a governing and mandatory requirement for the whole section. Cause if not disclosed on the trust agreement then it is not needed for processing, therefore it shall not be transmitted.    1   |           |                       |         |        |          | functioning of the system". While Line 1267 makes a MAY reference to "if stipulated and disclosed by        | 1                |
| 20 63C 3.9.1 228 1262 for processing, therefore it shall not be transmitted.  21 63C 3.10.2 30 1344 formatted as a MAY  22 63C 3.11.1 32 1389 No mentionning W3C DID sounds like an opiniated omission  23 63C 4.3.1 46 1779 requirements, this will be important or the IdP as it will have to provide the consent mechanism for  24 63C 4.6.5 57 2156 to have an example with SCIM for this section.  3.9.1 426 1779 requirements, this will be important of not led Pas it will have to provide the consent mechanism for  4.6.5 57 2156 to have an example with SCIM for this section.   |           |                       |         |        |          |   | 1                |
| 20 63C 3.9.1 28 1262 for processing, therefore it shall not be transmitted.  **Configuration management. If so, it may be a good idea to pass this information along to": May is not a start and a sta |           |                       |         |        |          |   | 1                |
| "configuration management. If so, it may be a good idea to pass this information along to": May is not formatted as a MAY  22 63C 3.1.1 32 1389 No mentionning W3C DID sounds like an opiniated omission  This section does not re-emphase the importance of Data Processing per susbcriber attribute  This section does not re-emphase the importance of Data Processing per susbcriber attribute  This section does not re-emphase the importance of Data Processing per susbcriber attribute  While the Identity information API definition had an example from OIDC, it would be consistently good  4.6.5 57 2156 to have an example with SCIM for this section.  "8. Nonce: A cryptographic nonce, if one is provided by the RP." is a SHALL but is optional as the RP is   | 20        | 63C                   | 3.9.1   | 25     | 1262     |   | 1                |
| 21 63C   3.10.2   30   1344   formatted as a MAY   | 20        |                       |         |        | 12.02    |   |                  |
| 22 63C 3.11.1 32 1389 No mentionning W3C DID sounds like an opiniated omission  This section does not re-emphase the importance of Data Processing per susbcriber attribute  23 63C 4.3.1 46 1779 requirements, this will be important for the IdP as it will have to provide the consent mechanism for  While the Identity information API definition had an example from OIDC, it would be consistently good  4.6.5 57 2156 to have an example with SCIM for this section.  "8. Nonce: A cryptographic nonce, if one is provided by the RP." is a SHALL but is optional as the RP is   | 21        | 63C                   | 3 10 2  | 31     | 13/1/    |   | 1                |
| This section does not re-emphase the importance of Data Processing per susbcriber attribute requirements, this will be important for the IdP as it will have to provide the consent mechanism for While the Identity information API definition had an example from OIDC, it would be consistently good While the Identity information API definition had an example from OIDC, it would be consistently good This section does not re-emphase the importance of Data Processing per susbcriber attribute requirements, this will be important for the IdP as it will have to provide the consent mechanism for While the Identity information API definition had an example from OIDC, it would be consistently good This section does not re-emphase the importance of Data Processing per susbcriber attribute requirements, this will be important for the IdP as it will have to provide the consent mechanism for While the Identity information API definition had an example from OIDC, it would be consistently good This section does not re-emphase the importance of Data Processing per susbcriber attribute requirements, this will be important for the IdP as it will have to provide the consent mechanism for While the Identity information API definition had an example from OIDC, it would be consistently good This section API are the IdP as it will have to provide the consent mechanism for While the Identity information API are the IdP as it will have to provide the consent mechanism for This section does not require the IdP as it will have to provide the consent mechanism for This section does not require the IdP as it will have to provide the consent mechanism for This section does not require the IdP as it will have to provide the consent mechanism for This section does not require the IdP as it will have to provide the consent mechanism for This section does not require the IdP as it will have to provide the consent mechanism for This section does not require the IdP as it will have to provide the consent mechanism for This section does not require th |           |                       |         |        |          |   |                  |
| 23 63C 4.3.1 46 1779 requirements, this will be important for the IdP as it will have to provide the consent mechanism for  While the Identity information API definition had an example from OIDC, it would be consistently good  4.6.5 57 2156 to have an example with SUM for this section.  8 8 Nonce: A cryptographic nonce, if one is provided by the RP." is a SHALL but is optional as the RP is   | - 22      |                       | J.11.1  | 3,     | 1363     | The menderning 1100 0.0 Sounds like an opiniated offission  |                  |
| 23 63C 4.3.1 46 1779 requirements, this will be important for the IdP as it will have to provide the consent mechanism for  While the Identity information API definition had an example from OIDC, it would be consistently good  4.6.5 57 2156 to have an example with SUM for this section.  8 8 Nonce: A cryptographic nonce, if one is provided by the RP." is a SHALL but is optional as the RP is   |           |                       |         |        |          | This section does not to emphase the importance of Data Processing per sucheribes attribute                 | 1                |
| While the Identity information API definition had an example from OIDC, it would be consistently good to have an example with SCIM for this section.  While the Identity information API definition had an example from OIDC, it would be consistently good to have an example with SCIM for this section.  "8. Nonce: A cryptographic nonce, if one is provided by the RP." is a SHALL but is optional as the RP is   | 22        | cac                   | 421     |        | 1770     |   | 1                |
| 24 63C 4.6.5 57 2156 to have an example with SCIM for this section.  8 8 Nonce: A cryptographic nonce, if one is provided by the RP." is a SHALL but is optional as the RP is  | 23        | 03C                   | 4.3.1   | 41     | 1//5     |   |                  |
| "8. Nonce: A cryptographic nonce, if one is provided by the RP." is a SHALL but is optional as the RP is   |           |                       |         |        |          |   | 1                |
|  | 24        | b3L                   | 4.6.5   | 5      | / 2156   |   |                  |
| 25 63C 4.9 63 2345 not forced to provide one. This sounds inconsistent.  |           |                       |         |        |          |   | 1                |
| <u> </u>   | 25        | 63C                   | 1       | 4.9 63 | 2345     | not forced to provide one. This sounds inconsistent.  | ı                |

| 26 | 63C | 4.1        | 65  | 2400 | See comment above, now the nonce is mandatory again through SHALL  |  |
|----|-----|------------|-----|------|--|--|
| 27 | 63C | 5.7        | 74  | 2641 | See comment above, now the nonce is mandatory again through SHALL  |  |
|    |     |            |     |      | "9. Nonce: A cryptographic nonce, if one is provided by the RP." is a SHALL but is optional as the RP is |  |
| 28 | 63C | 5.8        | 75  | 2664 | not forced to provide one. This sounds inconsistent.   |  |
|    |     |            |     |      | the first two lines of federation Threat / attacks should disjoint the "Assertion Manufacture and        |  |
|    |     |            |     |      | Modification" is two distinct threat for readability. "Assertion Manufacture" and "Assertion             |  |
| 29 | 63C | Table 2    | 79  | -    | Modification"  |  |
|    |     |            |     |      | Here, there is no mention of sending an update of the consent to the Authorized parties involved for     |  |
|    |     |            |     |      | application of the new consent. Also Consent through this document is not always called with the same    |  |
| 30 | 63C | 8.2.2      | 90  | 3101 | name, sometimes it is called "Control over Attribute disclosure"   |  |
|    |     |            |     |      | All OIDC references, where applicable, should at least point also to the newly ISO standardization and   |  |
| 31 | 63C | References | 105 | 3534 | corresponding URL for the ISO Standard   |  |