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

Please submit responses to dig-comments@nist.gov by March 24, 2023

Organization:	*Digital Agency Japan and OpenID Foundation Japan*
Name of Submitter/POC:	*- HAYASHI Tatsuya, YAMADA Tatsushi, SHINZAKI Takashi, MAEKAWA Sami, and other volunteer members of Digital Agency Japan* *- Volunteer members of OpenID Foundation Japan*
Email Address of Submitter/POC:	[REMOVED]

Comment #	Publication (Base, 63A, 63B, 63C)	Section	Page #	Line #	Comment (Include rationale for comment)	Suggested Change
1	63-Base	5.2.2.1. Identity Assurance Level	31	1197 - 1205	In SP800-63A-4, IAL0 (No identity proofing) is added (P4, L408), but Sec 5.2.2.1 only describes IAL1-3, and there is no description about IAL0. Since IAL0 is the successor of 63-3's IAL1, we think it should be also mentioned in 63A-4. On the other hand, we think that the reason why it's not listed on BaseVolume is that it is the same as AAL0 and FAL0 (because it is level 0 if it does not satisfy level 1). We would like you to add an explanation to BaseVolume with some background about the fact that 63B/63C does not have AAL0/FAL0, but only 63A has IAL0.	
2	63-Base	5.2.3.1 Selecting Initial IAL	32	1243	NIST should advise not to make the IAL larger than necessary, just as the attribute information to be collected should be minimized. The higher the IAL, the more kinds of information and the more sensitive the information tends to be collected. In other words, the higher the IAL, the higher the privacy risk. Using Federated Identity with a combination of higher IAL and lower AAL/FAL is more prone to privacy risks from* spoofing and phishing, which should be clarified this in the document.	
3	63-Base	A.1. Definitions	56	2028	Why did you separate AitM resistance from Phishing resistance? Is this because phishing does not always involve AitM? If so, we would like you to clarify it in the terms and definitions of the documents appropriately. If it is for other reasons, this should be clearly stated in the document.	
4	63A	2.2. Identity Assurance Levels	4	408	Can identity proofing by self-declaration or confirmation of mail delivery be understood as IAL0 under the new definition? Or will it be defined as IAL1? Most consumer IDs and platform vendor-provided IDs that use self-assessment or email delivery confirmation are understood as IAL0 under the new definition, is this understanding correct?	
5	63A	4.1.1 Process Flow	8	473	~~We think you have included examples of physical evidence, but I would like you to add examples of digital evidence as~~ well. We would like to know specific examples of using digital evidence, especially for Validation and Verification.	
6	63A	4.3.2 Digital Evidence	10	526	We would like you to change the word "3. The presented digital evidence contains the name of the issuer of the digital information" to "3. The presented digital evidence contains *the name of the issuer or a reference to the issuer* of the digital information". We don't think you necessarily need a name if you can identify the issuer. For example, the OpenID Connect for Identity Assuarance specification (a specification for federating Identity Proofing information) created by the OpenID Foundation contains a uri that represents an issuer, but does not contain an issuer name.	
7	63A	4.3.3. Evidence Strength Requirements, 5.6. Summary of Requirements	10, 33	574,etc	According to sec 4.3.3. and the summary table in Sec 5.6. , STRONG or SUPERIOR Evidence is required for IAL2 or higher, and STRONG or SUPERIOR Evidence SHALL contains a facial portrait or other biometric characteristic of the person to whom it relates. However, in the following cases where Federation is used, We feel that IAL2 or higher can be achieved without satisfying it. * The subscriber is identity proofed at high-level IAL on the IdP side * The subscriber is authenticated with a high-level AAL on the IdP side * The RP receives the results as an Assertion (not including biometric information) from IdP using a high-level FAL and uses it as Evidence. In other words, even if the RP side does not perform the necessary high-level validation and verification, we think it may be possible to create a situation where a higher level of IAL is guaranteed by the high-level AAL and FAL. For example, OpenID Connect for Identity Assurance, created by the OpenID Foundation, is being considered to enable identity proofing by the Federation. So we wolud like you to include a description that takes into account the way Federation is used as above.	

8	63A	4.3.3.2., 4.3.3.2.	11	560	The requirement states that it cannot be copied. Specifically, is an identity document with an IC chip envisaged? However, I would like to state that a PDF document with a facial image, difficult to alter and verifiable by signature also work as digital evidence? If it has the requirements of being difficult to alter, signature verifiable and verifiable binding of the document and the person, I think it still be digital evidence even if it can be copied?	
9	63A	4.3.3. Evidence Strength Requirements	11,12	533,570,588	It seems that in this document Evidence is only intended to be issued to the Applicant. (L553, L570, L588, etc.) If Federation is used, the Assertion used as Evidence will be issued for RP (not issued for Applicant), so we would like you to reconsider the content of the target part.	
10	63A	4.3.3.2. Strong Evidence Requirements, 4.3.3.3. Superior Evidence Requirements	11,12	576, 595	Since it says “The evidence includes physical security features that make it difficult to copy or reproduce”, we think that physical security is listed as a requirement for STRONG and SUPERIOR Evidence. We don't think it's appropriate that physical security is required even though Digital Evidence is also allowed as Evidence. In the case of Digital Evidence, it should be a different requirement. Furthermore, as long as the following conditions are satisfied, I think there is no problem even if it can be reproduce. * Falsification detection is possible * Verification of the issuer is possible (signature verification, etc.) * It is possible to verify the binding with the person We would like to ask you to reconsider the requirements, including this point.	
11	63A	4.3.3.3. Superior Evidence Requirements	12	594	The requirement “6. The evidence includes digital information that is cryptographically signed." of the SUPERIOR evidence is ambiguous as to what needs to be signed and by whom. Since "The CSP SHALL use the public key of the issuing authority of the evidence to verify digitally signed evidence or attribute data objects" is mentioned in Sec 4.3.4.1 and "Verification of the digital signature protecting digital evidence or attribute data objects using the public key of the issuing authority of the evidence” in Sec 4.3.3.3, the followings seem to be further requirements. * Signature by the issuing authority is required. * Signature is required for the evidence or attribute data object. We would like you to make it clear in the section of requirements for the evidence.	
12	63A	4.3.3.3. Superior Evidence Requirements	12	594	We think that verifiers must ensure that public keys used for verification belong to trusted authorities and manage a secure storage of trusted public keys in the verification environment.	
13	63A	4.3.3.3. Superior Evidence Requirements	12	594	If this document also assumes the application of cryptographic technologies such as zero-knowledge proof as a method of proving evidence, the terms of "proof" and "verification key" should be used instead of "signed" and "public key", respectively. The term "proof" and "verification key" can also cover conventional digital signature technologies.	
14	63A	4.4.1 Identity Verification Methods、Control of digital account	15	684	* When using Digital Account as a verification method, is it enough to satisfy AAL/FAL specified in IAL? Is it necessary to match the attribute information (name, date of birth, address, etc.) of the Digital Account? * Furthermore, when we want to raise the IAL of a user who has already subscribed with IAL1 from IAL1 to IAL2, is it possible to say that it has been Verified as IAL2 just by authenticating with AAL2 or higher? We don't think that alone is sufficient for IAL2. If this perception seems correct, We would like to ask you to add the necessary requirements.	
15	63A	5.1.9.1. Requirements for Trusted Referees	24	995	“CSPs SHALL provide the option for the use of trusted referees for remote identity proofing at IALs 1 and 2.” means that Trusted Referees are only available at IAL1 and IAL2. In order to secure the equity, we think it would be better to make it possible to use at IAL3 as well.	
16	63A	5.4..4.1. Remote Identity Proofing	29	1133	As a requirement of IAL2, it is said that it is "Demonstrated association with a digital account through an AAL2 authentication or an AAL2 and FAL2 federation protocol", but we think that IAL must also be 2 or higher. As a requirement of Federation, IAL, AAL, and FAL must be included in assertion at all FALs, so we think that IAL will always be included in the assertion when federation. Assertions that include"IAL1, AAL2, FAL2" meet the requirements currently described, but we don't think they actually meet IAL2.	
17	63A	5.5.4 Identity Verification Requirement	31	1191	The minimum level required for IAL3 is AAL2 or AAL2+FAL2, is this appropriate? (Is AAL3 unnecessary?).	

18	63A	5.5.4 Identity Verification Requirement	31	1191	We think it should be clearly stated that the requirement for Non-Federated Model is AAL2 authentication and the requirement for Federated Model is AAL2 and FAL2 federation protocol. In the Non-Federated Model, the CSP needs to authenticate the applicant with AAL2 before registering the applicant as a subscriber. But is this possible? Does it mean that if we verify in person that an applicant can be authenticated with AAL2 to a Digital Account of another service, the requirement will be satisfied?	
19	63A	6.2. Subscriber Account Access	35	1265	In addition to the content described in Section 6.2., please describe the requirements when the subscriber's IAL needs to be raised from IAL1 to IAL2(or from IAL2 to IAL3) depending on the service or function. For example, when raising from IAL1 to IAL2, "Subscriber SHALL authenticate with AAL2 and confirm Evidence and Verify described in Table 1 on P.33".	
20	63A	7. Threats and Security Considerations(63A)	37	Table 2. Enrollment and Identity Proofing Threat	The Threat Table in 63A-4 Sec. 7 should also cover threads related to mission delivery and privacy (e.g., excessive collection of user information, inability to receive services due to incorrect information, etc.). Not only in 63A, but also in 63B and 63C.	
21	63B	4.1.1./4.2.1/4.3.1 P	6,8,10,	Table 1. AAL S	The available authenticator types are defined at each AAL, but some of the types available in AAL3 are not available in AAL1 (e.g. SF Crypto Device plus Memorized Secret). It is unreasonable, costly, and inconvenient (reauthentication is required when using AAL1 service while already authenticated with AAL3) that an Authenticator prepared for AAL3 is not available for RPs that require AAL1. We would like you to change the definition as followings. * AAL3:aaa,bbb,ccc * AAL2:dddd,eee,fff in addition to those available in AAL3 * AAL1:ggg,hhh,iii in addition to those available in AAL2	
22	63B	4.2.3. Reauthentica	9	548	* The reauthentication time for each AAL, the current situation, 30 minutes, etc. are described, but the concept of reauthentication is not limited to time.Even with the same AAL, we think that what is required for each use case is different, so it is desirable to write in a risk-based way. * If we specify a number, it may not be able to keep up with the times. Caution is needed.	
23	63B	4.5. Summary of Requirements	13	Table 1. AAL S	* The table is difficult to understand. Items with different levels should be separated. * We want to read the table first. It is difficult to understand without reading the table first. (63C is at the beginning, but A and B are at the end, so it is better to match with C)	
24	63B	4.5. Summary of Requirements	13	Table 1. AAL S	It seems that AAL2 or higher authentication is required for government employees and related businesses in SP800-157r1. Since SP800-63B-4 covers AAL1, is it correct that AAL1 is acceptable for procedures such as applications to government agencies by citizens. This may be a comment on SP800-157r1, however we would like to submit it as a comment. In 3.1.3. Allowable Authenticator Types of the SP800-157r1 draft, the following is stated. All derived PIV credentials at both AAL2 and AAL3 SHALL meet the requirements for phishing resistance defined in [SP800-63B] Sec. 5.2.5. On the other hand, in 3.2.1. Allowable Authenticator Types, the following is stated. Phishing-resistant multi-factor or single-factor cryptographic authenticators SHALL be used for non-PKI-based derived PIV authentication. In draft SP800-63B-4, phishing resistance is recommended for AAL2 and mandatory for AAL3. Does this indicate that in PIV, phishing resistance may be mandatory even in AAL2?	
25	63B	5.1.1.2	14	683	As described in 63B-4 Sec 5.1.1.2., a verifier may allow subscribers to use password managers. In light of the recent password manager incidents, it would be better if there was a mention of the risk of identity compromise due to password manager or Passkey incidents. It is considered necessary to consider the following risk management issues with password managers including Passkey. * Evaluate password managers. * Know whether a subscriber is using a password manager, etc. or not. * Receive reports about security incidents of password managers or identity compromises from subscribers. * Understand password manager security incidents. * Evaluate and respond to impacts to CSPs and verifiers resulting from password security manager incidents. * Clarify responsibilities for the above issues and the entities responsible for them.	

26	63B	5.1.2., 5.1.3, 5.1.4, 5.1.5, 5.2.12		793, 830, 903, 956, 974,1006, 1028, 1527	Throughout 63-B, the expression of entropy is divided into three ways of writing with slightly different meanings. Is this split on purpose? Isn't it better to unify? * at least 20 bits * 6 decimal numbers (approximately 20bits) * 6 decimal numbers or at least 20 bits Specific descriptions are as follows. * 5.1.2.1. Look-Up Secret Authenticators ** L793: Look-up secrets SHALL have at least 20 bits of entropy. * 5.1.3. Out-of-Band Devices ** L830: For example, the claimant may receive the secret (typically a 6-digit code) on their mobile device * 5.1.3.2. Out-of-Band Verifiers ** L903: The verifier SHALL generate random authentication secrets with at least 20 bits of entropy using an approved random bit generator. * 5.1.4. Single-Factor OTP Device ** L956: An OTP device may, for example, display 6 characters at a time. * 5.1.4.1. Single-Factor OTP Authenticators ** L974: The authenticator output MAY be truncated to as few as 6 decimal digits (approximately 20 bits of entropy). * 5.1.5. Multi-Factor OTP Devices ** L1006: For example, an OTP device may display 6 characters at a time, thereby proving possession and control of the device. * 5.1.5.1. Multi-Factor OTP Device ** L1028: The authenticator output MAY be truncated to as few as 6 decimal digits (approximately 20 bits of entropy). * 5.2.12. Connected Authenticators ** L1527: The paring code SHALL be associated with either the authenticator or endpoint and SHALL have at least 20 bits or 6 decimal digits of entropy.	
27	63B	5.1.3 Out-of-band D	19,22	903	In Figure.1 "6 decimal number" which is less than 20 bits of entropyis used as an example, while 5.1.3.2 Out-of-band Verifiers says "at least 20 bits of entropy". Shouldn't one be fixed?	
28	63B	5.1.6.1.	27	1073	As you know, the Passkey allows key export, backup, use by 3rdParty, etc. Although the Cryptographic Software Authenticator in 63-3 did not allow key export, backup, etc., if the Passkey is included in the Cryptographic Software Authenticator in 63-4, the level of the Cryptographic Software Authenticator will be lowered down. We think it's better to treat Passkey and 63-3's Cryptographic Software Authenticator as separate type of authenticator.	
29	63B	5.1.6, 5.1.8	27, 29	1067, 518	As described as "External cryptographic authenticators that do not meet the requirements of cryptographic hardware authenticators (e.g. that have a mechanism to allow private keys to be exported) are also considered to be cryptographic software authenticators." in Sec 5.1.6.1.(line 1080) and "External cryptographic authenticators that do not meet the requirements of cryptographic hardware authenticators (e.g. that have a mechanism to allow private keys to be exported) are also considered to be cryptographic software authenticators" in Sec 5.1.8.1. (line 1154), Software Authenticators intentionally allow private keys to be exported. We assume this is intended change to accept Multi-device Passkeys (that are backed up by OS vendors or third-parties). However, if the private key is backed up in the cloud, etc., and the access to the backup is not properly protected, Software Authenticators are meaningless. Therefore, a requirement should be added for safeguards when keys are exported. For example; If Software Authenticators are designed to export keys from the device, * The key export shall not be externally activated by any means other than user interaction. * If the key is backed up in the cloud, etc., the cloud must be XX certified, and access to the key must be restricted to AAL2 or higher. * If the key is shared with other devices without going through the cloud, etc., the sharing mechanism shall be short-range wireless communication such as Bluetooth or QR code to prevent remote attack (assuming AirDrop).	
30	63B	5.1.6, 5.1.8	27, 29	1067, 518	We are also concerned that if the private key is backed up by the OS vendor or other providers, the security of key management will depend on the security requirements of the provider's account. Currently, CSPs and verifiers cannot confirm that the security level of the provider's account meets the expected level. We think the providers should at least attest their security levels.	

31	63B	5.1.8.2., 5.1.9.2.	29, 31	11,691,220	In Sec 5.1.8.2. (Multi-Factor Cryptographic Software Verifiers) and Sec 5.1.9.2. (Multi-Factor Cryptographic Device Verifiers), it should be stated that if the verifier or CSP cannot confirm that the authenticator is a multi-factor, it should be regarded as a single-factor. It is described as “The verifier or CSP SHALL also establish, by issuance of the authenticator, that the authenticator is a multi-factor device. Otherwise, the verifier SHALL treat the authenticator as single-factor, in accordance with Sec. 5.1.4.” in Sec 5.1.5.2. (line 1050). This means that in order for the authenticator to satisfy multiple factors, it needs to be verified. It is also described as “The CSP SHALL also verify the type of user-provided authenticator (e.g. single-factor cryptographic device v.s. multi-factor cryptographic device) so verifiers can determine compliance with requirements at each ALL.” in Sec 6.1. (line 1573) and "In situations where the authenticator strength is not self-evident (e.g. between single-factor and multi-factor authenticators of a given type), the CSP SHALL assume the use of the weaker authenticator unless it is able to establish that the stronger authenticator is in fact being used (e.g. by verification with the issuer of manufacturers of the authenticator)." in Sec 6.1.3. (line 1743). This means that the security level of an authenticator prepared by the user shall also be verified. However, as in Sec 5.1.8.2. (Multi-Factor Cryptographic Software Verifiers) and Sec 5.1.9.2. (Multi-Factor Cryptographic Device Verifiers), the requirements for Multi-Factor Verifiers are the same as Single-Factor Verifiers in Sec 5.1.7.2. (Single-Factor Cryptographic Device Verifiers), and there is no requirement that verifier or CSP shall regard an authenticator as single-factor if they cannot confirm that the authenticator has multiple factors.	
32	63B	5.2.5. Phishing (Ver	34	1342	“Phishing” is used in the sense of “Verifier Impersonation” as in Sec 5.2.5, and is also used in the general sense of “Phishing or Pharming” as in the table on page 54. Although the same word “Phishing” is used, it is difficult to understand because the meaning is different. Misunderstandings will occur if the different meanings are not clearly stated, so could you please use different words?	
33	63B	-	-	-	We do not see a requirement in 63-B to authenticate individuals using Federated Identity, so we would like you to make this clear in the documentation. It seems that an RP requiring AAL2 requires at least AAL2 at the IdP. On the other hand, is FAL OK with FAL1 or does it need FAL2? Or is it acceptable to determine the FAL by each RP, even with the same AAL2?	