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:	*Digital Agency (Government of Japan), MyDataJapan and OpenID Foundation Japan*
Name of Submitter/POC:	*- HAYASHI Tatsuya, YAMADA Tatsushi, OBATA Masato, SAKAMOTO Takahito, MAEKAWA Sami, and other volunteer members of Digital Agency (Government of Japan)* *- volunteer members of MyDataJapan* *- volunteer members of OpenID Foundation Japan*
Email Address of Submitter/POC:	[redacted]

Comment #	Publication (Base, 63A, 63B, 63C)	Section	Page #	Line #	Comment (Include rationale for comment)	Suggested Change
1	63-Base 63B 63C	2.5.(Base) 3.1.7.3.(63B) 5.(63C)	16(Base) 27(63B) 69(63C)	817(Base) 1171(63B) 2494(63C)	When using a Subscriber Controlled Wallet for authentication, the information for the federated identifier must be pre-registered in the RP Subscriber Accounts during the identity proofing and enrollment process. (This is assumed to be the Subject identifier, etc., in 63C 5.8 Assertion Contents) For this reason, even RP you only want to authenticate using a Subscriber Controlled Wallet, RP will still need to obtain the Core Attribute information each time, which is a privacy issue, so we would like it to be clearly stated that it is preferable to prepare the federated identifier as an Attribute Bundle.	
2	63-Base	1.2.	3	436-439	The title of 2.2 is changed to “Identity proofing and Enrollment” in the second public draft, so we believe that IAL covers “identity proofing and entrollment process” and “Identity proofing and process” should be revised to ”Identity Assurance Level (IAL) refers to the identity proofing and enrollment process. Similarly, AAL should be “Authentication and Authenticator Management process” and FAL should be “Federation and Assertions process.	
3	63-Base	2.1.	10	646	Please fix the following errors. Incorrect: Service provider: Service providers can perform any combination of functions involved in granting access to and delivering online services, such as a credential service provider, relyin party, verifier, and Identity provider. Correct: Service provider: Service providers can perform any combination of functions involved in granting access to and delivering online services, such as a credential service provider, relying party, verifier, and Identity provider.	
4	63-Base	2.1.	10	644	In 2. Digital Identity Model 2.1 Overview, it is stated that Service Providers have the “function” of CSP, RP, IDP, and Verifier. Since CSP, RP, IDP and Verifier are also used as ‘Entity’, why not clearly state that you should use the terms “Entity” and “Function” differently? In addition, we would like you to add the following specific explanations as examples. - In the case of Figure 3, “The Subject and Service Provider exist as Entities. The Service Provider provides the functions of RP, Verifier, and CSP.” - In the case of Figure 4, “The Subject, IDP, RP, and CSP exist as Entities. The IDP maintains Subscriber Accounts and provides the function of Verifier.” - In the case of Figure 5, “the Subject, Subscriber-controlled Wallet, RP, and CSP exist as entities. The CSP provides the function of identity proofing when onboard the Subscriber-controlled Wallet. In addition, the Subscriber-controlled Wallet functions as an IDP.” In the glossary at the end of the document, CSP, RP, IDP and Verifier are listed as entities, so we think it would be better to combine this with the description in 2.1 Overview. Also, instead of using Verifier as a function, why not use Verify as a function, and change the description to something like “RP verifies”?	
5	63-Base	2.5.	16	817	It would be easier to understand if the Digital Identity Models were divided into sections, so please organize the chapters as follows. 2.5.1 Non-Federated Digital Identity Model Example 2.5.2 Federated Digital Identity Model Example 2.5.3 Federated Digital Identity Model With Subscriber-Controlled Wallet Example	

6	63-Base	2.5.	20	898	In this diagram, the term “Verifier” seems to be used to mean the glossary definition of “Verifier” (An entity that verifies the claimant's identity by verifying the claimant's possession and control of one or more authenticators using an authentication protocol. To do this, the verifier needs to confirm the binding of the authenticators with the subscriber account and check that the subscriber account is active). If that is the case, then it seems inappropriate for the verifier to be written in the CSP. If it is not, the Subscriber Controlled Wallet has three main processes according to Fig. 13 Subscriber-Controlled Wallet in 63C, so we would like you to clarify which process it is and what meaning you are using for the term “verifier”. - The process by which a subject registers a Wallet (Provisioning the Subscriber-Controlled Wallet) - The process by which a subject registers a Wallet or a Wallet attribute bundle with the RP - The process by which a subject logs in to the RP using a Wallet In addition, it seems that the issue is not just with this section, but that throughout the volume, the terms “verify” and “verifying” are used in various contexts (as “verification”, as “verifier”, etc.). We would like you to make it easier to understand which meaning you are using for the terms “verify” and “verifying”.	
7	63-Base	3.2.2.	30	1206	We think that there are cases where it is necessary to select different levels for each of IAL, AAL, and FAL, as mentioned in the IPD, so we would like this to be clearly stated. If it is possible to evaluate them together, as mentioned in the 2nd PD, We would like it to be clearly stated in what cases this is possible.	
8	63-Base	3.2.1.	29	1151	“Degradation of mission delivery” is to be conducted in the Initial Impact Assessment, but mission delivery may be strongly affected by the results of the Initial IAL/AAL (e.g., not having the necessary identity documents, have difficulty in using the required Authenticator, etc.). Therefore, Mission Delivery should be conducted at the Tailoring phase (or verified again at the Tailoring) instead of Initial Impact Assessment.	
9	63-Base	3.3.2.2.	36	Table 2	In the AAL3 Summary, it says “AAL3: Provide phishing resistance and verifier compromise protections.” However, instead of requiring a “hardware-based authenticator with a non-exportable private key”, wouldn't it be more appropriate to state the requirement as “resistance to the threat of Authenticator Dupulication attacks” obtained by a hardware-based authenticator with a non-exportable private key?	
10	63-Base	3.5.2.	46	Table 4.	We think the following items should be added to Performance Metrics. We think they are necessary as part of Performance evaluation from the perspective of Mission Delivery, Usability, Equity, etc. - The number of issued IDs and the percentage of the total number of potential users, and the deviation from the projected number of issues - The number of IDs that have expired and an analysis of the reasons for this...same as above - Reasons for abandonment (probably a refinement of the identity proofing and enrollment processes and an analysis of where they stopped) The number of authenticators that have expired and been reissued...this should be similar to account recovery, but there should be cases where reissue is possible with the remaining authenticators.	
11	63-Base	3.5.3.	48	1730	In order to properly conduct Equity Assessments, it is often necessary to collect information on the attributes related to equity held by the applicant. This paper states that “Where possible, these efforts SHOULD avoid the collection of additional personal information and instead use informed analysis of proxy data to help provide indicators of potential disparities.” However, it should also include a more detailed explanation of the precautions that need to be taken when additional information needs to be collected (the purpose of use should be limited to the Equity Assessment, and the information should be deleted promptly after the necessary analysis is complete: this is obvious in terms of the principle of collecting personal information, but it is often even more sensitive).	

12	63-Base	Appendix B.	67	2322	Thank you for providing the definition of the term "Digital Identity." We believe that the current description is appropriate for the definition as it is used in SP 800-63. However, considering that this document may become a commonly referenced definition after publication, we feel that the phrase "that uniquely describes" might be too restrictive. As outlined in the definition provided by ISO/IEC 24760-1:2019, it is more common to define Digital Identity as a set of attributes linked to an entity. We believe modifying the definition or including this perspective would enhance the definition. ISO/IEC 24760-1:2019 > 3.1.2 > *identity* > *partial identity* > set of attributes (3.1.3) related to an entity (3.1.1) > Note 1 to entry: An entity can have more than one identity. > Note 2 to entry: Several entities can have the same identity. > Note 3 to entry: ITU-T X1252[13] specifies the distinguishing use of an identity. In this document, the term identifier implies this aspect. For example, how about the following revision? > An attribute or set of attributes that describes a subject within a given context.	
13	63A	2.2.	9	623	From line 623 onwards, it is stated that some attributes SHOULD be collected as core attributes, but it is not specified why this information is necessary or what purpose it serves. The reasons and purpose for why the collection of these attributes is recommended should be clearly stated. Also, if you are relying on Assertion/Presentation provided selectively by CSPs with a high IAL level for identity proofing, “which CSP confirmed it” and “the Assertion signed by the CSP” should be sufficient. If a photograph is required for account recovery, it is better to obtain it from the CSP when it is needed, rather than collecting it in advance. From the perspective of data minimization, such a method is preferable.	
14	63A	2.2.	9	618-631	While it is stated that “the minimum attributes necessary to accomplish identity proofing” and “the necessary core attributes for a given use case will change based on the nature of the community being served”, feel there is a contradiction in the fact that First Name, Last Name, Government Identifier, Physical Address or Digital Address are specified as the attributes that SHOULD be collected. For example, this would encourage the collection of real names even for services that do not necessarily require them. So it would be better to limit the Core Attributes to the minimum attributes required for identity proofing, and the listed attributes should not be described as ‘SHOULD be collected’, but rather as ‘is generally collected’ for example.	
15	63A	1.2.	2	412	There are two levels below IAL1: the case where “necessary Identity cannot be collected” and the case where “Identity should not be collected for privacy protection or other reasons”. Therefore after the paragraph ”No identity proofing: There is no requirement to link the applicant to a specific, real life person. Any attributes provided in conjunction with the subject’s activities are self-asserted or are treated as self-asserted. Evidence is not validated and attributes are neither validated nor verified.” How about adding the following sentence. ”and there is a chance of requirement to shouldn't link the applicant to a specific, real life person. In that case any attributes provided in conjunction with the subject’s activities shall be treated as self-asserted and shouldn't be validated nor verified.	
16	63A	4.1.10.	39	1622	In the Initial Authenticator binding in IAL1 and IAL2, the confirmation code is allowed when the authenticator binding is performed in a separate session from the identity proofing, but we believe that this is not strong enough, especially in IAL2. For that reason we suggest to add the sentence “Therefore, it is possible to issue an authenticator corresponding to the required AAL in the identity proofing session even if identity proofing has not been completed, and then continue identity proofing using that authenticator to satisfy the IAL requirements.”	
17	63A	2.4.	10	645	The Assertion sent as a result of the Federation should also be considered as Evidence, but it is difficult to read from the current description. Please clearly state this in the appropriate part of the main text. Also, please clearly state this in the evidence examples in Appendix A.	

18	63A	2.4.1.1. 2.4.1.2. 2.4.1.3.	10-12	664-732	The definition of the requirement to repeat the sentence slightly differently for each of FAIR, STRONG, and SUPERIOR makes it difficult to understand and compare the differences between the requirements. We would like you to write it in the following way: 'STRONG (or SUPERIOR) additionally requires that...'. In SUPERIOR, it seems that the requirement (The information on the evidence is able to be validated by an authoritative or credible source.) in FAIR/STRONG is missing. We would like you to eliminate this kind of omission, and we would like you to do the above.	
19	63A	2.4.1.1.	10-11	664-684	The requirements for FAIR evidence in 2.4.1.1. are excessive for the purpose of IAL1 (Limit highly scalable attacks) described in base volume 3.3.2.1. Identity Assurance Level. In addition, they are not consistent with the examples given later. The following revisions may be appropriate. - Item 2 (The evidence contains the name of the claimed identity.) should be deleted. Because there are services for which it is not necessary to have the name, and it is sufficient to meet item 3 (The evidence contains at least one reference number, a facial portrait, or sufficient attributes to uniquely identify the person to whom it relates.) - Item 4 (The evidence contains physical (e.g., security printing, optically variable features, holograms) or digital security features that make it difficult to reproduce.) should be deleted. Because it is expected that many evidence that could be used as Fair evidence will not meet the criteria. - Item 5 and 6, it is not necessary to go as far as 'is able to be validated/verified', and it is sufficient to stop at 'is highly likely to be able to be validated/verified'. Because it is sufficient if it is possible to do so by contacting the issuing institution when a problem is discovered.	
20	63A	2.5.1.	14	780	Verification can be achieved by "practicing authentication using a PIN linked to evidence". (e.g. authenticating by entering a PIN when reading the data on the IC chip installed in Evidenced) In order to increase the options for non-biometric methods, it should be included in "Authentication and Federation Protocols" or defined as a separate method.	
21	63A	3.1.8.	25	1161	It seems that SMS or voice are the only options when using a telephone number from the description of the validity period of the confirmation code as follows. "10 minutes, when sent to a validated telephone number (SMS or voice);" RCS should also be added, or SMS or voice should be expressed as examples. Also, in line 2357 of 8.3. Identity Proofing and Enrollment, it says that the confirmation code can be sent by "(e.g., physical mail, SMS, landline telephone, or email)." SMS is listed as one of the options, so we would like to see the description standardized.	
22	63A	2.1.3.	8	585	The combination of Remote/OnSIte and Attended/Unattended was defined as Identity Proofing Types, but it is easily misunderstood. In particular, the definition of KIOSK as OnSite is considered to be misleading. The essential difference between Remote/OnSite is whether the environment is controlled or not. so how about changing the name "Onsite/Remote to Controlled/Uncontrolled, etc. ?	
23	63A	2.4.1.1.	10-11	666 674	There are two item 1 for the FAIR requirements. (LINE 666, 674)	
24	63A	2.4.1.1.	11	681-682	LINE 681-682 says "validated by an authoritative source", but we think "validated against" is correct. It is assumed that it is practically impossible for an authoritative source to validate.	
25	63A	4.1.2.	36	1521	It says "evidence (FAIR or STRONG)", but why is SUPERIOR excluded? If there is a reason, it should be clearly stated. If there is no reason for exclusion, SUPERIOR should also be included in parentheses.	
26	63A	4.1.10.	39-40	1621-1638	In Appendix B of 63B-4, there is a description of the problem of sharing with regard to Syncable Authenticators, but isn't sharing a problem that can occur with authenticators other than Syncable Authenticators in the first place? For that reason, it would be good to clearly state a requirement such as "CSP SHALL inform the subscriber that they SHOULD NOT share authenticators." in Initial Authenticator Binding, etc. of 63A-4.	
27	63A	4.1.6. 4.2.6. 4.3.6.	37 42 46	1549 1701 1839	The concept of "verification pathways (non-biometric/digital evidence/biometric)" has been introduced, but it appears to be used only in IAL2. We would like to see Verification Requirements defined in this framework for IAL1 and IAL3 as well.	

28	63A	4.1.6. 4.2.6.	37 42	1552 1717 1727	There are slight differences in the descriptions of Verification Requirements in IAL1 and IAL2. If these are intended differences, please add additional information or examples to make it clear what kind of requirements are different. If they are not intended, please unify the expressions. Example: IAL1 and IAL2 Requirements for confirmation codes - IAL1: Confirming the applicant's ability to return a confirmation code delivered to a validated address associated with the evidence; - IAL2(FAIR Evidence): Confirming the applicant's ability to return a confirmation code delivered to a validated address associated with the evidence (e.g., postal address, email address, phone number) - IAL2(STRONG or SUPERIOR Evidence): Confirming the applicant's ability to return a confirmation code delivered to a physical address (i.e., postal address) that was obtained from the evidence and was validated with an authoritative source	
29	63A	4.1.7.	38	1587	In Remote Attended Requirements, countermeasures against deep fakes and recordings are defined as SHOULD. Given the recent threat trends, shouldn't this requirement be SHALL? Or, shouldn't IAL1/2 distinguish between SHOULD and SHALL?	
30	63A	6.1.	55	The last line of Table 3	In Table 3. Identity Proofing and Enrollment Threat Mitigation Strategies, there is a mention of PAD (Presentation Attack Detection) as a countermeasure against the threat/attack "Video or Image Injection Attack", but the corresponding Normative Reference(s) column states 3.1.8. However, 3.1.8 is Requirements for Confirmation Codes, and this alone may be insufficient as a reference for countermeasures against video injection attacks. For example, 4.1.7 (IAL1/2), 4.1.9 (IAL1/2), and 4.3.8 (IAL3) may also be referenced.	
31	63A	6.1.	55	The last line of Table 3	In Table 3, PAD (Presentation Attack Detection) is listed as a countermeasure against video or image injection attacks, but it appears that presentation attacks and injection attacks are being discussed together. Presentation attacks and injection attacks should be defined separately, and countermeasures should be defined as PAD (Presentation Attack Detection) and IAD (Injection Attack Detection) respectively.	
32	63A	7.1.	57	2039	Although it is stated that data collection should be limited to what is necessary for identity proofing, it would be preferable to also mention that data that is necessary for identity proofing but is not required for subsequent service provision should be deleted as soon as the necessary processing is complete.	
33	63A 63C	7.2.(63A) 7.2.(63C)	58(63A) 82(63C)	2069(63A) 2831(63C)	Since there are no references in 63A 7.2 Notice and Consent or 63C 7.2 Notice and Consent, how about referring to ISO/IEC 29184?	
34	63A	A.3.	82	Table 6.	If the European Digital Identity Wallet (EUDI Wallet) Personal Identification (PID) Element is listed as an example of Superior Evidence in Table 6, then the Japanese Individual Number Card (My Number Card) and JPKI (Japanese Public Key Infrastructure) should also be listed. If you are going to include them in the list, please contact POC of Digital Agency Japan listed at the beginning of this document. We will help with the content to be included in the table (Proofing/Validation/Verification).	
35	63B	3.1.5.1.	24	1059	Regarding OTP Authentication, "MAY truncate its output to as few as six decimal digits or equivalent." but "equivalent" can be misunderstood easily. so How about changing to "as few as six decimal digits or string with equal or more strong in entropy than that?"	
36	63B	2.3.2.	8	606-625	The description of AAL 3 in the Introduction states that it is a non-exportable private key and a phishing-resistant hardware-based authenticator as follows "Authentication Assurance Level 3: AAL3 provides very high confidence that the claimant controls one or more authenticators bound to the subscriber account being authenticated. Authentication at AAL3 is based on the proof of possession of a key through the use of a public-key cryptographic protocol. AAL3 authentication requires a hardware-based authenticator with a non-exportable private key and a phishing-resistant authenticator (see Sec. 3.2.5); the same device may fulfill both requirements. To authenticate at AAL3, claimants are required to prove possession and control of two distinct authentication factors." On the other hand, the AAL 3 requirements (Sec. 2.3.2) only state "The cryptographic authenticator used at AAL3 SHALL be hardware-based and SHALL provide phishing resistance, as described in Sec. 3.2.5.", and does not include a statement to the effect that the private key is non-exportable. Shouldn't 2.3.2 also include a statement to the effect that the private key is non-exportable? In Appendix B, it is stated as follows, and I think there is also a non-exportability requirement. "Syncing authentication keys inherently means that the key can be exported. Authentication at AAL2 may be supported subject to the above requirements. However, syncing violates the non-exportability requirements of AAL3. Similar protocols using keys not stored in an exportable manner that meet the other requirements of AAL3 may be used."	

37	63B	3.1.7.3.	27-28	1171-1191	In 63C 5.1., the Activation Factor is defined as SHOULD, and in 63B 3.1.7.3., the Wallet is defined as MF Crypt Authenticator. However, at present, there is no way to tell the Verifier whether the Wallet has been unlocked with the Activation Factor, and there is a concern that it will be treated as MF Crypt Authenticator even though it has not actually been unlocked with the Activation Factor. This should be clearly stated.	
38	63B	3.1.3.1.	19	889	3.1.3.1 Out-of-Band Authenticators says “Email SHALL NOT be used for out-of-band authentication because it may be vulnerable to” and that Email is not allowed, but in 4.2.1.2 Issued Recovery Codes, it says “CSPs that support this option allow the subscriber to maintain one or more recovery addresses (e.g., postal, email, text message, or voice). We felt that there was something strange about the fact that email was allowed as a destination for recovery codes. We want clarification on which IAL/AAL cases allow and do not allow the sending of secrets and codes by email. Alternatively, it might be better to use SHOULD NOT instead of SHALL NOT in 3.1.3.1.	
39	63B	5.1.1	50	1932-1946	We believe that there is a need to clarify specific security requirements for session management using Browser Cookies with high AAL (especially AAL2 and AAL3). We also believe that there is a need to present restrictions on the use of Browser Cookies and alternative methods. Specifically, we propose: Providing examples of session management techniques that meet non-export requirements and phishing resistance requirements Providing examples of session management methods using hardware-based authenticators, etc.	
40	63B	7	61	2078	We think there is little mention of security and privacy in terms of how vendors that provide authenticators handle data. Shouldn't we define requirements such as what kind of authenticators should be used, for example, not only requirements for authenticators such as FIPS140 certification, but also requirements for security certification that vendors providing authenticators should have, such as ISO27001?	
41	63B	B.4.	90	2994	Despite the statement “As indicated in Table 5,” Table 5 does not exist in the document. If the reference to another table or chapter seems correct, please specify the correct reference destination. If the table is missing from the B.4 chapter, please add the table.	
42	63C	1	1	396	Considering the existence of multi-factor authentication, wouldn't it be more appropriate to write “one or some of the authenticators” instead of “one of the authenticators” in the following description? “Federation is a process that enables the subscriber account defined in [SP800-63A] to be used with an RP that does not verify one of the authenticators bound to the subscriber 397 account.”	
43	63C	3.11.1.	31	1384-1407	The Requirements for Attribute Bundles are listed in the Common Federation Requirements. Shouldn't the requirements for wallets be listed in Chapter 5? Or is there a case where Attribute Bundles are handled by General IdPs? If so, we would like to see a specific example of a case where Attribute Bundles are used by General IdPs.	
44	63C	3.11.3.	33	1448	The following is written from line 1448 of Part C. "Access to the identity API SHOULD be limited to the duration of the federation transaction plus time necessary for synchronization of attributes," 4.6.4 is referenced in this regard, but 4.6.4 only gives an example of a use case where synchronization is performed at login, and it does not appear to be intended to cover cases such as updating attribute values for continuous access control in response to security events or sending push notifications based on attribute values when the user is offline. It seems that these cases should be added.	
45	63C	3.12.4.	36	1549	For audience restriction, it is mandatory that only a single RP is targeted for FAL2 and above, but for FAL1, it is also permissible to specify multiple RPs as the audience. We would like you to clarify what kind of difference in threat tolerance is created by this difference in requirements (in other words, what kind of threats are accepted by FAL1).	
46	63C	4.1.	43	1718	The following description in LINE 1718 mentions an undefined actor called “IdAM”. This should be replaced with a defined actor. “Such IdPs are generally in the same security domain as the IdAM that houses the subscriber account.”	
47	63C	4.7.	60	Figure 10	In Fig. 10, it is written as if the “Authenticator” is being sent from the Subject to the IdP. In reality, it should be written as “Authenticator output”. Reference: In Fig. 2 of 63-4 Base Volume, it is written as “Authenticator output”, so the description should be consistent.	

48	63C	4.8.	62	2298	Because sending more information than necessary is a concern for privacy, We would like it to be clearly stated that “sending as a signal of the specific content of the modified attribute information should be limited to what is necessary to determine whether compromise is suspected”. Also, on lines 2298-2299, it is stated that the transmission of a signal that “attributes have changed” SHOULD be sent, but since this is considered inappropriate for attribute information that is frequently changed (such as location information), please clearly state that it is also undesirable to send a signal other than the one necessary to determine that compromise is suspected, even if it is only a notification that attributes have changed.	
49	63C	4.10.	65	2401	Requirements that SHALL NOT be done should also be specified. For example, IdP and RP SHALL NOT implement the federation protocol that pass passwords between IdP and RP.	
50	63C	5.2.	70	Figure 13	In Fig. 13, it is written as if the “Authenticator” is being sent from the Subject to the IdP. In reality, it should be written as “Authenticator output”. Reference: In Fig. 2 of 63-4 Base Volume, it is written as “Authenticator output”, so the description should be consistent.	
51	63C	5.2.	71	2532	In LINE 2532, it says “5. The subscriber activates the wallet through an authentication factor”, but in Fig. 13. Subscriber-Controlled Wallet, the Activation of Wallet section says “Activation Factor”. I think Activation Factor is correct, so we propose a correction.	
52	63C	5.5.	73	2604	Isn't the “singing public key” in LINE 2604 actually a “signing public key”?	
53	63C	6.2.	80	Table 3	In the “Assertion Redirect” row of the Federation Threat/Attack in Table 3, the “Normative Reference(s)” column is blank. Shouldn't you be referring to 3.12.4. Audience Restriction?	
54	63C	7	81	2773	It would be better to directly mention cases where RP intentionally extracts a large amount of personal information (attributes that are not originally necessary for service provision) from IdP. It is difficult to imagine this from the minimisation of data provided by IdP and the Trust Agreement-related statements.	